

Cisco Reader Comment Card

General Information

- 1 Years of networking experience: _____ Years of experience with Cisco products: _____
- 2 I have these network types: LAN Backbone WAN
 Other: _____
- 3 I have these Cisco products: Switches Routers
 Other (specify models): _____
- 4 I perform these types of tasks: H/W installation and/or maintenance S/W configuration
 Network management Other: _____
- 5 I use these types of documentation: H/W installation H/W configuration S/W configuration
 Command reference Quick reference Release notes Online help
 Other: _____
- 6 I access this information through: _____% Cisco.com (CCO) _____% CD-ROM
_____% Printed docs _____% Other: _____
- 7 I prefer this access method: _____
- 8 I use the following three product features the most:

Document Information

Document Title: Cisco SN 5428 Storage Router Software Configuration Guide

Part Number: 78-14600-01

S/W Release: 2.3

On a scale of 1-5 (5 being the best), please let us know how we rate in the following areas:

_____ The document is written at my technical _____ The information is accurate.
level of understanding.

_____ The document is complete. _____ The information I wanted was easy to find.

_____ The information is well organized. _____ The information I found was useful to my job

Please comment on our lowest scores:

Mailing Information

Company Name

Date

Contact Name

Job Title

Mailing Address

City

State/Province

ZIP/Postal Code

Country

Phone ()

Extension

Fax ()

E-mail

Can we contact you further concerning our documentation? Yes No

You can also send us your comments by e-mail to bug-doc@cisco.com, or by fax to **408-527-8089**.

BUSINESS REPLY MAIL

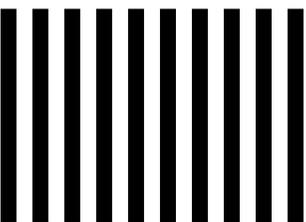
FIRST-CLASS MAIL PERMIT NO. 4631 SAN JOSE CA

POSTAGE WILL BE PAID BY ADDRESSEE

DOCUMENT RESOURCE CONNECTION
CISCO SYSTEMS INC
170 WEST TASMAN DR
SAN JOSE CA 95134-9916



NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES





Cisco SN 5428 Storage Router Software Configuration Guide

Release 2.3

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7814600=
Text Part Number: 78-14600-01



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.

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, GigaStack, IOS, IP/TV, LightStream, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0201R)

Cisco SN 5428 Storage Router Software Configuration Guide

Copyright © 2002, Cisco Systems, Inc.

All rights reserved.



About This Guide ix

Objectives	ix
Audience	ix
Organization	x
Command Syntax Conventions	xi
Related Documentation	xii
Obtaining Documentation	xii
World Wide Web	xii
Documentation CD-ROM	xii
Ordering Documentation	xiii
Documentation Feedback	xiii
Obtaining Technical Assistance	xiii
Cisco.com	xiii
Technical Assistance Center	xiv
Cisco TAC Web Site	xiv
Cisco TAC Escalation Center	xv

CHAPTER 1

Before Configuring SN 5428 Storage Router Software 1-1

SN 5428 Storage Router Software Overview	1-2
SCSI Routing Overview	1-3
SCSI Routing: Using iSCSI Protocol to Route SCSI Requests and Responses	1-4
SCSI Routing Basic Network Structure	1-5
SCSI Routing Mapping and Access Control	1-5
Available Instances of SCSI Routing	1-8
Transparent SCSI Routing Overview	1-8
Transparent SCSI Routing: Using iSCSI Protocol to Route SCSI Requests and Responses	1-10
Transparent SCSI Routing Basic Network Structure	1-11
Transparent SCSI Routing Mapping and Access Control	1-11
Available Instances of Transparent SCSI Routing	1-14
VLAN Access Overview	1-14
E_Port and FC Fabric Zoning Participation Overview	1-15
iSCSI Authentication Overview	1-17
SN 5428 Cluster Management Overview	1-17

Interface Naming 1-18
 Where to Go Next 1-19

CHAPTER 2

First-Time Configuration 2-1

Prerequisite Tasks 2-1
 Collecting Configuration Information 2-2
 Connecting a Console 2-6
 Initial System Configuration Script 2-6
 Running the Setup Configuration Wizard 2-7
 Introducing the CLI 2-8
 Character Case Sensitivity in the CLI 2-9
 Command Modes 2-9
 Command Prompt 2-9
 Reserved Words 2-9
 Show CLI Command 2-9
 Special Keys 2-10
 Starting a CLI Management Session 2-10
 Introducing the Web-Based GUI 2-11
 Logging In 2-11
 Monitor Mode 2-11
 Administrator Mode 2-11
 Menu Items and Links 2-12
 Where to Go Next 2-12

CHAPTER 3

Configuring System Parameters 3-1

Prerequisite Tasks 3-1
 Configuration Tasks 3-2
 Configuring the Management Interface 3-3
 Configuring Time and Date 3-4
 Configuring Network Management Access 3-5
 Configuring Passwords 3-6
 Configuring Administrator Contact Information 3-6
 Configuring the High-Availability Interface 3-7
 Verifying and Saving Configuration 3-8

CHAPTER 4

Configuring for VLAN 4-1

Prerequisite Tasks 4-1

VLAN Encapsulation	4-1
Configuration Tasks	4-2
Configuring for VLAN with VTP	4-3
Configuring for VLAN without VTP	4-3
Configuring an IP Route	4-4
Verifying and Saving Configuration	4-5
Assigning a VLAN to a SCSI Routing Instance	4-6

CHAPTER 5**Configuring for FC Fabric Zoning 5-1**

Prerequisite Tasks	5-1
Configuration Tasks	5-1
Configure Domain ID	5-2
Resetting E_Port	5-2
Verifying Configuration	5-3

CHAPTER 6**Configuring SCSI Routing 6-1**

Prerequisite Tasks	6-1
Configuration Tasks	6-2
Creating a SCSI Routing Instance	6-6
Configuring a Server Interface	6-6
Configuring iSCSI Targets	6-7
Configuring an Access List	6-9
Configuring Access	6-11
Verifying and Saving Configuration	6-13
Default Values For FC Interfaces	6-14

CHAPTER 7**Configuring Transparent SCSI Routing 7-1**

Prerequisite Tasks	7-1
Summary of Configuration Process	7-1
Verifying Configuration	7-2

CHAPTER 8**Configuring Authentication 8-1**

Prerequisite Tasks	8-1
Using iSCSI Authentication	8-2
AAA Security Services	8-2
Configuration Tasks	8-2

- Configuring Security Services 8-5
- Building the AAA Authentication List 8-7
- Testing iSCSI Authentication 8-8
- Enabling iSCSI Authentication 8-8
- Verifying and Saving Configuration 8-9

CHAPTER 9

Configuring a High Availability Cluster 9-1

- Prerequisite Tasks 9-1
- Adding the SN 5428 to a Cluster 9-2
 - Adding an Unconfigured SN 5428 Storage Router 9-2
 - Adding a Minimally Configured SN 5428 Storage Router 9-3
 - Adding Completely Configured SN 5428 Storage Routers 9-4
- Changing Clusters 9-5

CHAPTER 10

Maintaining and Managing the SN 5428 Storage Router 10-1

- Prerequisite Tasks 10-2
- Installing Updated Software 10-2
 - Specifying the Location to Retrieve Updated Software 10-3
 - Downloading Updated Software 10-5
 - Setting Updated Software as Boot Version 10-7
 - Precautions for Cluster Environments 10-7
- Backing Up System Configuration 10-8
- Restoring from Backups 10-9
- Powering Down the SN 5428 Storage Router 10-15
- Resetting the System 10-15
- Recovering Passwords 10-18
- Controlling SCSI Routing Instances in a Cluster 10-18
 - Making Changes to Instance Configurations 10-18
 - Enabling and Disabling Connections 10-19
 - Stopping & Starting Instances 10-20
 - Viewing Operational Statistics 10-21
 - Handling Failover 10-21
 - Manual Failover 10-21
- Managing CDP on the SN 5428 Storage Router 10-23
- Using Scripts to Automate Tasks 10-24
 - Running Command Scripts 10-25
- Managing the Log File 10-26

Gathering Troubleshooting Information	10-27
Using the Crash Log	10-27
Using FTP with the SN 5428 Storage Router	10-28
Understanding Diagnostics	10-30
Capturing System Messages at Bootup	10-30
Understanding Logging	10-30
Filtering and Routing Event Messages	10-32
Enabling and Disabling Logging	10-32
Viewing and Saving the Log File	10-33
Capturing the SN 5428 Configuration	10-33
Using Debug Facilities	10-33

CHAPTER 11**Command Line Interface Reference 11-1**

About CLI Commands	11-1
CLI Usage Tips	11-1
CLI Commands	11-2

INDEX



About This Guide

This preface describes the objectives, audience, organization and command syntax conventions of the *Cisco SN 5428 Storage Router Software Configuration Guide*. It also provides information on how to obtain related documentation and technical assistance.

Objectives

This software configuration guide describes how to configure software in a Cisco SN 5428 Storage Router. It does not describe every possible configuration but does describe those tasks commonly required to configure the software.



Note

This guide does not describe how to configure the iSCSI driver to be installed in each host requiring IP access to storage. Install and configure the Cisco Storage Networking iSCSI drivers according to the readme and example configuration files on the Cisco Storage Networking iSCSI Drivers CD shipped with your SN 5428 Storage Router. (In addition, you can access readme and example configuration files from Cisco.com.)

Audience

This guide is intended primarily for the following audiences:

- System administrators who are familiar with the fundamentals of router-based internetworking and network storage devices, but who might not be familiar with the specifics of Cisco products or the routing protocols supported by Cisco products.
- System administrators who are responsible for configuring network storage equipment.

Organization

This guide contains the following chapters (Table 1):

Table 1 Document Organization

Chapter	Title	Description
Chapter 1	Before Configuring SN 5428 Storage Router Software	Describes what you should understand prior to configuring storage router software.
Chapter 2	First-Time Configuration	Describes what configuration information to gather and explains the initial system configuration script and setup configuration wizard. This chapter also introduces the CLI and web-based GUI.
Chapter 3	Configuring System Parameters	Provides procedures for configuring system parameters.
Chapter 4	Configuring for VLAN	Provides procedures for configuring VLAN.
Chapter 5	Configuring for FC Fabric Zoning	Provides procedures for configuring FC fabric zoning.
Chapter 6	Configuring SCSI Routing	Provides procedures for configuring SCSI routing.
Chapter 7	Configuring Transparent SCSI Routing	Provides procedures for configuring transparent SCSI routing.
Chapter 8	Configuring Authentication	Provides procedures for configuring AAA authentication and enabling iSCSI authentication.
Chapter 9	Configuring a High Availability Cluster	Provides procedures for configuring a storage router cluster.
Chapter 10	Maintaining and Managing the SN 5428 Storage Router	Describes how to perform normal maintenance and management tasks associated with the storage router.
Chapter 11	Command Line Interface Reference	Provides information on the command line interface (CLI) and on all CLI commands.

Command Syntax Conventions

Table 2 describes the syntax used with the commands in this document.

Table 2 *Syntax Conventions*

Convention	Description
boldface font	Indicates commands and keywords that you enter literally as shown.
<i>italic font</i>	Indicates arguments for which you supply values.
[x]	Square brackets indicate an optional element (keyword or argument).
{ x }	Braces indicate a required element (keyword or argument).
{s y z}	Braces and vertical bars indicate a required choice of keywords or arguments, separated by the vertical bars within the braces.
[x {y z}]	Braces and vertical bars within square brackets indicate a required choice within an optional element.
<i>/bits</i>	The value entered for <i>/bits</i> specifies a network mask in classless interdomain routing (CIDR) style. That is, the value equals the number of bits in a network mask counting from the most significant side (left) of an IP address. For example, a <i>/bits</i> value of 24 is the equivalent of a network mask of 255.255.255.0. Similarly, a <i>/bits</i> value of 32 specifies using the entire IP address.
<i>“user text”</i>	Indicates that user text (a user-defined text string) that contains a space or spaces must be enclosed using double or single quotes. If single quotes or an apostrophe is used as part of the text string, enclose the string using double quotes. If double quotes are used as part of the text string, enclose the string using single quotes. For example, both “Pat’s storage router” and ‘number “2”’ are valid text string entries. Note The question mark (?) character cannot be used as part of a text string.
screen font	Examples of information displayed on the screen.
boldface screen font	Examples of information you must enter.
< >	Nonprinting characters, for example, passwords appear in angle brackets.
[]	Default responses to system prompts appear in square brackets.

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to additional information and material.

**Caution**

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

**Timesaver**

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Related Documentation

Refer to the following documents for additional information:

- *Cisco SN 5428 Storage Router Hardware Installation Guide*
- Release Notes for the Cisco SN 5428 Storage Router

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com>

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages

- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

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

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.



Before Configuring SN 5428 Storage Router Software

The Cisco SN 5428 Storage Router installation and configuration tasks consist of the following:

- Install the SN 5428 Storage Router according to the *Cisco SN 5428 Storage Router Hardware Installation Guide*.
- Select how the SN 5428 will be deployed; either SCSI routing or transparent SCSI routing.
- Configure the SN 5428 Storage Router software according to the *Cisco SN 5428 Storage Router Software Configuration Guide* (this manual).
- Install and configure iSCSI drivers in IP hosts connected to the storage router. The iSCSI driver is not required in IP hosts that have a TCP/IP Offload Engine (TOE) with embedded iSCSI protocol installed.

This chapter is the starting point for SN 5428 Storage Router software configuration. It provides some very basic, abbreviated information as background to help you understand the SN 5428 Storage Router features and the software configuration process. It contains the following topics:

- SN 5428 Storage Router Software Overview, page 1-2
- SCSI Routing Overview, page 1-3
- Transparent SCSI Routing Overview, page 1-8
- VLAN Access Overview, page 1-14
- E_Port and FC Fabric Zoning Participation Overview, page 1-15
- iSCSI Authentication Overview, page 1-17
- SN 5428 Cluster Management Overview, page 1-17
- Interface Naming, page 1-18
- Where to Go Next, page 1-19

SN 5428 Storage Router Software Overview

The Cisco SN 5428 Storage Router provides universal access to storage over IP networks. The storage router software controls the operation of the Cisco SN 5428 Storage Router. You can configure the software to provide one of two types of access to storage over IP networks; either SCSI routing, or Transparent SCSI routing.

SCSI routing provides IP hosts with access to Fibre Channel (FC) storage devices, using iSCSI protocol.

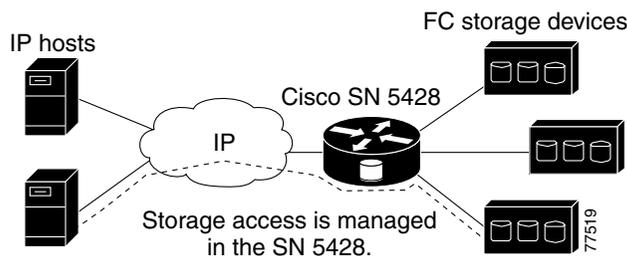


Note

The iSCSI protocol is an IETF-defined protocol for IP storage (ips). For more information about the iSCSI protocol, refer to the IETF standards for IP storage at <http://www.ietf.org>.

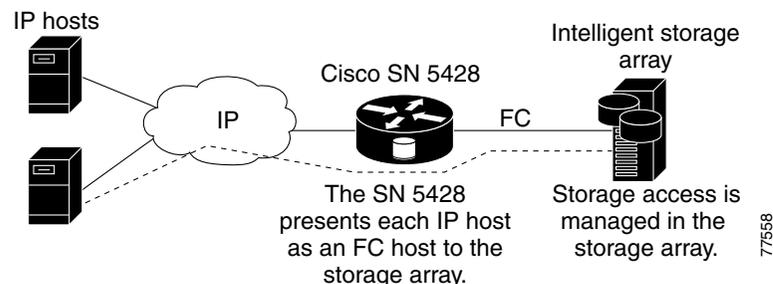
With SCSI routing, storage device access is managed primarily in the SN 5428. (See Figure 1-1.)

Figure 1-1 SCSI Routing



Transparent SCSI routing provides IP hosts with transparent access to intelligent storage arrays using iSCSI protocol; that is, each IP host is presented as an FC host to an intelligent storage array. With transparent SCSI routing, availability of storage devices is managed primarily in the intelligent storage array. (See Figure 1-4.)

Figure 1-2 Transparent SCSI Routing



In addition to providing services for accessing storage over IP networks, the SN 5428 Storage Router software provides the following services:

- VLAN Access Control—provides IP access control to storage based on a VLAN identifier (VID) number (in addition to access control through access lists)
- Authentication—provides iSCSI authentication using AAA authentication methods
- High Availability (HA)—provides the ability to group storage routers in a cluster for failover and other cluster-related functions (for SCSI routing only)

- E_Port with FC Fabric Zoning—provides the ability to connect FC ports to FC switches and participate in fabric zoning and support zone mergers
- SNMP/MIB support—provides network management of the SN 5428 through SNMP using selected MIBs
- A command-line interface (CLI) and a web-based GUI—provides user interfaces for configuration and maintenance of an SN 5428
- Secure Sockets Layer Support—provides HTTPS connection for secure access through the web-based GUI

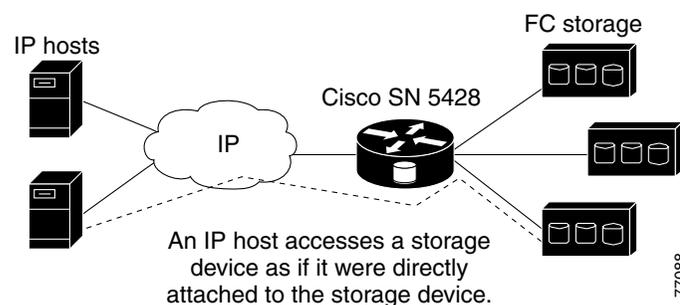


Note The web-based GUI is not available in SN 5428s deployed for transparent SCSI routing.

SCSI Routing Overview

SCSI routing provides IP hosts with access to FC storage devices as if the storage devices were directly attached to the hosts, with access to devices being managed primarily in the SN 5428 Storage Router. An iSCSI target (also called logical target) is an arbitrary name for a group of physical storage devices. The iSCSI targets are created and mapped to physical storage devices attached to the SN 5428. The storage router presents the iSCSI targets to IP hosts (iSCSI initiators) as if the physical storage devices were directly attached to the hosts. (See Figure 1-3.) With SCSI routing, storage devices are not aware of each IP host; the storage devices are aware of the SN 5428 and respond to it as if it were one FC host.

Figure 1-3 SCSI Routing Overview



To configure an SN 5428 Storage Router for SCSI routing, you should have a basic understanding of the following concepts:

- SCSI Routing: Using iSCSI Protocol to Route SCSI Requests and Responses, page 1-4
- SCSI Routing Basic Network Structure, page 1-5
- SCSI Routing Mapping and Access Control, page 1-5
- Available Instances of SCSI Routing, page 1-8



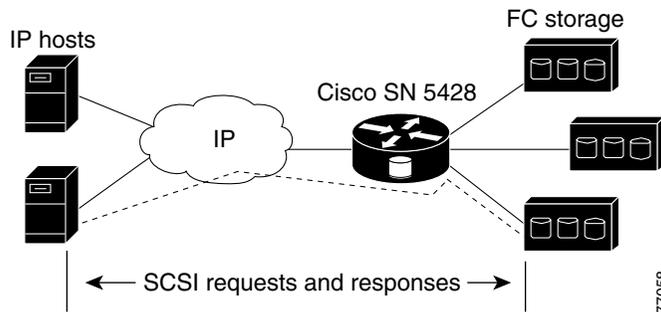
Note

Along with FC storage, FC host connections and FC switch connections are allowed; however, most of the illustrations in this manual show only storage connections for the purpose of describing the SN 5428 Storage Router features.

SCSI Routing: Using iSCSI Protocol to Route SCSI Requests and Responses

SCSI routing consists of routing SCSI requests and responses between hosts in an IP network and FC storage. (See Figure 1-4.)

Figure 1-4 Routing SCSI Requests and Responses for SCSI Routing

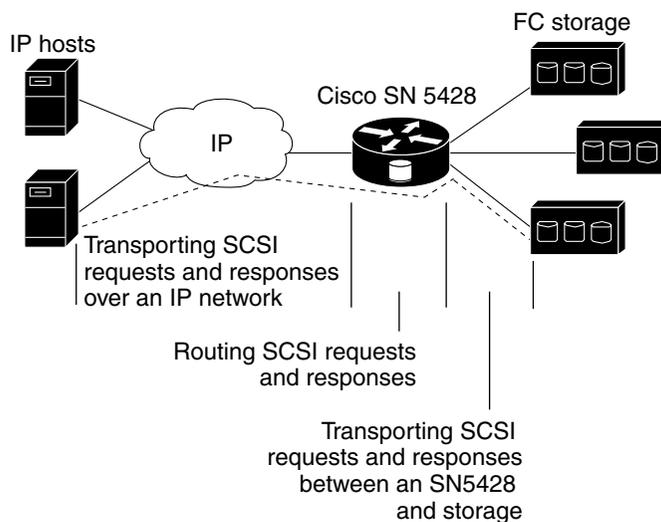


Each host that requires IP access to storage via an SN 5428 Storage Router needs to have a compatible iSCSI driver installed. Using the iSCSI protocol, the iSCSI driver allows an IP host to transport SCSI requests and responses over an IP network. From the perspective of a host operating system, the iSCSI driver appears to be a SCSI or Fibre Channel driver for a peripheral channel in the host.

SCSI routing consists of the following main actions (See Figure 1-5):

- Transporting SCSI requests and responses over an IP network between the hosts and the SN 5428 Storage Router
- Routing SCSI requests and responses between hosts on an IP network and FC storage
- Transporting SCSI requests and responses between the SN 5428 Storage Router and FC storage

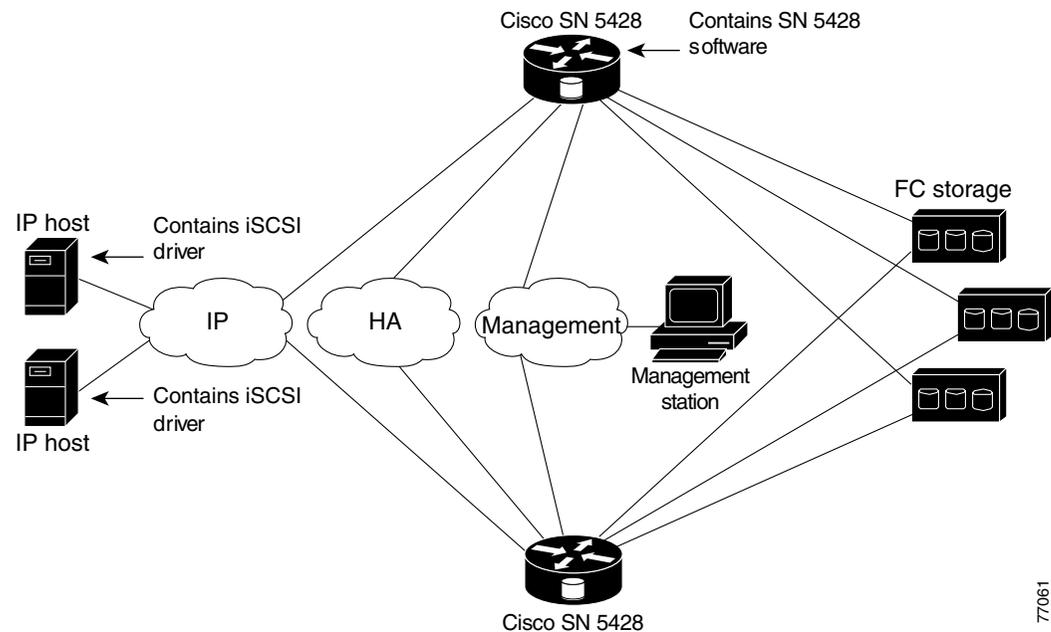
Figure 1-5 SCSI Routing Actions



SCSI Routing Basic Network Structure

Figure 1-6 shows the basic structure of a SCSI routing network. IP hosts with iSCSI drivers access the storage routers through an IP network connected to the Gigabit Ethernet interface of each storage router. The storage routers access storage devices connected to the Fibre Channel interfaces of each storage router. A management station manages the storage routers through an IP network connected to the management interface of each storage router. For high availability (HA) operation, the storage routers communicate with each other over two networks: the HA network connected to the HA interface of each storage router and the management network connected to the management interface of each storage router.

Figure 1-6 SCSI Routing Basic Network Structure



SCSI Routing Mapping and Access Control

SCSI routing occurs in the SN 5428 Storage Router through the mapping of physical storage devices to iSCSI targets. An iSCSI target (also called logical target) is an arbitrary name for a group of physical storage devices. You can map an iSCSI target to multiple physical devices. An iSCSI target always contains at least one Logical Unit Number (LUN). Each LUN on an iSCSI target is mapped to a single LUN on a physical storage target.

You can choose either of two types of storage mapping: target-and-LUN mapping or target-only mapping. Target-and-LUN mapping maps an iSCSI target and LUN combination to a physical storage target and LUN combination. Target-only mapping maps an iSCSI target to a physical storage target and its LUNs.

With target-and-LUN mapping, an iSCSI target name and iSCSI LUN number are specified and mapped to the physical storage address of one LUN; either a WWPN + LUN (World Wide Port Name + LUN) combination, a LUNWWN (LUN World Wide Name), or a LUN serial number. If the LUN is available, it is made available as an iSCSI LUN and numbered with the iSCSI LUN number specified. For example, if an iSCSI target and iSCSI LUN specified as *Database, LUN 9* were mapped to the physical storage

address, *WWPN ID*, *LUN 12*, then LUN 12 would be available as one iSCSI LUN. An iSCSI driver would see the iSCSI target named *Database*, with one iSCSI LUN identified as *LUN 9*. The iSCSI LUN would appear as one storage device to a host. (See Table 1-1.)

Table 1-1 Target-and-LUN Mapping Example

Apparent to Host as Local Disk	iSCSI Target Name	iSCSI LUN Available	Physical Storage Address	Physical LUN Available
Local Disk (D:)	Database	LUN 9	WWPN 070	LUN 12
Apparent as one locally attached storage device.	<i>Database</i> appears as one controller with one LUN available.	iSCSI LUN is numbered as specified and can be different than the physical LUN number.	Specifies the storage address of a storage controller.	The LUN number is specified as the only LUN to be mapped.

With target-only mapping, an iSCSI target name is specified and mapped to the physical storage address of a storage controller only; a WWPN. Any LUNs that are available in the storage controller are made available as iSCSI LUNs and are numbered the same as the LUNs in the storage controller. For example, if an iSCSI target specified as *Webserver2000* were mapped to the physical storage address *WWPN 050*, and LUNs 0 through 2 were available in that controller, those LUNs would become available as three iSCSI LUNs. An iSCSI driver would see the iSCSI target named *Webserver2000* as a controller with three iSCSI LUNs identified as *LUN 0*, *LUN 1*, and *LUN 2*. Each iSCSI LUN would appear as a separate storage device to a host. (See Table 1-2.)

Table 1-2 Target-only Mapping Example

Apparent to Host as Local Disk	iSCSI Target Name	iSCSI LUNs Available	Physical Storage Address	Physical LUNs Available
Local Disk (D:)	Webserver2000	LUN 0	WWPN 050	LUN 0
Local Disk (E:)	Webserver2000	LUN 1	WWPN 050	LUN 1
Local Disk (F:)	Webserver2000	LUN 2	WWPN 050	LUN 2
Apparent as three locally attached storage devices.	<i>Webserver2000</i> appears as one controller with LUNs 0, 1, and 2 available.	iSCSI LUNs are numbered the same as physical LUNs.	Specifies the storage address of a storage controller.	LUNs 0, 1, and 2 are available for mapping.

Access for SCSI routing is controlled in the IP hosts and the storage router. In an IP host, the Gigabit Ethernet IP address of the SCSI routing instance in the storage router with which the host is to transport SCSI requests and responses is configured in the iSCSI driver. In a storage router, access is controlled through an access list and a VLAN identifier (VID) number of the hosts. Additionally, access can be further controlled in the SN 5428 through authentication. For more information about authentication, see the “iSCSI Authentication Overview” section on page 1-17.

An access list enables access to storage devices attached to the SN 5428 according to any combination of host IP address(es), CHAP user name(s), or iSCSI name(s). An access list contains these combinations of hosts allowed to access the storage devices. Host VID enables access to storage devices according to the VID of each host. For more information about VLAN access, see the “VLAN Access Overview” section on page 1-14.

You can use a combination of access lists and VIDs to configure access in the SN 5428; that is, you can specify that certain hosts according to IP address in a VLAN can access storage devices attached to the SN 5428.

Once the access is configured in the hosts and the SN 5428, and once the storage mapping is configured in the SN 5428, the SN 5428 routes SCSI requests and responses between hosts and the mapped storage devices.

Figure 1-7 represents the concept of storage mapping and access control for SCSI routing. In the figure, the SN 5428 Storage Router provides three IP hosts with IP access to disk drives across four disk controllers. The SN 5428 contains two SCSI routing instances: one configured with IP address 10.1.2.3 for the Gigabit Ethernet interface and the other with IP address 10.1.2.4. The iSCSI drivers in each IP host are configured to access those SCSI routing instances by their IP addresses through the Gigabit Ethernet interface. An access list in the storage router or VID (or both) specifies that hosts A, B, and C are allowed to access the mapped storage devices. From the perspective of a host, each disk drive mapped to it appears as a locally attached disk drive. Table 1-3 shows the correlation between an access list and/or VID, the Gigabit Ethernet IP addresses of the SCSI routing instances, and the storage device mapping.


Note

The purpose of Figure 1-7 and Table 1-3 is only to illustrate the concept of storage mapping and access control. The IP addresses will vary according to each site. Similarly, the type of storage addressing (for example, LUNWWN, WWPN + LUN or LUN serial number) will vary according to the types of storage and the types of storage addressing preferred at each site. In addition, the figure and the table exclude any additional SN 5428 Storage Routers that could be configured for high availability.

Figure 1-7 SCSI Routing Storage Mapping and Access Control Concept

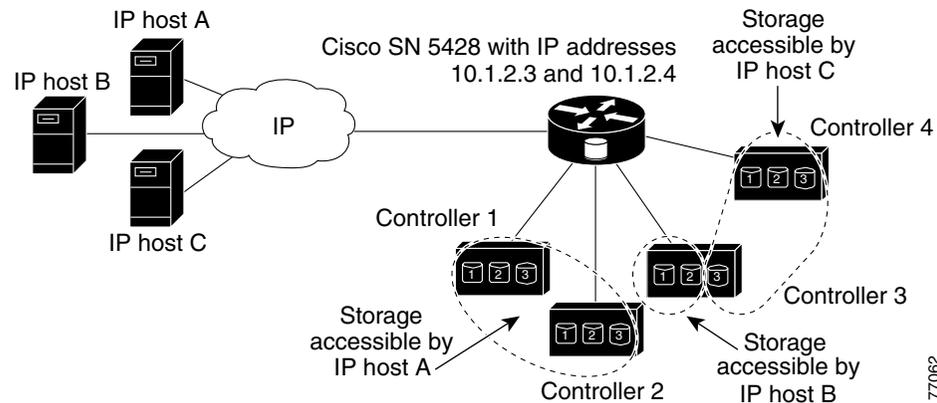


Table 1-3 SCSI Routing Storage Mapping and Access Control Concept

Hosts Allowed Access via SN 5428 Access List and/or VID	Storage Devices Apparent to Host as Locally Attached Devices	Via GbE IP Addresses of SCSI Routing Instances	Mapped To Controller	Mapped To Drive
Host A	Local Disk (D:)	10.1.2.3	1	1
	Local Disk (E:)	10.1.2.3	1	2
	Local Disk (F:)	10.1.2.3	1	3
	Local Disk (G:)	10.1.2.3	2	1
	Local Disk (H:)	10.1.2.3	2	2
	Local Disk (I:)	10.1.2.3	2	3
Host B	Local Disk (D:)	10.1.2.3	3	1
	Local Disk (E:)	10.1.2.3	3	2
Host C	Local Disk (D:)	10.1.2.4	4	1
	Local Disk (E:)	10.1.2.4	4	2
	Local Disk (F:)	10.1.2.4	4	3
	Local Disk (G:)	10.1.2.4	3	3

Available Instances of SCSI Routing

You can configure an SN 5428 Storage Router with up to 12 instances of SCSI routing services. Each instance needs to be configured with a Gigabit Ethernet IP address, mapping between iSCSI target names and physical storage addresses, and access control.

When an SN 5428 is part of a cluster, an instance of SCSI routing can run on only one storage router in a cluster at any given time. For more information about instances of SCSI routing in a cluster, see the “SN 5428 Cluster Management Overview” section on page 1-17. For more information about configuring an SN 5428 Storage Router, see the appropriate configuration chapters in this document.

Transparent SCSI Routing Overview

Transparent SCSI routing provides IP hosts with access to intelligent storage arrays as if the storage array(s) were directly attached to the hosts, with access to the storage devices managed primarily in each storage array. Deployed for transparent SCSI routing, the SN 5428 transparently presents each IP host to the storage array as if each host were an FC host. Typically, transparent SCSI routing is used with an intelligent storage array that is directly connected to the SN 5428 Fibre Channel interface. Managing access to storage devices consists of using configuration tools available with an intelligent storage array (to configure, for example, which hosts are granted access and to configure multiple paths between hosts and storage devices). With transparent SCSI routing, an intelligent storage array can manage each IP host as if it were directly attached to the array as an FC host.



Note

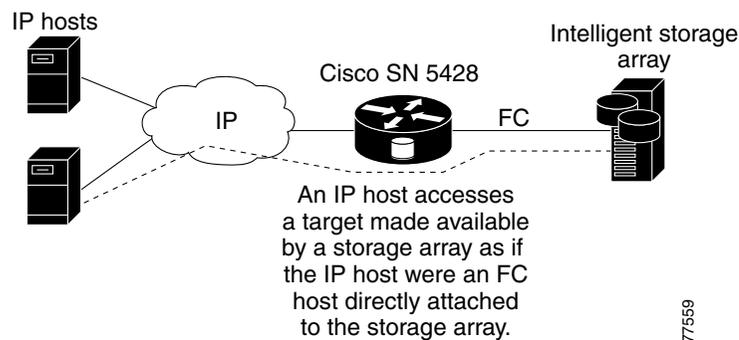
FC Fabric zoning participation is not allowed in a transparent SCSI router configuration.

**Note**

When operating in transparent mode, in order for the SN 5428 and the intelligent storage array to function together correctly, the storage array needs to support an FC extended port login, which contains the IP Host (iSCSI initiator name) and the associated IP address embedded in the FC login frame.

Transparent SCSI routing automatically creates iSCSI targets and maps them to physical targets available in the intelligent storage array. The storage router presents the iSCSI targets to IP hosts (iSCSI initiators) as if the physical targets were directly attached to the hosts. In conjunction with presenting iSCSI targets to hosts, transparent SCSI routing presents each IP host as an FC host to the intelligent storage array. The intelligent storage array is aware of each IP host and responds to each IP host as if it were an FC host connected to the storage array. (See Figure 1-8.) Transparent SCSI routing can present no more than 62 IP hosts as FC hosts to an intelligent storage array.

Figure 1-8 Transparent SCSI Routing Overview



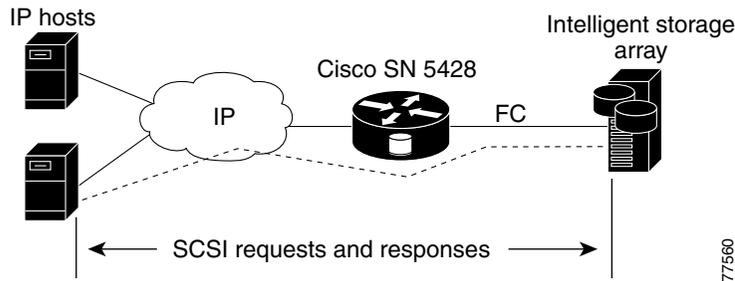
To configure an SN 5428 Storage Router that is deployed for transparent SCSI routing, you should have a basic understanding of the following concepts:

- Transparent SCSI Routing: Using iSCSI Protocol to Route SCSI Requests and Responses, page 1-10
- Transparent SCSI Routing Basic Network Structure, page 1-11
- Transparent SCSI Routing Mapping and Access Control, page 1-11
- Available Instances of Transparent SCSI Routing, page 1-14

Transparent SCSI Routing: Using iSCSI Protocol to Route SCSI Requests and Responses

Transparent SCSI routing consists of routing SCSI requests and responses between hosts in an IP network and an intelligent storage array that is directly connected to the SN 5428 Fibre Channel interface. (See Figure 1-9.)

Figure 1-9 Routing SCSI Requests and Responses for Transparent SCSI Routing

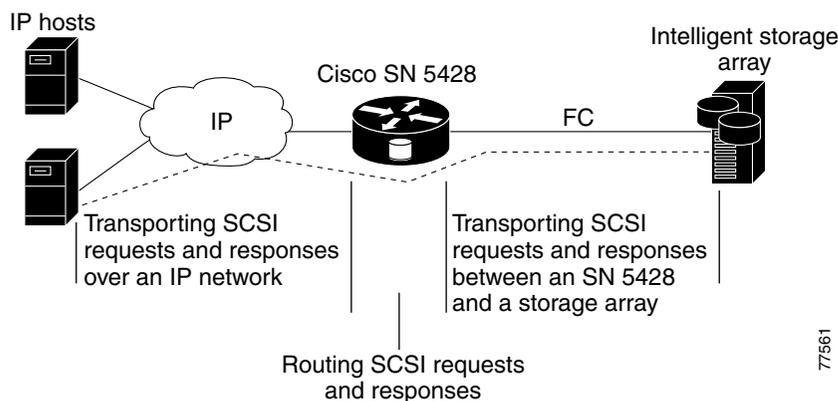


Each host that requires IP access to storage via an SN 5428 Storage Router needs to have a compatible iSCSI driver installed. Using the iSCSI protocol, the iSCSI driver allows an IP host to transport SCSI requests and responses over an IP network. From the perspective of a host operating system, the iSCSI driver appears to be a SCSI or Fibre Channel driver for a peripheral channel in the host. From the perspective of the storage array, each IP host appears as an FC host (with one Fibre Channel address for each host).

Transparent SCSI routing consists of the following main actions (Figure 1-10):

- Transporting SCSI requests and responses over an IP network between the hosts and the SN 5428 Storage Router.
- Routing SCSI requests and responses between hosts on an IP network and an intelligent storage array.
- Transporting SCSI requests and responses between the SN 5428 Storage Router and an intelligent storage array.

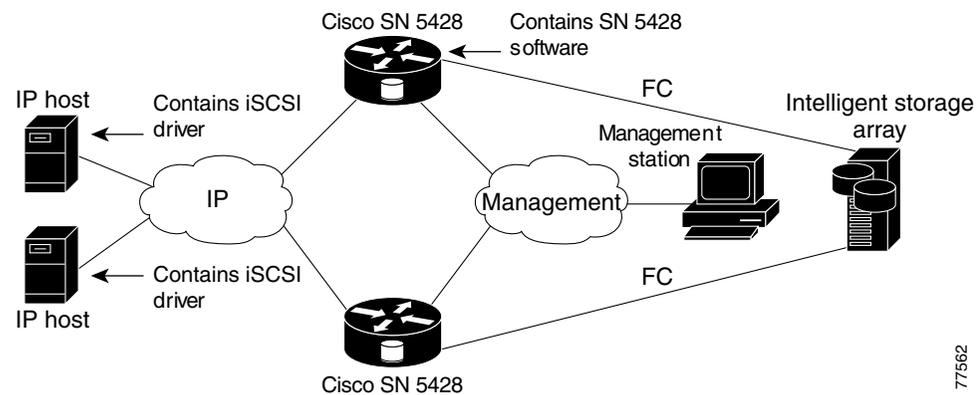
Figure 1-10 Transparent SCSI Routing Actions



Transparent SCSI Routing Basic Network Structure

Figure 1-11 shows the basic structure of a transparent SCSI routing network. IP hosts with iSCSI drivers access the storage routers through an IP network connected to one of the Gigabit Ethernet interfaces of each storage router. The storage routers access the intelligent storage array through a Fibre Channel interface of each storage router. A management station manages the storage routers through an IP network connected to the management interface of each storage router. High availability operation for transparent SCSI routing is controlled in the intelligent storage array; therefore, an SN 5428 HA network is not necessary, and the HA interface on the SN 5428 is disabled.

Figure 1-11 Transparent SCSI Routing Basic Network Structure



Transparent SCSI Routing Mapping and Access Control

Transparent SCSI routing occurs in an SN 5428 Storage Router through two types of mapping:

- Mapping iSCSI targets to physical targets
- Mapping each IP host to a Fibre Channel (FC) address

Mapping iSCSI targets to physical targets makes the physical targets accessible to IP hosts. Mapping each IP host to a FC address allows the host to be presented to a storage array as an FC host with its own FC WWPN.

Mapping iSCSI targets to physical targets consists of creating iSCSI targets that represent physical targets in an intelligent storage array. An iSCSI target is an arbitrary name for a group of physical storage devices. In an SN 5428 deployed for transparent SCSI routing, one iSCSI target is automatically created for each target made available by the intelligent storage array. The iSCSI target name is created automatically using the iSCSI extended unique identifier (EUI) format. The EUI format combines the prefix “eui” with each WWPN made available by the intelligent storage array. For example, if the WWPN of a target in a storage array were 31:00:11:22:33:44:55:66:77, then an iSCSI target would be created in the SN 5428 with the iSCSI target name of *eui.310011223344556677*.

Transparent SCSI routing maps iSCSI targets to physical targets using target-only mapping. Target-only mapping maps an iSCSI target to a physical storage target and its LUNs. Any LUNs that are available with a physical WWPN in the storage array are available with the corresponding iSCSI target and are numbered the same as the LUNs in the storage array. For example, if an iSCSI target were created for WWPN 31:00:11:22:33:44:55:66:77 in a storage array, and that WWPN contained LUNs 0 through 2,

those LUNs would become available to an IP host as LUNs 0 through 2. An iSCSI driver would see the iSCSI target named *eui.310011223344556677* as a controller with three iSCSI LUNs identified as *LUN 0*, *LUN 1*, and *LUN 2*. Each iSCSI LUN would appear as a separate storage device to an IP host.

Mapping each IP host to a Fibre Channel address consists of assigning a WWPN to an IP host that is requesting access to storage; the WWPN is used for presenting the IP host as an FC host to a storage array. In an SN 5428 deployed for transparent SCSI routing, the SN 5428 maintains a pool of 62 WWPNs that are assigned to IP hosts requesting access to storage. When an IP host is granted access, a WWPN is assigned to the IP host and the SN 5428 presents the host as an FC host to the storage array. That host continues using that WWPN until it is finished using the storage. Once the host is finished using the storage (logged out), the WWPN becomes available for assignment to other IP hosts requiring access to storage.

See Table 1-4 for an example of transparent SCSI routing mapping.

Table 1-4 Transparent SCSI Routing Mapping Example

WWPN assigned to IP Host	Apparent to IP Host	iSCSI Target Name	LUNs Apparent with iSCSI Target	WWPN of Storage Array Target	Physical LUNs Available
20:01:00:02:3D:00:01:00	Local Disk (E:)	eui.310011223344556677	LUN 0	31:00:11:22:33:44:55:66:77	LUN 0
	Local Disk (G:)	eui.310011223344556677	LUN 1	31:00:11:22:33:44:55:66:77	LUN 1
	Local Disk (H:)	eui.310011223344556677	LUN 2	31:00:11:22:33:44:55:66:77	LUN 2

Note In this mapping example, the WWPN, 20:01:00:02:3D:00:01:00, is assigned to the IP host. Using that WWPN, the SN 5428 presents the IP host as an FC host to the storage array. Three devices are made available as local storage devices: Local Disk (E:), Local Disk (F:), and Local Disk (G:). (Microsoft Windows devices are used as examples.) The iSCSI target, eui.310011223344556677, has been automatically created and mapped to a WWPN, 31:00:11:22:33:44:55:66:77, that was made available by the storage array. To the IP host, the iSCSI target appears as a controller with LUNs 0, 1, and 2 available. The LUNs are apparent as they are with the WWPN in the storage array.

Access for transparent SCSI routing is controlled in the IP hosts and the intelligent storage array. In an IP host, the Gigabit Ethernet IP address of the SCSI routing instance in the storage router with which the host is to transport SCSI requests and responses is configured in the iSCSI driver. In the intelligent storage array, access is controlled through its storage management tools. Additionally, access can be further controlled in the SN 5428 through authentication. For more information about authentication, see the “iSCSI Authentication Overview” section on page 1-17.

Once the access is configured in the hosts and the intelligent storage array, the SN 5428 transparently routes SCSI requests and responses between hosts and the mapped storage devices.

Figure 1-12 represents the concept of storage mapping and access control for transparent SCSI routing. In the figure, the SN 5428 Storage Router provides three IP hosts with access to disk drives made available by the intelligent storage array. A single SCSI routing instance in the storage router is configured with IP address 10.1.2.3 for the Gigabit Ethernet interface. The iSCSI driver in each IP host is configured to access that SCSI routing instance by its IP address 10.1.2.3 through the Gigabit Ethernet interface on the storage router. From the perspective of an IP host, each disk drive mapped to it appears as a locally attached disk drive. From the perspective of the storage array, each host is connected directly to it, with each host having a WWPN. Table 1-4 shows the correlation between the IP hosts, the Gigabit Ethernet IP address of the SCSI routing instance, storage device mapping, and IP-host-to-FC-address (WWPN) mapping.

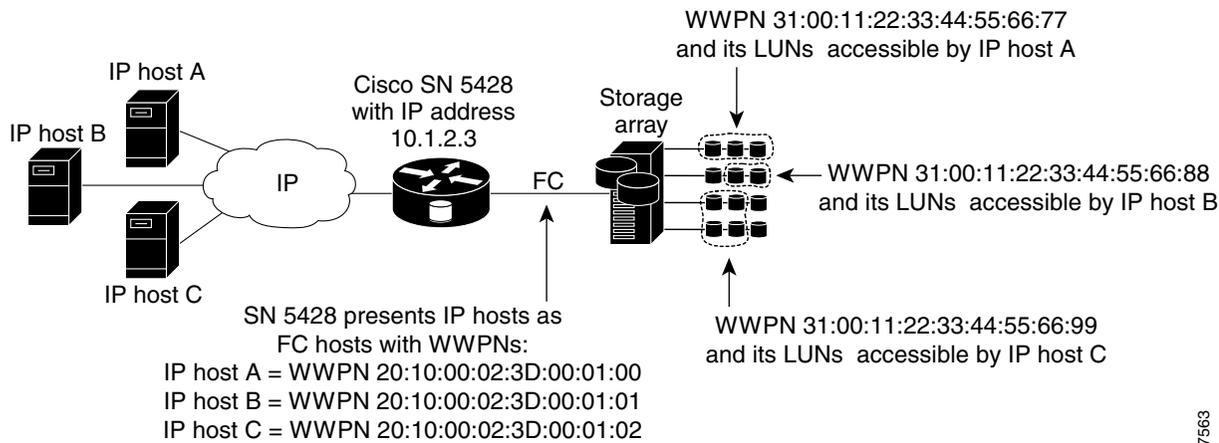
**Note**

The purpose of Figure 1-12 and Table 1-4 is only to illustrate the concept of storage mapping, FC address mapping, and access control. The IP addresses and WWPNs will vary according to each site. In addition, the figure and the table exclude any additional SN 5428 Storage Routers that could be configured for multiple paths between hosts and storage devices.

**Note**

Unlike the SCSI-routing mode, access lists are not used in transparent mode.

Figure 1-12 Transparent SCSI Routing Storage Mapping and Access Control Concept



77563

Figure 1-13 Transparent SCSI Routing Storage Mapping and Access Control Concept

Hosts Allowed Access by Intelligent Storage Array and SN 5428 Authentication	Storage Devices Apparent to Host as Locally Attached Devices	Via GbE IP Address of SCSI Routing Instance	Mapped To Storage	
			WWPN	Drive (LUN)
Host A: apparent to storage array as FC host with WWPN 20:10:00:02:3D:00:01:00	Local Disk (D:)	10.1.2.3	31:00:11:22:33:44:55:66:77	0
	Local Disk (E:)	10.1.2.3	31:00:11:22:33:44:55:66:77	1
	Local Disk (F:)	10.1.2.3	31:00:11:22:33:44:55:66:77	2
Host B: apparent to storage array as FC host with WWPN 20:10:00:02:3D:00:01:01	Local Disk (D:)	10.1.2.3	31:00:11:22:33:44:55:66:88	0
	Local Disk (E:)	10.1.2.3	31:00:11:22:33:44:55:66:88	1
Host C: apparent to storage array as FC host with WWPN 20:10:00:02:3D:00:01:02	Local Disk (D:)	10.1.2.3	31:00:11:22:33:44:55:66:99	0
	Local Disk (E:)	10.1.2.3	31:00:11:22:33:44:55:66:99	1
	Local Disk (F:)	10.1.2.3	31:00:11:22:33:44:55:66:99	2
	Local Disk (G:)	10.1.2.3	31:00:11:22:33:44:55:66:99	3

Available Instances of Transparent SCSI Routing

When an SN 5428 Storage Router is deployed for transparent SCSI routing, it is automatically configured for one instance of transparent SCSI routing service; only that one instance can exist in that SN 5428. This one instance is configured through one Gigabit Ethernet port on the SN 5428.

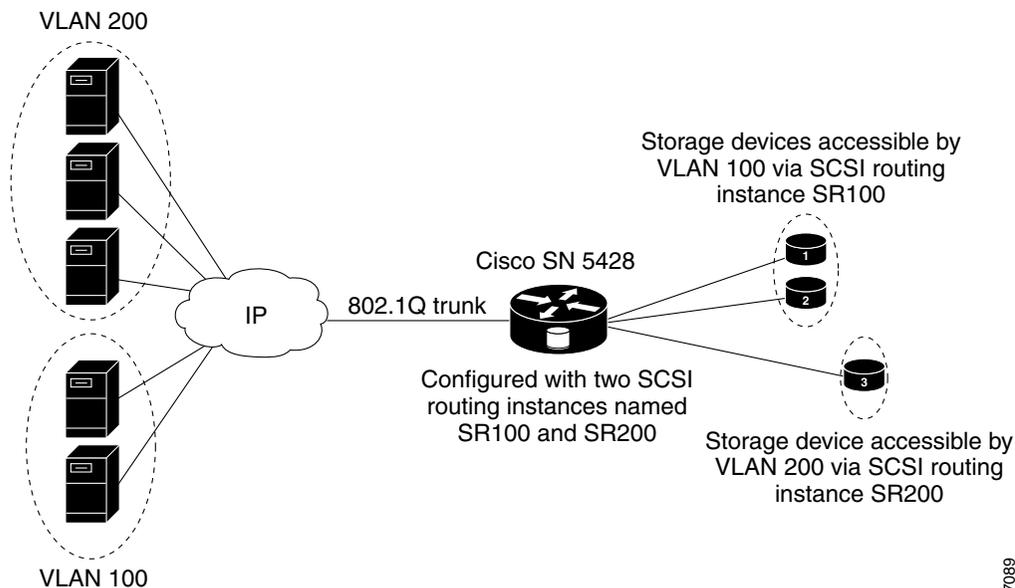
While the instance of transparent SCSI routing needs to be configured with a Gigabit Ethernet IP address, mapping between iSCSI target names and physical storage addresses is automatic and cannot be configured. When an SN 5428 is deployed for transparent SCSI routing, it cannot participate in a storage router cluster. However, multiple SN 5428s can be connected to an intelligent storage array, where it is possible to manage failover and multiple paths. In networks where multiple SN 5428 Storage Routers are connected to an intelligent storage array, each SN 5428 has one (and only one) instance of transparent SCSI routing; the instance is unique to that storage router and cannot fail over to another storage router. For more information about configuring an SN 5428 Storage Router, see the appropriate configuration chapters in this document.

VLAN Access Overview

SN 5428 VLAN access provides IP hosts with access to storage devices according to the VLAN to which each host belongs.

Figure 1-14 shows a sample network that employs SN 5428 VLAN access. In the figure, an SN 5428 Gigabit Ethernet interface is connected to an IP network through an IEEE 802.1Q trunk; the SN 5428 Fibre Channel interfaces are connected to storage devices 1, 2, and 3. The SN 5428 is configured with two SCSI routing instances named SR100 and SR200. The IP network contains two VLANs: VLAN 100 and VLAN 200. The SCSI routing instance, SR100, is configured to allow the hosts in VLAN 100 to access storage devices 1 and 2. The SCSI routing instance, SR200, is configured to allow the hosts in VLAN 200 to access storage device 3.

Figure 1-14 VLAN Access Overview



77089

If the SN 5428 is used in a Cisco switched network environment, configure the SN 5428 using the Cisco proprietary VLAN Trunking Protocol (VTP). With VTP, the SN 5428 will exchange VTP packets with an externally attached switch to dynamically learn about the VLANs that are accessible in the IP network. The SN 5428 then uses VTP to propagate VLAN information around the switched network using layer 2 multicast packets.

If the SN 5428 is used in a non-Cisco switched network environment, configure the SN 5428 for VLAN without using VTP. The SN 5428 does not exchange VTP packets to learn about the VLANs in the network. Instead, you must manually assign VLANs in the network with a VLAN identifier (VID) number. You can optionally assign each VLAN with a unique name and manually set the MTU size.

If the SN 5428 participates in a cluster, the VLAN information configured for the SN 5428 is propagated to all SN 5428s in the cluster.

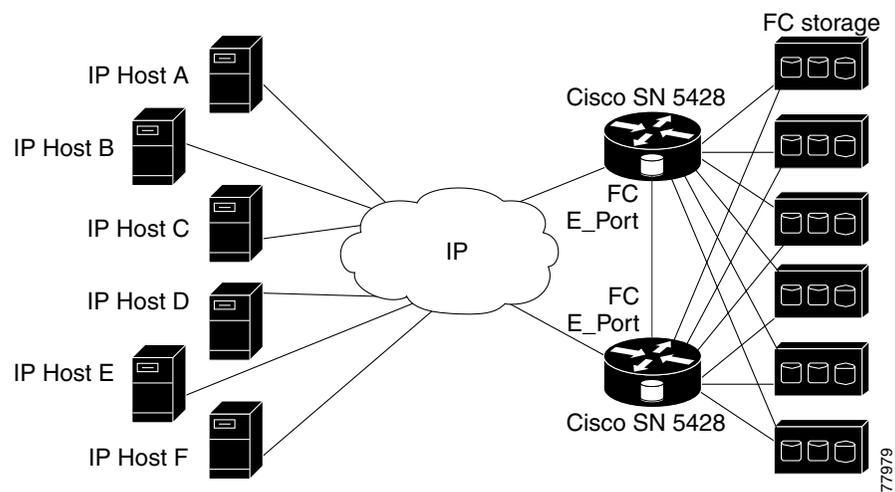
The SN 5428 uses IEEE 802.1Q standard for VLAN encapsulation. With 802.1Q encapsulation, VLAN information is carried in packets sent and received through the SN 5428 Gigabit Ethernet interface. These packets contain the VID and other VLAN information needed for VLAN members to participate in a VLAN.

A VLAN is granted access to storage devices via a SCSI routing instance configured in the SN 5428. The iSCSI targets assigned to the SCSI routing instance determine which storage devices the VLAN can access.

E_Port and FC Fabric Zoning Participation Overview

The SN 5428 Fibre Channel interfaces support E_Port protocol, which allows switch interconnect. Figure 1-15 shows a sample network of an SN 5428 interconnected to another SN 5428 creating an FC switched fabric. In the figure each SN 5428 is connected to an IP network through the Gigabit Ethernet interface; the FC storage interfaces are connected to each SN 5428 and the SN 5428s are connected to each other via a Fibre Channel interface. This allows all IP hosts A through F access to all the FC storage connected to each SN 5428. In this configuration, if an SN 5428 connection to the IP cloud is lost, or if the E_Port interconnect is lost, access to the FC storage is routed through the other SN 5428.

Figure 1-15 E_Port Overview



The SN 5428(s) can merge into existing FC switched fabric zones and participate in WWPN zoning. The FC switched fabric zones are managed by FC switched fabric management software. Zone participation is allowed to the SN 5428 by configuring a unique domain ID on the SN 5428 and by configuring your zone management software with both SN 5428 initiator WWPN1 and initiator WWPN2, see Chapter 5, “Configuring for FC Fabric Zoning”. The SN 5428 does not manage or create zones.

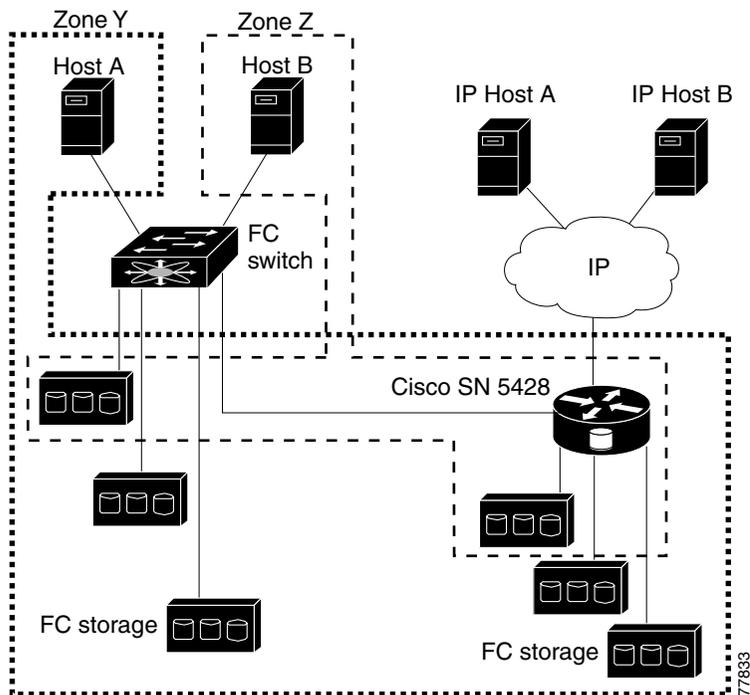
**Note**

FC Fabric zoning participation is not supported in a transparent SCSI router configuration.

Once initiator WWPN1 and initiator WWPN2 are configured, the SN 5428 will participate in fabric zoning using the WWPNs of each FC storage devices attached, either directly or on a fabric loop. The IP hosts participate in zoning via the access list. For more information about access lists, see the “SCSI Routing Mapping and Access Control” section on page 1-5.

Figure 1-16 shows an example network that employs SN 5428 FC fabric zoning. In the figure, the SN 5428 is connected to IP hosts A and B through the Gigabit Ethernet interface; the SN 5428 Fibre Channel interfaces are connected to FC storage and a zoned FC switched fabric. The IP hosts are allowed access to storage devices in both zones (Y and Z) and on the SN 5428 while zone Y has access to all the SN 5428 storage devices and zone Z have access to one storage device on the SN 5428.

Figure 1-16 FC Fabric Zoning Participation Overview



iSCSI Authentication Overview

iSCSI authentication is a software service that is available in each SN 5428. It authenticates IP hosts that request access to storage. iSCSI authentication is provided by an AAA (authentication, authorization, and accounting) subsystem configured in each SN 5428. AAA is Cisco's architectural framework for configuring a set of three independent security functions in a consistent and modular manner: authentication, authorization, and accounting. The SN 5428 Storage Router software implements the authentication function.

Authentication provides a method of identifying users (including login and password dialog, challenge and response, and messaging support) prior to receiving access to the requested object, function, or network service. AAA authentication is configured by defining a list of authentication services. iSCSI authentication, which uses the AAA authentication services list, can be enabled for specific SCSI routing instances in an SN 5428.

When iSCSI authentication is enabled, IP hosts (with iSCSI drivers) must provide user name and password information each time an iSCSI TCP connection is established. iSCSI authentication uses the iSCSI CHAP (Challenge Handshake Authentication Protocol) authentication method.

SN 5428 Cluster Management Overview

You can configure Cisco SN 5428 Storage Routers in a cluster to allow the storage routers to back each other up in case of failure.

**Note**

An SN 5428 storage router can participate in a cluster only if it is deployed for SCSI routing. An SN 5428 deployed for transparent SCSI routing can function only as a stand-alone system.

An SN 5428 Storage Router cluster consists of two storage routers connected as follows:

- Connected to the same hosts
- Connected to the same storage systems
- Connected to each other through their management and high availability (HA) interfaces

In a cluster, storage routers continually exchange HA information to propagate configuration data to each other and to detect failures in the cluster. The storage routers exchange HA information through two separate networks: one connected to the management interface of each storage router and the other connected to the HA interface of each storage router. To make sure that HA information is exchanged reliably between storage routers, the storage routers balance the transmission of HA information between the management and the HA interfaces.

A storage router cluster supports up to 12 active instances of SCSI routing. At any given time, an instance of SCSI routing can run on only one storage router in a cluster. The instance continues running on the storage router where it was started until one of the following actions occurs:

- The instance is explicitly stopped or failed over to the other storage router in the cluster.
- The instance automatically fails over to another storage router because an interface is unavailable or another software or hardware problem occurs.

Each storage router in a cluster can run up to 12 instances of SCSI routing. For example, if one storage router is already running two instances, it is eligible to run up to ten additional instances.

Interface Naming

Configuring the SN 5428 Storage Router software requires that you understand hardware interface naming. This section describes the interface naming system used with the SN 5428 Storage Router hardware.

Each storage router interface is assigned a three-character name consisting of two lower-case letters followed by a number. The letters designate the interface type; the number designates the chassis slot occupied by the interface (See Figure 1-17).

Figure 1-17 SN 5428 Interface Naming System

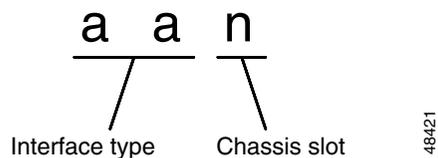
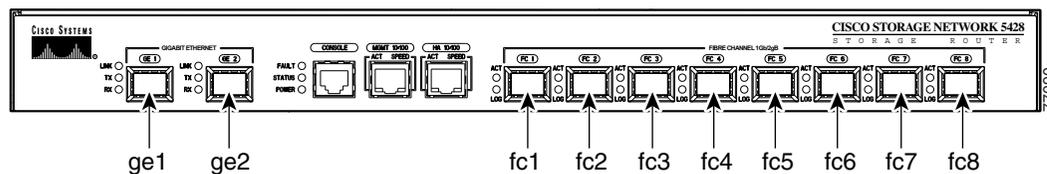


Table 1-5 shows valid interface type designators for the SN 5428; Figure 1-18 shows each interface location and interface name on the SN 5428.

Table 1-5 Interface Type Designators

Interface Type	Description
fc	Fibre Channel
ge	Gigabit Ethernet

Figure 1-18 SN 5428 Chassis-Slot Numbering



Where to Go Next

When you are ready to configure the SN 5428 software, proceed to one of the following chapters in this configuration guide according to your needs:

- Chapter 2, “First-Time Configuration”—For initial setup or after configuration has been reset to factory default configuration
- Chapter 3, “Configuring System Parameters”—Using the CLI for setting up and modifying system parameters
- Chapter 4, “Configuring for VLAN”—Using the CLI for setting up and modifying VLAN configurations
- Chapter 5, “Configuring for FC Fabric Zoning”—Using the CLI for setting up and modifying zoning configurations
- Chapter 6, “Configuring SCSI Routing”—Using the CLI for setting up and modifying SCSI routing configurations
- Chapter 7, “Configuring Transparent SCSI Routing”—Using the CLI for setting up and modifying transparent SCSI routing configurations
- Chapter 8, “Configuring Authentication”—Using the CLI for setting up and modifying authentication configurations
- Chapter 9, “Configuring a High Availability Cluster”—Using the CLI for setting up and modifying cluster configurations
- Chapter 10, “Maintaining and Managing the SN 5428 Storage Router”—Downloading software, backing up and restoring configurations, and other related maintenance and management tasks
- Chapter 11, “Command Line Interface Reference”—For a basic understanding of the command line interface and information on all CLI commands.

**Note**

This guide does not describe how to configure iSCSI drivers. Install and configure iSCSI drivers according to readme and example configuration files for each driver.

■ Where to Go Next



First-Time Configuration

This chapter describes what configuration information to gather and explains the initial system configuration script and setup configuration wizard for the first-time configuration of the Cisco SN 5428 Storage Router. This chapter also introduces the command line interface (CLI) and web-based GUI, which can be used for subsequent configuration tasks.

This chapter contains the following sections:

- Prerequisite Tasks, page 2-1
- Collecting Configuration Information, page 2-2
- Connecting a Console, page 2-6
- Initial System Configuration Script, page 2-6
- Running the Setup Configuration Wizard, page 2-7
- Introducing the CLI, page 2-8
- Introducing the Web-Based GUI, page 2-11
- Where to Go Next, page 2-12

Prerequisite Tasks

Before configuring the SN 5428 Storage Router for the first time, make sure you have completed the hardware installation according to the *Cisco SN 5428 Storage Router Hardware Installation Guide*.

Collecting Configuration Information

Use the Cisco SN 5428 Storage Router First-Time Configuration Checklist (Table 2-2) to help you gather the system and network information that is needed for the first-time configuration of your SN 5428 Storage Router. The items in the checklist are based on the information requested by the initial system configuration script and the setup configuration wizard. Refer to Table 2-1 for information on the configuration items needed for first-time configuration.

Table 2-1 Collecting Configuration Information

Configuration Item	Description	Required or Optional
Configuration deployment option	The SN 5428 can be configured for one of two kinds of deployments: <ol style="list-style-type: none"> 1. SCSI routing (SN 5428 enables iSCSI hosts to access Fibre Channel storage. SN 5428 manages access to the Fibre Channel storage.) 2. Transparent SCSI routing (SN 5428 enables iSCSI hosts to access Fibre Channel storage. SN 5428 does not manages access to the Fibre Channel storage.) 	Required
Management interface IP address and subnet mask	The IP address and subnet mask of the storage router management interface. Note The management interface for each storage router in a cluster must be on the same IP subnet.	Required
Static route for management interface	The destination IP address with subnet mask and then the gateway IP address.	Required if SN 5428 is managed from a subnet other than the one to which it is physically attached
System name	The name you want to use for the storage router. If you use the services of a domain name server (DNS), the system name is the same name you will enter and associate with the management interface. Maximum length is 19 characters.	Required
GE Interface	The Gigabit Ethernet interface used to communicate to the IP network, either ge1 or ge2. The default is ge1.	Required for Transparent SCSI routing only
High availability (HA) configuration	The SN 5428 can run in either <i>standalone</i> or <i>clustered</i> mode. The default is <i>clustered</i> . Standalone mode is recommended if the storage router is not intended to provide high availability along with other SN 5428s.	Required for SCSI routing only
High availability (HA) cluster name	The name of the cluster in which the storage router is to participate. Clusters are multiple storage routers that back each other up in case of hardware or software failure. All SN 5428s that participate in a cluster must have the same cluster name.	Required only if <i>clustered</i> was specified for the HA configuration

Table 2-1 Collecting Configuration Information (continued)

Configuration Item	Description	Required or Optional
High availability (HA) IP address and subnet mask	The IP address and subnet mask of the storage router HA interface. The HA interface and management interface must be on unique IP networks. If the SN 5428 is to participate in a cluster, the HA IP address is required; if the SN 5428 is a stand-alone machine, it is optional. Note The HA interface for each storage router in a cluster must be on the same IP subnet.	Required only if <i>clustered</i> was specified for the HA configuration
Primary DNS IP address	The IP address of the primary domain name server to be accessed by the storage router. Required if you refer to any other server via name rather than IP address.	Optional
Secondary DNS IP address	A backup domain name server from which the storage router can request services when the primary DNS is unavailable.	Optional
NTP server IP address	The IP address of the NTP server available to the storage router. This allows the storage router to keep the date and time synchronized with the rest of the network.	Optional
Time zone, current date and time	The format for the date is mm/dd/yyyy, and the time is hh:mm:ss.	Optional
Enable Telnet on all interfaces	Enable Telnet access on all interfaces. By default, Telnet access is enabled on only the management interface.	Optional
SNMP read community name	The name of the community having read-only access to the storage router network. The SN 5428 will respond to this community's GET commands. The default is <i>public</i> .	Optional
SNMP write community name	The name of the community having write access to the storage router network. The SN 5428 will respond to this community's SET commands. The default is <i>private</i> .	Optional
First SNMP trap manager IP address	The IP address of the first destination host used for SNMP notifications (traps). Required if you wish to use SNMP traps.	Optional
Trap version for first SNMP IP address	The version number of the traps that are to be sent to the first SNMP trap manager IP address. The default is <i>1</i> .	Optional
Second SNMP trap manager IP address	An optional IP address of the second destination host used for SNMP notifications (traps).	Optional
Trap version for second SNMP IP address	The version number of the traps that are to be sent to the second SNMP trap manager IP address. The default is <i>1</i> .	Optional
Send authentication failure option	Enable an authentication failure trap to be sent when a user specifies an incorrect community.	Optional
Send link up/down traps option	Enable link up/down traps to be sent for the Management, HA, Gigabit, and/or Fibre Channel interfaces when the link goes up and when it goes down.	Optional
Monitor-level password	A password for users who will only monitor storage router operations. The default password is <i>cisco</i> .	Optional

Table 2-1 Collecting Configuration Information (continued)

Configuration Item	Description	Required or Optional
Administrator-level password	A password for users who will configure and administer the storage router. The default password is <i>cisco</i> .	Optional
Password applied to EIA/TIA-232 console interface (yes/no)	Choose whether or not the user is required to enter the monitor and administrator password when accessing the storage router via the EIA/TIA-232 console interface. The default is <i>no</i> .	Optional
System administrator contact information	The name, e-mail address, phone number, and pager number of the system administrator of the SN 5428. Usage is completely site-specific.	Optional
Name of SCSI routing instance	<p>A unique name for a SCSI routing instance. Names of instances can be up to 32 characters in length. A maximum of 12 unique SCSI routing instances are allowed. Only one instance can be named in the setup configuration wizard.</p> <p>Note If the storage router is going to be a member of a cluster, do not define more than 12 SCSI routing instances across all storage routers in the cluster. For additional information about HA, cluster configuration and failover, see Chapter 9, “Configuring a High Availability Cluster,” and Chapter 10, “Maintaining and Managing the SN 5428 Storage Router.”</p> <p>Note Do not name the SCSI routing instance with the setup configuration wizard if you are using the VLAN service with your SN 5428. See Chapter 4, “Configuring for VLAN,” before naming and configuring SCSI routing instances.</p>	Required

Once you have completed the first-time configuration checklist, you are ready to continue with the first-time configuration of the SN 5428 Storage Router using the initial system configuration script and the setup configuration wizard.

Table 2-2 Cisco SN 5428 Storage Router First-Time Configuration Checklist

Configuration Item	Value
Configuration deployment option (1 or 2)	
Management interface IP address and subnet mask	
Static route for management interface	
System name	
GE Interface	
High availability (HA) configuration (standalone or clustered)	
HA cluster name	
HA interface IP address and subnet mask	
Primary DNS IP address	
Secondary DNS IP address	
NTP server IP address	
Enable Telnet on all interfaces (yes/no)	
SNMP read community name (default <i>public</i>)	
SNMP write community name (default <i>private</i>)	
First SNMP trap manager IP address	
Trap version for first SNMP IP address	
Second SNMP trap manager IP address	
Trap version for second SNMP IP address	
Send authentication failure trap when incorrect community specified (yes/no)	
Modify link up/down traps for one or more interfaces (yes/no)	
Send link up/down traps for Management interface (yes/no)	
Send link up/down traps for HA interface (yes/no)	
Send link up/down traps for Gigabit Ethernet interface (yes/no)	
Send link up/down traps for Fibre Channel interface (yes/no)	
Monitor-level password	
Administrator-level password	
Apply passwords to EIA/TIA-232 console interface (yes/no)	
System administrator name	
System administrator e-mail address	
System administrator phone number	
System administrator pager number	
Name of SCSI routing instance (if using the VLAN service, do not configure a SCSI routing instance with the setup configuration wizard)	

Connecting a Console

To begin configuration of your SN 5428 Storage Router, use the command line interface (CLI), by connecting a PC with a terminal emulation program to the EIA/TIA-232 console interface according to the *Cisco SN 5428 Storage Router Hardware Installation Guide*. Then make sure that the terminal emulation program is configured for a CLI session with the values provided in Table 2-3.

Table 2-3 Terminal Emulation Configuration

Setting	Value
Terminal mode	VT-100
Baud	9600
Parity	No parity
Stop bits	1 stop bit

Initial System Configuration Script

The initial system configuration script runs on the CLI and ensures that a few required values are entered to make the SN 5428 Storage Router operational. When you first power up the storage router and after the initial boot process, the script will run automatically on the CLI session running on the terminal emulation program via an EIA/TIA-232 console connection.

After the first running of the script, the script will run automatically whenever the storage router is not configured with an IP address for the management interface, due most likely to a **clear conf** command, which requires the system to be configured again.

The initial system configuration script provides explanatory text before prompting you to enter configuration values. There are two versions of the script. The values asked for by the script are determined by the configuration deployment option entered for the first prompt.

Table 2-4 lists the configuration items in the order they will appear in the script.

Table 2-4 Configuration Items in Initial System Configuration Script

Configuration Item	Configuration Deployment
Configuration deployment option: 1 for SCSI routing or 2 for transparent SCSI routing	All
Management interface IP address and subnet mask in CIDR style (for example: 10.1.10.244/24)	All
(Optional) The destination IP address with subnet mask and then the gateway IP address. (for example 1.0.1.0/24 10.0.1.2)	All
SN 5428 system name (maximum length allowed is 19 characters)	All
HA configuration (standalone or clustered)	SCSI routing
Cluster name (asked for only when HA configuration is set to <i>clustered</i>)	SCSI routing
HA interface IP address and subnet mask in CIDR style (for example: 10.1.20.56/24; asked for only when HA configuration is set to <i>clustered</i>)	SCSI routing

Table 2-4 Configuration Items in Initial System Configuration Script (continued)

Configuration Item	Configuration Deployment
Gigabit Ethernet interface used to communicate to IP network, select either ge1 or ge2	Transparent SCSI routing
Gigabit Ethernet interface IP address and subnet mask in CIDR style (for example: 10.1.0.45/24)	Transparent SCSI routing

When the script completes, the system will automatically reboot. When the command prompt returns, continue configuration with the setup configuration wizard.

Running the Setup Configuration Wizard

The setup configuration wizard is available from the CLI and is a script that consists of a series of prompts asking you to enter values to provide a basic system configuration for your SN 5428. You will be asked to enter values to configure the following:

- Management interface (this includes primary and secondary DNS servers)
- Time zone, NTP server, current date and time
- Network management access (this includes SNMP)
- Monitor and administrator passwords
- Console interface password
- System administrator contact information
- SCSI routing (this section of the wizard only appears if SCSI routing was the configuration deployment selected in the initial system configuration script; if you are using the VLAN service, do not configure SCSI routing with the setup configuration wizard)

You can run the setup configuration wizard through an EIA/TIA-232 console interface connection, or through a Telnet session using the management interface if the IP address is already configured in the storage router. If you choose to complete the configuration using the management interface, use the default password, *cisco*, to establish your CLI session.

The values entered for the setup configuration wizard are saved at the end of the wizard's script. To quit the configuration wizard at any time without saving changes, press **Ctrl-C**, and reboot the storage router to restore previous values.



Note

The factory default listening port used for iSCSI traffic is 3260. This is a port number assigned by IANA. You can change this value for your network configuration if needed. See the CLI **setup iscsi-port** command in Chapter 11, "Command Line Interface Reference," for details.

Use the following procedure to start the setup configuration wizard.

	Command	Description
Step 1	enable	Enter Administrator mode. If prompted for an Administrator password, use the default password, <i>cisco</i> .
Step 2	setup	<p>Start the setup configuration wizard.</p> <p>The wizard can run in either of two modes: novice or expert. The novice level provides information before the prompt explaining what is being requested. The expert level does not provide the explanatory text. The wizard will ask you to choose one of the two levels.</p> <p>Respond to the prompts using your Cisco SN 5428 Storage Router First-Time Configuration Checklist. For multiple choice questions, the choices are shown in square brackets. For values requiring a specific format, the required format is shown in square brackets. If values have already been entered (for instance, via the initial system configuration script), the current value saved in the system are shown in square brackets. Default values are shown in parentheses within the square brackets. If you want to accept the current or default value, press Enter. If there is no default and you want to bypass the question (that is, you do not want to change or provide a value), simply press Enter.</p>

If you configured any interfaces or identified any servers to the SN 5428 that are outside the storage router management subnet, you must update the SN 5428 route table with the appropriate gateways that will provide access to these interfaces or servers. See the CLI **ip route** command in Chapter 11, “Command Line Interface Reference,” for details.

You can use the **setup** command again to change these basic configuration parameters. You can also use the command line interface (CLI) or the web-based GUI to make changes to the basic storage router configuration or to configure the storage router more extensively. To access the web-based GUI, point your browser to the SN 5428 management interface IP address.

Introducing the CLI

The CLI is available via a Telnet session to the management interface. It is also available via a direct EIA/TIA-232 connection on the console interface. The CLI provides commands to perform all necessary SN 5428 management functions, including software upgrades and maintenance.

All CLI commands are capable of prompting for further information as the user types. Pressing the Tab key completes the current command word at any point after it is unique. Pressing the question mark (?) key lists all of the options available at that point in the command syntax. Each word can be truncated at any point after it is unique.

Character Case Sensitivity in the CLI

CLI commands, keywords, and reserved words are not case-sensitive. Commands, keywords, and reserved words can be entered in upper and lower case. User-defined text strings can be defined in both upper and lower case (including mixed cases) and is preserved in the configuration.

Command Modes

The SN 5428 management interface is password protected. You must enter passwords when accessing the SN 5428 via Telnet (for the CLI) or web-based GUI.

There are two levels of authority:

- Monitor mode—Allows view-only access to the SN 5428 status and system configuration information.
- Administrator mode—Allows the user to configure and actively manage the SN 5428, its access lists and SCSI routing instances, and the SN 5428 cluster.

Passwords for Monitor and Administrator mode can be initially configured through the setup configuration wizard (see “Running the Setup Configuration Wizard” section on page 2-7). The factory default password for both modes is *cisco*.

Command Prompt

The CLI command prompt includes the SN 5428 system name. An asterisk (*) appears at the beginning of the prompt if the system configuration has been modified but not saved.

Reserved Words

Reserved words cannot be used as values or names in CLI commands. Words that are used as commands or as keywords in commands are reserved words. The following are additional reserved words in the CLI.

- acl
- canonical
- iprouter
- iptan
- loglevel

Show CLI Command

Use the **show cli** command to display the complete CLI command syntax tree, along with helpful information about command parameters and arguments. Only valid commands will display for the current command mode of your SN 5428.

You can choose specific commands to display by specifying desired commands with the **show cli** command. For example, **show cli aaa debug scsirouter** displays the syntax tree for all *aaa* commands, all *debug* commands, and all *scsirouter* commands.

Special Keys

The CLI supports the use of special keyboard keys. Table 2-5 lists the special keys and describes their function.

Table 2-5 *Special Keys*

Key	Function
?	List choices
Backspace	Delete character backwards
Tab	Command word completion
Ctrl-A	Go to the beginning of the line
Ctrl-B or Left Arrow	Go backwards one character
Ctrl-D	Delete current character
Ctrl-E	Go to the end of the line
Ctrl-F or Right Arrow	Go forward one character
Ctrl-K	Delete from current position to the end of the line
Ctrl-N or Down Arrow	Go to the next line in the history buffer
Ctrl-P or Up Arrow	Go to the previous line in the history buffer
Ctrl-T	Transpose the current and previous character
Ctrl-U	Delete the line
Ctrl-W	Delete the previous word

Starting a CLI Management Session

Follow these steps to start a CLI management session via a Telnet connection to the storage router.

-
- Step 1** Establish a Telnet session to the SN 5428.
 - Step 2** Enter the appropriate password at the logon prompt.
 - Step 3** (Optional) Enter **enable** to change to Administrator mode.



Note If you need to make changes to the configuration of the storage router, you need to enable the Administrator mode.

- Step 4** (Optional) Enter the Administrator password at the prompt.
 - Step 5** Issue the appropriate CLI commands to complete the desired task.
-

Introducing the Web-Based GUI

As an alternative to the CLI, you can configure your SN 5428 Storage Router using the web-based GUI. You can use the GUI for configuration after completing the initial system configuration script, which assures that the SN 5428 management interface is configured with an IP address.

To access the GUI, enter the URL for the SN 5428 by pointing your browser to the SN 5428 management interface IP address using the HTTP protocol (for example, type **http://10.1.10.244**).

Logging In

After entering the URL for your SN 5428, a login page will appear. You can log in as *monitor* or as *admin*, and you will be asked for your user name and password. See Table 2-6 for the user name and factory default password to use for the two login options. If you already configured new passwords for the monitor and/or the administrator mode, use them when logging in.

Table 2-6 Logging into Web-Based GUI

Login Options	User Name	Factory Default Password
Monitor	monitor	cisco
Admin	admin	cisco

Monitor Mode

Monitor mode in the web-based GUI will only allow you to monitor the storage router. You cannot configure, maintain, or troubleshoot the storage router in monitor mode. If you click on the Configuration, Maintenance, and Troubleshooting menu items in the GUI, a login dialog box will appear asking for a user name and password for administrator mode.

Administrator Mode

In administrator mode, you can configure, maintain, and troubleshoot the storage router. If you click the Monitor menu item, a login dialog box will appear asking for a user name and password for monitor mode.

Menu Items and Links

The GUI's menu items and links appear horizontally at the top of the browser page. Table 2-7 lists the menu items and links, the action that takes place when they are clicked, and the login modes from which they are available.

Table 2-7 *Menu Items and Links in the GUI*

Menu Items and Links	Action	Login Mode
Monitor	Lists menu options in left frame to be displayed in main frame.	Monitor only
Configuration	Lists menu options in left frame to be displayed in main frame.	Admin only
Maintenance	Lists menu options in left frame to be displayed in main frame.	Admin only
Troubleshooting	Lists menu options in left frame to be displayed in main frame.	Admin only
Support	Opens the Cisco.com “Service & Support” page in a new browser window.	Monitor and Admin
Home	Returns to the GUI's login page where you select to log in as either Monitor or Admin.	Monitor and Admin
Help	Opens the GUI's online help in a new browser window.	Monitor and Admin

Where to Go Next

If you did not run the complete SN 5428 setup configuration wizard, or if you want to make system configuration additions, changes, or corrections, continue with the procedures described in Chapter 3, “Configuring System Parameters.”

If you are using the VLAN service with the storage router and you entered all desired parameters—except for SCSI routing—with the setup configuration wizard (see “Running the Setup Configuration Wizard” section on page 2-7 for details), configure for VLAN using the procedures described in Chapter 4, “Configuring for VLAN.”

If you are participating in FC zoning with the storage router, configure for zoning using the procedures described in Chapter 5, “Configuring for FC Fabric Zoning.”

If you do not need to configure for VLAN or zoning, go directly to Chapter 6, “Configuring SCSI Routing,” to configure SCSI routing more extensively.



Note

If you are going to add the storage router to an existing storage router cluster, review the information and procedures in Chapter 9, “Configuring a High Availability Cluster,” before configuring SCSI routing.



Configuring System Parameters

This chapter explains how to configure system parameters on your SN 5428 Storage Router and contains the following sections:

- Prerequisite Tasks, page 3-1
- Configuration Tasks, page 3-2
- Configuring the Management Interface, page 3-3
- Configuring Time and Date, page 3-4
- Configuring Network Management Access, page 3-5
- Configuring Passwords, page 3-6
- Configuring Administrator Contact Information, page 3-6
- Configuring the High-Availability Interface, page 3-7
- Verifying and Saving Configuration, page 3-8

System parameters can be configured or changed using CLI commands, as described in this chapter, or via the web-based GUI. To access the web-based GUI, point your browser to the storage router's management interface IP address. After logging on, click the Help link to access online help for the GUI.

Prerequisite Tasks

Before configuring system parameters, make sure you have finished the following tasks:

- Completed the hardware installation according to the *Cisco SN 5428 Storage Router Hardware Installation Guide*.
- Entered values as requested by the initial system configuration script (for more information, see the “Initial System Configuration Script” section on page 2-6).



Note

You do not need to perform the configuration tasks in this chapter if you ran the complete SN 5428 setup configuration wizard (using the **setup** CLI command with no keyword), or if you ran the wizards separately using all the **setup** CLI commands except **setup scsi**.

Configuration Tasks

To configure system parameters on your SN 5428 Storage Router, perform the following steps:

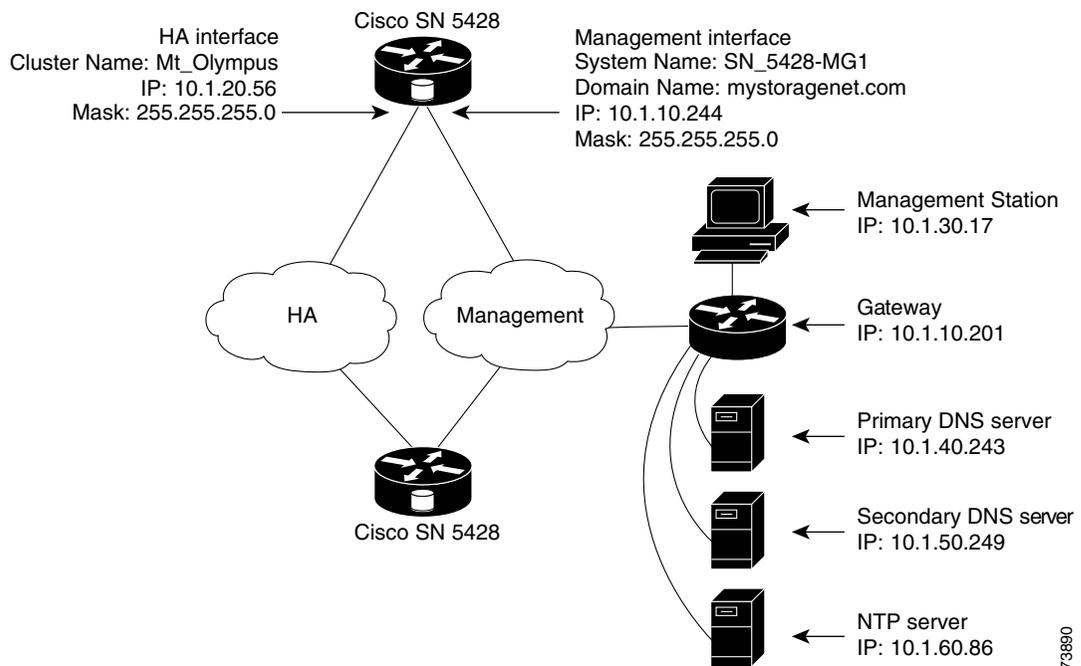
- Step 1** Configure the management interface.
- Step 2** Configure the time and date.
- Step 3** (Optional) Configure network management access.
- Step 4** Configure passwords.
- Step 5** Configure administrator contact information.
- Step 6** (Optional) Configure the high-availability (HA) interface.
- Step 7** Verify and save configuration.



Note You can verify and save the configuration (by using the **save system bootconfig** or **save all bootconfig** command) at any point in the process of performing the configuration tasks.

Figure 3-1 illustrates the example configuration used in this chapter.

Figure 3-1 System Parameters Example Configuration



Configuring the Management Interface

Configuring the management interface consists of tasks for setting the system name, IP address and mask, gateway, and DNS servers. Use the following procedure to configure the management interface.



Note The purpose of Figure 3-1 is an example system configuration only. The IP addresses and all names given below are examples only.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	hostname <i>SN_5428-MG1</i>	Specify or change the system name. The system name identifies the SN 5428 through the management interface and appears immediately in the prompt.
Step 3	interface mgmt ip-address <i>10.1.10.244/24</i>	Specify or change the IP address and subnet mask for the management interface. Note If this storage router is to participate in a cluster, the management interface for all storage routers in the cluster must be on the same IP subnet.
Step 4	ip route <i>10.1.30.0/24 10.1.10.201</i>	(Optional) Configure a gateway IP address if the storage router is to be managed from a management station outside the storage router management subnet. The second IP address specifies a gateway on the storage router management network that will provide access to a management station. Note In this configuration example, the mask is set to 24 (255.255.255.0) to allow any host on subnet 10.1.30.0 to be a management station.
Step 5	ip name-server <i>10.1.40.243</i> <i>10.1.50.249</i>	(Optional) Set the primary and secondary DNS IP addresses. Specifies the IP address of the primary DNS server if the management interface IP address is to be correlated with a DNS host name. If there is a secondary DNS, the second IP address specifies the IP address of the secondary DNS server.
Step 6	ip domain-name <i>mystoragenet.com</i>	(Optional) Specify the domain name of the storage router. Use this command in conjunction with the ip name-server command.

	Command	Description
Step 7	ip route <i>10.1.40.243/32</i> <i>10.1.10.201</i>	(Optional) Configure a gateway IP address if the primary DNS server is outside the storage router management subnet. The second IP address specifies a gateway on the storage router management network that will provide access to a primary DNS server. Note In this configuration example, the mask is set to 32 (255.255.255.255) to specify the host with IP address 10.1.40.243 (the primary DNS server).
Step 8	ip route <i>10.1.50.249/32</i> <i>10.1.10.201</i>	(Optional) Configure a gateway IP address if the secondary DNS server is outside the storage router management subnet. The second IP address specifies a gateway on the storage router management network that will provide access to a secondary DNS server. Note In this configuration example, the mask is set to 32 (255.255.255.255) to specify the host with IP address 10.1.50.249 (the secondary DNS server).

Configuring Time and Date

Configuring time and date parameters consists of specifying the time zone, time, date and time server. Use the following procedure to configure the time and date parameters.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	clock timezone <i>US/Pacific</i>	Identify the time zone where the storage router is located. If a time zone is not identified, time is assumed to be GMT. Note To use the clock timezone command, you must use a valid time-zone string. For a list of valid time-zone strings, use the clock timezone ? command. See Chapter 11, “Command Line Interface Reference,” for details.
Step 3	clock set <i>08:20:00 02 15 2002</i>	Set time and date (for example: time, 8:20 A.M.; date, April 15, 2002).
Step 4	ntp peer <i>10.1.60.86</i>	(Optional) Specify the name or IP address of the network time protocol (NTP) server with which the storage router will synchronize the date and time.
Step 5	ip route <i>10.1.60.86/32</i> <i>10.1.10.201</i>	(Optional) Specify the gateway IP address if the time server is outside the storage router management subnet. The second IP address specifies the gateway on the storage router management network that provides access to the time server. Note In this configuration example, the mask is set to 32 (255.255.255.255) to specify the host with IP address 10.1.60.86.

Configuring Network Management Access

Configuring network management access consists of tasks for configuring SNMP. Use the following procedure to configure SNMP for network management access.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	no restrict all telnet	(Optional) Enable Telnet access on all interfaces. By default, Telnet access is enabled on only the management interface.
Step 3	snmp-server community <i>world</i> ro	(Optional) Specify the name of the community having read-only access of the storage router network (that is, to which community's GET commands the storage router will respond). The default read community is <i>public</i> .
Step 4	snmp-server community <i>mynetmanagers</i> rw	(Optional) Specify the name of the community having write access to the storage router network (that is, to which community's SET commands the storage router will respond). The default write community is <i>private</i> .
Step 5	snmp-server host <i>10.1.30.17</i> version 2 traps	Specify the IP address for the first destination host used for a specified version of notifications (traps). Version 1 traps is the default version. Note In this configuration example, the trap hosts have IP addresses that are outside the storage router management subnet. In an earlier step in the Configuring the Management Interface section, a gateway was already specified providing access to hosts on the 10.1.30.0 subnet.
Step 6	snmp-server host <i>10.1.30.18</i> traps	(Optional) Specify the IP address for the second destination host used for notifications (traps). Version 1 traps is the default version.
Step 7	snmp-server sendauthtraps	(Optional) Enable sending of authentication failure traps.
Step 8	no snmp-server linkupdown all	(Optional) By default, the SNMP agent is enabled to generate link up/down traps for all interfaces. In this configuration example, the command disables this setting for all interfaces. To disable this setting for individual interfaces, see Chapter 11, "Command Line Interface Reference."

Configuring Passwords

Configuring passwords consists of setting the Monitor-mode and Administrator-mode passwords for access to the 10/100 Ethernet management interface (used for the CLI via Telnet and the web-based GUI via HTTP). You can enable these passwords to restrict access to the EIA/TIA-232 console interface. Use the following procedure to configure passwords.



Note The factory default password for both Monitor and Administrator modes is *cisco*.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	monitor password <i>janu\$01</i>	Set the monitor password (for users who only monitor storage router operation).
Step 3	admin password <i>electr@50</i>	Set the administrator password (for system administrators, allowing configuration changes).
Step 4	restrict console	(Optional) Enable the Monitor-mode and Administrator-mode passwords to be required when accessing the SN 5428 via a console connected to the EIA/TIA-232 console interface.

Configuring Administrator Contact Information

Configuring administrator contact information consists of tasks for specifying the name, e-mail address, phone number, and pager number of the system administrator for the storage router. Use the following procedure to configure administrator contact information.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	admin contactinfo name <i>“Pat J. Smith”</i> email <i>pjsmith@mystoragenet.com</i> phone <i>“763 555-1117”</i> pager <i>“763 555-7766”</i>	Provide contact name, e-mail address, phone number, and pager number. Enclose each string that contain spaces in single or double quotes. Note The admin contactinfo command requires that you specify either one parameter or all four parameters.

Configuring the High-Availability Interface

When the storage router is part of a storage router cluster, you will need to configure the high availability (HA) interface. Use the following procedure to configure the HA interface parameters.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	show cluster	Display cluster information and refer to the HA Configuration field to verify if the storage router is running as standalone or clustered. Also, verify if the HA interface is configured with a correct IP address.
Step 3	setup cluster	<p>Run the setup cluster wizard. The wizard prompts you to do the following:</p> <ul style="list-style-type: none"> • Select the appropriate HA configuration mode (standalone or clustered). • Specify HA interface IP address and subnet mask (The HA and management interfaces must not be on the same network; each interface must be on a unique IP network. In a cluster, the HA interfaces for all storage routers must be on the same IP subnet.) • Change cluster name (if necessary). <p>You will be asked if you want to retain or delete the current configuration of the storage router:</p> <ul style="list-style-type: none"> • Retaining means that the configuration of this storage router (including SCSI routing instances) is propagated to the other storage router in the same cluster. • Deleting means that the existing configuration (including SCSI routing instances) will be deleted from the storage router. <p>If you are joining an existing cluster, any access lists that you have previously defined will be overwritten by the access lists available to the cluster. This occurs regardless of your decision to retain or delete configuration information. If you wish to make your current access lists available to the cluster, you must save them to a file before joining the cluster, then restore them. See Chapter 9, “Configuring a High Availability Cluster” for complete details.</p> <p>As prompted, type <i>yes</i> to confirm your choice to retain or delete the current configuration of the SN 5428. The system will then automatically reboot.</p>

Verifying and Saving Configuration

Verify the system parameters using the following procedure. You can save the configuration at any time using either the **save system bootconfig** or **save all bootconfig** commands. You must save the running configuration to the bootable configuration for it to be retained in the storage router when it is rebooted.

Use the following procedure to verify configuration information.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	show system	Display system information, such as system name, software version, date and time (including time zone), NTP server, DNS (name server), and management and HA interface IP addresses.
Step 3	show ip route	(Optional) Display the system route table, if you added any routing information.
Step 4	show snmp	(Optional) Display SNMP management configuration information for the storage router, if set.
Step 5	show admin	(Optional) Display contact information for the system administrator of the storage router, if set.
Step 6	show cluster	(Optional) Display cluster name and other cluster information, if you configured the storage router as a member of a cluster.
Step 7	show bootconfig	(Optional) Display the current boot configuration of the SN 5428.
Step 8	show runningconfig	(Optional) Display the current running configuration of the SN 5428.



Configuring for VLAN

This chapter explains how to configure your SN 5428 Storage Router for a virtual local area network (VLAN) and contains the following sections:

- Prerequisite Tasks, page 4-1
- VLAN Encapsulation, page 4-1
- Configuration Tasks, page 4-2
- Configuring for VLAN with VTP, page 4-3
- Configuring for VLAN without VTP, page 4-3
- Configuring an IP Route, page 4-4
- Verifying and Saving Configuration, page 4-5
- Assigning a VLAN to a SCSI Routing Instance, page 4-6

You can configure for VLAN using CLI commands, as described in this chapter, or via the web-based GUI. To access the web-based GUI, point your browser to the storage router's management interface IP address. After logging on, click the Help link to access online help for the GUI.

Prerequisite Tasks

Before configuring for VLAN, make sure you have configured all system parameters as described in Chapter 2, “First-Time Configuration,” or Chapter 3, “Configuring System Parameters.”

VLAN Encapsulation

The SN 5428 Storage Router uses the IEEE 802.1Q standard for VLAN encapsulation.



Note

If the storage router is connected to a Cisco switch, the switch port must be configured as a trunk port and the encapsulation set to 802.1Q, not Inter-Switch Link (ISL), which is the default setting for trunk ports.

Configuration Tasks

To configure for VLAN on the SN 5428 Storage Router, perform the following steps:

- Step 1** Configure for VLAN using the VLAN Trunking Protocol (VTP).
or
Configure for VLAN without using VTP.
- Step 2** Configure an IP route.
- Step 3** Verify and save configuration.

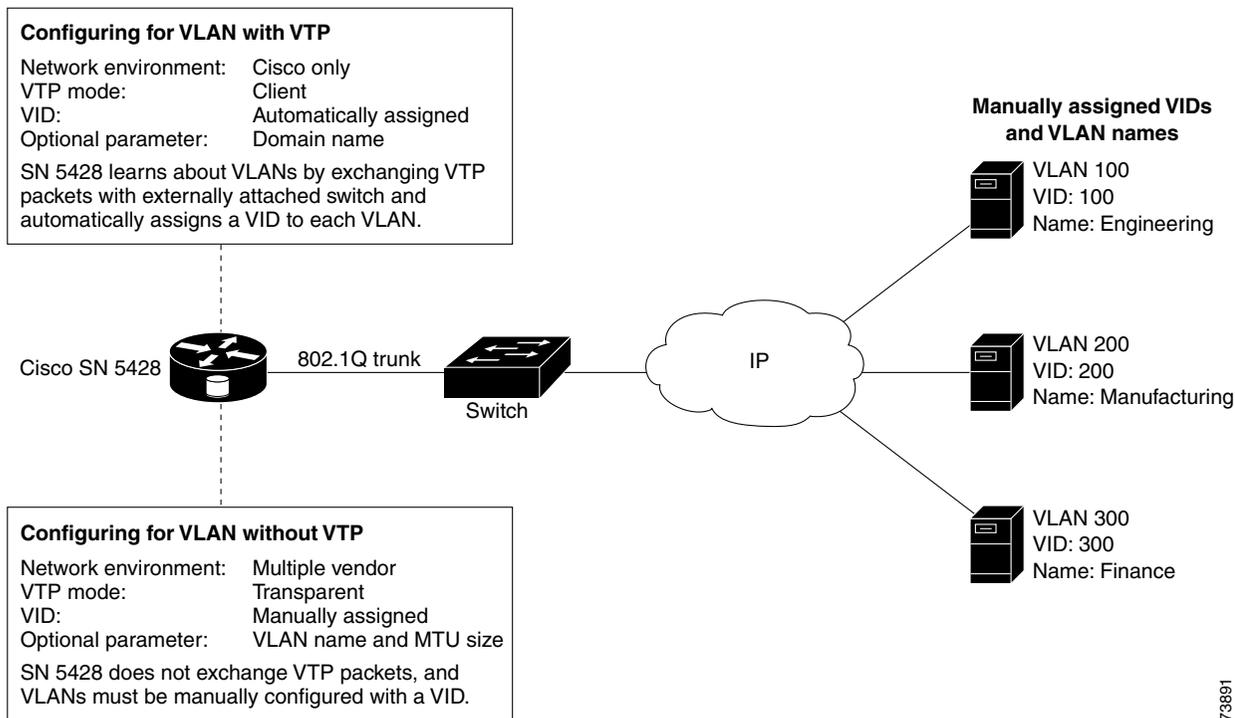


Note You can verify and save the configuration at any point in the process of performing the configuration tasks. Save your configuration by using the **save all bootconfig** CLI command. This command saves all configuration data to the bootable configuration, which is then used when the storage router is rebooted.

- Step 4** Proceed to Chapter 6, “Configuring SCSI Routing,” to configure SCSI routing and to assign a VLAN to a SCSI routing instance.

Figure 4-1 contrasts configuring the SN 5428 Storage Router for VLAN with VTP and without VTP.

Figure 4-1 Contrast of Configuring for VLAN with VTP and without VTP



73891

Configuring for VLAN with VTP

Configuring for VLAN using the VLAN Trunking Protocol (VTP) consists of assigning the VTP domain name and setting the VTP mode to client. VTP, a proprietary protocol of Cisco Systems, is used to propagate VLAN information around a switched network.

Use the following procedure to configure VLAN using VTP.


Note

VTP can only be used in a Cisco network environment.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	vtp domain <i>opus</i>	(Optional) Assign a VTP domain name (<i>opus</i>) to which the SN 5428 Storage Router belongs. If a domain name is not specified, the SN 5428 will assign itself to the first domain from which it receives a VTP message. The default setting is <i>none</i> .
Step 3	vtp mode client	<p>The default setting for the VTP mode is <i>client</i>. Set the VTP mode to <i>client</i> if the current setting is <i>transparent</i>.</p> <p>In client mode, the SN 5428 will exchange VTP packets with an externally attached switch to learn about the VLANs that are accessible in the network.</p> <p>Note The VTP mode is a cluster-wide configuration item. When set by the user and saved, the mode setting becomes active on all storage routers in the cluster.</p>

Configuring for VLAN without VTP

Configuring for VLAN without using VTP consists of setting the VTP mode to transparent, assigning a VID, and optionally assigning a name and maximum transmission unit (MTU) size to the VLAN.

Use the following procedure to configure VLAN without using VTP.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	vtp mode transparent	Set the VTP mode for the storage router to <i>transparent</i> . In transparent mode, the SN 5428 does not exchange VTP packets, and VLANs must be manually configured. The default setting is <i>client</i> . Note The VTP mode is a cluster-wide configuration item. When set by the user and saved, the mode setting becomes active on all storage routers in the cluster.
Step 3	vlan 100 or vlan 100 name Engineering mtusize 9000	Assign a VLAN identifier (VID) number that uniquely identifies the VLAN. The VID can be any integer from 1 to 4095. Optionally, a VLAN can be assigned a unique name (<i>Engineering</i>) up to 32 characters in length. If a name is not specified, a default name is automatically assigned. The default name has <i>VLAN</i> as the prefix followed by the VID, left padded to four bytes (for example, <i>VLAN0100</i>). Optionally, an MTU size can be specified using a value from 1500 to 9000. The default value is 1500. Note VLANs are a cluster-wide configuration item. When set by the user and saved, the VLAN information is propagated to all storage routers in the cluster.

Configuring an IP Route

Configuring an IP route to access the VLAN consists of specifying a static route that uses a gateway attached to the desired VLAN. Use the following procedure to configure an IP route.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	ip route 10.2.90.285/32 10.2.10.233 interface ge2 vlan 100	Specify the IP address and subnet mask (<i>10.2.90.285/32</i>) of the destination. Set the subnet mask to <i>255.255.255.255</i> . In this example, the subnet mask was set using CIDR style (<i>/32</i>). In addition, specify the gateway IP address (<i>10.2.10.233</i>), the interface name (<i>ge2</i>), and the VID (<i>100</i>). Note To find the desired VID number, use the show vlan command. VIDs are listed in the VLAN column.

Verifying and Saving Configuration

Verify VTP and VLAN operational and configuration information using the procedures that follow. You can save the configuration at any time by using the **save all bootconfig** command. You must save the running configuration to the bootable configuration for it to be retained in the storage router when it is rebooted. Once you have saved the configuration, you can verify that the configuration to be used when the storage router is rebooted matches the currently running configuration.

Use the following procedure to verify VTP operational information.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	show vtp	Display VTP operational information (Example 4-1).

Example 4-1 Verifying VTP Operational Information

```
→ [SN5428]# show vtp
Configuration Revision   : 8
Number of existing VLANs : 4
VTP Operating Mode      : Client
VTP Domain Name         : opus
```

Use the following procedure to verify VTP configured settings.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	show vtp config	Display VTP configured settings (Example 4-2).

Example 4-2 Verifying VTP Configured Settings

```
→ [SN5428]# show vtp config
vtp mode client
vtp domain opus
```

Use the following procedure to verify current operational information for all VLANs either learned from the network using VTP in client mode or configured locally while in transparent mode.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	show vlan	Display current VLAN operational information (Example 4-3).

Example 4-3 Verifying VLAN Operational Information

```

→ [SN5428]# show vlan
VLAN Name                Status    Ports
-----
100 Engineering            active    ge2
200 Manufacturing         active    ge2

VLAN Type  MTU  Interfaces
-----
100  enet  1500  ge2VLAN100
200  enet  1500  ge2VLAN200

```

Use the following procedure to verify configured VLAN information.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	show vlan config	Display VLAN configuration information (Example 4-4).

Example 4-4 Verifying VLAN Configuration Information

```

→ [SN5428]# show vlan config
vlan 100 name Engineering mtu 1500
vlan 200 name Manufacturing mtu 1500

```

Assigning a VLAN to a SCSI Routing Instance

Assigning a VLAN to a SCSI routing instance is achieved with the `scsirouter serverif vlan` command. This procedure is provided in the “Configuring a Server Interface” section of Chapter 6, “Configuring SCSI Routing.” We recommend that you follow the configuration tasks to configure SCSI routing in the order given in that chapter at the time you are ready to configure SCSI routing.



Configuring for FC Fabric Zoning

This chapter explains how to configure your SN 5428 Storage Router for FC fabric zoning participation and contains the following sections:

- Prerequisite Tasks, page 5-1
- Configuration Tasks, page 5-1
- Configure Domain ID, page 5-2
- Resetting E_Port, page 5-2
- Verifying Configuration, page 5-3

You can configure for zoning using CLI commands, as described in this chapter, or via the web-based GUI. To access the web-based GUI, point your browser to the storage router's management interface IP address. After logging on, click the Help link to access online help for the GUI.

Prerequisite Tasks

Before configuring for zone participation, make sure you have configured all system parameters as described in Chapter 2, “First-Time Configuration,” or Chapter 3, “Configuring System Parameters.”

Configuration Tasks

To configure the SN 5428 for participating in FC zoning, perform the following steps:

-
- Step 1** Set a unique domain ID in the SN 5428.
 - Step 2** Provide fabric administrator with initiator WWPN1 and initiator WWPN2.
 - Step 3** Reset the SN 5428 E_Port.
 - Step 4** Verify configuration.
-



Note

When moving the SN 5428 from one FC zoned fabric to another; after you disconnect from the fabric and prior to connecting to the new fabric, make sure you clear the current zone configuration using the **clear fc zones** command. See Chapter 11, “Command Line Interface Reference,” for details.

Configure Domain ID

Each switch in the FC switched fabric zone has a domain ID, the SN 5428 must be configured with a domain ID that is unique and compatible with the FC switched fabric zone. Use the following procedure to configure the unique domain ID.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	interface fc domainid 79	Assign a unique domain ID. The default setting for the SN 5428 is 1. Note The domain ID must be within the operable range, see your Fibre Channel switched fabric administrator for the value.
Step 3	show debug fc brief	Display FC operational information (Example 5-1). In the display fci1 is initiator WWPN1 and fci2 is initiator WWPN2.

Example 5-1 Display Initiator WWPN1 and Initiator WWPN2

```
[sn5428]# show debug fc brief
Interface WWPN switch port
-----
fc0          200000023d071161
fc15         200f00023d071161

Interface WWPN internal
-----
→fci1        280000023d071160
→fci2        290000023d071160
.
.
.
```

Provide your Fibre Channel switched fabric administrator with both initiator WWPN1 and initiator WWPN2.

Resetting E_Port

To ensure the SN 5428 participates in the switched fabric zoning, you must reset the E_Port after setting the domain ID. Use the following procedure to reset the E_Port.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	no interface fc3 enable	Disable fc3 interface. In this example fc3 is the E_Port that is connected to your Fibre Channel switched zoned fabric.
Step 3	interface fc3 enable	Enable fc3 interface. In this example fc3 is the E_Port that is connected to your Fibre Channel switched zoned fabric.



Note Removing the cable to your E_Port and re-attaching the cable also resets the E_Port.

Verifying Configuration

Verify zone participation is operation using the following procedure.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	show device	Display all attached devices to the SN 5428 (Example 5-2).
Step 3		

Example 5-2 Verifying Zone Participation

```

→ [sn5428]# show device
Fabric Attached Devices detected
Interface lunwwn          wwpn          portId  lun  vendor      product      serial
-----
fc4      20000004cf22eafe 21000004cf22eafe 0x6204cd 0    SEAGATE     ST336605FC  3FP0K3P9000072117S7U
fc4      20000004cf22e9bf 21000004cf22e9bf 0x6204ce 0    SEAGATE     ST336605FC  3FP0KA7V000072117T5L
fc4      20000004cf22ead5 21000004cf22ead5 0x6204d1 0    SEAGATE     ST336605FC  3FP0JXR80000721155P3
fc4      20000004cf22eb84 21000004cf22eb84 0x6204d2 0    SEAGATE     ST336605FC  3FP0KABC000072116JEV
          20000004cf22eafe 22000004cf22eafe 0x6306cd 0    SEAGATE     ST336605FC  3FP0K3P9000072117S7U
          20000004cf22e9bf 22000004cf22e9bf 0x6306ce 0    SEAGATE     ST336605FC  3FP0KA7V000072117T5L
          20000004cf22ead5 22000004cf22ead5 0x6306d1 0    SEAGATE     ST336605FC  3FP0JXR80000721155P3
          20000004cf22eb84 22000004cf22eb84 0x6306d2 0    SEAGATE     ST336605FC  3FP0KABC000072116JEV

```

The show device command will display an interface number for each device directly attached to that FC interface. An interface number is not displayed for devices that are not directly connected to an FC interface (Example 5-2), these devices are connected in the FC fabric.



Configuring SCSI Routing

This chapter explains how to configure your SN 5428 Storage Router for SCSI routing and contains the following sections:

- Prerequisite Tasks, page 6-1
- Configuration Tasks, page 6-2
- Creating a SCSI Routing Instance, page 6-6
- Configuring a Server Interface, page 6-6
- Configuring iSCSI Targets, page 6-7
- Configuring an Access List, page 6-9
- Configuring Access, page 6-11
- Verifying and Saving Configuration, page 6-13
- Default Values For FC Interfaces, page 6-14

SCSI routing can be configured using CLI commands, as described in this chapter, or via the web-based GUI. To access the web-based GUI, point your browser to the storage router's management interface IP address. After logging on, click the Help link to access online help for the GUI.

Prerequisite Tasks

Before configuring SCSI routing, make sure you have configured all system parameters as described in Chapter 2, “First-Time Configuration,” or Chapter 3, “Configuring System Parameters.”

If the VLAN service is to be used with the SN 5428 Storage Router, configure VLANs as described in Chapter 4, “Configuring for VLAN,” before proceeding.

Configuration Tasks

To configure SCSI routing on your SN 5428 Storage Router, perform the following steps:

-
- Step 1** Create a SCSI routing instance. Once an instance is created, you will configure that instance with parameters for a server interface, iSCSI targets, and access by IP hosts.
 - Step 2** Configure the server interface with or without VLAN.
 - Step 3** Configure iSCSI targets.
 - Step 4** (Optional) Configure an access list identifies which IP hosts can access iSCSI targets configured as part of a SCSI routing instance. An access list is necessary if you want to specify access to iSCSI targets on a per-IP host basis. An access list is *not* necessary if you want to specify that all IP hosts have access to the iSCSI targets configured in a SCSI routing instance.
 - Step 5** Configure access. This identifies which IP hosts can access the iSCSI targets configured as part of a SCSI routing instance.
 - Step 6** Verify and save configuration.



Note Although this is shown as the last step, you can verify and save the configuration at any point in the process of performing the configuration tasks. Save your configuration by using the **save all bootconfig** CLI command. This command saves all configuration data to the bootable configuration, which is then used when the storage router is rebooted.



Caution

When making changes to a SCSI routing instance (such as adding or deleting targets or changing access) be sure to make the complementary changes to the iSCSI driver configuration of IP hosts that use that SCSI routing instance to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. (You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.)

Figure 6-1 illustrates SCSI routing configuration elements, and Figure 6-2 illustrates the example configuration used in this chapter. Figure 6-3 illustrates how the configuration of SCSI routing instances determines VLAN access to storage devices.



Note

Configuring the SCSI routing instance does not include configuring the FC interfaces. Once the SCSI routing instance is configured, all the FC interfaces are available. For more information on the FC interfaces default characteristics, see the “Default Values For FC Interfaces” section on page 6-14.

Figure 6-1 Configuration Elements for SCSI Routing

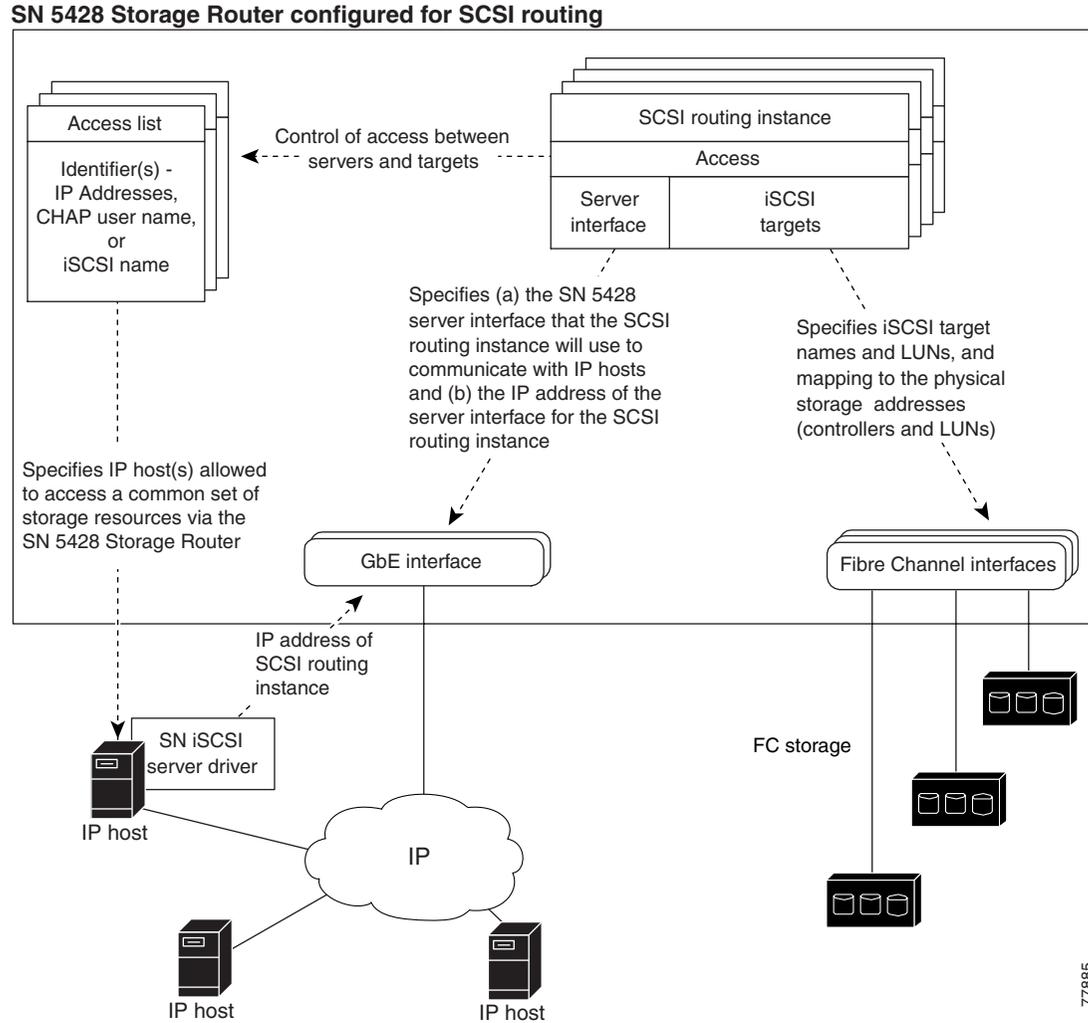
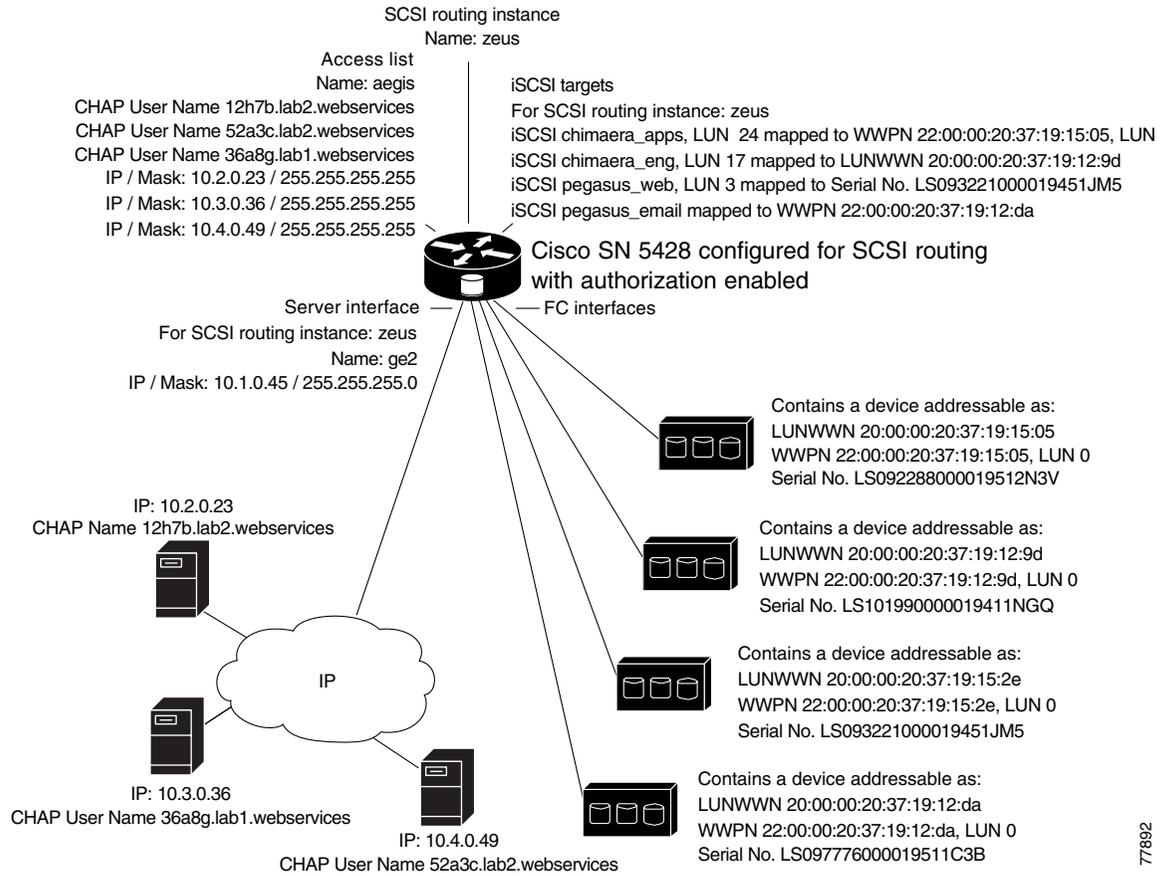


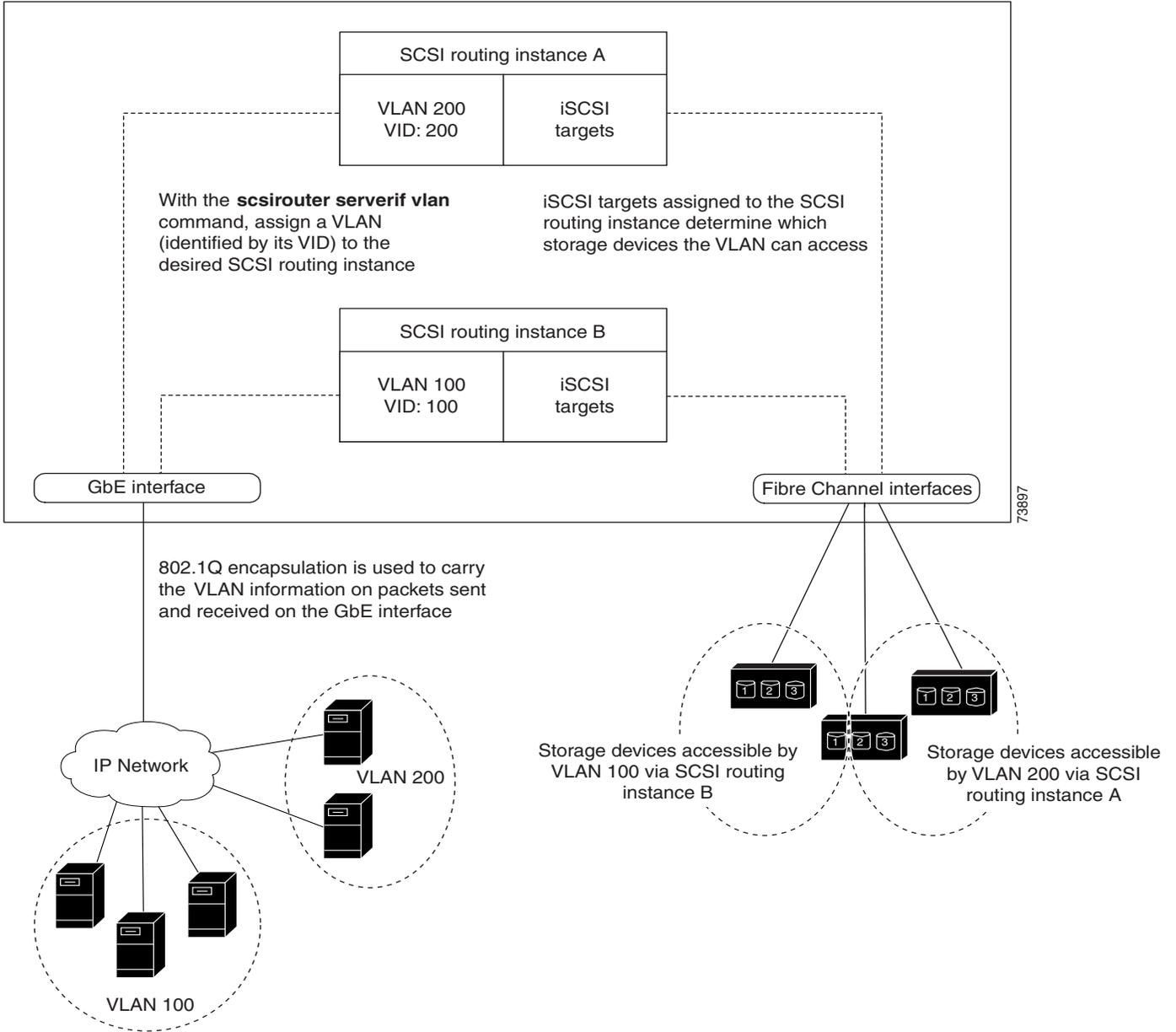
Figure 6-2 SCSI Routing Parameters Example Configuration



77892

Figure 6-3 Configuration of SCSI Routing Instance Determines VLAN Access to Storage Devices

SN 5428 Storage Router configured for SCSI routing



Creating a SCSI Routing Instance

Creating a SCSI routing instance consists of naming the new instance. Use the following procedure to create a SCSI routing instance.

	Command	Description
Step 1	<code>enable</code>	Enter Administrator mode.
Step 2	<code>scsirouter zeus</code>	Create a SCSI routing instance by naming the new instance (<i>zeus</i>). Note You can define up to 12 instances on a single SN 5428 or across a cluster. For additional details about configuring SN 5428 clusters for high availability, see Chapter 9, “Configuring a High Availability Cluster.”

Configuring a Server Interface

Configuring a server interface consists of assigning a server interface along with an IP address and subnet mask to the desired SCSI routing instance. If the SN 5428 is to be used with VLAN, specify the VLAN by its VID.

Without VLAN

Use the following procedure to configure a server interface for a SCSI routing instance.

	Command	Description
Step 1	<code>enable</code>	Enter Administrator mode.
Step 2	<code>scsirouter zeus serverif ge2 10.1.0.45/24</code>	Assign a server interface (<i>ge2</i>) to the desired SCSI routing instance (<i>zeus</i>). Specify the IP address and subnet mask (<i>10.1.0.45/24</i>) that IP hosts will use to access the SCSI routing instance. In this example, the subnet mask of 255.255.255.0 was set using CIDR style (<i>/24</i>).

With VLAN

Use the following procedure to assign a server interface and VLAN to a SCSI routing instance.

	Command	Description
Step 1	<code>enable</code>	Enter Administrator mode.
Step 2	<code>scsirouter zeus serverif ge2 vlan 100 10.1.0.45/24</code>	Assign a VLAN, identified by its VID (<i>100</i>), to the desired SCSI routing instance (<i>zeus</i>). Specify the server interface (<i>ge2</i>) and the IP address and subnet mask (<i>10.1.0.45/24</i>) that the VLAN will use to access the SCSI routing instance. In this example, the subnet mask of 255.255.255.0 was set using CIDR style (<i>/24</i>). Note To look up the VID, use the <code>show vlan</code> command. VIDs are listed in the VLAN column.

Configuring iSCSI Targets

Configuring iSCSI targets consists of specifying the SCSI routing instance to which an iSCSI target is to be assigned, specifying the iSCSI target, and mapping the iSCSI target to a physical storage device. When assigning an iSCSI target, you can specify the physical storage device either by physical storage address, serial number, or by an index number assigned to the device.



Note

When a new iSCSI target is configured, IP hosts do not have access to it. You need to configure access to newly created iSCSI targets according to the “Configuring Access” section later in this chapter.

Use the procedures that follow according to mapping type and storage addressing type:

- Target-and-LUN mapping using WWPN addressing
- Target-and-LUN mapping using LUNWWN addressing
- Target-and-LUN mapping using Serial Number addressing
- Target-only mapping using WWPN addressing

Example 6-1 Indexed List of Storage Devices

```

id interface lunwwn          wwpn          tgtid lun vendor  product
      serial number
1 fc4 20000020371912d5 22000020371912d5 n/a 0 SEAGATE ST318451FC
      LS099969000019511C2H
2 fc4 20000020371912da 22000020371912da n/a 0 SEAGATE ST318451FC
      LS097776000019511C3B
3 fc4 200000203719129d 220000203719129d n/a 0 SEAGATE ST318451FC
      LS101990000019411NGQ
4 fc4 2000002037191505 2200002037191505 n/a 0 SEAGATE ST318451FC
      LS101990000019451JM5
5 fc4 20000020371912b2 22000020371912b2 n/a 0 SEAGATE ST318451FC
      LS099843000019430RC7
6 fc4 200000203719152e 220000203719152e n/a 0 SEAGATE ST318451FC
      LS093221000019451JM5

```

Target-and-LUN mapping using WWPN addressing

Use the following procedure to map iSCSI targets to storage devices by physical storage address.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	scsirouter zeus target chimaera_apps lun 24 wwpn 22:00:00:20:37:19:15:05 lun 0	Specify desired SCSI routing instance (<i>zeus</i>). Specify iSCSI target (<i>chimaera_apps</i>) and LUN (24), and map it to the desired physical address (WWPN 22:00:00:20:37:19:15:05 LUN 0).

Use the following procedure to map iSCSI targets to storage devices by an index number.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	scsirouter zeus target chimaera_apps lun 31 wwpan #?	Specify desired SCSI routing instance (<i>zeus</i>). Specify iSCSI target (<i>chimaera_apps</i>) and LUN (31), and prompt for an indexed list of available storage addresses using the number sign and a question mark (#?).
Step 3	scsirouter zeus target chimaera_apps lun 31 wwpan #4	Choose a physical address designated by an index number (see index number 4 in Example 6-1) to map the iSCSI target (<i>chimaera_apps</i>) and LUN (31) combination to the desired physical address (WWPN 22:00:00:20:37:19:15:05, LUN 0).

Target-and-LUN mapping using LUNWWN addressing

Use the following procedure to map iSCSI targets to storage devices by physical storage address.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	scsirouter zeus target chimaera_eng lun 17 lunwwn 20:00:00:20:37:19:12:9d	Specify desired SCSI routing instance (<i>zeus</i>). Specify iSCSI target (<i>chimaera_eng</i>) and LUN (17), and map it to the desired physical address (LUNWWN 20:00:00:20:37:19:12:9d).

Use the following procedure to map iSCSI targets to storage devices by an index number.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	scsirouter zeus target chimaera_eng lun 17 lunwwn #?	Specify desired SCSI routing instance (<i>zeus</i>). Specify iSCSI target (<i>chimaera_eng</i>) and LUN (17), and prompt for an indexed list of available storage addresses using the number sign and a question mark (#?).
Step 3	scsirouter zeus target chimaera_eng lun 17 lunwwn #3	Choose a physical address designated by an index number (see index number 3 in Example 6-1) to map the iSCSI target (<i>chimaera_eng</i>) and LUN (17) combination to the desired physical address (LUNWWN 20:00:00:20:37:19:12:9d)

Target-and-LUN mapping using Serial Number addressing

Use the following procedure to map iSCSI targets to storage devices by serial number.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	scsirouter zeus target pegasus_web lun 3 serial LS093221000019451JM5	Specify desired SCSI routing instance (<i>zeus</i>). Specify iSCSI target (<i>pegasus_web</i>) and LUN (3), and map it to the desired physical address (serial number LS093221000019451JM5).

Use the following procedure to map iSCSI targets to storage devices by an index number.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	scsirouter zeus target <i>pegasus_web lun 3 serial #?</i>	Specify desired SCSI routing instance (<i>zeus</i>). Specify iSCSI target (<i>pegasus_web</i>) and LUN (3), and prompt for an indexed list of available storage addresses using the number sign and a question mark (#?).
Step 3	scsirouter zeus target pegasus_web lun 3 serial #	Choose a physical address designated by an index number (see index number 6 in Example 6-1) to map the iSCSI target (<i>pegasus_web</i>) and LUN (3) combination to the desired physical address (serial number LS093221000019451JM5)

Target-only mapping using WWPN addressing

Use the following procedure to map iSCSI targets to storage devices by physical storage address.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	scsirouter zeus target <i>pegasus_email wwpn</i> <i>22:00:00:20:37:19:12:da</i>	Specify desired SCSI routing instance (<i>zeus</i>). Specify iSCSI target (<i>pegasus_email</i>), and map it to the desired physical address (WWPN 22:00:00:20:37:19:12:da) and any LUNs available as part of that WWPN.

Use the following procedure to map iSCSI targets to storage devices by index numbers.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	scsirouter zeus target <i>pegasus_email wwpn #?</i>	Specify desired SCSI routing instance (<i>zeus</i>). Specify iSCSI target (<i>pegasus_email</i>), and prompt for an indexed list of available storage addresses using the number sign and a question mark (#?).
Step 3	scsirouter zeus target pegasus_email wwpn #2	Choose a physical address designated by an index number (see index number 2 in Example 6-1) to map the iSCSI target (<i>pegasus_email</i>) to desired physical address (WWPN 22:00:00:20:37:19:12:da).

Configuring an Access List

Configuring an access list consists of creating an access list by naming it and identifying the IP hosts that have permission to access storage devices via iSCSI target names. IP hosts can be identified by:

- IP address
- CHAP user name (used for iSCSI authentication)
- iSCSI Name of the IP host - The iSCSI Name is a UTF-8 character string based on iSCSI functional requirements. It is a location-independent permanent identifier for an iSCSI node, and is generated when a target is initially created.

An access list can contain one or more types of identification entries. If an identification entry type exists in the access list, the IP host attempting to access the associated storage target must have a matching entry defined in the access list. For example, if an access list contains both IP address and iSCSI Name identification entry types, then every IP host that requires access to the associated set of storage resources must have a matching IP address and iSCSI Name entry in the access list.

An access list is necessary if you want to specify access to iSCSI targets on a per-IP host basis. An access list is *not* necessary if you want to specify that all IP hosts have access to the iSCSI targets configured in a SCSI routing instance.

**Note**

If there is a CHAP user name entry in the access list, the SCSI routing instance used to access the storage target must also have iSCSI authentication enabled. See Chapter 8, “Configuring Authentication” for additional information about AAA and iSCSI authentication.

Use the following procedure to create an access list. In this procedure, the access list is called *aegis* and the IP host identifiers include three IP addresses (10.2.0.23, 10.3.0.36, and 10.4.0.49) and a CHAP user name (12h7b.lab2.webservices).

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	accesslist <i>aegis</i>	Create an access list by naming it (<i>aegis</i>). There is a 31 character limit.
Step 3	accesslist <i>aegis</i> description “Access to zeus SCSI routing service”	(Optional) Add a string as a description for the access list. Enclose the string using single or double quotes.
Step 4	accesslist <i>aegis</i> 10.2.0.23/32 10.3.0.36/32 10.4.0.49/32	Add IP addresses of IP hosts to the access list. Separate multiple IP addresses with a space. To limit the access to each IP address, set the subnet mask to 255.255.255.255. In this example, the subnet mask was set using CIDR style (/32).
Step 5	accesslist <i>aegis</i> chap-username 12h7b.lab2.webservices	Add CHAP user names in the access list. To limit the access to each CHAP user name. The password it supplies must be successfully validated using the AAA method configured. Note Authentication must be enabled when using CHAP user names in the access list.

**Note**

In a cluster environment, all access lists must be created and maintained on the first storage router to join the cluster. If you issue the **accesslist** commands from another storage router in the cluster, the CLI displays an informational message with the IP address of the storage router that is currently handling all access list functions. For more information on operating the SN 5428 in a cluster, see Chapter 10, “Maintaining and Managing the SN 5428 Storage Router.”

Configuring Access

Configuring access consists of specifying which iSCSI targets can be accessed by IP hosts. When configuring access, you can specify one iSCSI target at a time or all iSCSI targets. Similarly, you can specify one access list at a time or all IP hosts using a SCSI routing instance. In addition, you can deny access to iSCSI targets one at a time or all at once.

The default for access to newly configured iSCSI targets is *none*. You must configure access according to the information provided in this section.



Note

In a cluster environment, all access lists must be created and maintained on the first storage router to join the cluster. If you issue the **accesslist** commands from another storage router in the cluster, the CLI displays an informational message with the IP address of the storage router that is currently handling all access list functions. For more information on operating the SN 5428 in a cluster, see Chapter 10, “Maintaining and Managing the SN 5428 Storage Router.”

Use the procedures that follow according to the type of access:

- Access an iSCSI target by IP hosts identified in an access list
- Access an iSCSI target by all IP hosts
- Access all iSCSI targets by IP hosts identified in an access list
- Access all iSCSI targets by all IP hosts
- Access denied to one iSCSI target
- Access denied to all iSCSI targets

Access an iSCSI target by IP hosts identified in an access list

Use the following procedure to specify one iSCSI target at a time to be accessible by IP hosts listed in an access list.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	scsirouter zeus target chimaera_email accesslist aegis	Specify that an iSCSI target (<i>chimaera_email</i>), configured as part of a SCSI routing instance (<i>zeus</i>), can be accessed by IP hosts listed in an access list (<i>aegis</i>).

Access an iSCSI target by all IP hosts

Use the following procedure to specify one iSCSI target at a time to be accessible by all IP hosts.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	scsirouter zeus target chimaera_apps accesslist all	Specify that an iSCSI target (<i>chimaera_apps</i>), configured as part of a SCSI routing instance (<i>zeus</i>), can be accessed by all IP hosts.

Access all iSCSI targets by IP hosts identified in an access list

Use the following procedure to specify all iSCSI targets to be accessible by IP hosts listed in an access list.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	scsirouter zeus target all accesslist aegis	Specify that all iSCSI targets that were configured as part of the specified SCSI routing instance (<i>zeus</i>) can be accessed by IP hosts listed in an access list (<i>aegis</i>).

Access all iSCSI targets by all IP hosts

Use the following procedure to specify all iSCSI targets to be accessible by all IP hosts.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	scsirouter zeus target all accesslist all	Specify that all iSCSI targets that were configured as part of the specified SCSI routing instance (<i>zeus</i>) can be accessed by all IP hosts.

Access denied to one iSCSI target

Use the following procedure to deny access by IP hosts to one iSCSI target at a time.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	scsirouter zeus target chimaera_apps accesslist none	Specify that no IP host can access the iSCSI target (<i>chimaera_apps</i>), configured as part of the specified SCSI routing instance (<i>zeus</i>).

Access denied to all iSCSI targets

Use the following procedure to deny access by all IP hosts to all iSCSI targets at once.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	scsirouter zeus target all accesslist none	Specify that no IP hosts can access any iSCSI targets that were configured as part of the specified SCSI routing instance (<i>zeus</i>).

Verifying and Saving Configuration

Verify the access list configuration and the SCSI routing configuration using the procedures that follow. You can save the configuration at any time by using the **save all bootconfig** command. You must save the running configuration to the bootable configuration for it to be retained in the storage router when it is rebooted. Once you have saved the configuration, you can verify that the configuration to be used when the storage router is rebooted matches the currently running configuration.

Use the following procedure to verify access list configuration.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	show accesslist	Display a list of all existing access lists (Example 6-2).
Step 3	show accesslist <i>aegis</i>	Display the IP host identifies in an access list (Example 6-3).

Example 6-2 Verifying Existence of an Access List

```
→ [SN5428]# show accesslist
aegis
hris-mgmt
```

Example 6-3 Verifying IP Addresses in an Access List Named *aegis*

```
→ [SN5428]# show accesslist aegis
accesslist aegis description "Access to zeus SCSI routing service"
accesslist aegis 10.2.0.23/255.255.255.255
accesslist aegis 10.3.0.36/255.255.255.255
accesslist aegis 10.4.0.49/255.255.255.255
accesslist aegis chap-username 12h7b.lab2.webservices
```

Use the following procedure to verify the configuration of a SCSI routing instance.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	show scsirouter zeus	Display the parameters configured for the specified SCSI routing instance (Example 6-4).

Example 6-4 Verifying Configuration for a SCSI Routing Instance

```

→ [SN5428]# show scsirouter zeus
zeus description "(not set)"
zeus authenticate "none"
zeus primary "none"
zeus proxy server disabled
zeus failover primary "none"
zeus failover secondary "none"
zeus target naming authority "none"
zeus target log level is not available
zeus target chimaera_apps description "(not set)"
zeus target chimaera_apps Name "iqn.1987-05.com.cisco.00.d3f8a9a1872650c7deaced967e1812d.chimaera_"
zeus target chimaera_apps enabled "TRUE"
zeus target chimaera_apps accesslist "all"
zeus target chimaera_apps lun 24 wwpn "22:00:00:20:37:19:15:05" lun "0" I/F fc11
zeus target chimaera_eng description "(not set)"
zeus target chimaera_eng enabled "TRUE"
zeus target chimaera_eng accesslist "all"
zeus target chimaera_eng lun 17 lunwn "22:00:00:20:37:19:12:9d" I/F fc11
zeus target pegasus_web description "(not set)"
zeus target pegasus_web Name "iqn.1987-05.com.cisco.00.d6bf2b11ed9c88ce9299ea3f0961ad94.pegasus_web"
zeus target pegasus_web enabled "TRUE"
zeus target pegasus_web accesslist "all"
zeus target pegasus_web lun 3 serial "LS0932210000019451JMS" I/F fc11

```

Default Values For FC Interfaces

The following are the default operational characteristics for the Fibre Channel interfaces 1 through 8:

- Fairness disabled (switch has priority)
- Fabric Address Notification (FAN) enabled
- Automatically negotiated transfer rate (linkspeed auto)
- Multi-Frame sequence bundling enabled
- Automatic selection of port type as:
 - auto - Port type is gl-port
 - e-port - Port type is switch to switch
 - f-port - Port type is Fabric
 - fl-port - Port type is Fabric Loop (public loop)
 - g-port - Port type is Generic either f-port or e-port
 - gl-port - Port type is Generic Loop either fl-port, e-port, or g-port
 - tl-port - Port type is Translated Loop



Configuring Transparent SCSI Routing

This chapter explains the configuration process for a transparent SCSI routing deployment of your SN 5428 Storage Router and provides procedures to verify the configuration. It contains the following sections:

- Prerequisite Tasks, page 7-1
- Summary of Configuration Process, page 7-1
- Verifying Configuration, page 7-2

Transparent SCSI routing is configured with the values entered with the initial system configuration script. To verify the configuration, use the CLI commands as described in this chapter. The web-based GUI is not available for transparent SCSI routing, since this deployment option requires minimal configuration of the SN 5428.

Prerequisite Tasks

Before verifying the transparent SCSI routing configuration, make sure you have configured all system parameters as described in Chapter 2, “First-Time Configuration,” or Chapter 3, “Configuring System Parameters.”

Summary of Configuration Process

The configuration parameters needed for a transparent SCSI routing deployment of the SN 5428 Storage Router are entered with the initial system configuration script. Option number 2 (transparent SCSI routing) must be chosen as the configuration deployment for the SN 5428 for the first question in the script. The other parameter needed for a transparent SCSI routing deployment is the IP address assigned to the Gigabit Ethernet interface.

Although two Gigabit Ethernet ports are available on the SN 5428, only one is used when running in transparent mode. Either port can be selected at startup.

Once all requested values have been entered and the script completes, a single SCSI routing instance named, *transparent*, is automatically created. The SN 5428 then initiates the target discovery process and creates an iSCSI logical target for each Fibre Channel target discovered.

Afterwards, the SN 5428 will discover new targets whenever any of the following occurs:

- A new target or Fibre Channel switch or hub is added to the SN 5428.
- A cable is plugged in causing a loop initialization primitive LIP.
- The SN 5428 is rebooted.

Verifying Configuration

Use the following procedure to verify the configuration of the SCSI routing instance.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	show scsirouter <i>transparent</i>	Display configuration for SCSI routing instance (Example 7-1).
	or show scsirouter all	Note As shown in the second command, you can type the keyword, all , as a shortcut, instead of the SCSI routing instance name, <i>transparent</i> .

Example 7-1 Verifying Configuration of Transparent SCSI Routing Instance

```

→ [SN5428]# show scsirouter transparent
transparent description "(not set)"
transparent authenticate "none"
transparent lun reset no
transparent cdb retry counter 30
transparent target 21000020371912ee description "(not set)"
transparent target 21000020371912ee Name "eui.21000020371912ee"
transparent target 21000020371912ee enabled "TRUE"
transparent target 21000020371912ee accesslist "all"
transparent target 21000020371912ee wwpn "21000020371912ee"
transparent target 21000020371912a2 description "(not set)"
transparent target 21000020371912a2 Name "eui.21000020371912a2"
transparent target 21000020371912a2 enabled "TRUE"
transparent target 21000020371912a2 accesslist "all"
transparent target 21000020371912a2 wwpn "21000020371912a2"
transparent target 21000020371912a3 description "(not set)"
transparent target 21000020371912a3 Name "eui.21000020371912a3"
transparent target 21000020371912a3 enabled "TRUE"
transparent target 21000020371912a3 accesslist "all"
transparent target 21000020371912a3 wwpn "21000020371912a3"
transparent target 21000020371912d1 description "(not set)"
transparent target 21000020371912d1 Name "eui.21000020371912d1"
transparent target 21000020371912d1 enabled "TRUE"
transparent target 21000020371912d1 accesslist "all"
transparent target 21000020371912d1 wwpn "21000020371912d1"
transparent target 2100002037c59e27 description "(not set)"
transparent target 2100002037c59e27 Name "eui.2100002037c59e27"
transparent target 2100002037c59e27 enabled "TRUE"
transparent target 2100002037c59e27 accesslist "all"
transparent target 2100002037c59e27 wwpn "2100002037c59e27"

```

Use the following procedure to verify logged-in IP hosts and bound Fibre Channel targets.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	show interface fci1 iscsilogins	Display logged-in IP hosts and bound Fibre Channel targets on port fci1 (Example 7-2).
Step 3	show interface fci2 iscsilogins	Display logged-in IP hosts and bound Fibre Channel targets on port fci2 (Example 7-3).

Example 7-2 Verifying Logged-in IP Hosts and Bound Fibre Channel Targets on fci1

```

→ [SN5428]# show interface fci1 iscsilogins
Initiator      Target
  ALPA  portID  State      WWPN          IP Host
                IP address  IP Host Name
0    ef    e0      6      2100005028b64d1a  10.1.10.244  iqn.1987-05.com.cisco.00.sn5428
                dc      6      2100005028b6431c
                b6      6      2100005028b64d0a
1    e8    e0      6      2100005028b64d1a  10.0.5.159   iqn.1987-05.com.cisco.02.9FD38900B2FAC8E036D3D3.NT10
                dc      6      2100005028b6431c
                b6      6      2100005028b64d0a
2    e4    e0      6      2100005028b64d1a  10.0.5.226   iqn.1987-05.com.cisco.02.B826B52E725BAFA5CAB913.NT9
                dc      6      2100005028b6431c
                b6      6      2100005028b64d0a
3    e2    e0      6      2100005028b64d1a  10.0.5.112   iqn.1987-05.com.cisco.02.16E9C60D686BC79113C401.WIN1
                dc      6      2100005028b6431c
                b6      6      2100005028b64d0a

```

Example 7-3 Verifying Logged-in IP Hosts and Bound Fibre Channel Targets on fci2

```

→ [SN5428]# show interface fci2 iscsilogins
Initiator      Target
  ALPA  portID  State      WWPN          IP Host
                IP address  IP Host Name
0    ef    203e1    6      2200002037a7c100  10.0.5.208   iqn.1987-05.com.cisco.00.sn5428
                203ef     6      2200002037a7c3f9
1    e8    29010023d0712c0  10.0.5.10   iscsi.cisco.snow110
                20101    6      210000d0b20036a0
                202e4    6      21000080e5118ab2
2    e4    290200023d0712b0  10.0.5.12   iscsi.cisco.snow112
                20101    6      210000d0b20036c0
                203d9    6      2200002037a7a0c5
                203da    6      2200002037b99fzf
3    e2    290300023d0712c0  10.0.5.15   iscsi.cisco.snow115
                20101    6      210000d0b20036d0
                202e4    6      21000080e5118ag2
4    e1    290400023d0712g0  10.0.5.17   iscsi.cisco.snow117
                20101    6      210000d0b20036g0
5    e0    290500023d0712n0  10.0.5.18   iscsi.cisco.snow118
                20101    6      210000d0b20036v0
6    dc    290600023d0712e0  10.0.5.27   iscsi.cisco.snow127
                20101    6      210000d0b20036a0
7    da    290700023d0712c0  10.0.5.28   iscsi.cisco.snow128
                20101    6      210000d0b20036d0

```

The following explains the Initiator and State fields:

Initiator	<p>Initiator 0 is reserved for the primary initiator port. This port performs the discovery of the target devices—the same devices that appear in the show devices command. This port is not available to IP hosts. The port's IP address is the one assigned to the SN 5428 management interface, and its IP host name is the system name of the SN 5428 with "iqn.1987-05.com.cisco.00." preceding it.</p> <p>Initiators 1 to 62 (1 to 31 on each port) are used for IP hosts that are logged in. For instance in Example 7-2, IP host, NT10, is bound to initiator port 1 with WWPN 200100023d070740.</p>
State	<p>Login state:</p> <ul style="list-style-type: none"> 0 and 1—(<i>not used</i>) 2—PLOGI request has queued to request queue 3—PLOGI response has been received 4—PLOGI response received and PRLI request queued to request queue 5—PRLI response received 6—PRLI ACC received (login successful) 7—Initial port state (not logged in) 8—LOGO is queued to request queue 9—LOGO has been transmitted

Use the following procedure to verify discovered targets.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	show devices	Display discovered targets (Fibre Channel devices). (Example 7-4.)

Example 7-4 Verifying Discovered Targets

```

→ [sn5428]# show device
Fabric Attached Devices detected
Interface lunwwn          wwpn          portId  lun  vendor      product      serial
-----
fc4      20000004cf22eafe 21000004cf22eafe 0x6204cd 0    SEAGATE     ST336605FC   3FP0K3P9000072117S7U
fc4      20000004cf22e9bf 21000004cf22e9bf 0x6204ce 0    SEAGATE     ST336605FC   3FP0KA7V000072117T5L
fc4      20000004cf22ead5 21000004cf22ead5 0x6204d1 0    SEAGATE     ST336605FC   3FP0JXR80000721155P3
fc4      20000004cf22eb84 21000004cf22eb84 0x6204d2 0    SEAGATE     ST336605FC   3FP0KABC000072116JEU

```



Configuring Authentication

This chapter explains how to configure the authentication portion of Cisco's authentication, authorization and accounting (AAA) methods on the SN 5428 Storage Router and how to enable iSCSI authentication, which uses the AAA authentication methods.

The following tasks are covered:

- Prerequisite Tasks, page 8-1
- Using iSCSI Authentication, page 8-2
- Configuration Tasks, page 8-2
- Configuring Security Services, page 8-5
- Building the AAA Authentication List, page 8-7
- Testing iSCSI Authentication, page 8-8
- Enabling iSCSI Authentication, page 8-8
- Verifying and Saving Configuration, page 8-9

The AAA authentication function is always enabled for the SN 5428; it cannot be disabled.

Authentication parameters can be configured using CLI commands, as described in this chapter, or via the web-based GUI. To access the web-based GUI, point your browser to the SN 5428's management interface IP address. After logging on, click the Help link to access online help for the GUI.



Note

The web-based GUI is not available for storage routers deployed for transparent SCSI routing.

Prerequisite Tasks

Before performing AAA and iSCSI authentication configuration tasks on the SN 5428, make sure you have configured system parameters as described in Chapter 2, "First-Time Configuration," or Chapter 3, "Configuring System Parameters." If the SN 5428 is deployed for SCSI routing, you should also configure SCSI routing instances as described in Chapter 6, "Configuring SCSI Routing," before proceeding. See the iSCSI driver readme file for details on configuring IP hosts for iSCSI authentication.



Note

AAA and iSCSI authentication configuration settings are system-wide parameters and are not shared across a cluster. However, you may prefer to configure all SN 5428s in a cluster with the same authentication settings.

Using iSCSI Authentication

iSCSI authentication provides a mechanism to authenticate all IP hosts that request access to storage via a SCSI routing instance. When enabled, iSCSI drivers provide user name and password information each time an iSCSI TCP connection is established. iSCSI authentication uses the iSCSI CHAP (Challenge Handshake Authentication Protocol) authentication method. Authentication services are provided by the AAA subsystem configured for each SN 5428.

Authentication, authorization and accounting (AAA) is Cisco's architectural framework for configuring a set of three independent security functions in a consistent, modular manner. The SN 5428 Storage Router implements the authentication function.

Authentication provides a method of identifying users (including login and password dialog, challenge and response, and messaging support) prior to receiving access to the requested object, function, or network service. AAA authentication is configured by defining a list of authentication services. iSCSI authentication, which uses the AAA authentication services list, can be enabled for specific SCSI routing instances.

AAA Security Services

iSCSI authentication uses AAA security services to administer its security functions. If you are using remote security servers, AAA is the means through which you establish communications between the SN 5428 and the remote RADIUS or TACACS+ security server.

This chapter describes how to configure the following AAA security services:

- **RADIUS**—A distributed client/server system implemented through AAA that secures networks against unauthorized access. In this implementation, the SN 5428 sends authentication requests to a central RADIUS server that contains all user authentication and network service access information.
- **TACACS+**—A security application implemented through AAA that provides centralized validation of users attempting to gain access to storage targets through specified SCSI routing instances. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. TACACS+ provides for separate and modular authentication, authorization, and accounting facilities.
- **Local or local-case**—Uses a local username database on the SN 5428 for authentication. Local-case indicates that the user name authentication is case-sensitive. Passwords authentication is always case-sensitive.

Configuration Tasks

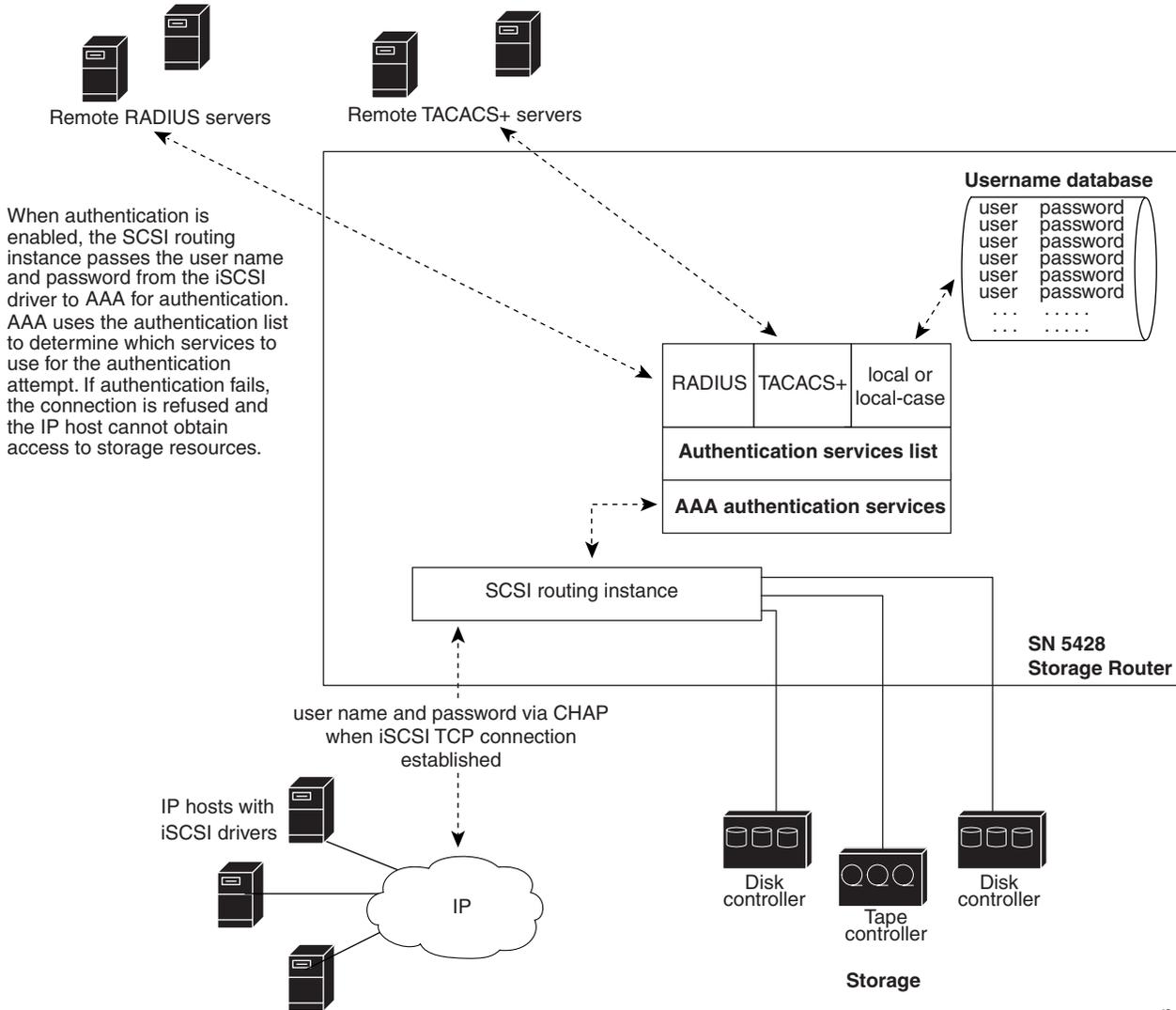
To configure iSCSI authentication and the associated AAA authentication services on the SN 5428, perform the following steps:

-
- Step 1** Configure the desired security services, such as RADIUS, TACACS+, or the local username database.
 - Step 2** Build the AAA authentication list.
 - Step 3** Test the iSCSI authentication services.
 - Step 4** Enable iSCSI authentication for individual SCSI routing instances.

Step 5 Verify and save AAA and iSCSI authentication configuration.

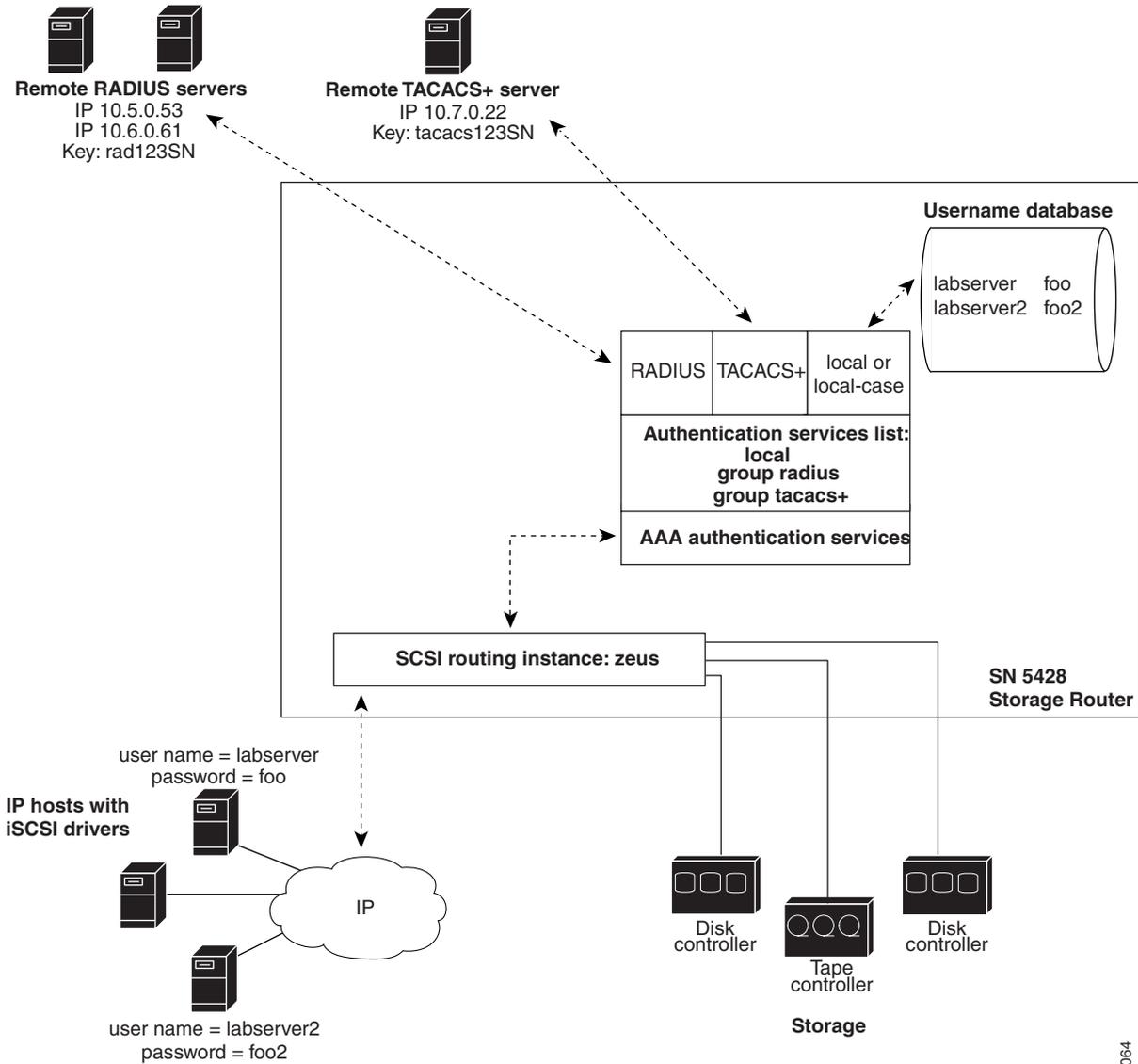
Figure 8-1 illustrates AAA authentication configuration elements and Figure 8-2 illustrates the example configuration of iSCSI authentication and AAA authentication services used in this chapter.

Figure 8-1 iSCSI Authentication Configuration Elements



77063

Figure 8-2 iSCSI Authentication Example Configuration



77064

Configuring Security Services

Configuring security services consists of setting the appropriate parameters for the various service options that can be used by the SN 5428. The SN 5428 can use any or all of the supported security services.

Use the procedures that follow to configure the SN 5428 to use the appropriate security services:

- RADIUS
- TACACS+
- Local username database



Note

See the iSCSI driver readme file for details on configuring user names and passwords for iSCSI authentication.

RADIUS Servers

Use the commands in the following procedure to configure RADIUS security services.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	radius-server host <i>10.5.0.53</i>	Specify the RADIUS server to be used for AAA authentication services. For example, specify the RADIUS server at <i>10.5.0.53</i> for use by the SN 5428. Because no port is specified, the authentication requests use the default UDP port 1645. Global timeout and retransmit values are also used. See the radius-server host command in Chapter 11, “Command Line Interface Reference,” for additional details.
Step 3	radius-server host <i>10.6.0.61</i>	Specify a secondary RADIUS server. RADIUS servers are accessed in the order in which they are defined. For example, specify the RADIUS server at <i>10.6.0.61</i> as the second RADIUS server to be used for AAA authentication services.
Step 4	radius-server key <i>rad123SN</i>	Configure the global authentication and encryption key to be used for all RADIUS communications between the SN 5428 and the RADIUS daemon. For example, set the key to <i>rad123SN</i> . This key must match the key used on the RADIUS daemon.

TACACS+ Hosts

Use the commands in the following procedure to configure TACACS+ security services.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	tacacs-server host <i>10.7.0.22</i>	Specify the TACACS+ server to be used for AAA authentication services. For example, specify the TACACS+ server at <i>10.7.0.22</i> for use by the SN 5428. Because no port is specified, the authentication requests use the default port 49. The global timeout value is also used. See the tacacs-server host command in Chapter 11, “Command Line Interface Reference,” for additional details.
Step 3	tacacs-server key <i>tacacs123SN</i>	Configure the global authentication and encryption key to be used for all TACACS+ communications between the SN 5428 and the TACACS+ server. For example, set the key to <i>tacacs123SN</i> . This key must match the key used by the TACACS+ daemon.

Local Username Database

Use the commands in the following procedure to configure a local username database.

**Note**

Passwords are entered in clear text, but are changed to “XXXXX” in the CLI command history cache, and are stored in the local username database in encrypted format.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	username <i>labserver</i> password <i>foo</i> username <i>labserver2</i> password <i>foo2</i>	Enter a user name and password for each device requiring authentication prior to access to storage. For example, add the following user name and password combinations: <ul style="list-style-type: none"> • <i>labserver</i> and <i>foo</i> • <i>labserver2</i> and <i>foo2</i> <p>User name and password pairs must match the user name and password pairs configured for the iSCSI drivers that require access to storage via the SCSI routing instances that have iSCSI authentication enabled. If other authentication services are also used (such as RADIUS or TACACS+), these user name and password pairs must also be configured within the databases those services use for authentication purposes.</p>

The following rules apply to passwords:

- Passwords are entered in clear text. However, they are stored in an encrypted format.
- If the password contains embedded spaces, enclose it with single or double quotes.

- After initial entry, passwords display in their encrypted format. Use the **show aaa** command to display the local username database entries. The following is an example display:

```
username "foo" password "9 ea9bb0c57ca4806d3555f3f78a4204177a"
```

The initial “9” in the example display indicates that the password is encrypted.

- You can re-enter an encrypted password using the normal **username password** command. Enter the encrypted password in single or double quotes, starting with 9 and a single space. For example, copying and pasting `password "9 ea9bb0c57ca4806d3555f3f78a4204177a"` from the example above into the **username pat** command would create an entry for `pat` in the username database. The user named `pat` would have the same password as the user named `foo`. This functionality allows user names and passwords to be restored from saved configuration files.
- When entering a password, a zero followed by a single space indicates that the following string is not encrypted; 9 followed by a single space indicates that the following string is encrypted. To enter a password that starts with 9 or zero, followed by one or more spaces, enter a zero and a space and then enter the password string. For example, to enter the password “0 123” for the user named `pat`, enter this command:

```
username pat password "0 0 123"
```

To enter the password “9 73Zjm 5” for user name `lab1`, use this command:

```
username lab1 password '0 9 73Zjm 5'
```

Building the AAA Authentication List

iSCSI authentication uses a list of defined AAA authentication services to administer its security functions. The list that is created must be named *default*.

Use the commands in the following procedure to build a list of AAA authentication services to be used for iSCSI authentication.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	aaa authentication iscsi default local group radius group tacacs+	Create a list (named <i>default</i>) of authentication services. For example, build a list so that AAA first tries to perform authentication using the local username database. If AAA fails to find a user name match, an attempt is made to contact a RADIUS server. If no RADIUS server is found, RADIUS returns an error and AAA tries to use a TACACS+ server. If no TACACS+ server is found, TACACS+ returns an error and AAA authentication fails. If a RADIUS or TACACS+ server does not find a user name and password match, authentication fails and no other methods are attempted.



Note

If local or local-case is the first service in the authentication list and a user name match is not found, the next service in the list will be tried. If local or local-case is not the first service, authentication fails if a user name match is not found. Authentication always fails if a RADIUS or TACACS+ server fails to find a user name match.

Testing iSCSI Authentication

Before enabling iSCSI authentication for a SCSI routing instance, you can test iSCSI authentication from the SN 5428. The user name and password are passed to AAA authentication, which performs authentication using the iSCSI default authentication list. The command response indicates a pass or fail status.

Use the commands in the following procedure to test iSCSI authentication.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	aaa test authentication iscsi default labserver foo aaa test authentication iscsi default labserver2 foo2	Test the user names and passwords listed in the username database. AAA authentication uses the services in the default list for authentication (Example 8-1).

Example 8-1 Testing Authentication

```

→ *[SN5428-MG1]# aaa test authentication iscsi default labserver foo
Sep 02 14:37:00:aaa:AS_NOTICE :Auth test request being queued

Sep 02 14:37:00:aaa:AS_NOTICE :Auth test request complete, status = pass

```

Enabling iSCSI Authentication

iSCSI authentication is enabled for specific SCSI routing instances. By default, iSCSI authentication is not enabled.

Use the commands in the following procedure to enable iSCSI authentication using the AAA authentication methods configured in the default AAA authentication list.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	scsirouter zeus authenticate yes	Enable authentication for the named SCSI routing instance. For example, enable authentication for the SCSI routing instances named <i>zeus</i> .

Verifying and Saving Configuration

You can save the configuration at any time using either the **save aaa bootconfig** or **save all bootconfig** commands. You must save the authentication configuration for it to be retained in the SN 5428 when it is rebooted.

Use the following procedure to verify and save authentication settings.

	Command	Description
Step 1	enable	Enter Administrator mode.
Step 2	show aaa	Display AAA authentication configuration (Example 8-2).
Step 3	show scsirouter zeus	Verify that iSCSI authentication is enabled for SCSI routing instances <i>zeus</i> (Example 8-3).
Step 4	save aaa bootconfig	Save authentication settings.
Step 5	save scsirouter zeus bootconfig	Save the SCSI routing instances.
Step 6	save all bootconfig	(Optional) Save all configuration settings. This command may be used in place of individual save aaa bootconfig and save scsirouter bootconfig commands described in Steps 4 and 5.

Example 8-2 Display AAA Authentication Configuration

```

→ [SN5428-MG1]# show aaa
aaa new-model
aaa authentication iscsi default local group radius group tacacs+
username "LabServer" password "9 3b7e1560943b2c3df73ae16dd8c21406ad"
username "LabServer2" password "9 5a034dba7085f7628852db4637787b3f9e"
radius-server key "9 4f5e3deda858731566fa8c7fa23d8a5b4d"
radius-server timeout 100
radius-server retransmit 3
radius-server host 10.5.0.53 auth-port 1645
radius-server host 10.6.0.61 auth-port 1645
tacacs-server key "9 10d2a453d607e75f36ca96dfc5d36b4495"
tacacs-server host 10.7.0.22 auth-port 49

```

Example 8-3 Verify iSCSI Authentication for SCSI Routing Instance

```

[SN5428-MG1]# show scsirouter zeus
zeus description "(not set)"
→ zeus authentication "yes"
zeus proxy server disabled
zeus failover primary "none"
zeus failover secondary "none"
zeus lun reset no
zeus cdb retry counter 30
zeus serverif ge2 10.1.0.45/24
zeus target chimaera_apps description "(not set)"
zeus target chimaera_apps WWUI
"iqn.1987-05.com.cisco.00.0b1aaa415a4146aa2d899c47070c3c06.chimaera_apps"
zeus target chimaera_apps enabled "TRUE"
zeus target chimaera_apps accesslist "none"
zeus target chimaera_apps lun 24 wwpn "22:00:00:20:37:19:15:05" lun "0"
zeus target chimaera_eng description "(not set)"
zeus target chimaera_eng WWUI
"iqn.1987-05.com.cisco.00.0b1aaa415a4146ab2d799c45070c3d06.chimaera_eng"
zeus target chimaera_eng enabled "TRUE"
zeus target chimaera_eng accesslist "aegis"
zeus target chimaera_eng lun 17 wwnn "22:00:00:20:37:19:12:9d"
zeus target pegasus_email description "(not set)"
zeus target pegasus_email WWUI
"iqn.1987-05.com.cisco.00.0b1aca415a6146ea2d809c44070c2c06.pegasus_email"
zeus target pegasus_email enabled "TRUE"
zeus target pegasus_email accesslist "all"
zeus target pegasus_email wwpn "22:00:00:20:37:19:12:da"

```



Configuring a High Availability Cluster

This chapter explains how to configure SN 5428 Storage Routers in a cluster to allow the SN 5428s to back each other up in case of failure. The following tasks are covered:

- Prerequisite Tasks, page 9-1
- Adding the SN 5428 to a Cluster, page 9-2
- Changing Clusters, page 9-5

High availability clusters can be configured using CLI commands, as described in this chapter, or via the web-based GUI. To access the web-based GUI, point your browser to the SN 5428's management interface IP address. After logging on, click the Help link to access online help for the GUI.



Note

SN 5428 Storage Routers that are deployed for transparent SCSI routing cannot participate in a high availability cluster.

Prerequisite Tasks

Before performing any high availability cluster configuration tasks, make sure you have configured system parameters, including the HA interface, as described in Chapter 2, “First-Time Configuration,” or Chapter 3, “Configuring System Parameters.”

When you configure SCSI routing instances to run in a high availability cluster, follow these guidelines:

- If you map targets using WWPN, be sure to specify both the primary WWPN (the WWPN associated with the storage resource as known to the primary SN 5428 in the cluster) and the secondary WWPN (the WWPN associated with the storage resource as known to the second SN 5428 in the cluster).
- Automatic failover of a SCSI routing instance occurs if the Gigabit Ethernet interface is unavailable or if all mapped targets are unavailable. If some targets are available and others are not, the SCSI routing instance will not automatically fail over. All SCSI routing instances will failover if the SN 5428 running the instances fails to exchange heartbeats within the high availability cluster.

To maximize the potential for automatic failover in case of target unavailability, map the targets associated with a single SCSI routing instance to storage that is available through one Fibre Channel interface. Do not map the targets associated with a single SCSI routing instance to storage that is available through multiple FC interfaces.

This type of mapping minimizes the potential for a mixed target availability condition, which prevents IP hosts from accessing some storage but does not cause an automatic failover of the SCSI routing instance.

Adding the SN 5428 to a Cluster

In most situations, you will completely configure a principal SN 5428 Storage Router (including all cluster-wide settings), and then add a new, unconfigured SN 5428 or a minimally configured SN 5428 to the cluster. A high availability cluster is composed of two SN 5428 Storage Routers.

The following SN 5428 configuration settings are shared cluster-wide, and when configured on the first SN 5428 in the cluster, will be shared with the other SN 5428 that joins the cluster.

- Access lists
- Cluster name
- SCSI routing instances
- VLAN information (VID, VTP mode, domain name, etc.)

**Note**

A minimally configured SN 5428 is one in which the management IP address, system name, and optional network management interfaces have been configured. Other system information, such as HA IP address, administrator and monitor passwords, may also have been configured. A minimally configured SN 5428, however, must not have had any cluster-wide settings configured.

Adding an Unconfigured SN 5428 Storage Router

To add a new, unconfigured SN 5428 to an existing cluster, perform the following steps:

Step 1 Respond to the prompts from the SN 5428 initial system configuration script. This script configures the following settings:

- Management IP address
- System name
- HA configuration mode
- Cluster name
- HA IP address

When prompted to select HA configuration mode, choose *clustered*. When prompted for cluster name, enter the name of the existing cluster. At the end of the initial system configuration script, the SN 5428 automatically reboots.

Step 2 When the SN 5428 restarts, it communicates with the other member of the cluster to obtain current cluster configuration information. Once the SN 5428 is completely restarted, verify the new cluster configuration. Issue the **show cluster** command to verify the cluster name and confirm that the SN 5428 is exchanging heartbeats with the other member of the cluster.

- Step 3** To verify that both SN 5428 Storage Routers in the cluster include the same configuration, issue the following commands from the principal SN 5428 in the cluster:
- **show accesslist all from bootconfig**
 - **show scsirouter all from bootconfig**
 - **show vlan**
 - **show vtp**
- Issue the same commands from the SN 5428 just added to the cluster. The displays should be the same.
- Step 4** Use the **setup** configuration wizard, CLI commands, or the GUI to complete SN 5428 configuration. See Chapter 2, “First-Time Configuration,” or Chapter 3, “Configuring System Parameters,” for complete details.
- Step 5** (Optional) Save any changes made to the configuration by issuing the appropriate **save** command with the **bootconfig** keyword, which updates the bootable configuration for the SN 5428 and notifies all SN 5428s in the cluster of the configuration changes.
- Step 6** (Optional) To divide the workload between the SN 5428s in the cluster, you can manually failover selected SCSI routing instances using the **failover scsirouter** command. For additional information about failing over SCSI routing instances, see the section “Controlling SCSI Routing Instances in a Cluster” in Chapter 10, “Maintaining and Managing the SN 5428 Storage Router.”
-

Adding a Minimally Configured SN 5428 Storage Router

To add a minimally configured SN 5428 to an existing cluster, perform the following steps:

- Step 1** Run the **setup cluster** configuration wizard.
- When prompted to select HA configuration mode, choose **clustered**.
 - When prompted for cluster name, enter the name of the existing cluster.
 - When prompted to retain or delete scsirouter instances, enter **delete**. Deleting means that any existing SCSI routing instances will be deleted from this SN 5428. (Since this is a minimally configured SN 5428, there should be no SCSI routing instances to delete.)
 - Enter **yes** to confirm your changes. The SN 5428 automatically reboots.
- Step 2** When the SN 5428 restarts, it communicates with other member of the cluster to obtain current cluster configuration information. Once the SN 5428 is completely restarted, verify the new cluster configuration. Issue the **show cluster** command to verify the cluster name and confirm that the SN 5428 is exchanging heartbeats with the other member of the cluster.
- Step 3** To verify that both SN 5428 Storage Routers in the cluster include the same configuration, issue the following commands from the principal SN 5428 in the cluster:
- **show accesslist all from bootconfig**
 - **show scsirouter all from bootconfig**
 - **show vlan**
 - **show vtp**

Issue the same commands from the SN 5428 just added to the cluster. The displays should be the same.

- Step 4** Complete additional system configuration of the SN 5428 just added to the cluster, as needed. For example:
- Use the **setup access** configuration wizard to configure passwords for the SN 5428.
 - Use the **setup netmgmt** configuration wizard to configure the SN 5428 for network management via SNMP.
 - Use the **setup time** configuration wizard to configure the SN 5428 date and time, and optional NTP server information.
 - Use the CLI or GUI to configure AAA authentication. See Chapter 8, “Configuring Authentication,” for additional information.
- Step 5** Save any changes to the configuration by issuing the appropriate **save** command with the **bootconfig** keyword, which updates the bootable configuration for the SN 5428 and notifies all SN 5428s in the cluster of the configuration changes.
- Step 6** (Optional) To divide the workload between the SN 5428s in the cluster, you can manually failover selected SCSI routing instances using the **failover scsirouter** command. For additional information about failing over SCSI routing instances, see the section “Controlling SCSI Routing Instances in a Cluster” in Chapter 10, “Maintaining and Managing the SN 5428 Storage Router.”

Adding Completely Configured SN 5428 Storage Routers

In some cases you may prefer to completely configure both SN 5428s (including SCSI routing instances and access lists) as standalone systems before joining them into a cluster.

The following example explains the steps required to create a cluster named *Cluster1*, composed of two SN 5428s named *SN5428Sys1* and *SN5428Sys2*. This example assumes that both SN 5428s are fully configured with SCSI routing instances and access lists. (See Chapter 6, “Configuring SCSI Routing,” for details.) Use the **scsirouter primary** command to assign a preferred SN 5428 to any or all of the SCSI routing instances, if desired.



Note

A cluster supports up to 12 active SCSI routing instances.

To create a cluster from fully configured SN 5428s, perform the following steps:

- Step 1** Use the **setup cluster** configuration wizard to define *SN5428Sys1* as a member of the cluster *Cluster1*. When prompted, enter **retain** to keep the access list and SCSI routing instance information already defined.
- Step 2** Use the **show cluster** command to verify the cluster name after *SN5428Sys1* reboots. Verify that all instances and access lists are still available, using **show scsirouter** and **show accesslist** commands.
- Step 3** (Optional) On *SN5428Sys2*, save any access list information that you want to make available in the cluster to a file, using the **save accesslist** command. For example, to save all access lists to a file named *SN5428Sys2_AccessLists.xml*:
- ```
save accesslist all SN5428Sys2_AccessLists.xml
```
- Step 4** (Optional) Because access lists can only be manipulated from the first SN 5428 in a cluster, the saved configuration file from *SN5428Sys2* must be made available to *SN5428Sys1*. See Chapter 10, “Maintaining and Managing the SN 5428 Storage Router,” for information on managing SN 5428 saved configuration files using either the **copy savedconfig** command or FTP.

- 
- Step 5** Join *SN5428Sys2* to the new cluster named *Cluster1*, using the **setup cluster** configuration wizard. When prompted, enter **retain** to share the existing SCSI routing instances across the cluster.
  - Step 6** Use the **show cluster** command to verify the cluster name after *SN5428Sys2* reboots. Verify that the defined SCSI routing instances were retained, using **show scsirouter** command.
  - Step 7** (Optional) Restore any access lists saved in Step 3 using the **restore accesslist from** command. Access lists can only be manipulated from the first SN 5428 in a cluster, so these commands must be issued from the system *SN5428Sys1*.
  - Step 8** (Optional) Save all configuration information on system *SN5428Sys1* by issuing a **save all bootconfig** command, which updates the bootable configuration of all SN 5428s in the cluster.
  - Step 9** Verify that all SCSI routing instances are active using the **show scsirouter stats** command on both SN 5428s.
- 

## Changing Clusters

In some situations, you may need to move the SN 5428 from one cluster to another cluster. Moving a fully configured SN 5428 from one cluster to another is more complex than simply adding the SN 5428 to a cluster. Advanced planning is required.

To successfully move the SN 5428 from one cluster to another, perform the following steps:

- 
- Step 1** Verify that the SN 5428 to be moved has the same hardware configuration as the other SN 5428s in the cluster you are planning to join. Each SN 5428 in the cluster must have connectivity to the same IP hosts and Fibre Channel storage. All management interfaces for the SN 5428s within a cluster must be on the same IP subnet, and all HA interfaces for the SN 5428s within a cluster must be on the same IP subnet. However, the management interfaces must be on a different IP network than the HA interfaces.
  - Step 2** Decide if you need to retain any SCSI routing instances defined on the SN 5428 joining the cluster. Retaining data means all SCSI routing instances existing on the SN 5428 joining the cluster will be added to those already defined for the cluster. If the existing instances are not retained, they are deleted.
  - Step 3** If you are going to retain data, determine if you have any duplicate SCSI routing instance names. When the SN 5428 is added to the cluster, the data in the cluster will overwrite the existing data. You may prefer to change the configuration in the SN 5428 before it joins the cluster to prevent this situation.
  - Step 4** If you are going to retain data, determine if you need to save existing access list information. Access lists are not retained. Any access lists on the SN 5428 will be discarded when it joins the new cluster. You can save the access list information and then restore it to the cluster. Access list information can be restored before or after the SN 5428 joins the cluster by transferring the saved configuration file to the first SN 5428 in the cluster and performing the restore.
  - Step 5** Use the **setup cluster** configuration wizard to join the new cluster. Respond to the prompts to retain or delete configuration as required. The SN 5428 will automatically reboot at the end of the configuration wizard.
  - Step 6** Perform any additional configuration that may be needed. You can fail over SCSI routing instances to this new cluster member to balance traffic load between all SN 5428s in the cluster.
  - Step 7** Use the **save all** command with the **bootconfig** keyword to copy and save the SN 5428 configuration, thereby updating the cluster.
-





# Maintaining and Managing the SN 5428 Storage Router

---

This chapter explains how to perform normal maintenance and management tasks associated with the Cisco SN 5428 Storage Router. The following tasks are covered:

- Prerequisite Tasks, page 10-2
- Installing Updated Software, page 10-2
- Backing Up System Configuration, page 10-8
- Restoring from Backups, page 10-9
- Powering Down the SN 5428 Storage Router, page 10-15
- Resetting the System, page 10-15
- Recovering Passwords, page 10-18
- Controlling SCSI Routing Instances in a Cluster, page 10-18
- Managing CDP on the SN 5428 Storage Router, page 10-23
- Using Scripts to Automate Tasks, page 10-24
- Managing the Log File, page 10-26
- Gathering Troubleshooting Information, page 10-27

SN 5428 Storage Router maintenance and management tasks can be performed using CLI commands, as described in this chapter, or via the web-based GUI. To access the web-based GUI, point your browser to the SN 5428's management interface IP address. After logging on, click the Help link to access online help for the GUI.



**Note**

Not all maintenance and management tasks are appropriate for all SN 5428s. For example, tasks related to high availability clusters (such as failover of SCSI routing instances) are not necessary for SN 5428 Storage Routers configured as standalone systems or deployed for transparent SCSI routing.

---

## Prerequisite Tasks

Before performing any SN 5428 maintenance tasks, make sure you have configured system parameters as described in Chapter 2, “First-Time Configuration,” or Chapter 3, “Configuring System Parameters.”



### Note

Certain configuration tasks, such as identifying a location from which to download software, are optional and may not have been performed during initial configuration. You may perform these tasks at any time, via the CLI or the GUI. Where necessary, this chapter will identify the relevant tasks and commands.

## Installing Updated Software

The SN 5428 Storage Router is designed to run on a continual basis without significant maintenance. However, from time to time, you may need to install updated software. The SN 5428 stores software images (along with configuration files, log files, and other information) on a local file system. This file system is stored on an internal, non-volatile Flash disk. The **show software version all** command displays a list of all software versions stored on the SN 5428 and the amount of disk space available for additional software.

Cisco.com provides registered users access to SN 5428 Storage Router software updates. (See the “Obtaining Technical Assistance” section on page xiii for details on using Cisco.com.) You can download updated software directly to the SN 5428 from Cisco.com via standard HTTP, or via HTTP using a proxy server. You can also use a standard browser to download software updates and associated readme files from Cisco.com to a location of your choosing. Using the CLI or the web-based GUI, you can then make software available from this location (known as the “download location”) to the SN 5428 via HTTP, HTTP using a proxy server, or Trivial File Transport Protocol (TFTP).



### Note

Always review the README file before making updated software available to the SN 5428.

If you plan to use the CLI **download software http** or **download software proxy** commands to make the updated software available to the SN 5428, the machine hosting the download location must be running a web server. If you plan to use the CLI **download software tftp** command, the machine must be accessible using the Trivial File Transport Protocol. If the machine is not running a web server or accessible via TFTP, use the SN 5428 web-based GUI to make the updated software available to the SN 5428. (See the online Help for details.)

The download location used for retrieving updated SN 5428 software is set using the **software http url**, **software proxy url**, or the **software tftp** commands. To view the download location currently specified, use the **show software version all** command (Example 10-1). The **show software version all** command identifies the HTTP URL, Proxy URL, and TFTP host name and other information used to identify the download location, the current version of software running on the SN 5428, and the version that will be used at system restart. In the example, all default locations and related user names and passwords are set.



### Note

If you are a registered Cisco.com user, you can download a TFTP server tool for Microsoft Windows 95, Microsoft Windows 98, and Microsoft Windows NT. You can reach the TFTP server tool on Cisco.com at the Software Center under Service & Support: <http://www.cisco.com/cgi-bin/tablebuild.pl/tftp>.

**Example 10-1 Results of “show software version all” Command**

```
[SN5428_A01]# show software version all
Version Boot Hash Sign Crash Size Date

2.3.0.49 OK OK N/A 0 18585600 Mar 21 18:08 CST 2002
2.3.1 OK OK N/A 0 18616320 Mar 22 16:35 CST 2002

 Http Url: http://www.cisco.com
 Http Username: SWAdmin01
 Http Password: *****

 Proxy Address: 10.1.12.32
 Proxy Port: 3122
 Proxy Url: http://www.cisco.com
 Proxy Username: SWAdmin01
 Proxy Password: *****

 Tftp Hostname: 10.1.1.122
 Tftp Directory: sn5428/v2.3/

Disk Space Available: 13357.0 KB
Current Version: 2.3.1
Boot Version: 2.3.1
```

To update SN 5428 software, perform the following steps:

- 
- Step 1** (Optional) Identify the location from which to retrieve the updated SN 5428 software. (This is either Cisco.com or another download location of your choosing, as previously described.)
- Step 2** Make the selected version of software available on the SN 5428 local file system.
- Step 3** (Optional) Set the new version as the version to be booted during the next system restart, and reboot the SN 5428.
- 

## Specifying the Location to Retrieve Updated Software

You must specify the location from which to retrieve updated software. If the current download location is not appropriate, you can reset it. Use the following procedures to specify the desired download location:

- Using HTTP
- Using Proxy Services
- Using TFTP

When you are finished, verify the new settings using the **show software version all** command, then save them using the **save system bootconfig** or **save all bootconfig** command.

**Using HTTP**

Use the following procedure to specify the HTTP download location:

|        | Command                                                                         | Description                                                                                                                                                                                                                                                                                                      |
|--------|---------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                                   | Enter Administrator mode.                                                                                                                                                                                                                                                                                        |
| Step 2 | <b>show software version all</b>                                                | List the software versions currently available for booting, along with the current download locations. Verify that the version of software required is not already available. Verify that the current download location information for HTTP is correct.                                                         |
| Step 3 | <b>software http url</b><br><i>http://10.1.11.32/~software/sn5428</i>           | (Optional) If the current download location is not the one from which you would normally retrieve updated software, reset the current download location. For example, reset your current download location to <i>http://10.1.11.32/~software/sn5428</i> .                                                        |
| Step 4 | <b>software http username</b> <i>webadmin</i><br><b>password</b> <i>webword</i> | (Optional) Use this command to define the user name and password needed to access the selected location. For example, specify user name <i>webadmin</i> and password <i>webword</i> . If no user name and password are required, use the keyword <b>none</b> (for example, <b>software http username none</b> ). |

**Note**

If you are using the default URL, <http://www.cisco.com>, the username and password must be the same as your Cisco.com login ID and password.

**Using Proxy Services**

Use the following procedure to specify a download location via proxy services:

|        | Command                                                                             | Description                                                                                                                                                                                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                                       | Enter Administrator mode.                                                                                                                                                                                                                                                                                                     |
| Step 2 | <b>show software version all</b>                                                    | List the software versions currently available for booting, along with the current download locations. Verify that the version of software required is not already available. Verify that the current download location information for HTTP via proxy server is correct.                                                     |
| Step 3 | <b>software proxy url default</b>                                                   | (Optional) If the current download location is not the one from which you would normally retrieve updated software, reset the current download location. For example, reset your current download location to the default ( <a href="http://www.cisco.com">http://www.cisco.com</a> ).                                        |
| Step 4 | <b>software proxy address</b><br><i>http://10.1.10.126 port 32</i>                  | (Optional) This is the address and port number of the proxy server that will be used to access the URL specified in Step 3 (for example, <i>http://10.1.10.126, port 32</i> ).                                                                                                                                                |
| Step 5 | <b>software proxy username</b> <i>Ciscouser</i><br><b>password</b> <i>Ciscopswd</i> | (Optional) Use this command to define the user name and password needed to access the selected download location. For example, specify user name <i>Ciscouser</i> and password <i>Ciscopswd</i> . If no user name and password are required, use the keyword <b>none</b> (for example, <b>software proxy username none</b> ). |



**Note** If you are using the default URL, <http://www.cisco.com>, the username and password must be the same as your Cisco.com login ID and password.

#### Using TFTP

Use the following procedure to specify the TFTP download location:

|        | Command                                                                       | Description                                                                                                                                                                                                                                                                                                                                                |
|--------|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                                 | Enter Administrator mode.                                                                                                                                                                                                                                                                                                                                  |
| Step 2 | <b>show software version all</b>                                              | List the software versions currently available for booting, along with the current download locations. Verify that the version of software required is not already available. Verify that the current download location information for TFTP is correct.                                                                                                   |
| Step 3 | <b>software tftp hostname <i>TFTPHost1</i><br/>directory <i>/tftpboot</i></b> | If the current host name and base directory location are not the ones from which you would normally retrieve updated software, reset the host and optional base directory. For example, set the host name to <i>TFTPHost1</i> and the base directory to <i>/tftpboot</i> . If a DNS is not defined for the SN 5428, enter the IP address of the TFTP host. |

## Downloading Updated Software

The **download software** command makes a new version of software available to the SN 5428 for boot purposes. You can store two versions of software on the SN 5428. Before attempting to download updated software, verify that only a single version of software exists on the SN 5428.

Use the following procedures to make a new version of software available to the SN 5428 Storage Router:

- Using HTTP
- Using Proxy Services
- Using TFTP

#### Using HTTP

Use the following procedure to make a new version of software available to the SN 5428 Storage Router via HTTP:

|        | Command                                                | Description                                                                                                                                                                                                     |
|--------|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                          | Enter Administrator mode.                                                                                                                                                                                       |
| Step 2 | <b>show software version all</b>                       | Verify that there is only one version of software on the SN 5428. If two versions exist, use the <b>delete software version</b> command to delete the old version of software to make room for the new version. |
| Step 3 | <b>download software http version<br/><i>2.3.1</i></b> | Download a new software version to the SN 5428 (for example, <i>2.3.1</i> ).                                                                                                                                    |

**Timesaver**

There may be times when you need to make special software available to the SN 5428, for example, under the guidance of a Cisco Technical Support professional. If you isolate this software from standard updates by placing it in another location (not the default download location), you could change the default download location, download the software, and then reset the default download location. An easier way, however, is to specify the download location via the URL parameter on the **download software http** command. For example, to download a file named *231.tar* containing version 2.3.1 software from *http://your.website.com/sn5428*, issue this command:  
**download software http url** *http://your.website.com/sn5428/231.tar*.

**Using Proxy Services**

Use the following procedure to make a new version of software available to the SN 5428 Storage Router via proxy services:

|        | Command                                      | Description                                                                                                                                                                                                     |
|--------|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                | Enter Administrator mode.                                                                                                                                                                                       |
| Step 2 | <b>show software version all</b>             | Verify that there is only one version of software on the SN 5428. If two versions exist, use the <b>delete software version</b> command to delete the old version of software to make room for the new version. |
| Step 3 | <b>download software proxy version 2.3.1</b> | Make a new software version available to the SN 5428 (for example, 2.3.1).                                                                                                                                      |

**Timesaver**

There may be times when you need to make special software available to the SN 5428, for example, under the guidance of a Cisco Technical Support professional. If you isolate this software from standard updates by placing it in another location (not the default download location), you could change the default download location, download the software, and then reset the default download location. An easier way, however, is to specify the download location via the URL parameter on the **download software proxy** command. For example, to download a file named *231.tar* containing version 2.3.1 software from *http://your.website.com/sn5428* using the services of a proxy server, issue this command: **download software proxy url** *http://your.website.com/sn5428/231.tar*.

**Using TFTP**

Use the following procedure to make a new version of software available to the SN 5428 Storage Router via TFTP:

|        | Command                                     | Description                                                                                                                                                                                                     |
|--------|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                               | Enter Administrator mode.                                                                                                                                                                                       |
| Step 2 | <b>show software version all</b>            | Verify that there is only one version of software on the SN 5428. If two versions exist, use the <b>delete software version</b> command to delete the old version of software to make room for the new version. |
| Step 3 | <b>download software tftp version 2.3.1</b> | Make a new software version available to the SN 5428 (for example, 2.3.1).                                                                                                                                      |

**Timesaver**

There may be times when you need to make special software available to the SN 5428, for example, under the guidance of a Cisco Technical Support professional. If you isolate this software from standard updates by placing it in another location (not the default download location), you could change the default download location, download the software, and then reset the default download location. An easier way, however, is to specify the download location via the **hostname** and **filename** parameters on the **download software tftp** command. For example, to download a file named *231.tar* containing version 2.3.1 software from *my\_ftpHost* using TFTP, issue this command:  
**download software tftp hostname my\_ftpHost filename 231.tar**. The *231.tar* file must reside in the default base directory defined for the TFTP host.

## Setting Updated Software as Boot Version

Downloading updated software to the SN 5428 does not change the currently running version of the software, nor does it automatically set the new version to be booted at next system restart. You must take specific action to make the new software version bootable.

Setting software as the bootable version consists of verifying the software integrity and performing internal checks to ensure that the SN 5428 can boot the specified version of software.

Use the following procedure to set the new software as the version to be booted.

|        | Command                           | Description                                                                                                                                                                                                        |
|--------|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                     | Enter Administrator mode.                                                                                                                                                                                          |
| Step 2 | <b>software version 2.3.1</b>     | Select the software to be booted when the system next starts (for example, boot 2.3.1 when the system restarts). The system checks the integrity of the specified software version to be sure that it is bootable. |
| Step 3 | <b>show software version boot</b> | Verify that the correct version is shown as the bootable version (identified as <i>Boot Version</i> ).                                                                                                             |
| Step 4 | <b>reboot</b>                     | (Optional) Restart the SN 5428 to run the new software.                                                                                                                                                            |

When you set a new software version as the bootable version, internal checks are made to ensure that the new software can be run.

## Precautions for Cluster Environments

In a cluster environment, the **software version** command may temporarily suspend normal HA communications, while internal checks are made to ensure that the new software can be run. A suspension will cause a failover of any SCSI routing instances active on the SN 5428.

Any instances with the **primary** attribute set to the name of the SN 5428 will resume running on the SN 5428 after it is rebooted. If you are not going to reboot the SN 5428 immediately, use the **failover scsirouter** command to return the desired SCSI routing instances to the SN 5428.

If the SN 5428 is running in a cluster environment, issuing the **reboot** command will attempt failover for all SCSI routing instances to another SN 5428 in the cluster. The iSCSI drivers handle reconnection of users to the appropriate storage resources, minimizing the effects of the reboot sequence on those users.

# Backing Up System Configuration

Backing up the system configuration consists of saving selected SN 5428 configuration information to XML files that can be stored both locally and remotely. Should problems occur, AAA authentication information, SCSI routing instances, access lists, VLANs and other SN 5428 system configuration information can be restored from these files. (See Chapter 11, “Command Line Interface Reference,” for details about what information is saved.)

While you can issue a **save** command at any time during a CLI command session, best practices suggest that you should back up the SN 5428 system configuration to a file on a regular basis.

Configuration files are normally maintained in the *savedconfig* directory on the SN 5428. You can use the **copy** command to copy the configuration file to a server running TFTP, allowing you to integrate the SN 5428 Storage Router backups with other software archives. By accessing the web-based GUI from a remote server, you can create SN 5428 backup files directly on that server. See the GUI online help for details.



## Note

See Chapter 11, “Command Line Interface Reference,” for complete details on using the **save** and **copy** commands.

### Creating Local Backups

Local backups allow you to store the resulting XML configuration file in the *savedconfig* directory on the SN 5428.

Use the following procedure to perform a local backup that saves the configuration of all the current SCSI routing instances to a file named *backup1* in the *savedconfig* directory.

|        | Command                            | Description                                                              |
|--------|------------------------------------|--------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                      | Enter Administrator mode.                                                |
| Step 2 | <b>save scsirouter all backup1</b> | Save all defined SCSI routing instances to a file named <i>backup1</i> . |

### Storing Backups to a Remote TFTP Server

Use the following procedure to create a backup configuration file named *backup1* and to copy that backup file to another file named *back1.xml*, located on the TFTP host, *tftpserver1*, in the default directory, */tftpboot*.

|        | Command                                                   | Description                                                                                                                                                                                                                                                                                                                                                         |
|--------|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                             | Enter Administrator mode.                                                                                                                                                                                                                                                                                                                                           |
| Step 2 | <b>save all backup1</b>                                   | Save the current running configuration to a file called <i>backup1</i> in the <i>savedconfig</i> directory.                                                                                                                                                                                                                                                         |
| Step 3 | <b>copy savedconfig:backup1 tftp://tserver1/back1.xml</b> | Copy the saved configuration file, <i>backup1</i> , to a file called <i>back1.xml</i> , located on the TFTP server, <i>tserver1</i> , in the default directory.<br><br><b>Note</b> The <i>back1.xml</i> file must already exist in the default directory with the appropriate permissions that allow it to be overwritten. You cannot create a new file using TFTP. |

## Restoring from Backups

AAA authentication information, SCSI routing instances, access lists, VLANs, and selected system configuration data can be restored from previously saved configuration files. You may choose to restore selected data such as a specific SCSI routing instance, or all data, using the **restore** command with the **from** keyword.

The file from which configuration is restored must reside in the *savedconfig* directory (*/ata3/savedconfig*). If you need to restore configuration data from a backup file existing elsewhere in the network, use the **copy** command to make the desired file available in the *savedconfig* directory.

Restoring configuration data copies all or part of the contents of the specified file into persistent memory; it does not always change the storage router's running configuration. For example, the configuration of a restored SCSI routing instance may only be completely visible via the **show scsirouter** command using the **from bootconfig** keywords, until the instance has been restarted.

### Restoring a Deleted SCSI Routing Instance

For example, suppose the SCSI routing instance, *scsi1*, was inadvertently deleted. Use the following procedure to restore *scsi1* from a configuration file that was saved to a URL.

|        | Command                                                                                   | Description                                                                                                                                                                                          |
|--------|-------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                                             | Enter Administrator mode.                                                                                                                                                                            |
| Step 2 | <b>copy</b> <i>http://10.1.1.44/~s1/back1.xml</i><br><b>savedconfig:scsi1_restore.xml</b> | Copy the specified configuration file from the designated URL and place it in the <i>savedconfig</i> directory, using the file name, <i>scsi1_restore.xml</i> .                                      |
| Step 3 | <b>show savedconfig</b>                                                                   | Verify that the imported file now exists in the <i>savedconfig</i> directory.                                                                                                                        |
| Step 4 | <b>show scsirouter all from</b><br><i>scsi1_restore.xml</i>                               | Verify that SCSI routing instance, <i>scsi1</i> , exists in this configuration file.                                                                                                                 |
| Step 5 | <b>restore scsirouter scsi1 from</b><br><i>scsi1_restore.xml</i>                          | Restores SCSI routing instance, <i>scsi1</i> , from the specified file.                                                                                                                              |
| Step 6 | <b>show scsirouter scsi1 from</b><br><b>bootconfig</b>                                    | Display the restored SCSI routing instance, <i>scsi1</i> , to verify configuration is as expected.                                                                                                   |
| Step 7 | <b>scsirouter scsi1 enable</b>                                                            | Start the restored SCSI routing instance, updating the running configuration of the SN 5428. Once the instance has been restored and restarted, modifications to its configuration can also be made. |
| Step 8 | <b>save scsirouter scsi1 bootconfig</b>                                                   | (Optional) If changes are made to the SCSI routing instance configuration, save the SCSI routing instance to the SN 5428 bootable configuration.                                                     |

### Restoring an Existing SCSI Routing Instance

If you need to restore the configuration of a SCSI routing instance that is still active in the SN 5428, you must stop the instance, restore the configuration from the selected file, then restart the instance. For example, use the following procedure to restore the SCSI routing instance, *scsi2*, from the file, *scsi2\_backup*.

|         | Command                                                         | Description                                                                                                                                                                                                                                                                       |
|---------|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | <b>enable</b>                                                   | Enter Administrator mode.                                                                                                                                                                                                                                                         |
| Step 2  | <b>show scsirouter <i>scsi2</i> stats</b>                       | Display current status of the SCSCI routing instance, <i>scsi2</i> . If the status is active, issue the <b>no scsirouter enable</b> command shown in Step 3 to stop the instance.                                                                                                 |
| Step 3  | <b>no scsirouter <i>scsi2</i> enable</b>                        | (Optional) Disable an active SCSI routing instance. You cannot restore an active instance.                                                                                                                                                                                        |
| Step 4  | <b>show savedconfig</b>                                         | Confirm that the desired backup file exists in the <i>savedconfig</i> directory.                                                                                                                                                                                                  |
| Step 5  | <b>show scsirouter all from <i>scsi2_backup</i></b>             | (Optional) Verify that the instance saved in the configuration file is the one you want to restore.                                                                                                                                                                               |
| Step 6  | <b>restore scsirouter <i>scsi2</i> from <i>scsi2_backup</i></b> | Restore the SCSI routing instance.                                                                                                                                                                                                                                                |
| Step 7  | <b>show scsirouter <i>scsi2</i> from bootconfig</b>             | Confirm that the configuration of the SCSI routing instance is now correct.                                                                                                                                                                                                       |
| Step 8  | <b>scsirouter <i>scsi2</i> enable</b>                           | Restart the SCSI routing instance.                                                                                                                                                                                                                                                |
| Step 9  | <b>show scsirouter <i>scsi2</i></b>                             | (Optional) Verify the configuration of the restored and restarted SCSI routing instance. The running configuration should now match the restored permanent configuration. Once the instance has been restored and restarted, modifications to its configuration can also be made. |
| Step 10 | <b>save scsirouter <i>scsi2</i> bootconfig</b>                  | (Optional) If changes are made to the SCSI routing instance configuration, save the restored SCSI routing instance to the SN 5428's bootable configuration.                                                                                                                       |

### Restoring an Access List

When you restore an access list, existing entries are never deleted. The restore will add missing entries and overwrite entries of the same name, but will never purge or delete existing entries. If necessary, you can delete an entire access list and then restore it from a saved configuration file.

Use the following procedure to restore the access list, *mylist1*, from the file, *accesslist\_backup.xml*. In this example, *mylist1* in the running configuration contains the following entries:

- 10.1.1.30/32
- 172.16.255.220/32
- chap-username 12h7b.lab2.webservices
- chap-username 12784.lab1.webservices

The saved access list in the configuration file, *accesslist\_backup.xml*, contains these entries:

- 209.165.200.225/32
- 10.1.1.30/32

- chap-username 12h7b.lab2.webservices
- chap-username test2.sys3



**Note** In a cluster environment, access lists management functions are handled by a single SN 5428. If you issue an access list command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the SN 5428 that is currently handling those functions.

|        | Command                                                      | Description                                                                                                                                                                                                                                                                                                                                         |
|--------|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                | Enter Administrator mode.                                                                                                                                                                                                                                                                                                                           |
| Step 2 | <b>show accesslist mylist1</b>                               | Display the current entries associated with access list, <i>mylist1</i> .                                                                                                                                                                                                                                                                           |
| Step 3 | <b>show accesslist mylist1 from accesslist_backup.xml</b>    | Display the entries associated with access list, <i>mylist1</i> , saved in the configuration file, <i>accesslist_backup.xml</i> . The configuration file must exist in the <i>savedconfig</i> directory.                                                                                                                                            |
| Step 4 | <b>restore accesslist mylist1 from accesslist_backup.xml</b> | Restore the access list entries for <i>mylist1</i> from the saved configuration file, <i>accesslist_backup.xml</i> .                                                                                                                                                                                                                                |
| Step 5 | <b>show accesslist mylist1</b>                               | Display the entries for the restored access list, <i>mylist1</i> . The entries are: <ul style="list-style-type: none"> <li>• 10.1.1.30/32</li> <li>• 172.16.255.220/32</li> <li>• 209.165.200.225/32</li> <li>• chap-username 12h7b.lab2.webservices</li> <li>• chap-username 12784.lab1.webservices</li> <li>• chap-username test2.sys3</li> </ul> |
| Step 6 | <b>save accesslist mylist1 bootconfig</b>                    | (Optional) If any entries prior to the restore were not saved, issue the <b>copy</b> command to save the current access list configuration to the SN 5428 bootable configuration.                                                                                                                                                                   |

**Restoring AAA Authentication Information**

When you restore AAA authentication information, the following configuration settings are updated:

- AAA authentication list
- The user names and passwords in the local username database
- Radius servers and associated server and global authentication port, retransmit, time-out, and key values
- TACACS+ servers, and associated server and global authentication port, time-out, and key values.

Use the following procedure to restore the AAA authentication configuration that exists in the saved configuration file *aaa\_backup.xml*.

|        | Command                                          | Description                                                                                                                                                                              |
|--------|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                    | Enter Administrator mode.                                                                                                                                                                |
| Step 2 | <b>show savedconfig</b><br><i>aaa_backup.xml</i> | Display the contents of the backup file, and verify that this is the AAA authentication configuration that you want to restore. The file must exist in the <i>savedconfig</i> directory. |
| Step 3 | <b>restore aaa from</b> <i>aaa_backup.xml</i>    | Restore the AAA authentication from the saved configuration file, <i>aaa_backup.xml</i> .                                                                                                |
| Step 4 | <b>show aaa</b>                                  | Display the AAA authentication information and verify that it is now correct.                                                                                                            |
| Step 5 | <b>save aaa bootconfig</b>                       | (Optional) If you make any changes to the restored AAA authentication configuration, save the changed configuration to the SN 5428 bootable configuration.                               |

**Restoring VLANs**

You can restore specific VLANs or all VLANs. When you restore a VLAN, the VTP mode is also restored.

Use the following procedure to restore a VLAN. In this example, VLAN 10 (named *TestLab*) will be restored from the saved configuration file named *VLAN\_backup.xml*.

**Note**

In a cluster environment, VLAN configuration must be performed on the first SN 5428 to join the cluster. If you issue a VLAN command from another SN 5428 in the cluster, the CLI displays an informational message with the system name and IP address of the SN 5428 that is currently handling all VLAN functions.

|        | Command                                               | Description                                                                                                                                                                                     |
|--------|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                         | Enter Administrator mode.                                                                                                                                                                       |
| Step 2 | <b>show savedconfig</b><br><i>VLAN_backup.xml</i>     | Display the contents on the saved configuration file <i>VLAN_backup.xml</i> . Verify that the file contains the VLAN and VTP configuration information that you want to restore (Example 10-2). |
| Step 3 | <b>restore vlan 10 from</b><br><i>VLAN_backup.xml</i> | Restore VLAN 10 from the saved configuration file <i>VLAN_backup.xml</i> .                                                                                                                      |
| Step 4 | <b>show vlan</b>                                      | Verify that the VLAN is restored and the configuration is correct.                                                                                                                              |

|        | Command                              | Description                                                                                                                             |
|--------|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <code>show vtp</code>                | Verify that the VTP configuration is correct.                                                                                           |
| Step 6 | <code>save vlan 10 bootconfig</code> | (Optional) If you make any configuration changes to the VLAN after restoration, save the changes to the SN 5428 bootable configuration. |

#### Example 10-2 Show VLAN Information from Saved Configuration File

```

!
! VTP DOMAIN
!
vtp domain none
!
! VTP MODE
!
vtp mode transparent
!
! VLAN
!
vlan 10 name TestLab mtusize 1500

```

#### Restoring System Configuration

You can restore selected system information using the **restore system** command. You can restore the following information:

- Administrator contact settings
- SNMP network management configuration
- NTP server and date, time, and time zone settings
- DNS configuration
- IP address of remote syslog host
- Software default download locations and associated user names and passwords
- CDP configuration
- Restrict service setting for all interfaces
- SN 5428 routing table
- SN 5428 event message logging table
- Configuration settings for all Fibre Channel interfaces

Use the following procedure to restore system configuration information. In this example, SNMP network management configuration and administrator contact settings will be restored from the saved configuration file named *system\_backup.xml*.

|        | Command                                             | Description                                                                                                                                                                                                              |
|--------|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code>                                 | Enter Administrator mode.                                                                                                                                                                                                |
| Step 2 | <code>show savedconfig<br/>system_backup.xml</code> | Display the contents of the saved configuration file, <i>system_backup.xml</i> . Verify that the file contains the SNMP network management configuration and administrator contact information that you want to restore. |

|        | Command                                                            | Description                                                                                                                                                                                  |
|--------|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>restore system snmp from</b><br><i>system_backup.xml</i>        | Restore SNMP network management configuration.                                                                                                                                               |
| Step 4 | <b>show snmp</b>                                                   | Verify that the SNMP network management information is restored and that the configuration is correct (Example 10-3).                                                                        |
| Step 5 | <b>restore system contactinfo from</b><br><i>system_backup.xml</i> | Restore administrator contact settings.                                                                                                                                                      |
| Step 6 | <b>show admin</b>                                                  | Verify that the administrator contact information is restored and that the configuration is correct (Example 10-4).                                                                          |
| Step 7 | <b>save system bootconfig</b>                                      | (Optional) If you make any configuration changes to the SNMP configuration or administrator contact information after restoration, save the changes to the SN 5428's bootable configuration. |

### Example 10-3 Verify SNMP Configuration

```

→ [SN5428_PR1]# show snmp
First Trap Host: 10.1.32.200
Second Trap Host: 10.2.12.242
Get Community String: public
Set Community String: private
Send Authentication Traps: enabled
Link Up/Down Enable for mgmt: enabled
Link Up/Down Enable for fc1: enabled
Link Up/Down Enable for fc2: enabled
Link Up/Down Enable for fc3: enabled
Link Up/Down Enable for fc4: enabled
Link Up/Down Enable for fc5: enabled
Link Up/Down Enable for fc6: enabled
Link Up/Down Enable for fc7: enabled
Link Up/Down Enable for fc8: enabled
Link Up/Down Enable for ge1: enabled
Link Up/Down Enable for ge2: enabled

```

### Example 10-4 Verify Administrator Contact Information

```

[SN5428_PR1]# show admin
Administrator Contact Information
 Name: Pat Hurley
 Email: phurley@abc123z.com
 Phone: 123.456.7890
 Pager: 123.456.3444 pin 2234

```

## Powering Down the SN 5428 Storage Router

If you need to make changes to the physical location or cabling of the SN 5428, you may need to schedule a time to power down the unit. Use the following procedure to properly power down a SN 5428. These steps assure that the file system is in the appropriate state prior to shutdown.

|        | Command       | Description                                                                                                                                                                                  |
|--------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b> | Enter Administrator mode.                                                                                                                                                                    |
| Step 2 | <b>halt</b>   | Assure that all configuration information is saved. Respond to any prompts to save information as desired. The SN 5428 can be safely powered down when the [HALTED]# command prompt appears. |

## Resetting the System

There may be times when you need to return some or all of the SN 5428 configuration to factory defaults, for example, when moving a system between environments (such as test and production) or for troubleshooting purposes.

To reset the SN 5428 Storage Router, perform the following steps:

- 
- Step 1** (Optional) Save existing configuration information to a file.
  - Step 2** Clear the current configuration and restore some or all factory defaults, using the **clear conf** command.



**Note** If the SN 5428 is operating in a cluster environment, any SCSI routing instances running on this SN 5428 fail over to another SN 5428 in the cluster. If you are operating in a cluster environment but do not want SCSI routing instances to fail over, issue the **no scsirouter enable** command for all instances (or selected instances that should not fail over) before you issue the **clear conf** command. (This will permanently delete the SCSI routing instances from the cluster.) See the “Controlling SCSI Routing Instances in a Cluster” section on page 10-18 for additional information on operating the SN 5428 in a cluster environment.

---

- Step 3** (Optional) Run the initial configuration script to configure the management interface via an EIA/TIA-232 console connection.
  - Step 4** Restore specific configuration information or reconfigure the SN 5428 using CLI commands or the web-based GUI.
-

**Reset All to Factory Defaults**

Use the following procedure if an existing SN 5428 is to be physically moved to another environment, and it is not necessary to retain any current configuration information, because the system setup will be completely different.

|        | Command                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                          | Enter Administrator mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 2 | <b>clear conf</b><br>or<br><b>clear conf all cisco</b> | <p>Clear the current system configuration, including network management information.</p> <p>For SN 5428s deployed for SCSI routing, you can use the <b>clear conf</b> wizard. At the prompt, enter the Administrator password. Enter <b>all</b> to erase system configuration and management port settings, and all saved configurations and SCSI routing instances (Example 10-5).</p> <p>For SN 5428s deployed for transparent SCSI routing, enter the <b>clear conf all</b> command, followed by the Administrator password (for example, <i>cisco</i>). This command is also available in SN 5428s deployed for SCSI routing.</p> <p>After either of the commands completes, the SN 5428 will reboot.</p> |

**Example 10-5 Reset SN 5428 Storage Router Configuration**

Enter admin password: \*\*\*\*\*

This process can restore factory default settings for the SN5428.

- \* Select "apps" to remove active applications and retain system configuration settings.
- \* Select "system" to remove active applications and system configuration settings.
- \* Select "saved" to remove all backup configurations from disk.
- \* Select "all" to remove active applications, system configuration, and saved configurations.

The system configuration includes the management port, dns, admin and monitor login, ntp, and snmp. You will need to use the console to reconfigure the management port if you erase the system configuration.

The system will reboot if you select "apps", "system", or "all".

Erase what? [apps/system/saved/all/cancel (cancel)]

**Note**

After the move, use the EIA/TIA-232 console connection to configure the management interface IP address and other required system information. (See the “Initial System Configuration Script” section in Chapter 2, “First-Time Configuration,” for details.) Then configure the SN 5428 via the **setup** configuration wizards or other CLI commands, or via the web-based GUI.

### Reset and Retain System Settings

Use the following procedure if an existing SN 5428 is going to be used for testing purposes and then is to be restored to its current configuration, and for the test, the SN 5428's system configuration information is not going to change. The following procedure retains the system configuration and saved configuration files over the system reset.

|        | Command                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                         | Enter Administrator mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 2 | <b>save all</b> <i>myfile</i>         | Save all configuration information in a file called <i>myfile</i> . This file is stored in the <i>savedconfig</i> directory.                                                                                                                                                                                                                                                                                                                                                                           |
| Step 3 | <b>clear conf</b>                     | Clear the current configuration but retain system information (such as management and HA interfaces, logging table, DNS, Administrator and Monitor passwords, NTP server, and SNMP information) and saved configuration files.<br><br>At the prompt, enter the Administrator password. Enter <b>apps</b> to retain system configuration settings.<br><br>The SN 5428 will reboot.<br><br>Perform the required user testing. When finished, continue with Step 4 to restore the original configuration. |
| Step 4 | <b>restore all from</b> <i>myfile</i> | Restore original configuration, which was retained over the <b>clear conf</b> command.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 5 | <b>reboot</b>                         | Reboot to restore the original application configuration into running memory.                                                                                                                                                                                                                                                                                                                                                                                                                          |

### Reset to Remove Saved Configuration Files

Use the following procedure if a stand-alone SN 5428 has joined a cluster and adopted the new cluster's configuration. The procedure removes previously saved configuration files from the stand-alone period, but the SN 5428's system configuration, management information, and SCSI routing instances remain unchanged.

|        | Command                 | Description                                                                                                                                                                                                                                                                                          |
|--------|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>           | Enter Administrator mode.                                                                                                                                                                                                                                                                            |
| Step 2 | <b>clear conf</b>       | Remove all saved configuration files from the <i>savedconfig</i> directory.<br><br>At the prompt, enter the Administrator password. Enter <b>saved</b> to retain system configuration settings.<br><br>All files are removed from the <i>savedconfig</i> directory, but the SN 5428 does not reboot. |
| Step 3 | <b>show savedconfig</b> | Verify that all files have been removed from the <i>savedconfig</i> directory.                                                                                                                                                                                                                       |



#### Note

You can also use the **delete savedconfig** command to delete selected saved configuration files from the *savedconfig* directory.

## Recovering Passwords

The SN 5428 management interface is password protected. You must enter passwords when accessing the SN 5428 via Telnet (for the CLI) or the web-based GUI. Password protection can also be enabled for the SN 5428 console interface, thereby requiring that the same Administrator and Monitor mode passwords that are configured for the management interface be applied to the console interface.

If the passwords have been enabled for the console interface and are lost, you can recover management access to the SN 5428 using the password recovery procedure. The password recovery procedure requires physical access to the SN 5428 console and can be found at the following URL:

<http://www.cisco.com/warp/public/474/>

## Controlling SCSI Routing Instances in a Cluster

It is important to know where SCSI routing instances are running. While automatic failover capabilities keep the SN 5428 cluster operational in times of system difficulties, manual HA controls provide the ability to distribute SCSI routing instances between the SN 5428s in a cluster to meet your specific network requirements.

The following are typical activities involved with controlling SCSI routing instances in a cluster environment. While most of these activities are performed infrequently, some (such as viewing operational statistics) may be performed on a regular basis.

- Making Changes to Instance Configurations
- Enabling and Disabling Connections
- Stopping & Starting Instances
- Viewing Operational Statistics
- Handling Failover

## Making Changes to Instance Configurations

**Note**

---

To assure that changes are correctly propagated to all SN 5428s within a cluster, always modify the configuration of a SCSI routing instance from the SN 5428 where the instance is currently active.

---

From time to time, you will make changes to the SCSI routing instance configurations. Changes include such actions as adding or deleting a target, adding or deleting a LUN, remapping a target, or modifying access. It is important to understand the ramifications of these changes on the IP hosts accessing the associated storage resources. For example, changing the instance configuration may change the device presentation to the IP host, effectively changing the name or number assigned to the device by the host operating system. Certain instance configuration changes, such as adding or deleting targets, adding or deleting LUNs within a particular target, or adding or deleting entire instances may change the order of the devices presented to the host. Even if the host is only associated with one SCSI routing instance, the device order could make a difference.

Typically, the IP host operating system assigns drive identifications in the order they are received based on certain criteria. For example, a Linux system assigns drive identifications in the order they are received based on host, bus, target, and LUN information. Changing the order of the storage discovery may result in a changed drive identification. Applications running on the host may require modification to appropriately access the current drives.

If an entire SCSI routing instance is removed, or there are no targets available for the host, the host's iSCSI driver configuration file must be updated to remove the appropriate reference before restarting the iSCSI driver. If a host's iSCSI configuration file contains a reference to an instance which does not exist or has no targets available for the host, the iSCSI driver will not complete a login and will not discover targets associated with any SCSI routing instance.

For additional information and recommended procedures for changing iSCSI driver configuration, see the iSCSI driver readme and example configuration files. You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.

## Enabling and Disabling Connections

A SCSI routing instance becomes active, by default, once it is associated with a Gigabit Ethernet interface to IP hosts. Each target that is added to an instance is also, by default, enabled. However, no IP hosts can connect or log in to that target because the target has no access list association. Once you associate an access list with a target, it is automatically enabled; the IP hosts specified by access list entries are allowed to connect or log in to the target.

Use the **scsirouter target disabled** command to control access to the target without changing the access list association or stopping the entire SCSI routing instance. Existing connections and logins are not affected, but future connections and logins are prohibited.

Use the **scsirouter target enabled** command when you are ready to allow connections and logins again.

For example, suppose you have a problem with an entry in the access list, *webserver2*. This access list is associated with the target, *webstorage2*, which is, in turn, associated with the SCSI routing instance *foo*.

Use the following procedure to temporarily disable access to the target associated with a problem access list.

|        | Command                                                             | Description                                                                                                                                                                                                      |
|--------|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                       | Enter Administrator mode.                                                                                                                                                                                        |
| Step 2 | <b>show scsirouter <i>foo</i> stats</b>                             | Display status to confirm the SCSI routing instance, <i>foo</i> , is active on this SN 5428.                                                                                                                     |
| Step 3 | <b>show scsirouter <i>foo</i></b>                                   | Verify the name and current status of the target and access list. The target, <i>webstorage2</i> , should be associated with the <i>webserver2</i> access list and the target should be enabled. (Example 10-6.) |
| Step 4 | <b>scsirouter <i>foo</i><br/>target <i>webstorage2</i> disabled</b> | Disable access to the target, <i>webstorage2</i> . (Example 10-7.)                                                                                                                                               |

**Example 10-6 Verify Target, Access List, and Target Status**

```
[SN5428_PR1]# show scsirouter foo
foo description "test SCSI routing instance"
foo authenticate "none"
foo primary "none"
foo proxy server disabled
foo failover primary "none"
foo failover secondary "none"
foo lun reset no
foo cdb retry counter 30
foo serverif ge2 10.1.0.45/24, TCP port:3260
foo target webstorage2 description "Web Storage"
foo target webstorage2 Name "ign.1987-05.com.cisco.00.0b1aaa415....webstorage2"
→ foo target webstorage2 enabled "TRUE"
→ foo target webstorage2 accesslist "webserver2"
foo target webstorage2 wwpn "21:00:00:05:ae:42:2f:12"
```

**Example 10-7 Verify New Target Status**

```
[SN5428_PR1]# show scsirouter foo
foo description "test SCSI routing instance"
foo authenticate "none"
foo primary "none"
foo proxy server disabled
foo failover primary "none"
foo failover secondary "none"
foo lun reset no
foo cdb retry counter 30
foo serverif ge2 10.1.0.45/24,TCP port:3260
foo target webstorage2 description "Web Storage"
foo target webstorage2 Name "ign.1987-05.com.cisco.00.0b1aaa415....webstorage2"
→ foo target webstorage2 enabled "FALSE"
foo target webstorage2 accesslist "webserver2"
foo target webstorage2 wwpn "21:00:00:05:ae:42:2f:12"
```

## Stopping & Starting Instances

If the SN 5428 is experiencing a problem with a specific set of IP hosts or storage resources, you may wish to stop the associated SCSI routing instance from running anywhere in the cluster. The **no scsirouter enable** command causes the specified SCSI routing instance to cease running on the SN 5428, but does not cause a failover to another SN 5428 in the cluster. This command effectively stops an instance from running anywhere in the cluster.

Once a SCSI routing instance has been stopped, it can be re-activated by issuing the **scsirouter enable** command. The **scsirouter enable** command must be issued from the same SN 5428 as the **no scsirouter enable** command.

See Chapter 11, “Command Line Interface Reference,” for command details.

## Viewing Operational Statistics

Use the **show scsirouter stats** command to display the status of the SCSI routing instance and to see the number of active connections and the number of logins that have occurred since the SN 5428 was last restarted (or since statistics were last cleared).

For example, the **show scsirouter stats** command in Example 10-8 shows that SCSI routing instance, *foo*, is currently active.

### Example 10-8 Results of “show scsirouter stats” Command

```
[SN5428_PR1]# show scsirouter foo stats

router status started iSCSI ver (Min/Max) logins active
foo ACTIVE Jan 11 23:06:08 2/2 10 7
```

## Handling Failover

In a cluster, SN 5428s continually exchange information as heartbeats to detect failures in the cluster. HA messages are sent using UDP over IP and, depending on the message type or situation, may be sent as unicast or multicast messages. To make sure that HA information is exchanged reliably between SN 5428s, the SN 5428s alternate transmission of heartbeats between the management and the HA interfaces.

Failover of SCSI routing instances is automatic when the SN 5428 detects that another SN 5428 in the cluster is no longer responding to heartbeats. Failover of a SCSI routing instance also occurs if the associated Gigabit Ethernet interface is unavailable or if all targets are unavailable.



### Note

If some targets are available but others are not, failover of the SCSI routing instance does not occur.

Each cluster supports up to 12 active SCSI routing instances. Since each SN 5428 can also support up to 12 SCSI routing instances, high availability is ensured for each instance in the cluster (regardless of the division of those instances between SN 5428s).

## Manual Failover

While failover of SCSI routing instances is automatic, there may be times when you wish to manually move a SCSI routing instance from one SN 5428 to another. The move may be temporary, after which the instance will be moved back to its original location. At other times, you may want to move a SCSI routing instance permanently to another SN 5428, ensuring that the instance will continue running on the specified SN 5428 whenever possible.

As an example cluster scenario, a cluster is composed of two SN 5428s, *SN5428Sys1* and *SN5428Sys2*. *SN5428Sys1* is currently running instances, *scsi1* and *scsi2*, and is the primary SN 5428 for both instances. *SN5428Sys2* is currently running instances, *scsi3* and *scsi4*. The primary attribute for *scsi3* and *scsi4* is set to the default setting of **none**, indicating no preferred SN 5428 for failover for either instance.

**Failover as Temporary Move**

Referring to the example cluster scenario just described, the following procedure moves the SCSI routing instance, *scsi1*, from its primary, or preferred, SN 5428, *SN5428Sys1*, to the other SN 5428 on a temporary basis. The commands in this procedure are issued from a CLI session from SN 5428, *SN5428Sys1*.

|        | Command                                                                | Description                                                                                                                                                            |
|--------|------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                          | Enter Administrator mode.                                                                                                                                              |
| Step 2 | <b>show cluster</b><br>or<br><b>show scsirouter <i>scsi1</i> stats</b> | Verify that the instance to be moved, <i>scsi1</i> , is indeed running on SN 5428, <i>SN5428Sys1</i> .                                                                 |
| Step 3 | <b>failover scsirouter <i>scsi1</i></b>                                | Failover SCSI routing instance, <i>scsi1</i> .<br><b>Note</b> Because there are only two SN 5428s in the cluster, you do not need to specify the failover destination. |
| Step 4 | <b>show cluster</b><br>or<br><b>show scsirouter <i>scsi1</i> stats</b> | Verify that the specified SCSI routing instance, <i>scsi1</i> , is no longer running on the SN 5428, <i>SN5428Sys1</i> .                                               |

Once the failover is complete, establish a Telnet session to *SN5428Sys2* and verify—using CLI commands described in Step 1 and Step 2 above—that the SCSI routing instance, *scsi1*, is now running on that SN 5428.

This is considered a temporary move because *SN5428Sys1* is still designated as the primary SN 5428 for the SCSI routing instance, *scsi1*. If, for example, *SN5428Sys1* is rebooted, *scsi1* will stop running on *SN5428Sys2* and will start up and run on *SN5428Sys1*.

**Note**

Use caution if you change the configuration of a SCSI routing instance while it is running on the SN 5428 that is not the instance's configured primary SN 5428. If the instance's configuration changes while the designated primary SN 5428 for that instance is down (or otherwise removed from the cluster), the changes will not be propagated to that SN 5428. When the primary SN 5428 reboots (or otherwise returns to the cluster), it will reassert itself as the primary and will start to run the instance using the last configuration it had before leaving the cluster.

**Failover as Permanent Move**

Referring to the example cluster scenario previously described, the following procedure moves the SCSI routing instance, *scsi2*, from its primary, or preferred, SN 5428, *SN5428Sys1*, to the other SN 5428 on a permanent basis. The commands in this procedure are issued from a CLI session from SN 5428, *SN5428Sys1*.

|        | Command                                                                | Description                                                                                            |
|--------|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                          | Enter Administrator mode.                                                                              |
| Step 2 | <b>show cluster</b><br>or<br><b>show scsirouter <i>scsi2</i> stats</b> | Verify that the instance to be moved, <i>scsi2</i> , is indeed running on SN 5428, <i>SN5428Sys1</i> . |

|        | Command                                              | Description                                                                                                                                      |
|--------|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>scsirouter scsi2 primary</b><br><i>SN5428Sys2</i> | Set <i>SN5428Sys2</i> as the primary SN 5428 for the desired SCSI routing instance, <i>scsi2</i> .                                               |
| Step 4 | <b>save scsirouter scsi2 bootconfig</b>              | Save the current SCSI routing instance configuration, including the primary setting, and circulate the changed configuration around the cluster. |
| Step 5 | <b>failover scsirouter scsi2</b>                     | Failover the desired SCSI routing instance, <i>scsi2</i> .                                                                                       |

Once the failover is complete, establish a Telnet session to *SN5428Sys2* and verify—using the **show scsirouter scsi2** command—that the SCSI routing instance, *scsi2*, is now running on *SN5428Sys2* and that *SN5428Sys2* is designated as the primary SN 5428 for that instance.

#### Failover for Distribution Purposes

In the example cluster scenario previously described, there is a significant increase in traffic for SCSI routing instance, *scsi4*, and as a result, you decide to distribute all of the other instances (*scsi1*, *scsi2*, and *scsi3*) to the *SN5428Sys1* SN 5428. *SN5428Sys1* is already running *scsi1* and *scsi2*.

The following procedure moves the SCSI routing instance, *scsi3*, to *SN5428Sys1*. The commands in this procedure are issued from a CLI session from SN 5428, *SN5428Sys2*.

|        | Command                                                         | Description                                                                                         |
|--------|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                   | Enter Administrator mode.                                                                           |
| Step 2 | <b>show cluster</b><br>or<br><b>show scsirouter scsi3 stats</b> | Verify that the SCSI routing instance to be moved is indeed running on SN 5428, <i>SN5428Sys2</i> . |
| Step 3 | <b>failover scsirouter scsi3 to SN5428Sys1</b>                  | Failover the desired SCSI routing instance, <i>scsi3</i> , to <i>SN5428Sys1</i> .                   |

Once the failover is complete, establish a Telnet session to *SN5428Sys1* and verify—using the **show scsirouter** command—that instances, *scsi1*, *scsi2*, and *scsi3*, are now running there.



#### Note

Because *scsi3* has no primary setting, it will remain running on *SN5428Sys1* until it is explicitly stopped or failed over, or until it automatically fails over because an interface is unavailable or a software or hardware problem occurred.

## Managing CDP on the SN 5428 Storage Router

Cisco Discovery Protocol (CDP) is primarily used to obtain protocol addresses of neighboring devices and to discover the platform of those devices. CDP is media- and protocol-independent and runs on all Cisco-manufactured equipment including routers, bridges, access servers, and switches.

Each device configured for CDP sends periodic messages, known as advertisements, to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime, information, which indicates the length of time a

receiving device should hold CDP information before discarding it. Each device also listens to the periodic CDP messages sent by others in order to learn about neighboring devices and determine when their interfaces to the media go up or down.

The SN 5428 Storage Router is enabled, by default, to exchange CDP information with other CDP-enabled devices in the network. CDP can be enable or disabled for individual interfaces on the SN 5428, and the holdtime for receiving devices and the frequency of CDP transmissions from the SN 5428 can be modified.

#### Disable CDP for Selected Interfaces

CDP can be enabled or disabled for the management, HA, and Gigabit Ethernet interfaces on the SN 5428. By default, all interfaces are enabled for CDP. Use the following procedure to disable CDP for an interface.

|        | Command                            | Description                                                             |
|--------|------------------------------------|-------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                      | Enter Administrator mode.                                               |
| Step 2 | <b>no cdp interface ge2 enable</b> | Disable CDP on the desired interface ( <i>ge2</i> ).                    |
| Step 3 | <b>show cdp interface</b>          | Confirm that CDP is disabled for the interface.                         |
| Step 4 | <b>save system bootconfig</b>      | (Optional) Save the CDP change to the SN 5428's bootable configuration. |

#### Modify the CDP Holdtime and Timeout Values

Holdtime is the amount of time the receiving device should hold a CDP packet from the SN 5428 before discarding it. The CDP holdtime value must be set to a higher number of seconds than the CDP timer value (the time between CDP transmissions from the SN 5428). For example, the default CDP holdtime value is 180 seconds. The default CDP timer value is 60 seconds.

Use the following procedure to change the CDP holdtime value and the CDP timer value.

|        | Command                       | Description                                                                                          |
|--------|-------------------------------|------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                 | Enter Administrator mode.                                                                            |
| Step 2 | <b>show cdp</b>               | Verify the current CDP configuration.                                                                |
| Step 3 | <b>cdp holdtime 300</b>       | Set the number of seconds ( <i>300</i> ) that a receiving device should hold the SN 5428 CDP packet. |
| Step 4 | <b>cdp timer 120</b>          | Set the number of seconds ( <i>120</i> ) between transmissions of CDP packets from the SN 5428.      |
| Step 5 | <b>show cdp</b>               | (Optional) Verify the new CDP configuration.                                                         |
| Step 6 | <b>save system bootconfig</b> | (Optional) Save the CDP changes to the SN 5428's bootable configuration.                             |

## Using Scripts to Automate Tasks

If you frequently issue a series of CLI commands, you can save time by entering those commands into a script for execution purposes. Command scripts are stored in the *script* directory and are simply ASCII text files containing CLI commands.

Follow these rules when creating a command script:

- Commands can start anywhere on a line. The first word on any line that is not preceded by a comment character is considered to be the start of a command string.
- Comments can be added by placing an exclamation point (!) or number sign (#) character at the beginning of the line or as the first character at any position in the line. Comments are useful for documenting the contents of the file and the expected results. Comments can also be used to prevent a command from executing without removing it from the file by inserting a comment character before the command string.
- You can extend commands across line boundaries by ending a line with a backslash (\) as the continuation character. Use the continuation character to make long commands more readable. The line sequence is continued until a command line without a continuation character is encountered. If a comment line is used to end a line continuation sequence, you must add a blank line after the comment.

For example:

```
radius-server host 10.5.0.53 \
 auth-port 1644 \
 timeout 60 \
 retransmit 5
! Configure 1st RADIUS server

radius-server host 10.6.0.61
. . .
```

- Scripts can be invoked from other scripts.

When scripts run, the commands and any responses are echoed on the SN 5428 console.

Scripts can be created on any system using any text editor and placed in the *script* directory (*/ata3/script*) of the target SN 5428 using FTP. See the “Using FTP with the SN 5428 Storage Router” section on page 10-28 for details. You can also use the **copy** command to copy the script file to the SN 5428 using HTTP or TFTP.

## Running Command Scripts

Use the following procedure to execute the CLI commands stored in a script file. In this example, the script file is named *CreateSc* and must exist in the *script* directory.

|        | Command                                                                                     | Description                                                                                                                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                                               | Enter Administrator mode.                                                                                                                                                                                                                                 |
| Step 2 | <b>show script</b> <i>CreateSc</i>                                                          | Verify that the script, <i>CreateSc</i> , exists in the <i>script</i> directory and that it contains the configuration that you want to recreate.                                                                                                         |
| Step 3 | <b>read script</b> <i>CreateSc</i><br>or<br><b>read script</b> <i>CreateSc</i> <b>force</b> | Read and execute the CLI commands in the script file. When prompted, confirm that you want to continue and execute the script commands.<br><br>(Optional) Use the <b>force</b> keyword to execute the script immediately without asking for confirmation. |

After the script completes, issue the appropriate **show** commands to verify that the script executed as expected.

# Managing the Log File

The SN 5428 can log event information to a series of log files, based on the routing rules specified in the SN 5428 logging table. The default configuration routes all SN 5428 event messages at notification level *info* or lower to the logfile. Use the **show logging** commands to display log file entries and to search for entries that match specific text strings or regular expressions.

Log files are created in the SN 5428 *log* directory (*/ata4/log*). They can occupy up to 4 MB of memory. Once this limit has been reached, the oldest file is removed and a new one is created. The **show logging size** command can be used to display the size of the existing log files. The **show system** command can be used to display the amount of space allocated to log files, and the amount of log file space currently available.

The name of the log file is *messages*, followed by a number (for example, *messages3* or *messages12*). The first log file is named *messages0*, the next log file is named *messages1*, etc.

Depending on the needs of your enterprise, you can archive log files to a remote server, or you can clear log files on a periodic basis. You can use FTP to transfer files from the SN 5428 to a remote server (see the “Using FTP with the SN 5428 Storage Router” section on page 10-28 for details), or you can use the web-based GUI to display the contents of the log file and use cut-and-paste techniques to save the information to a local file. You can also issue the **show logging all** command and redirect the output of your console using the logging facilities for your specific console interface.



## Note

See the “Understanding Logging” section on page 10-30 for more information about adding routing rules to the SN 5428 logging table.

## Clearing the Log Files

Use the following procedure to periodically clear the SN 5428 log files.

|        | Command                                                      | Description                                                                                                                                                          |
|--------|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                | Enter Administrator mode.                                                                                                                                            |
| Step 2 | <b>show logging size</b>                                     | (Optional) Check the current size of the SN 5428 log files (Example 10-9).                                                                                           |
| Step 3 | <b>show logging all</b><br>or<br><b>show logging last 50</b> | (Optional) Display all the current log file entries (first command), or display a selected number of entries, such as 50, from the end of the file (second command). |
| Step 4 | <b>clear log</b>                                             | Clear the existing log file. The SN 5428 clears the existing log file and starts a new log file.                                                                     |

### Example 10-9 Results of “show logging size” Command

```
[SN5428_PRA]# show logging size
5120 messages (342797 bytes) logged
```

# Gathering Troubleshooting Information

If you experience problems with the SN 5428, you may need to obtain troubleshooting information for Cisco technical support personnel. The SN 5428 Storage Router provides several features that can help you assemble the necessary information.

The following are typical activities involved with troubleshooting the SN 5428:

- Using the Crash Log
- Using FTP with the SN 5428 Storage Router
- Understanding Diagnostics
- Capturing System Messages at Bootup
- Understanding Logging
- Capturing the SN 5428 Configuration
- Using Debug Facilities

## Using the Crash Log

If the SN 5428 experiences an unexpected problem that forces it to automatically reboot, a special log file is generated. The file is named *crash.txt* and is stored in the *log* directory (*/ata4/log*). You can display the contents of this file to the console using the **show crash** command.

To save the **show crash** command output, redirect the output of your console using the logging facilities for your specific console interface. Depending on your console interface and scroll buffer size, you may also be able to copy and paste the contents from your console into an ASCII text file.

The crash log provides the following information:

- Exception information
- Boot information, including the kernel version and creation date
- Software information
- A list of all tasks, including entry point, task ID and priority for each task
- Task registers and stack trace for each task in the task list
- Net job ring
- A list of all modules, including module ID, data start addresses, etc.
- A list of all devices and associated drivers
- A list of all drivers, including the number of create, delete, open, close, read, write, and I/O control actions performed
- A list of free memory addresses and a summary of memory usage information
- A list of open file descriptors
- Network interface information, including flags, interface type, addresses, and MTU information for all SN 5428 interfaces
- The SN 5428 route table
- The ARP table
- The SN 5428 host table

- Active Internet connection information, including PCB, connection type (TCP or UDP), receive and send queues, local and foreign addresses, and state for each connection
- Routing statistics
- IP statistics
- ICMP statistics
- TCP statistics
- UDP statistics
- Network stack data pool (MBufs) and cluster pool table information
- NFS authorization
- Mounted NFS filesystem information
- IDE disk or Flash information, including device types and parameters
- Registered crash dump functions
- Sample registered dump functions
- CPC710 registers at time of exception

Information used to create the *crash.txt* file is periodically written to the *tmpcrash.txt* file in the *log* directory. If a crash occurred at the current time, use the **show crash current** command to display the information as it would be written to the crash log.

## Using FTP with the SN 5428 Storage Router

In certain cases, you may want to copy log files from the SN 5428 to another server in your network for analysis purposes, or you may want to copy configuration or script files to another server prior to making them available to another SN 5428. The SN 5428 includes an FTP daemon; however, the FTP port (port 21) is, by default, restricted.

Use the following procedure to enable FTP and to copy the current message log file from the SN 5428 to another server in the network.

|        | Command                     | Description                                                                                                                    |
|--------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>               | Enter Administrator mode.                                                                                                      |
| Step 2 | <b>show restrict</b>        | Display interface restrictions. If port 21 on the management interface (fei0) is closed, use the command in Step 3 to open it. |
| Step 3 | <b>no restrict mgmt ftp</b> | (Optional) Allow FTP functions on the management interface.                                                                    |

Once the function is enabled, open the FTP session to the SN 5428 from the server. You will be prompted for a user name and password. The user name is *admin* and the password is the SN 5428 Administrator password. The default Administrator password is *cisco*.



**Note** The user name and the password are both case sensitive.

The SN 5428 Storage Router log files and crash trace files are stored in the */ata4/log* directory. Saved configuration files are stored in the */ata3/savedconfig* directory. Script files are stored in the */ata3/script* directory.

To use FTP to retrieve the SN 5428 Storage Router log file, change to the */ata4/log* directory using the FTP *cd* command. List the files to determine what log file you want to retrieve. (In our example, the log file is *messages0*.) If necessary, specify the binary flag using the FTP *binary* command. Issue the FTP *get* command to retrieve the log file and to copy it to the specified file on your server. When the process completes, close the FTP connection using the FTP *bye* command.

Example 10-10 illustrates the FTP session just described. In this example, the SN 5428 management interface IP address is 10.1.11.210.

#### Example 10-10 FTP Session

```
Server1> ftp 10.1.11.210
Connected to 10.1.11.210.
220 VxWorks (5.4.1) FTP server ready
Name: admin
331 Password required
Password:*****
230 User logged in
ftp> cd /ata4/log
250 Changed directory to "/ata4/log"
ftp> dir
200 Port set okay
150 Opening ASCII mode data connection
 size date time name

 512 Apr-09-2002 20:46:18 . <DIR>
 512 Apr-09-2002 20:46:18 .. <DIR>
 13803 May-16-2002 15:13:56 messages0
 92167 Apr-10-2002 19:14:06 tmpcrash.txt
226 Transfer complete
ftp: 374 bytes received in 0.02Seconds 23.38Kbytes/sec.
ftp> binary
200 Type set to I, binary mode
ftp> get
(remote-file) messages0
(local-file) SN5428Sys1_Messages
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
40863 bytes received in 0.049 seconds (8.1e+02 Kbytes/s)
ftp> bye
221 Bye...see you later
```

If you had to remove the restriction on the management interface before proceeding with the FTP session, return to the SN 5428 CLI session and re-enable the restriction, using the following procedure.

|        | Command                  | Description                                                                        |
|--------|--------------------------|------------------------------------------------------------------------------------|
| Step 1 | <b>show restrict</b>     | Verify that port 21 on the management interface is currently open.                 |
| Step 2 | <b>restrict mgmt ftp</b> | Close the management interface to FTP functions. No FTP functions will be allowed. |

## Understanding Diagnostics

The SN 5428 Storage Router performs hardware diagnostics when the unit is powered up. Hardware diagnostics cannot be bypassed. If a hardware diagnostic fails, the SN 5428 halts. The boot process cannot be reinitiated.

If you experience a hardware diagnostic failure, contact Cisco technical support personnel as described in the “Obtaining Technical Assistance” section on page xiii for further instructions.

The SN 5428 performs additional “soft” diagnostics after the hardware diagnostics complete on power up and after every system reboot. If necessary, the soft diagnostics can be bypassed.

If you experience problems with soft diagnostics, contact Cisco technical support personnel for assistance.

## Capturing System Messages at Bootup

The SN 5428 Storage Router logs a variety of messages to the console during the system boot process. If you are experiencing problems with the SN 5428, it may be helpful to capture these messages. Use the console interface to perform the boot process and capture the console log using typical external methods.

## Understanding Logging

The SN 5428 Storage Router generates a variety of system event messages. All SN 5428 event and debug messages are issued in the following format:

### Example 10-11 Event Message

```
Mar 18 11:48:05: %SNMP-5-SASAS: SnmpApp starting...
<timestamp>: %<facility>-<level_number>-<mnemonic>: <message text>
```

All messages are assigned a notification level, which reflects the priority of the message in the system. Messages with the highest priority are assigned a notification level of *emergency*. Messages at this level indicate that the system is unusable. Messages with the lowest priority are assigned a notification level of *debug*. Messages at this level are for troubleshooting purposes. In Example 10-11, the message level number is 5, indicating a notification level of *notice*.

Table 10-1 lists the notification levels, their level number, and their description.

**Table 10-1 Event Message Notification Levels**

| Notification Level | Level Number | Description                              |
|--------------------|--------------|------------------------------------------|
| emergency          | 0            | System unusable                          |
| alert              | 1            | Immediate action needed                  |
| critical           | 2            | Critical conditions                      |
| error              | 3            | Error conditions                         |
| warning            | 4            | Non-fatal warning conditions             |
| notice             | 5            | Normal but significant conditions        |
| info               | 6            | Informational messages only              |
| debug              | 7            | Information for troubleshooting purposes |

Event, trace and debug messages can be routed to various destinations, based on the notification level of the message and the application area (facility) that generated the message. Table 10-2 lists the logging destinations and their descriptions; Table 10-3 lists the logging facilities and their descriptions.

**Table 10-2 Event Message Logging Destinations**

| Destination | Description                                                                                                                                   |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| all         | Logs the message to all destinations.                                                                                                         |
| none        | The message is not logged; it is discarded.                                                                                                   |
| console     | The message is logged to a serial console CLI session.                                                                                        |
| logfile     | The message is logged to the SN 5428 logfile.                                                                                                 |
| rslog       | The message is logged to a remote syslog server. Use the <b>logging syslog</b> command to specify the IP address of the remote syslog server. |
| vty         | The message is logged to all Telnet or other virtual terminal CLI sessions.                                                                   |

**Table 10-3 Event Message Facilities**

| Facility | Description                          |
|----------|--------------------------------------|
| AUTH     | AAA authentication.                  |
| CDP      | Cisco Discovery Protocol.            |
| CONF     | Configuration functions.             |
| FC       | SN 5428 Fibre Channel interfaces.    |
| GE       | SN 5428 Gigabit Ethernet interfaces. |
| HA       | SN 5428 high availability clusters.  |
| IF       | Interface manager.                   |
| INVALID  | Generic functions.                   |
| IPROUTER | SN 5428 IP functions.                |
| ISCSI    | iSCSI functions.                     |
| MON      | Hardware monitor.                    |
| SNMP     | Simple Network Management Protocol.  |
| SYSLOG   | Syslog functions.                    |
| UI       | SN 5428 user interface.              |
| VTP      | VTP and VLAN functions.              |

Messages are routed by creating a list of routing rules that is searched for a facility and notification level match whenever an event or debug message is received. This list of routing rules is known as the SN 5428 *logging table*.

By default, the logging table includes rules to log all messages at notification level *notice* (or numerically lower levels) to all destinations, and to log all messages at notification level *info* to the SN 5428 log file. Any message that does not find a matching rule is not logged to any destination.

Use the **show logging** command to display the current logging table routing rules and other logging information.

## Filtering and Routing Event Messages

The SN 5428 logging table allows messages to be filtered by their facility and notification level and routed to the specified destination(s). When an event message arrives, the logging table rules are searched by facility name and by level until the first match is found. The message is sent to all the destinations specified by the matching rule. If no match is found, the event message is discarded.

When a new routing rule is added, it is appended to the existing table. Use the **logging level** command to add a new routing rule to the logging table; use the **logging #?** command to insert a routing rule into the logging table before the specified entry.

Each facility can have eight notification levels. Each facility and notification level pair can have up to seven destinations.

In Example 10-11, the facility is SNMP, and the notification level is 5 (*notice*). If the logging table included the entries in Example 10-12, the event message in Example 10-11 would match on the first routing rule, and would be sent to all valid destinations. Any message from the SNMP facility at notification level *info*, and any message from another facility at notification level *info* (or lower) would match on the second rule and be sent to the SN 5428 console and log file. All messages from any facility at notification level *debug* would be discarded.

### Example 10-12 Example Log Route Entries List

| Index | Level  | Priority | Facility | Route           |
|-------|--------|----------|----------|-----------------|
| 1     | notice | 5        | SNMP     | all             |
| 2     | info   | 6        | all      | console logfile |

The logging table can be saved and retained across the SN 5428 restart. The order of the rules in the logging table is preserved when entries are deleted.

## Enabling and Disabling Logging

Logging is enabled by default. By default, the SN 5428 Storage Router includes the following routing rules in the logging table:

- All messages at notification level notice or lower are logged to all valid destinations.
- All messages at notification level info are logged to the SN 5428 log file.
- All debug messages are discarded.

Use the **no logging on** command to quickly disable logging for all destinations without modifying the SN 5428 logging table. No logging will take place until logging is re-enabled by the **logging on** command.

If you clear the logging table without returning to the factory defaults, all rules are removed from the logging table. This causes all messages to be discarded because there are no matching rules in the logging table. To resume logging, you can add new routing rules, restore a previously saved logging table, or clear the logging table back to the factory defaults.

## Viewing and Saving the Log File

You can view the entire SN 5428 log file or selected portions of the log file using the **show logging** command. You can also view the log file using the web-based GUI. If you want to analyze or search the log file in more detail, you can use FTP to retrieve a copy of the log file. See the “Using FTP with the SN 5428 Storage Router” section on page 10-28 for details.

For additional information about managing the SN 5428 log file, see the “Managing the Log File” section on page 10-26.

## Capturing the SN 5428 Configuration

You can use the **show runningconfig** or **show bootconfig** command to display the SN 5428’s current running configuration or bootable configuration. You can then redirect this display to create a script file in the SN 5428’s *script* directory. The resulting file can be used as a basis to create command scripts to automate common tasks. See the “Using Scripts to Automate Tasks” section on page 10-24 for more details.

## Using Debug Facilities

The SN 5428 includes debug facilities for SCSI routing instances. Running debug traces can impact the operation of the SN 5428. If you experience problems with a SCSI routing instance that cannot be resolved, Cisco technical support personnel may ask you to capture some debug traces. They will assist you to properly configure the SN 5428 to accomplish this task. By default, debug facilities are disabled for all SCSI routing instances.

See the **debug scsirouter** and **debug scsirouter target** commands in Chapter 11, “Command Line Interface Reference,” for more information on using the SN 5428 debug facilities.





## Command Line Interface Reference

---

The Cisco SN 5428 Storage Router provides three interfaces for operation, configuration, administration, maintenance, and support tasks: command line interface (CLI), web-based GUI, and SNMP.

This chapter documents the SN 5428 CLI. For help on the web-based GUI, point your browser to the SN 5428's management interface IP address. After logging on, click the Help link to access the online help system.

This chapter provides information about the following CLI topics:

- About CLI Commands, page 11-1
- CLI Usage Tips, page 11-1
- CLI Commands, page 11-2

### About CLI Commands

This chapter lists all possible CLI commands. However, the set of CLI commands and keywords that are available to you depends on the level of authority associated with your CLI management session and the deployment option selected for the SN 5428 Storage Router during initial configuration.

Use the **show cli** command to view all CLI commands and keywords that are valid for your current CLI management session.

### CLI Usage Tips

- Commands and keywords can be truncated at any point after they are unique.
- Use the Tab key to complete the current word.
- Use the question mark ( ? ) key to list all of the options available at that point in the command line.
- CLI commands and keywords are not case-sensitive. Commands and keywords can be entered in any case (including mixed case).
- User-defined strings are case-sensitive. User-defined strings must be entered in the appropriate case (including mixed case). Case for user-defined strings is preserved in the configuration.
- An asterisk ( \* ) at the beginning of the CLI command prompt indicates that the system configuration has been changed but not saved.

# CLI Commands

This section lists all CLI commands in alphabetical order. The **no** form of any command is shown with the primary command entry. Command information includes syntax, defaults, mode, history, usage guidelines, examples, and related commands.

## aaa authentication iscsi

To configure authentication, authorization and accounting (AAA) authentication services for iSCSI authentication of IP hosts requesting access to storage via SCSI routing instances, use the **aaa authentication iscsi** command. To disable this authentication, use the **no** form of this command.

```
aaa authentication iscsi default services1 [services2...]
```

```
no aaa authentication iscsi default
```

### Syntax Description

|                                 |                                                                             |
|---------------------------------|-----------------------------------------------------------------------------|
| <b>default</b>                  | The name of the authentication list. The list name must be <i>default</i> . |
| <i>services1 [services2...]</i> | At least one of the services described in Table 11-1.                       |

### Defaults

If iSCSI authentication is enabled and the default authentication list is not configured, only the local user database is selected. This has the same effect as the following command:

```
aaa authentication iscsi default local
```

### Command Modes

Administrator.

### Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

### Usage Guidelines

iSCSI authentication uses AAA authentication services to provide authentication of IP hosts that request access to storage from SCSI routing instances that have authentication enabled.

AAA attempts to use each service in the order listed in the iSCSI default authentication list, until authentication succeeds or fails. If the authentication service fails to find a user name match, authentication fails. If AAA returns an error (because the RADIUS or TACACS+ server is not available, for example), AAA attempts to use the next service in the list for authentication.

If either the local or local-case authentication service is the first service on the iSCSI authentication list and AAA fails to find a user name match, AAA attempts to use the next method on the list for authentication. If the local or local-case authentication service is in any other position on the list and AAA fails to find a user name match, authentication fails and access is denied. If a RADIUS or TACACS+ server fails to find a user name match (regardless of position on the iSCSI authentication list), authentication fails and access is denied.

Use the **show runningconfig** command to display the current list of authentication services.



#### Note

In Table 11-1, the **group radius** and **group tacacs+** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the servers.

**Table 11-1** *aaa authentication iSCSI default services*

| Keyword              | Description                                              |
|----------------------|----------------------------------------------------------|
| <b>group radius</b>  | Uses the list of all RADIUS servers for authentication.  |
| <b>group tacacs+</b> | Uses the list of all TACACS+ servers for authentication. |
| <b>local</b>         | Uses the local username database for authentication.     |
| <b>local-case</b>    | Uses case-sensitive local username authentication.       |
| <b>none</b>          | Uses no authentication.                                  |

**Note**

If the local authentication service is selected, the user name validation is not case-sensitive. If local-case authentication service is selected, the user name validation is case-sensitive. The password validation for both the local service and the local-case service is case-sensitive.

**Examples**

The following example creates a new AAA authentication list. When iSCSI authentication is required, AAA first tries to use the local username database for authentication. If no match is found, AAA attempts to contact a TACACS+ server. If no server is found, TACACS+ returns an error and the user is allowed access with no authentication.

```
[SN5428A]# aaa authentication iscsi default local group tacacs+ none
```

**Related Commands**

| Command                        | Description                                                          |
|--------------------------------|----------------------------------------------------------------------|
| <b>aaa test authentication</b> | Enable testing of the default AAA authentication list.               |
| <b>debug aaa</b>               | Enable debugging for the AAA authentication services.                |
| <b>radius-server host</b>      | Configure remote RADIUS servers for AAA authentication services.     |
| <b>restore aaa</b>             | Restore AAA authentication services from a saved configuration file. |
| <b>save aaa</b>                | Save the current AAA configuration information.                      |
| <b>scsirouter authenticate</b> | Enable iSCSI authentication for the named SCSI routing instance.     |
| <b>show aaa</b>                | Display AAA configuration information.                               |
| <b>tacacs-server host</b>      | Configure remote TACACS+ servers for AAA authentication services.    |

# aaa new-model

To enable the AAA access control model, issue the **aaa new-model** command.

**aaa new-model**

**no aaa new-model**

## Syntax Description

This command has no arguments or keywords.

## Defaults

AAA is enabled. AAA cannot be disabled on the SN 5428.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

This command enables the AAA access control model. The **no aaa new-model** command is available for completeness only; AAA cannot be disabled for the SN 5428.

AAA authentication services are used to provide iSCSI authentication of IP hosts requiring access to storage via SCSI routing instances. iSCSI authentication is disabled by default, and can be enabled for specific SCSI routing instances using the **scsirouter authenticate** CLI command.

## Examples

The following example initializes AAA:

```
[SN5428A] # aaa new-model
```

## Related Commands

| Command                         | Description                                                                    |
|---------------------------------|--------------------------------------------------------------------------------|
| <b>aaa authentication iscsi</b> | Configure the AAA authentication services to be used for iSCSI authentication. |
| <b>aaa test authentication</b>  | Enable testing of the default AAA authentication list.                         |
| <b>debug aaa</b>                | Enable debugging for the AAA authentication services.                          |
| <b>radius-server host</b>       | Configure remote RADIUS servers for AAA authentication services.               |
| <b>restore aaa</b>              | Restore AAA authentication services from a saved configuration file.           |
| <b>save aaa</b>                 | Save the current AAA configuration information.                                |
| <b>scsirouter authenticate</b>  | Enable iSCSI authentication for the named SCSI routing instance.               |
| <b>show aaa</b>                 | Display AAA configuration information.                                         |
| <b>tacacs-server host</b>       | Configure remote TACACS+ servers for AAA authentication services.              |

# aaa test authentication

To test authentication using the iSCSI default authentication list, use the **aaa test authentication** command.

```
aaa test authentication iscsi default username password
```

```
aaa test authentication cancel
```

| Syntax Description | iscsi default   | Use the services in the iSCSI authentication list for testing. The name of the list must be <i>default</i> . |
|--------------------|-----------------|--------------------------------------------------------------------------------------------------------------|
|                    | <i>username</i> | The user name to be tested.                                                                                  |
|                    | <i>password</i> | The password associated with the specified user name.                                                        |
|                    | <b>cancel</b>   | Cancel any outstanding test authentication requests.                                                         |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** AAA uses the services in the iSCSI default authentication list to authenticate the specified user name and password. Use this command to test iSCSI authentication prior to enabling authentication for SCSI routing instances or for troubleshooting purposes.

Use the **cancel** keyword to terminate any outstanding test authentication requests. For example, if a RADIUS or TACACS+ server is configured with a very long timeout value, you can cancel the request rather than waiting for the timeout to occur.

**Examples** The following example tests AAA authentication for the user named, *user1*, with a password of *password1*:

```
[SN5428A]# aaa test authentication iscsi default user1 password1
```

| Related Commands | Command                         | Description                                                                    |
|------------------|---------------------------------|--------------------------------------------------------------------------------|
|                  | <b>aaa authentication iscsi</b> | Configure the AAA authentication services to be used for iSCSI authentication. |
|                  | <b>debug aaa</b>                | Enable debugging for the AAA authentication services.                          |
|                  | <b>radius-server host</b>       | Configure remote RADIUS servers for AAA authentication services.               |

| <b>Command</b>                     | <b>Description</b>                                                   |
|------------------------------------|----------------------------------------------------------------------|
| <b>restore aaa</b>                 | Restore AAA authentication services from a saved configuration file. |
| <b>save aaa</b>                    | Save current AAA configuration information.                          |
| <b>scsirouter<br/>authenticate</b> | Enable iSCSI authentication for the named SCSI routing instance.     |
| <b>show aaa</b>                    | Display AAA configuration information.                               |
| <b>tacacs-server host</b>          | Configure remote TACACS+ servers for AAA authentication services.    |

# accesslist

To create an access list entity, use the **accesslist** command.

**accesslist** *name*

|                           |                |                                                                                               |
|---------------------------|----------------|-----------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>name</i>    | The name of the access list entity created by this command. Enter a maximum of 31 characters. |
| <b>Defaults</b>           | None.          |                                                                                               |
| <b>Command Modes</b>      | Administrator. |                                                                                               |
| <b>Command History</b>    | <b>Release</b> | <b>Modification</b>                                                                           |
|                           | 2.2.1          | This command was introduced.                                                                  |

## Usage Guidelines

Access lists identify the IP hosts allowed to access a common set of storage resources and are associated with specific storage targets. IP hosts can be identified by:

- IP address
- CHAP user name (used for iSCSI authentication)
- iSCSI Name

An access list can contain one or more types of identification entries. If an identification entry type exists in the access list, the IP host attempting to access the associated storage target must have a matching entry defined in the access list. For example, if an access list contains both IP address and iSCSI Name identification entry types, then every IP host that requires access to the associated set of storage resources must have a matching IP address and iSCSI Name entry in the access list.



### Note

If there is a CHAP user name entry in the access list, the SCSI routing instance used to access the storage target must also have iSCSI authentication enabled. See Chapter 8, “Configuring Authentication” for additional information about AAA and iSCSI authentication.

In a cluster environment, access list management functions are handled by a single SN 5428. To determine which SN 5428 is performing access list management functions, issue the **show cluster** command. If you issue an **accesslist** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the SN 5428 that is currently handling those functions.

For more information on operating the SN 5428 in a cluster, see Chapter 10, “Maintaining and Managing the SN 5428 Storage Router.”

**Examples**

The following command creates an access list named *webserver2*:

```
[SN5428A] # accesslist webserver2
```

**Related Commands**

| Command                             | Description                                                                            |
|-------------------------------------|----------------------------------------------------------------------------------------|
| <b>accesslist A.B.C.D/bits</b>      | Add IP addresses to an access list.                                                    |
| <b>accesslist chap-username</b>     | Add CHAP user name entries to an access list.                                          |
| <b>accesslist description</b>       | Add a description to an access list.                                                   |
| <b>accesslist iscsi-name</b>        | Add iSCSI Name entries to an access list.                                              |
| <b>delete accesslist</b>            | Delete a specific access list entry or an entire access list.                          |
| <b>restore accesslist</b>           | Restore the named access list or all access lists from the named configuration file.   |
| <b>save accesslist</b>              | Save configuration data for the named access list or all access lists.                 |
| <b>scsirouter target accesslist</b> | Associate an access list with a specific SCSI routing instance target or all targets.  |
| <b>show accesslist</b>              | Display the contents of the named access list or all access lists.                     |
| <b>show scsirouter</b>              | Display configuration and operational information for the named SCSI routing instance. |

## accesslist A.B.C.D/bits

To add the IP address and subnet mask of IP hosts to the named access list, use the **accesslist A.B.C.D/bits** command.

```
accesslist name A.B.C.D/bits | A.B.C.D/1.2.3.4 [A.B.C.D/bits | A.B.C.D/1.2.3.4] . . .
[A.B.D.F/bits | A.B.C.D/1.2.3.4]
```

### Syntax Description

|                        |                                                                                                                                                                                                            |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>            | The name of an access list to which you are adding information.                                                                                                                                            |
| <i>A.B.C.D/bits</i>    | IP address and subnet mask of the IP host being added to the access list. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The <i>/bits</i> specifies the subnet mask in CIDR style.          |
| <i>A.B.C.D/1.2.3.4</i> | The IP address and subnet mask of the IP host being added to the access list. <i>A.B.C.D</i> is the dotted quad notation of the IP address. <i>1.2.3.4</i> is the dotted quad notation of the subnet mask. |

### Defaults

None.

### Command Modes

Administrator.

### Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

### Usage Guidelines

Use the **accesslist A.B.C.D/bits** command after creating an access list to populate the list with IP address entries. Enter multiple addresses and masks, separating each by a space.

Access lists identify the IP hosts allowed to access a common set of storage resources and are associated with specific storage targets. IP hosts can be identified by:

- IP address
- CHAP user name (used for iSCSI authentication)
- iSCSI Name

An access list can contain one or more types of identification entries. If an identification entry type exists in the access list, the IP host attempting to access the associated storage target must have a matching entry defined in the access list. For example, if an access list contains both IP address and iSCSI Name identification entry types, then every IP host that requires access to the associated set of storage resources must have a matching IP address and iSCSI Name entry in the access list.

In a cluster environment, access list management functions are handled by a single SN 5428. To determine which SN 5428 is performing access list management functions, issue the **show cluster** command. If you issue an **accesslist A.B.C.D/bits** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the SN 5428 that is currently handling those functions.

For more information on operating the SN 5428 in a cluster, see Chapter 10, “Maintaining and Managing the SN 5428 Storage Router.”

### Examples

The following commands add the specified entries to the named access lists:

```
[SN5428A]# accesslist myAccessList 192.168.54.12/32 192.168.54.15/32
*[SN5428A]# accesslist Webserver5 209.165.201.1/255.255.255.0 209.165.201.5/255.255.255.0
```

### Related Commands

| Command                             | Description                                                                            |
|-------------------------------------|----------------------------------------------------------------------------------------|
| <b>accesslist</b>                   | Create an access list entity.                                                          |
| <b>accesslist chap-username</b>     | Add CHAP user name entries to an access list.                                          |
| <b>accesslist description</b>       | Add a description to an access list.                                                   |
| <b>accesslist iscsi-name</b>        | Add iSCSI Name entries to an access list.                                              |
| <b>delete accesslist</b>            | Delete a specific access list entry or an entire access list.                          |
| <b>restore accesslist</b>           | Restore the named access list or all access lists from the named configuration file.   |
| <b>save accesslist</b>              | Save configuration data for the named access list or all access lists.                 |
| <b>scsirouter target accesslist</b> | Associate an access list with a specific SCSI routing instance target or all targets.  |
| <b>show accesslist</b>              | Display the contents of the named access list or all access lists.                     |
| <b>show scsirouter</b>              | Display configuration and operational information for the named SCSI routing instance. |

# accesslist chap-username

To add the CHAP user name of IP hosts to the named access list, use the **accesslist chap-username** command.

```
accesslist name chap-username username
```

| Syntax Description |                                         |                                                                                                                         |
|--------------------|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
|                    | <i>name</i>                             | The name of an access list to which you are adding information.                                                         |
|                    | <b>chap-username</b><br><i>username</i> | The CHAP user name (used for iSCSI authentication purposes) configured for the IP host that requires access to storage. |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.3.1   | This command was introduced. |

**Usage Guidelines** Use the **accesslist chap-username** command after creating an access list to populate the list with iSCSI user name entries.

Access lists identify the IP hosts allowed to access a common set of storage resources and are associated with specific storage targets. IP hosts can be identified by:

- IP address
- CHAP user name (used for iSCSI authentication)
- iSCSI Name

An access list can contain one or more types of identification entries. If an identification entry type exists in the access list, the IP host attempting to access the associated storage target must have a matching entry defined in the access list. For example, if an access list contains both IP address and iSCSI Name identification entry types, then every IP host that requires access to the associated set of storage resources must have a matching IP address and iSCSI Name entry in the access list.

The iSCSI driver is configured with a user name and password when SCSI routing instances have iSCSI authentication enabled. AAA security services authenticate the IP host using the iSCSI user name and password. An access list can also use the iSCSI user name (CHAP user name) to identify IP hosts allowed access to a common set of storage resources.



**Note** If there is a CHAP user name entry in the access list, the SCSI routing instance used to access the storage target must also have iSCSI authentication enabled. See Chapter 8, “Configuring Authentication” for additional information about AAA and iSCSI authentication.

In a cluster environment, access list management functions are handled by a single SN 5428. To determine which SN 5428 is performing access list management functions, issue the **show cluster** command. If you issue an **accesslist chap-username** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the SN 5428 that is currently handling those functions.

For more information on operating the SN 5428 in a cluster, see Chapter 10, “Maintaining and Managing the SN 5428 Storage Router.”

### Examples

The following commands add the specified entries to the named access lists:

```
[SN5428A]# accesslist myAccessList chap-username foo
*[SN5428A]# accesslist Webserver5 chap-username server1
```

### Related Commands

| Command                             | Description                                                                            |
|-------------------------------------|----------------------------------------------------------------------------------------|
| <b>accesslist</b>                   | Create an access list entity.                                                          |
| <b>accesslist A.B.C.D/bits</b>      | Add IP addresses to an access list.                                                    |
| <b>accesslist description</b>       | Add a description to an access list.                                                   |
| <b>accesslist iscsi-name</b>        | Add iSCSI Names to an access list.                                                     |
| <b>delete accesslist</b>            | Delete a specific access list entry or an entire access list.                          |
| <b>restore accesslist</b>           | Restore the named access list or all access lists from the named configuration file.   |
| <b>save accesslist</b>              | Save configuration data for the named access list or all access lists.                 |
| <b>scsirouter target accesslist</b> | Associate an access list with a specific SCSI routing instance target or all targets.  |
| <b>show accesslist</b>              | Display the contents of the named access list or all access lists.                     |
| <b>show scsirouter</b>              | Display configuration and operational information for the named SCSI routing instance. |

# accesslist description

To add a description to an existing access list entity, use the **accesslist description** command.

```
accesslist name description "text"
```

| Syntax Description             |                                                                                                                                                       |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>                    | The name of an existing access list entity.                                                                                                           |
| <b>description</b> <i>text</i> | User-defined identification information associated with this access list. Enclose the description string in quotes. Enter a maximum of 64 characters. |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Access lists identify the IP hosts allowed to access a common set of storage resources and are associated with specific storage targets. IP hosts can be identified by:

- IP address
- CHAP user name (used for iSCSI authentication)
- iSCSI Name

An access list can contain one or more types of identification entries. If an identification entry type exists in the access list, the IP host attempting to access the associated storage target must have a matching entry defined in the access list. For example, if an access list contains both IP address and iSCSI Name identification entry types, then every IP host that requires access to the associated set of storage resources must have a matching IP address and iSCSI Name entry in the access list.

In a cluster environment, access list management functions are handled by a single SN 5428. To determine which SN 5428 is performing access list management functions, issue the **show cluster** command. If you issue an **accesslist description** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the SN 5428 that is currently handling those functions.

For more information on operating the SN 5428 in a cluster, see Chapter 10, “Maintaining and Managing the SN 5428 Storage Router.”

**Examples** The following command adds a description to the access list named *webserver2*:

```
[SN5428A]# accesslist webserver2 description "Access list for company web servers"
```

| <b>Related Commands</b> | <b>Command</b>                      | <b>Description</b>                                                                     |
|-------------------------|-------------------------------------|----------------------------------------------------------------------------------------|
|                         | <b>accesslist</b>                   | Create an access list entity.                                                          |
|                         | <b>accesslist A.B.C.D/bits</b>      | Add IP addresses to an access list.                                                    |
|                         | <b>accesslist chap-username</b>     | Add CHAP user name entries to an access list.                                          |
|                         | <b>accesslist iscsi-name</b>        | Add iSCSI Name entries to an access list.                                              |
|                         | <b>delete accesslist</b>            | Delete a specific access list entry, or an entire access list.                         |
|                         | <b>restore accesslist</b>           | Restore the named access list or all access lists from the named configuration file.   |
|                         | <b>save accesslist</b>              | Save configuration data for the named access list or all access lists.                 |
|                         | <b>scsirouter target accesslist</b> | Associate an access list with a specific SCSI routing instance target or all targets.  |
|                         | <b>show accesslist</b>              | Display the contents of the named access list or all access lists.                     |
|                         | <b>show scsirouter</b>              | Display configuration and operational information for the named SCSI routing instance. |

## accesslist iscsi-name

To add the iSCSI Name of IP hosts to the named access list, use the **accesslist iscsi-name** command.

```
accesslist name iscsi-name string
```

| Syntax Description              |                                                                                                                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>                     | The name of an access list to which you are adding information.                                                                                                                                                                                                                 |
| <b>iscsi-name</b> <i>string</i> | The iSCSI Name of IP host that requires access to storage. The iSCSI Name is a UTF-8 character string based on iSCSI functional requirements. It is a location-independent permanent identifier for an iSCSI node. An iSCSI node can be either an initiator, a target, or both. |

| Defaults |       |
|----------|-------|
|          | None. |

| Command Modes |                |
|---------------|----------------|
|               | Administrator. |

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.3.1   | This command was introduced. |

| Usage Guidelines |                                                                                                                          |
|------------------|--------------------------------------------------------------------------------------------------------------------------|
|                  | Use the <b>accesslist iscsi-name</b> command after creating an access list to populate the list with iSCSI Name entries. |

If you do not know the iSCSI Name of the IP host, configure the IP host and attempt to access the desired storage targets. Use the **show scsirouter** command with the **host table** keywords to then display the iSCSI Name (along with the initiator alias, IP address and CHAP user name) of all IP hosts that have attempted to access storage resources.

Access lists identify the IP hosts allowed to access a common set of storage resources and are associated with specific storage targets. IP hosts can be identified by:

- IP address
- CHAP user name (used for iSCSI authentication)
- iSCSI Name

An access list can contain one or more types of identification entries. If an identification entry type exists in the access list, the IP host attempting to access the associated storage target must have a matching entry defined in the access list. For example, if an access list contains both IP address and iSCSI Name identification entry types, then every IP host that requires access to the associated set of storage resources must have a matching IP address and iSCSI Name entry in the access list.

In a cluster environment, access list management functions are handled by a single SN 5428. To determine which SN 5428 is performing access list management functions, issue the **show cluster** command. If you issue an **accesslist iscsi-name** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the SN 5428 that is currently handling those functions.

For more information on operating the SN 5428 in a cluster, see Chapter 10, “Maintaining and Managing the SN 5428 Storage Router.”

### Examples

The following command add the specified iSCSI Name to the access list named *foo*:

```
[SN5428A] # accesslist foo iscsi-name ign.1987-05.com.cisco.01.88e8b25a6bf3372a34567123f
```

### Related Commands

| Command                             | Description                                                                            |
|-------------------------------------|----------------------------------------------------------------------------------------|
| <b>accesslist</b>                   | Create an access list entity.                                                          |
| <b>accesslist A.B.C.D/bits</b>      | Add IP addresses to an access list.                                                    |
| <b>accesslist chap-username</b>     | Add CHAP user name entries to an access list.                                          |
| <b>accesslist description</b>       | Add a description to an access list.                                                   |
| <b>delete accesslist</b>            | Delete a specific access list entry or an entire access list.                          |
| <b>restore accesslist</b>           | Restore the named access list or all access lists from the named configuration file.   |
| <b>save accesslist</b>              | Save configuration data for the named access list or all access lists.                 |
| <b>scsirouter target accesslist</b> | Associate an access list with a specific SCSI routing instance target or all targets.  |
| <b>show accesslist</b>              | Display the contents of the named access list or all access lists.                     |
| <b>show scsirouter</b>              | Display configuration and operational information for the named SCSI routing instance. |

# admin contactinfo

To provide basic contact information for the system administrator of this SN 5428 Storage Router, use the **admin contactinfo** command.

```
admin contactinfo [name "string" | email "string" | phone "string" | pager "string"]
```

```
admin contact info name "string" email "string" phone "string" pager "string"
```

## Syntax Description

|                            |                                                                                                             |
|----------------------------|-------------------------------------------------------------------------------------------------------------|
| <b>name</b> <i>string</i>  | (Optional) The name of the SN 5428 administrator.                                                           |
| <b>email</b> <i>string</i> | (Optional) The e-mail address of the SN 5428 administrator. This is an address to which alerts may be sent. |
| <b>phone</b> <i>string</i> | (Optional) The phone number of the SN 5428 administrator.                                                   |
| <b>pager</b> <i>string</i> | (Optional) The pager number of the SN 5428 administrator.                                                   |

## Defaults

None.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

Use the **admin contactinfo** command to provide site-specific information for the system administrator of the SN 5428. The command accepts each parameter separately, or all parameters together. If all parameters are specified, they must be in the sequence shown. Usage is completely site-specific.

Enclose each string containing spaces in single or double quotes. If a string contains a single quote, enclose it in double quotes; if it contains a double quote, enclose it in single quotes. A string cannot contain both single and double quotes.

## Examples

The following commands set the system administrator name and e-mail address:

```
[SN5428A]# admin contactinfo name "Pat Hurley"
[SN5428A]# admin contactinfo email "hurley@abc123z.com"
```

The following command sets all system administrator contact information:

```
[SN5428A]# admin contactinfo name "Chris Smith" email "chris.smith@zxy478x.com" phone
"123.555.5555 ext 97" pager "555.3444 pin 2234"
```

| <b>Related Commands</b> | <b>Command</b>        | <b>Description</b>                                                                                      |
|-------------------------|-----------------------|---------------------------------------------------------------------------------------------------------|
|                         | <b>admin password</b> | Set the login password for administrative access to the SN 5428 management interface.                   |
|                         | <b>save all</b>       | Save all configuration information, including the system administrator contact information.             |
|                         | <b>save system</b>    | Save selected system configuration information, including the system administrator contact information. |
|                         | <b>show admin</b>     | Display system administrator contact information.                                                       |

# admin password

To set the password used for administrative access to the SN 5428 Storage Router management interface, use the **admin password** command. Access may be via Telnet (for CLI), or web-based GUI.

**admin password** *string*

## Syntax Description

|               |                                                                                                                                                                                                                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>string</i> | The password associated with administrative access to the SN 5428 management interface. The string can be enclosed in quotes, and must be enclosed in quotes if the password includes one or more spaces. A string value of "" clears the password. The default password is <i>cisco</i> . |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Defaults

The default password is *cisco*.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

The SN 5428's management interface is password protected. You must enter passwords when accessing the SN 5428 via Telnet (for CLI) or web-based GUI. The Monitor mode password provides view-only access to the management interface, while the Administrator mode password allows the user to create entities and make changes to the configuration of the SN 5428. Password protection can also be extended to the SN 5428 console, using the **restrict console** command.

The password can contain one or more spaces, if the password string is enclosed in quotes. A string value of "" clears the password, effectively setting it to nothing.



### Note

The password is displayed in clear text as the command is entered, but it is changed to a series of number signs (#####) when the change is acknowledged.

## Examples

The following example sets the Administrator mode password to *foo73G*. All passwords are case sensitive.

```
[SN5428A]# admin password foo73G
```

The following example sets the Administrator mode password to "xZm! 673":

```
[SN5428A]# admin password "xZm! 673"
```

| <b>Related Commands</b> | <b>Command</b>          | <b>Description</b>                                                                          |
|-------------------------|-------------------------|---------------------------------------------------------------------------------------------|
|                         | <b>enable</b>           | Enter Administrator mode.                                                                   |
|                         | <b>exit</b>             | Leave Administrator mode and enter Monitor mode.                                            |
|                         | <b>monitor password</b> | Set the login password for view-only access to the SN 5428 management interface.            |
|                         | <b>restrict console</b> | Enable or disable password checking on the SN 5428 console interface.                       |
|                         | <b>save all</b>         | Save all configuration information, including the administrator password.                   |
|                         | <b>save system</b>      | Save selected system configuration information, including the Administrator mode passwords. |
|                         | <b>setup access</b>     | Run the wizard to configure Monitor mode and Administrator mode passwords.                  |

# cdp enable

To enable Cisco Discovery Protocol (CDP) on the SN 5428 Storage Router, use the **cdp enable** command. To disable CDP on the SN 5428, use the **no** form of this command.

**cdp enable**

**no cdp enable**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** CDP is enabled.

---

**Command Modes** Administrator.

---

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

---



---

**Usage Guidelines** CDP is enabled by default in order to send or receive CDP information. CDP can be switched on or off for each specific interface. See the **cdp interface** command for more information.

---

**Examples** The following example enables CDP on the SN 5428:

```
[SN5428A] # cdp enable
```

---

| Related Commands | Command              | Description                                                                                                                    |
|------------------|----------------------|--------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>cdp holdtime</b>  | Specify the amount of time the receiving device should hold a CDP packet from the SN 5428 Storage Router before discarding it. |
|                  | <b>cdp interface</b> | Switch CDP on or off for the specified interface.                                                                              |
|                  | <b>cdp timer</b>     | Specify the amount of time between transmissions of CDP packets from the SN 5428 Storage Router.                               |

---

# cdp holdtime

To specify the amount of time the receiving device should hold a CDP packet from the SN 5428 Storage Router before discarding it, use the **cdp holdtime** command. To revert to the default setting, use the **no** form of this command.

**cdp holdtime** *nn*

**no cdp holdtime**

## Syntax Description

|           |                                                                |
|-----------|----------------------------------------------------------------|
| <i>nn</i> | The holdtime to be sent in the CDP update packets, in seconds. |
|-----------|----------------------------------------------------------------|

## Defaults

The default holdtime is 180 seconds.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

The CDP holdtime must be set to a higher number of seconds than the time between CDP transmissions, which is set using the **cdp timer** command.

## Examples

The following example sets the CDP holdtime to 60, meaning that the CDP packet being sent from the SN 5428 should be held by the receiving device for 60 seconds before being discarded. You may want to set the holdtime lower than the default setting of 180 seconds if information about the SN 5428 changes frequently.

```
[SN5428A]# cdp holdtime 60
```

## Related Commands

| Command              | Description                                                                                      |
|----------------------|--------------------------------------------------------------------------------------------------|
| <b>cdp enable</b>    | Enable or disable CDP on the SN 5428 Storage Router.                                             |
| <b>cdp interface</b> | Switch CDP on or off for the specified interface.                                                |
| <b>cdp timer</b>     | Specify the amount of time between transmissions of CDP packets from the SN 5428 Storage Router. |

# cdp interface

To enable CDP for a specific interface, use the **cdp interface** command. To disable CDP for a specific interface, use the **no** form of this command.

**cdp interface** *if-name* **enable**

**no cdp interface** *if-name* **enable**

|                           |                |                                                                                                                                                                                                                                                                                                      |
|---------------------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>if-name</i> | The name of the interface for which you are enabling or disabling CDP. CDP can be enabled on the management (mgmt), HA, and Gigabit Ethernet (ge2) interfaces. When you type the <b>cdp interface ?</b> command, the CLI lists the interfaces available. You cannot specify a nonexistent interface. |
|---------------------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |                                    |
|-----------------|------------------------------------|
| <b>Defaults</b> | CDP is enabled for all interfaces. |
|-----------------|------------------------------------|

|                      |                |
|----------------------|----------------|
| <b>Command Modes</b> | Administrator. |
|----------------------|----------------|

|                        |                |                              |
|------------------------|----------------|------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|                        | 2.2.1          | This command was introduced. |

|                         |                                                                                                                                             |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | CDP must be enabled for the SN 5428 Storage Router, using the <b>cdp enable</b> command, before it can be enabled for a specific interface. |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|

**Examples** The following example enables CDP for the Gigabit Ethernet interface, *ge2*:

```
[SN5428A] # cdp interface ge2 enable
```

The following example disables CDP for the management interface:

```
[SN5428A] # no cdp interface mgmt enable
```

|                         |                     |                                                                                                                                |
|-------------------------|---------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Related Commands</b> | <b>Command</b>      | <b>Description</b>                                                                                                             |
|                         | <b>cdp enable</b>   | Enable or disable CDP on the SN 5428 Storage Router.                                                                           |
|                         | <b>cdp holdtime</b> | Specify the amount of time the receiving device should hold a CDP packet from the SN 5428 Storage Router before discarding it. |
|                         | <b>cdp timer</b>    | Specify the amount of time between transmissions of CDP packets from the SN 5428 Storage Router.                               |

# cdp timer

To specify the amount of time between transmissions of CDP packets from the SN 5428 Storage Router, use the **cdp timer** command. To revert to the default setting, use the **no** form of this command.

**cdp timer** *nn*

**no cdp timer**

|                           |                                                                                                                                                                                                                                                                                          |                                                                                                                                |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>nn</i>                                                                                                                                                                                                                                                                                | The number of seconds between transmissions of CDP packets from the SN 5428 Storage Router.                                    |
| <b>Defaults</b>           | The default is 60 seconds.                                                                                                                                                                                                                                                               |                                                                                                                                |
| <b>Command Modes</b>      | Administrator.                                                                                                                                                                                                                                                                           |                                                                                                                                |
| <b>Command History</b>    | <b>Release</b>                                                                                                                                                                                                                                                                           | <b>Modification</b>                                                                                                            |
|                           | 2.2.1                                                                                                                                                                                                                                                                                    | This command was introduced.                                                                                                   |
| <b>Usage Guidelines</b>   | The time between CDP transmissions must be set to a lower number than the CDP holdtime, which is set using the <b>cdp holdtime</b> command. There is a trade-off between sending more frequent CDP updates and bandwidth utilization.                                                    |                                                                                                                                |
| <b>Examples</b>           | <p>The following example sets the CDP timer to 90, meaning that CDP updates are sent every 90 seconds, which is less frequently than the default of 60 seconds. You may want to make this change if you are concerned about preserving bandwidth.</p> <pre>[SN5428A]# cdp timer 90</pre> |                                                                                                                                |
| <b>Related Commands</b>   | <b>Command</b>                                                                                                                                                                                                                                                                           | <b>Description</b>                                                                                                             |
|                           | <b>cdp enable</b>                                                                                                                                                                                                                                                                        | Enable or disable CDP on the SN 5428 Storage Router.                                                                           |
|                           | <b>cdp holdtime</b>                                                                                                                                                                                                                                                                      | Specify the amount of time the receiving device should hold a CDP packet from the SN 5428 Storage Router before discarding it. |
|                           | <b>cdp interface</b>                                                                                                                                                                                                                                                                     | Switch CDP on or off for the specified interface.                                                                              |

# clear conf

To return certain configuration settings to factory defaults, use the **clear conf** wizard. The **clear conf** wizard prompts the user to enter the Administrator mode password and then to indicate which settings to restore to factory defaults.

## clear conf

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** The **clear conf** wizard is only available when the storage router is deployed for SCSI routing. If the storage router is deployed for transparent SCSI routing, use the **clear conf {all | system}** command to return the storage router configuration to factory default settings.

Follow these guidelines when using the **clear conf** wizard:

- Select **apps** to remove all SCSI routing instances but retain system configuration settings.
- Select **system** to remove all SCSI routing instances and system configuration settings.
- Select **saved** to delete all backup configuration files from disk.
- Select **all** to remove all SCSI routing instances, system configuration settings, and saved configuration files.

The system will reboot if you select **apps**, **system**, or **all**.

System configuration settings include:

- The management and HA interface IP addresses
- Configuration information for Fibre Channel interfaces
- Saved zone configuration information
- Domain name servers
- NTP server and time zone information
- SNMP information
- Administrator and Monitor passwords, and administrator contact information
- AAA authentication configuration information
- VLAN and VTP information

Deleting system configuration makes the SN 5428 unavailable to Telnet or web-based GUI sessions until the management interface is reconfigured with an IP address via a console connection. See the “Initial System Configuration Script” section in Chapter 2, “First-Time Configuration,” for details.

### Examples

The following example removes all SCSI routing instances from the SN 5428. The system configuration settings are retained.

```
[SN5428_A1]# clear conf
```

```
Enter admin password: *****
```

This process can restore factory default settings for the SN5428.

- \* Select "apps" to remove active applications and retain system configuration settings.
- \* Select "system" to remove active applications and system configuration settings.
- \* Select "saved" to remove all backup configurations from disk.
- \* Select "all" to remove active applications, system configuration, and saved configurations.

The system configuration includes the management port, dns, admin and monitor login, ntp, and snmp. You will need to use the console to reconfigure the management port if you erase the system configuration.

The system will reboot if you select "apps", "system", or "all".

```
Erase what? [apps/system/saved/all/cancel (cancel)] apps
```

```
Configuration cleared. System configuration settings retained.
System halting.....!
```

```
System has been halted
```

### Related Commands

| Command              | Description                                                                |
|----------------------|----------------------------------------------------------------------------|
| <b>setup access</b>  | Run the wizard to configure Monitor mode and Administrator mode passwords. |
| <b>setup cluster</b> | Change the configuration of the SN 5428's high availability environment.   |
| <b>setup mgmt</b>    | Run the wizard to configure the management interface.                      |
| <b>setup netmgmt</b> | Run the wizard to configure network management.                            |
| <b>setup scsi</b>    | Run the wizard to configure a SCSI routing instance.                       |
| <b>setup time</b>    | Run the wizard to configure the system date and time.                      |

# clear conf {all | system}

To return certain configuration settings to factory defaults, use the **clear conf {all | system}** command.

**clear conf {all | system} password**

| Syntax Description |  |                                                                                                                                                                                                    |
|--------------------|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>all</b>         |  | Remove all storage router configuration information, including system configuration settings, saved configuration files, SCSI routing instances, access lists, and cluster configuration settings. |
| <b>system</b>      |  | Remove all system configuration settings, SCSI routing instances, access lists and cluster configuration settings. Saved configuration files will be retained.                                     |
| <i>password</i>    |  | The Administrator mode password.                                                                                                                                                                   |

| Defaults      | None.          |
|---------------|----------------|
| Command Modes | Administrator. |

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

| Usage Guidelines | <p>System configuration settings include:</p> <ul style="list-style-type: none"> <li>• The management and HA interface IP addresses</li> <li>• Configuration information for Fibre Channel interfaces</li> <li>• Saved zone configuration information</li> <li>• Domain name servers</li> <li>• NTP server and time zone information</li> <li>• SNMP information</li> <li>• Administrator and Monitor passwords, and administrator contact information</li> <li>• AAA authentication information</li> <li>• VLAN and VTP information</li> </ul> |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Issuing the **clear conf** command with either the **system** or **all** keyword causes the storage router to reboot.

Deleting system configuration makes the storage router unavailable to Telnet or web-based GUI sessions until the management interface is reconfigured with an IP address via a console connection. See the “Initial System Configuration Script” section in Chapter 2, “First-Time Configuration,” for details.

**Examples**

The following example removes all storage router configuration information, returning the storage router to its initial default configuration. The example uses the default Administrator mode password, *cisco*.

```
[SN5428_A1]# clear conf all cisco
```

```
Clearing configuration...
```

```
Current configuration and named configurations cleared.
```

```
System halting.....
```

**Related Commands**

| Command              | Description                                                                     |
|----------------------|---------------------------------------------------------------------------------|
| <b>clear conf</b>    | Run the wizard to reset the storage router to factory defaults.                 |
| <b>setup access</b>  | Run the wizard to configure Monitor mode and Administrator mode passwords.      |
| <b>setup cluster</b> | Change the configuration of the storage router's high availability environment. |
| <b>setup mgmt</b>    | Run the wizard to configure the management interface.                           |
| <b>setup netmgmt</b> | Run the wizard to configure network management.                                 |
| <b>setup scsi</b>    | Run the wizard to configure a SCSI routing instance.                            |
| <b>setup time</b>    | Run the wizard to configure the system date and time.                           |

# clear counters interface

To clear all counters associated with the specified interface, or all interfaces, use the **clear counters interface** command.

```
clear counters interface {if-name | all}
```

| Syntax Description |  |                                                                                                                                                                                                                                                                                                                                |
|--------------------|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>if-name</i>     |  | The name of the interface. Counters can be cleared for the management (mgmt), Fibre Channel (fc?) and Gigabit Ethernet (ge?) interfaces, and the HA interface (if available). When you type the <b>clear counters interface ?</b> command, the CLI lists the interfaces available. You cannot specify a nonexistent interface. |
| <b>all</b>         |  | Clear counters for all interfaces.                                                                                                                                                                                                                                                                                             |

| Defaults |       |
|----------|-------|
|          | None. |

| Command Modes |                           |
|---------------|---------------------------|
|               | Administrator or Monitor. |

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

| Usage Guidelines |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <p>This command resets all accumulated operational statistics for the specified interface. Operational statistics can include counters for packets received and transmitted, collisions, octets, multicast packets, dropped and unsupported protocol, exception status IOCBs (such as LIP reset aborts, port unavailable or logged out, DMA errors, port configuration changed, command timeout, data overrun, write or read data underrun, and queue full), Fibre Channel errors, and other general events.</p> <p>Clear counters before beginning a troubleshooting session, so you can quickly identify the counters that are changing.</p> |

| Examples |                                                                                                                                 |
|----------|---------------------------------------------------------------------------------------------------------------------------------|
|          | <p>The following example clears all accumulated operational statistics counters for the Fibre Channel interface <i>fc1</i>.</p> |

```
[SN5428A]# clear counters interface fc1
```

| Related Commands | Command               | Description                                                                                      |
|------------------|-----------------------|--------------------------------------------------------------------------------------------------|
|                  | <b>show interface</b> | Display operational and configuration information for the specified interface or all interfaces. |

# clear counters scsirouter

To reset accumulated operational statistics for the specified SCSI routing instance, use the **clear counters scsirouter** command.

```
clear counters scsirouter {name | all} {connection | host | target {name | all}}
```

| Syntax Description        |  |                                                                           |
|---------------------------|--|---------------------------------------------------------------------------|
| <i>name</i>               |  | The name of the SCSI routing instance for which counters will be cleared. |
| <b>all</b>                |  | Clear counters for all SCSI routing instances.                            |
| <b>connection</b>         |  | Clear operational statistics related to connections only.                 |
| <b>host</b>               |  | Clear operational statistics related to currently connected hosts only.   |
| <b>target</b> <i>name</i> |  | Clear operational statistics related to the specified target.             |
| <b>target all</b>         |  | Clear operational statistics related to all targets.                      |

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** This command resets the specified operational statistics. It does not display the accumulated statistics before resetting the counters.

Clear counters before beginning a troubleshooting session, so you can quickly identify the counters that are changing.

**Examples** The following example clears the connection counters for the SCSI routing instance *myScsi1*.

```
[SN5428A]# clear counters scsirouter myScsi1 connection
```

| Related Commands | Command                | Description                                                                            |
|------------------|------------------------|----------------------------------------------------------------------------------------|
|                  | <b>show scsirouter</b> | Display configuration and operational information for the named SCSI routing instance. |

# clear fc

To clear the switch log files of all entries or to clear stored zoning configuration information, issue the **clear fc** command.

```
clear fc {devlog | syslog | zones}
```

| Syntax Description | devlog | The switch development log file.                                                                                                                                                           |
|--------------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | syslog | The switch system log file.                                                                                                                                                                |
|                    | zones  | Zoning changes received from switches in the fabric and stored by the SN 5428. All ports operating as E_Ports must be inactive or disabled before the zoning configuration can be cleared. |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                        |
|-----------------|---------|-------------------------------------|
|                 | 2.2.1   | This command was introduced.        |
|                 | 2.3.1   | The keyword <b>zones</b> was added. |

**Usage Guidelines** Clear the switch development or system log file if it is large, or if you are going to perform testing and want to be sure the switch log files only reflects information from the testing session.

Clear zoning configuration if you are moving the SN 5428 from one FC switched zoned fabric to another or removing a switch from the fabric, or when other network changes have been made that render the saved zoning information inaccurate. All ports operating as E\_Ports must be inactive or disabled prior to clearing zone configuration. A warning message displays if the **clear fc zones** command is issued when there is an active E\_Port on the SN 5428 Storage Router.

**Examples** The following example clears the switch development log files:

```
[SN5428A]# clear fc devlog
```

The following example clears the switch system log files:

```
[SN5428A]# clear fc syslog
```

The following example clears all saved zoning information:

```
[SN5428A]# clear fc zones
```

**Related Commands**

| <b>Command</b>                      | <b>Description</b>                                                                 |
|-------------------------------------|------------------------------------------------------------------------------------|
| <b>interface fc devlog</b>          | Specify logging parameters for the switch development log file.                    |
| <b>interface fc domainid</b>        | Set the SN 5428's domain ID for FC switched fabric zoning.                         |
| <b>interface fc syslog</b>          | Specify logging parameters for the switch system log file.                         |
| <b>interface fc zoning autosave</b> | Configure the SN 5428 to participate in FC switched fabric zones.                  |
| <b>show debug fc</b>                | Display internal Fibre Channel interface parameters, including switch log entries. |

# clear log

To clear the SN 5428 Storage Router log file of all entries, issue the **clear log** command.

```
clear log
```

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** None.

---

**Command Modes** Administrator.

---

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1.  | This command was introduced. |

---



---

**Usage Guidelines** Clear the SN 5428 log file if it is large, or if you are going to perform testing and want to be sure the log file only reflects information from the testing session.

---

**Examples** The following example clears all entries from the SN 5428 log file:

```
[SN5428A]# clear log
```

---

| Related Commands | Command              | Description                                                                                                                         |
|------------------|----------------------|-------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>logging level</b> | Add rule entries to route SN 5428 event, debug and trace messages to various destinations based on facility and notification level. |
|                  | <b>show logging</b>  | Display the routing rules in the logging table and the contents of the SN 5428 log file.                                            |

---

# clear logging table

To clear the SN 5428 Storage Router logging table of all entries, or to reset the table to factory defaults, issue the **clear logging table** command.

**clear logging table [to factory\_defaults]**

|                           |                            |                                                                               |
|---------------------------|----------------------------|-------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>to factory_defaults</b> | Return the SN 5428 logging table to the factory default logging rule entries. |
|---------------------------|----------------------------|-------------------------------------------------------------------------------|

|                 |       |
|-----------------|-------|
| <b>Defaults</b> | None. |
|-----------------|-------|

|                      |                |
|----------------------|----------------|
| <b>Command Modes</b> | Administrator. |
|----------------------|----------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 2.3.1.         | This command was introduced. |

**Usage Guidelines**

Use this command to remove all rules for routing SN 5428 event messages. If the logging table is cleared, logging is still enabled but all messages will be discarded.

To return the logging table to the factory default logging rules, use the **to factory\_defaults** keywords. The factory default logging rules are as follows:

- All messages from all facilities at notice level or lower levels are logged to all destinations.
- All messages from all facilities at info level or lower levels are logged to the SN 5428 log file.

The following example clears all entries from the SN 5428 logging table and returns the table to the default logging rules:

```
[SN5428A]# clear logging table to factory_defaults
```

| <b>Related Commands</b> | <b>Command</b>        | <b>Description</b>                                                                                                                  |
|-------------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------|
|                         | <b>delete logging</b> | Delete a rule from the logging table.                                                                                               |
|                         | <b>logging #?</b>     | Insert a routing rule entry into the SN 5428 logging table.                                                                         |
|                         | <b>logging level</b>  | Add rule entries to route SN 5428 event, debug and trace messages to various destinations based on facility and notification level. |
|                         | <b>logging on</b>     | Enable or temporarily disable logging of SN 5428 event message.                                                                     |
|                         | <b>show logging</b>   | Display the routing rules in the logging table and the contents of the SN 5428 log file.                                            |

# clear scsirouter failover

To clear the designated primary or secondary SN 5428 from the HA failover list for the specified SCSI routing instance, use the **clear scsirouter failover** command.

```
clear scsirouter name failover {primary | secondary}
```

## Syntax Description

|                  |                                                               |
|------------------|---------------------------------------------------------------|
| <i>name</i>      | The name of the SCSI routing instance.                        |
| <b>primary</b>   | Delete the current primary SN 5428 from the HA failover list. |
| <b>secondary</b> | Delete the secondary SN 5428 from the HA failover list.       |

## Defaults

None.

## Command Modes

Administrator or Monitor.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

Use the **clear scsirouter failover** command to reset the primary or secondary SN 5428 on the HA failover list for the specified SCSI routing instance. If there is no primary or secondary SN 5428 on the HA failover list when the SCSI routing instance fails over, the cluster attempts to run the instance on the first SN 5428 that is available.

Use the **scsirouter failover** command to add a SN 5428 to the HA failover list.



### Note

This command causes the SCSI routing instance configuration information to be saved and all nodes in the cluster to be updated.

## Examples

The following example removes the current primary SN 5428 from the HA failover list for SCSI routing instance *foo*:

```
[SN5428A]# clear scsirouter foo failover primary
```

**Related Commands**

| <b>Command</b>             | <b>Description</b>                                                               |
|----------------------------|----------------------------------------------------------------------------------|
| <b>failover scsirouter</b> | Cause the named SCSI routing instance to cease running on the SN 5428.           |
| <b>scsirouter failover</b> | Add the SN 5428 to the HA failover list for the specified SCSI routing instance. |

# clock set

To set the SN 5428 system clock to the given date and time, use the **clock set** command. Date and time information is used for log files and the user interface.

**clock set** *hh:mm:ss mm dd yyyy*

|                           |                            |                                                                                                                                  |
|---------------------------|----------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>hh:mm:ss mm dd yyyy</i> | The current time in hours, minutes, and seconds, followed by the current month, day, and year. For example, 13:55:22 06 22 2001. |
|---------------------------|----------------------------|----------------------------------------------------------------------------------------------------------------------------------|

|                 |       |
|-----------------|-------|
| <b>Defaults</b> | None. |
|-----------------|-------|

|                      |                |
|----------------------|----------------|
| <b>Command Modes</b> | Administrator. |
|----------------------|----------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 2.2.1          | This command was introduced. |

|                         |                                                                                                                                 |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | If the SN 5428 should synchronize its date and time with a network time protocol (NTP) server, see the <b>ntp peer</b> command. |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------|

|                 |                                                                                                                                           |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Examples</b> | The following example sets the SN 5428 date and time to June 22, 2001 at 14:39:00.<br><pre>[SN5428A]# clock set 14:39:00 06 22 2001</pre> |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------|

| <b>Related Commands</b> | <b>Command</b>        | <b>Description</b>                                                                                      |
|-------------------------|-----------------------|---------------------------------------------------------------------------------------------------------|
|                         | <b>clock timezone</b> | Specify the time zone for the SN 5428.                                                                  |
|                         | <b>ntp peer</b>       | Specify the name or IP address of the NTP server with which the SN 5428 will synchronize date and time. |
|                         | <b>setup time</b>     | Run the wizard to configure the system date and time.                                                   |
|                         | <b>show clock</b>     | Display the current system date and time, including the system timezone.                                |

# clock timezone

To specify the time zone for the SN 5428, use the **clock timezone** command.

```
clock timezone {string | ?}
```

| Syntax Description | string | A character string representing the time zone of the SN 5428. For example, <i>America/Chicago</i> or <i>Europe/Amsterdam</i> .               |
|--------------------|--------|----------------------------------------------------------------------------------------------------------------------------------------------|
|                    | ?      | Display a list of all valid time zones. Use any time zone in this list for the <i>string</i> parameter to set the SN 5428 to that time zone. |

|          |       |
|----------|-------|
| Defaults | None. |
|----------|-------|

|               |                |
|---------------|----------------|
| Command Modes | Administrator. |
|---------------|----------------|

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Unless you specify the time zone, the clock setting is assumed to be in Universal time, also known as Greenwich Mean Time (GMT).

You can use the **setup time** wizard to select a time zone, set the clock and date, and identify an NTP server for the SN 5428.

To use the **clock timezone** command, you must know the appropriate time zone string. Use the “?” to display a list of valid time zone strings.

**Examples** The following example sets the SN 5428 time zone to US/Mountain:

```
[SN5428A]# clock timezone US/Mountain
```

| Related Commands | Command           | Description                                                                                             |
|------------------|-------------------|---------------------------------------------------------------------------------------------------------|
|                  | <b>clock set</b>  | Set the SN 5428 system clock.                                                                           |
|                  | <b>ntp peer</b>   | Specify the name or IP address of the NTP server with which the SN 5428 will synchronize date and time. |
|                  | <b>setup time</b> | Run the wizard to configure the system date and time.                                                   |
|                  | <b>show clock</b> | Display the current system date and time, including the system time zone.                               |

# copy

To copy the named configuration file or script file from the specified location to the *savedconfig* or *script* directory, or from the SN 5428 to the specified location, use the **copy** command. The exchange is via HTTP or TFTP. When copying files to the SN 5428, any file of the same name in the *savedconfig* or *script* directory is overwritten.

```
copy http://FileUrl {savedconfig:configfilename | script:scriptfilename}
```

```
copy tftp://Location/Directory/Filename {savedconfig:configfilename | script:scriptfilename}
```

```
copy {savedconfig:configfilename | script:scriptfilename} tftp://Location/Directory/Filename
```

## Syntax Description

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>FileUrl</i>                      | The URL (including the file name) of the configuration or script file to be copied to the SN 5428, such as <i>http://acme/~myhome/allconf.xml</i> . (In this example, the host name <i>acme</i> can be used if the <b>ip name-server</b> command was previously issued.) Configuration files are transferred to the <i>savedconfig</i> directory; script files are transferred to the <i>script</i> directory. |
| <i>configfilename</i>               | The name of the saved configuration file. If the file is being copied from the SN 5428 to a TFTP server, it must exist in the SN 5428's <i>savedconfig</i> directory.                                                                                                                                                                                                                                          |
| <i>scriptfilename</i>               | The name of the saved script file. If the file is being copied from the SN 5428 to a TFTP server, it must exist in the SN 5428's <i>script</i> directory.                                                                                                                                                                                                                                                      |
| <i>Location/Directory/File name</i> | The name of the TFTP server and default directory, followed by the file name. The file must currently exist in the directory. It will be overwritten by the file copied from the SN 5428.                                                                                                                                                                                                                      |

## Defaults

None.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

The **copy** command does not affect the running or persistent configuration of the SN 5428 or high availability cluster. However, the **restore** command can be used to copy the contents of a saved configuration file into persistent memory, while the **read** command can be used to execute the commands in a script file to rebuild a SN 5428 configuration.

Because TFTP does not require a user name and password, directories and files cannot be created. When you copy a file to a TFTP server, you must have read/write permissions for the complete file path, and the file copied from the SN 5428 must already exist.

**Examples**

The following example copies the saved configuration file *myFoo.xml* from a server with an IP address of 10.1.40.10 to the SN 5428. The file name is changed to *myFoo\_restore.xml* when it is written to the SN 5428's *savedconfig* directory.

```
[SN5428A]# copy http://10.1.40.10/usr/SN5428/savedconfig/myFoo.xml
savedconfig:myFoo_restore.xml
```

The following example copies the script file *SN5428\_Lab* from a server named *acme*. The file name is unchanged when it is written to the SN 5428's *script* directory.

```
[SN5428A]# copy http://acme/~myhome/SN5428_Lab script:SN5428_Lab
```

The following example copies the saved configuration file *backup\_23.xml* to the *daily\_backup.xml* file in the *tftpboot* directory of the *tftp\_primary* server. The file *daily\_backup.xml* must already exist in the *tftpboot* directory of the *tftp\_primary* server. This command will overwrite the existing *daily\_backup.xml* file.

```
[SN5428A]# copy savedconfig:backup_23.xml tftp://tftp_primary/tftpboot/daily_backup.xml
```

**Related Commands**

| Commands                  | Description                                                                                               |
|---------------------------|-----------------------------------------------------------------------------------------------------------|
| <b>read</b>               | Read and execute the CLI commands in the named script file.                                               |
| <b>restore aaa</b>        | Restore AAA authentication services from a saved configuration file.                                      |
| <b>restore accesslist</b> | Restore the named access list or all access lists from the named configuration file.                      |
| <b>restore all</b>        | Restore the contents of the named configuration file into memory.                                         |
| <b>restore scsirouter</b> | Restore the named SCSI routing instance from the named configuration file.                                |
| <b>restore system</b>     | Restore selected system information from the named configuration file.                                    |
| <b>restore vlan</b>       | Restore VLAN configuration information from the named configuration file.                                 |
| <b>save aaa</b>           | Save the current AAA configuration information.                                                           |
| <b>save accesslist</b>    | Save configuration data for the named access list or all access lists.                                    |
| <b>save all</b>           | Save all configuration information.                                                                       |
| <b>save scsirouter</b>    | Save configuration information for the named SCSI routing instance.                                       |
| <b>save system</b>        | Save selected system configuration information.                                                           |
| <b>save vlan</b>          | Save configuration information for the named VLAN or for all VLANs.                                       |
| <b>show savedconfig</b>   | Display the contents of the <i>savedconfig</i> directory or the contents of the named configuration file. |
| <b>show script</b>        | Display the contents of the <i>script</i> directory or the contents of the named command file.            |

# debug aaa

To enable debugging for authentication, authorization, and accounting (AAA) services, which provide iSCSI authentication for IP hosts requesting access to storage via SCSI routing instances, use the **debug aaa** command. To disable debugging for AAA authentication services, use the **no** form of this command.

**debug aaa**

**no debug aaa**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Debugging is not enabled.

**Command Modes** Administrator.

| Command History | Release | Modifications                |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command to debug problems with iSCSI authentication or general AAA authentication services. Create log route entries for notification level *debugging* to send the trace and debug messages to the desired destination, using the **logging level** command.

**Examples** The following example enables AAA debugging:

```
[SN5428A] # debug aaa
```

| Related Commands | Command                         | Description                                                                                                                         |
|------------------|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>aaa authentication iscsi</b> | Configure the AAA authentication services to be used for iSCSI authentication.                                                      |
|                  | <b>aaa test authentication</b>  | Enable testing of AAA authentication services.                                                                                      |
|                  | <b>debug scsirouter</b>         | Enable debugging for the named SCSI routing instance.                                                                               |
|                  | <b>logging level</b>            | Add rule entries to route SN 5428 event, debug and trace messages to various destinations based on facility and notification level. |
|                  | <b>restore aaa</b>              | Restore AAA configuration services from a saved configuration file.                                                                 |
|                  | <b>save aaa</b>                 | Save the current AAA configuration information.                                                                                     |

| <b>Command</b>                     | <b>Description</b>                                               |
|------------------------------------|------------------------------------------------------------------|
| <b>scsirouter<br/>authenticate</b> | Enable iSCSI authentication for the named SCSI routing instance. |
| <b>show aaa</b>                    | Display AAA configuration information.                           |

# debug cmd

To run any operating system command with up to five arguments from the CLI, use the **debug cmd** command.

```
debug cmd os-command [parameters]
```

| Syntax Description | <i>os-command</i> | Any valid operating system command. Do not invoke interactive functions. |
|--------------------|-------------------|--------------------------------------------------------------------------|
|                    | <i>parameters</i> | Up to five command parameters.                                           |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modifications                |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** The **debug cmd** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

**Examples** The following example displays usage information for the debug cmd:

```
[SN5428A]# debug cmd dbgRunOSCmdHelp
[SN5428A]# debug cmd dbgRunOSCmdHelp 0c 1a c4 3c
```

```
Running command dbgRunOSCmdHelp(0xc1ac43c) with args 0 0 0 0 0
```

```
CLI usage: debug cmd symbol arg1 .. arg5
symbol -- any named OS function
arg1 .. arg5 -- numbers (interpreted as hex) or
 strings if escaped with an initial '$', such as $fcl
 Anything that doesn't convert to a number is a string
```

```
Return value is 0 = 0x0 (OK)
```

| Related Commands | Command                 | Description                                           |
|------------------|-------------------------|-------------------------------------------------------|
|                  | <b>debug aaa</b>        | Enable debugging for AAA authentication services.     |
|                  | <b>debug scsirouter</b> | Enable debugging for the named SCSI routing instance. |

# debug scsirouter

To enable trace facilities for debugging SCSI routing instances, use the **debug scsirouter** command. To disable debugging, use the **no** form of this command.

**debug scsirouter** *name* **scsitrace**

**no debug scsirouter** *name* **scsitrace**

| Syntax Description |                                                       |
|--------------------|-------------------------------------------------------|
| <i>name</i>        | The name of the SCSI routing instance to be debugged. |
| <b>scsitrace</b>   | Keyword indicating tracing services will be enabled.  |

**Defaults** All trace facilities are enabled by default.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** When enabled at this level, debug tracing will trace traffic to and from all targets associated with the named SCSI routing instance. Use the **show debug scsirouter** command to view the trace buffer output.

**Examples** The following example enables debug tracing facilities for a SCSI routing instance named *foo*:

```
[SN5428A] # debug scsirouter foo scsitrace
```

| Related Commands | Command                        | Description                                                                       |
|------------------|--------------------------------|-----------------------------------------------------------------------------------|
|                  | <b>debug aaa</b>               | Enable debugging for AAA authentication services.                                 |
|                  | <b>debug scsirouter target</b> | Enable debugging for a specific SCSI routing instance target and LUN combination. |
|                  | <b>show debug scsirouter</b>   | Display trace buffer output.                                                      |

# debug scsirouter target

To enable trace facilities for debugging a specific SCSI routing instance target and LUN combination, use the **debug scsirouter target** command. To disable debugging, use the **no debug scsirouter target** form of this command.

```
debug scsirouter name target name lun nn scsitrace
```

```
no debug scsirouter name target name lun nn scsitrace
```

## Syntax Description

|                           |                                                       |
|---------------------------|-------------------------------------------------------|
| <i>name</i>               | The name of the SCSI routing instance to be debugged. |
| <b>target</b> <i>name</i> | The name of the target to be included in the trace.   |
| <b>lun</b> <i>nn</i>      | The specific LUN associated with the target.          |
| <b>scsitrace</b>          | Keyword indicating tracing services will be enabled.  |

## Defaults

All trace facilities are enabled by default.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

When enabled at this level, SCSI tracing will trace traffic to and from the specified target and LUN combination associated with the named SCSI routing instance. Use the **show debug scsirouter** command to view the trace buffer output.

## Examples

The following example enables SCSI tracing facilities for the target and LUN combination *myTarget*, LUN 0, associated with the SCSI routing instance named *foo*:

```
[SN5428A]# debug scsirouter foo target myTarget lun 0 scsitrace
```

## Related Commands

| Command                      | Description                                           |
|------------------------------|-------------------------------------------------------|
| <b>debug aaa</b>             | Enable debugging for AAA authentication services.     |
| <b>debug scsirouter</b>      | Enable debugging for the named SCSI routing instance. |
| <b>show debug scsirouter</b> | Display trace buffer output.                          |

# delete accesslist

To delete an entire access list, all access lists, or a specified entry from the named access list, use the **delete accesslist** command. This command does not change the persistent SN 5428 configuration until the relevant configuration information has been saved using the appropriate **save** command with the **bootconfig** keyword.

**delete accesslist all**

**delete accesslist** *name* [*A.B.C.D/bits* | *A.B.C.D/1.2.3.4*]

**delete accesslist** *name* [**chap-username** *username* | **iscsi-name** *string*]

**delete accesslist** *name* **all**

## Syntax Description

|                                         |                                                                                                                                                                                                                       |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>                             | The name of the access list.                                                                                                                                                                                          |
| <i>A.B.C.D/bits</i>                     | (Optional) IP address and subnet mask of the IP host being deleted from the access list. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The <i>/bits</i> specifies the subnet mask in CIDR style.      |
| <i>A.B.C.D/1.2.3.4</i>                  | (Optional) IP address and subnet mask of the IP host being deleted from the access list. <i>A.B.C.D</i> is the dotted quad notation of the IP address. <i>1.2.3.4</i> is the dotted quad notation of the subnet mask. |
| <b>chap-username</b><br><i>username</i> | (Optional) The CHAP user name configured for the IP host being deleted from the access list. The CHAP user name is used for iSCSI authentication purposes.                                                            |
| <b>iscsi-name</b> <i>string</i>         | (Optional) The iSCSI Name of the IP host being deleted from the access list.                                                                                                                                          |
| <i>name</i> <b>all</b>                  | Delete all entries from the named access list.                                                                                                                                                                        |
| <b>all</b>                              | Delete all access lists.                                                                                                                                                                                              |

## Defaults

None.

## Command Modes

Administrator.

## Command History

| Release | Modification                                                        |
|---------|---------------------------------------------------------------------|
| 2.2.1   | This command was introduced.                                        |
| 2.3.1   | The <b>chap-username</b> and <b>iscsi-name</b> keywords were added. |

## Usage Guidelines

Because access lists are cluster entities, this operation affects all targets associated with this access list, regardless of where the associated SCSI routing instance is running within the SN 5428 cluster.

- Use the **delete accesslist** *name* **all** to clear all entries from the access list, but retain the access list entity.

- Use the **delete accesslist** *name* command with no additional parameters to completely delete the named access list.

Changes to access lists do not impact currently connected IP hosts; changes are effective for all subsequent connections.

In a cluster environment, access list management functions are handled by a single SN 5428. To determine which SN 5428 is performing access list management functions, issue the **show cluster** command. If you issue a **delete accesslist** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the SN 5428 that is currently handling those functions.

For more information on operating the SN 5428 in a cluster, see Chapter 10, “Maintaining and Managing the SN 5428 Storage Router.”

## Examples

The following example completely deletes the access list named *fooList* from the SN 5428’s currently running configuration:

```
[SN5428A]# delete accesslist fooList
```

The following example deletes all entries from the access list named *fooList1*. The access list entity itself is not deleted from the SN 5428’s currently running configuration:

```
[SN5428A]# delete accesslist fooList1 all
```

The following example deletes all access lists from the SN 5428’s currently running configuration:

```
[SN5428A]# delete accesslist all
```

The following example deletes the specified IP address from the named access list, *fooList2*. This command does not update the SN 5428’s bootable configuration until a **save accesslist bootconfig** or **save all bootconfig** command is issued.

```
[SN5428A]# delete fooList2 192.168.54.12/32
```

The following example deletes the specified CHAP user name from the named accesslist, *fooList3*. This command does not updated the SN 5428’s bootable configuration until a **save accesslist bootconfig** or **save all bootconfig** command is issued.

```
[SN5428A]# delete fooList3 chap-username webserver15
```

The following example deletes the specified iSCSI Name from the named accesslist, *fooList4*. This command does not updated the SN 5428’s bootable configuration until a **save accesslist bootconfig** or **save all bootconfig** command is issued.

```
[SN5428A]# delete fooList4 iscsi-name webserver15 ign.1987-05.com.cisco.01.8838a325b4017f
```

## Related Commands

| Command                         | Description                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------|
| <b>accesslist</b>               | Create an access list entity.                                                        |
| <b>accesslist A.B.C.D/bits</b>  | Add IP addresses to an access list.                                                  |
| <b>accesslist chap-username</b> | Add CHAP user name entries to an access list.                                        |
| <b>accesslist iscsi-name</b>    | Add iSCSI Name entries to an access list.                                            |
| <b>restore accesslist</b>       | Restore the named access list or all access lists from the named configuration file. |

| <b>Command</b>                      | <b>Description</b>                                                           |
|-------------------------------------|------------------------------------------------------------------------------|
| <b>save accesslist</b>              | Save configuration data for the named access list or for all access lists.   |
| <b>scsirouter target accesslist</b> | Associate an access list with a specific SCSI routing target or all targets. |
| <b>show accesslist</b>              | Display the contents of the named access list or all access lists.           |

# delete logging

To delete a rule from the logging table, use the **delete logging** command.

**delete logging level** *notification-level* **from** {**all** | *facility-name*}

**delete logging** **#?**

**delete logging** **#nn**

## Syntax Description

|                                  |                                                                                                                                                                                                         |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>notification-level</i>        | The notification level of the routing rules entry to be deleted. See Table 11-12 in the Usage Guidelines section for a list of valid names that can be used for the <i>notification-level</i> argument. |
| <b>from all</b>                  | Keyword, indicating all facilities.                                                                                                                                                                     |
| <b>from</b> <i>facility-name</i> | The name of the facility. A facility is the feature area from which the message is received. See Table 11-11 in the Usage Guidelines section for a list of valid facility names.                        |
| <b>#?</b>                        | Request an indexed list of entries in the logging table.                                                                                                                                                |
| <b>#nn</b>                       | The index number from the displayed list of entries. The specified routing rule will be deleted.                                                                                                        |

## Defaults

None.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.3.1   | This command was introduced. |

## Usage Guidelines

Event, trace and debug messages can be routed to various destinations, based on the notification level of the message and the application area (facility) that generated the message. When a log message is received by the SN 5428, the logging table rules are searched by facility name and by message level until a match is found. The log message is sent to all the destinations specified by the matching rule.

Use this command to delete logging rules based on notification level and facility name, or by index number.

To display an indexed lists of entries in the logging table, use the number sign (#) character followed by a question mark (?). That action will cause the routing rules in the logging table to be displayed as a numbered (indexed) set of lines. The command is displayed at the prompt below the list to the point of the # keyword. Complete the command by entering the appropriate index number. The specified routing rule will be deleted.

The level limits logging to messages of the specified level or lower levels, based on level number. Table 11-2 describes the available logging levels.

**Table 11-2 Logging Level Message Levels and Corresponding Numbers**

| Notification Level | Level Number | Description                              |
|--------------------|--------------|------------------------------------------|
| <b>emergency</b>   | 0            | System unusable                          |
| <b>alert</b>       | 1            | Immediate action needed                  |
| <b>critical</b>    | 2            | Critical conditions                      |
| <b>error</b>       | 3            | Error conditions                         |
| <b>warning</b>     | 4            | Non-fatal warning conditions             |
| <b>notice</b>      | 5            | Normal but significant conditions        |
| <b>info</b>        | 6            | Informational messages only              |
| <b>debug</b>       | 7            | Information for troubleshooting purposes |

**Note**

The *debug* notification level should be used for specific troubleshooting purposes only. System performance and HA behavior may be adversely affected by logging at the *debug* notification level.

Each facility can have up to eight notification levels. Each facility and notification level pair can have up to seven destinations. Table 11-3 describes the available facility names.

**Table 11-3 Logging Level Facilities**

| Facility Name   | Description                          |
|-----------------|--------------------------------------|
| <b>AUTH</b>     | AAA authentication.                  |
| <b>CDP</b>      | Cisco Discovery Protocol.            |
| <b>CONF</b>     | Configuration functions.             |
| <b>FC</b>       | SN 5428 Fibre Channel interfaces.    |
| <b>GE</b>       | SN 5428 Gigabit Ethernet interfaces. |
| <b>HA</b>       | SN 5428 high availability clusters.  |
| <b>IF</b>       | Interface manager.                   |
| <b>INVALID</b>  | Generic functions.                   |
| <b>IPROUTER</b> | SN 5428 IP functions.                |
| <b>ISCSI</b>    | iSCSI functions.                     |
| <b>MON</b>      | Hardware monitor.                    |
| <b>SNMP</b>     | Simple Network Management Protocol.  |
| <b>SYSLOG</b>   | Syslog functions.                    |
| <b>UI</b>       | SN 5428 user interface.              |
| <b>VTP</b>      | VTP and VLAN functions.              |

Use the **save system bootconfig** or **save all bootconfig** commands to save the updated logging table.

**Examples**

The following example displays the logging table and then deletes the routing rule entry for messages at level *info* from facility *all*:

```
[SN5428A]# show logging
Logging is enabled
Logging to syslog host is enabled, ip-address is 10.1.1.144
```

| Index | Level | Priority | Facility | Route           |
|-------|-------|----------|----------|-----------------|
| 1     | info  | 6        | all      | console logfile |
| 2     | debug | 7        | HA       | logfile rslog   |

```
[SN5428A]# delete logging level info from facility all
```

The following example displays an indexed list of the routing rules in the logging table and then deletes the third entry:

```
[SN5428A]# delete logging #?

Logging is enabled
Logging to syslog host is enabled, ip-address is 10.1.1.144
```

| Index | Level    | Priority | Facility | Route           |
|-------|----------|----------|----------|-----------------|
| 1     | critical | 2        | all      | console logfile |
| 2     | debug    | 7        | SNMP     | rslog           |
| 3     | notice   | 5        | HA       | all             |
| 4     | warning  | 4        | CDP      | rslog           |

```
[SN5428A]# delete logging #3
```

**Related Commands**

| Command                    | Description                                                                                                                         |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>clear logging table</b> | Clear the SN 5428 Storage Router logging table of all entries, or to reset the table to factory defaults.                           |
| <b>logging #?</b>          | Insert a routing rule entry into the SN 5428 logging table.                                                                         |
| <b>logging level</b>       | Add rule entries to route SN 5428 event, debug and trace messages to various destinations based on facility and notification level. |
| <b>logging on</b>          | Enable or temporarily disable logging of SN 5428 event message.                                                                     |
| <b>show logging</b>        | Display the routing rules in the logging table and the contents of the SN 5428 log file.                                            |

# delete savedconfig

To remove the named file from the *savedconfig* directory, use the **delete savedconfig** command.

**delete savedconfig** {*filename* | **all**}

| Syntax Description |  |                                                                                                             |
|--------------------|--|-------------------------------------------------------------------------------------------------------------|
| <i>filename</i>    |  | The name of the configuration file to be deleted. This file must exist in the <i>savedconfig</i> directory. |
| <b>all</b>         |  | Keyword, indicating that all configuration files in the <i>savedconfig</i> directory are to be deleted.     |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use the **show savedconfig** command to display the contents of the *savedconfig* directory.

**Examples** The following example removes the configuration file named *foo\_config* from the SN 5428:

```
[SN5428A]# delete savedconfig foo_config
```

| Related Commands | Command                 | Description                                                                                                                  |
|------------------|-------------------------|------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>copy</b>             | Copy the named configuration or script file from a remote location to the SN 5428, or from the SN 5428 to a remote location. |
|                  | <b>restore all</b>      | Restore the contents of the named configuration file into memory.                                                            |
|                  | <b>save all</b>         | Save all configuration information.                                                                                          |
|                  | <b>save system</b>      | Save selected system configuration information                                                                               |
|                  | <b>show savedconfig</b> | Display the contents of the <i>savedconfig</i> directory or the contents of the named configuration file.                    |
|                  | <b>show script</b>      | Display the contents of the script directory or the contents of the named command file.                                      |

# delete script

To remove the named command file from the *script* directory, use the **delete script** command.

```
delete script {filename | all}
```

| Syntax Description |  |                                                                                                  |
|--------------------|--|--------------------------------------------------------------------------------------------------|
| <i>filename</i>    |  | The name of the command file to be deleted. This file must exist in the <i>script</i> directory. |
| <b>all</b>         |  | Keyword, indicating that all command files in the <i>script</i> directory are to be deleted.     |

| Defaults | None. |
|----------|-------|
|----------|-------|

| Command Modes | Administrator. |
|---------------|----------------|
|---------------|----------------|

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

| Usage Guidelines | Use the <b>show script</b> command to display the contents of the <i>script</i> directory or the specified command file. |
|------------------|--------------------------------------------------------------------------------------------------------------------------|
|------------------|--------------------------------------------------------------------------------------------------------------------------|

| Examples | The following example removes the command file named <i>foo_script</i> from the SN 5428: |
|----------|------------------------------------------------------------------------------------------|
|----------|------------------------------------------------------------------------------------------|

```
[SN5428A]# delete script foo_script
```

| Related Commands | Command                   | Description                                                                                                                  |
|------------------|---------------------------|------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>copy</b>               | Copy the named configuration or script file from a remote location to the SN 5428, or from the SN 5428 to a remote location. |
|                  | <b>read</b>               | Read and execute the CLI commands in the named script file.                                                                  |
|                  | <b>restore all</b>        | Restore the contents of the named configuration file into memory.                                                            |
|                  | <b>save all</b>           | Save all configuration information.                                                                                          |
|                  | <b>save system</b>        | Save selected system configuration information.                                                                              |
|                  | <b>show bootconfig</b>    | Display the SN 5428's bootable configuration, or create a command file based on the SN 5428's bootable configuration.        |
|                  | <b>show runningconfig</b> | Display the SN 5428's running configuration, or create a command file based on the SN 5428's running configuration.          |

| Command                       | Description                                                                                            |
|-------------------------------|--------------------------------------------------------------------------------------------------------|
| <code>show savedconfig</code> | List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file. |
| <code>show script</code>      | Display the contents of the script directory or the contents of the named command file.                |

## delete scsirouter

To delete the named elements from the SCSI routing instance, use the **delete scsirouter** command. This command does not change the persistent SN 5428 configuration until the relevant configuration information has been saved using the appropriate **save** command with the **bootconfig** keyword.

```
delete scsirouter {all | name} [connection nn | serverif ge? [vlan vid]]
```

```
delete scsirouter {all | name} target {name | all} [lun nn]
```

```
delete scsirouter {all | name} target {name | all} [lun nn] force
```

```
delete scsirouter {all | name} force
```

| Syntax Description          |                                                                                                                                                                                           |  |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| <b>all</b>                  | Delete all SCSI routing instances from the SN 5428.                                                                                                                                       |  |
| <i>name</i>                 | The name of the SCSI routing instance.                                                                                                                                                    |  |
| <b>connection</b> <i>nn</i> | (Optional) Delete the specified connection from the named instance or all instances. Use the <b>show scsirouter</b> command with the <b>connection</b> keyword to display connection IDs. |  |
| <b>serverif</b> <i>ge?</i>  | (Optional) Delete the server interface for the named SCSI routing instance or all instances.                                                                                              |  |
| <b>target</b> <b>all</b>    | Delete all targets from the named instance.                                                                                                                                               |  |
| <b>target</b> <i>name</i>   | The name of the specific target to delete.                                                                                                                                                |  |
| <b>lun</b> <i>nn</i>        | (Optional) Delete the specified iSCSI LUN from the named target or all targets.                                                                                                           |  |
| <b>vlan</b> <i>vid</i>      | (Optional) Delete the specified VLAN from the named SCSI routing instance or all instances.                                                                                               |  |
| <b>force</b>                | (Optional) Keyword that overrides normal protections, allowing the action to be performed.                                                                                                |  |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines**

In a cluster environment, changes to the SCSI routing instance can only be made on the SN 5428 that is the currently running that instance. The SCSI routing instance may be in a stopped state at the time it is deleted.

The **force** option allows the SCSI routing instance to be deleted from a SN 5428 that is not currently running the instance. The **force** option should only be used when the SN 5428, or a specific SCSI routing instance, is in an abnormal state and cannot be recovered without rebooting.

When used with the **target** or **LUN** keywords, the **force** option allows the specified object to be deleted, even if in use by an iSCSI driver. Under normal circumstances, a target or LUN cannot be deleted if an iSCSI driver is logged in.

**Note**

When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.

**Examples**

The following example deletes all targets associated with the SCSI routing instance named *foo*:

```
[SN5428A] # delete scsirouter foo target all
```

The following example deletes the specified VLAN from the Gigabit Ethernet interface used by the SCSI routing instance named *foo2*:

```
[SN5428A] # delete scsirouter foo2 serverif ge2 vlan 101
```

The following example deletes the entire SCSI routing instance named *foo4*:

```
[SN5428A] # delete scsirouter foo4
```

**Note**

All examples update the SN 5428's currently running configuration only. To make a deletion permanent, issue the appropriate **save all bootconfig** or **save scsirouter bootconfig** command.

**Related Commands**

| Command                    | Description                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------|
| <b>restore scsirouter</b>  | Restore the named SCSI routing instance from the named configuration file.                                 |
| <b>save scsirouter</b>     | Save configuration information for the named SCSI routing instance.                                        |
| <b>scsirouter</b>          | Create a SCSI routing instance.                                                                            |
| <b>scsirouter enable</b>   | Start and stop the named SCSI routing instance.                                                            |
| <b>scsirouter serverif</b> | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
| <b>setup scsi</b>          | Run the wizard to configure a SCSI routing instance.                                                       |
| <b>show accesslist</b>     | Display the contents of the named access list or all access lists.                                         |
| <b>show scsirouter</b>     | Display configuration and operational information for the named SCSI routing instance.                     |

# delete software version

To delete a version of software from the SN 5428, use the **delete software version** command.



## Note

The version of software currently running and the version that will be booted when the system is restarted may not be deleted.

```
delete software version {x.y.z | all}
```

## Syntax Description

|              |                                                            |
|--------------|------------------------------------------------------------|
| <i>x.y.z</i> | The version of SN 5428 software to be deleted.             |
| <b>all</b>   | Delete all non-bootable and non-current software versions. |

## Defaults

None.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

Use this command to remove old versions of software from the SN 5428.

## Examples

The following example removes version 2.0.1 from the SN 5428:

```
[SN5428A]# delete software version 2.0.1
```

## Related Commands

| Command                        | Description                                                                                                    |
|--------------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>download software</b>       | Download the list of available software versions or the specified version of software from the named location. |
| <b>software http url</b>       | Specify the default location from which to download updated SN 5428 software via HTTP.                         |
| <b>software proxy url</b>      | Specify the default location from which to download updated SN 5428 software via HTTP, using a proxy server.   |
| <b>software tftp</b>           | Specify the default location from which to download updated SN 5428 software via TFTP.                         |
| <b>verify software version</b> | Check the specified software version for problems.                                                             |

# download software

To fetch the specified object from the named location or the default download location, use the **download software list** command.

```
download software {http | proxy} {list | url full_url | version x.y.z}
```

```
download software tftp {hostname host filename file | list | version x.y.z}
```

| Syntax Description          |                                                                                                                                          |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>http</b>                 | Download using the HTTP protocol.                                                                                                        |
| <b>proxy</b>                | Download using a proxy server.                                                                                                           |
| <b>list</b>                 | (Optional) Download a list of available versions.                                                                                        |
| <b>url</b>                  | (Optional) Keyword indicating that the download is from the specified URL.                                                               |
| <i>full_url</i>             | The fully qualified URL from which to download this version of SN 5428 software. For example, <i>http://anywebserver.com/2.2.1.tar</i> . |
| <b>version</b> <i>x.y.z</i> | (Optional) Download the specified version of SN 5428 software from the default location.                                                 |
| <b>tftp</b>                 | Download using the TFTP protocol                                                                                                         |
| <b>hostname</b> <i>host</i> | The name of the TFTP host.                                                                                                               |
| <b>filename</b> <i>file</i> | The name of the file to be downloaded, such as <i>2.2.1.tar</i> . This file contains the SN 5428 software.                               |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** The list of available software versions is stored in the file named *sw-version.txt*. This text file must contain one line for each version of software that is available from the download location. If you store and download software from a site other than the system default (<http://www.cisco.com>), create this file and update it whenever a new version of software is available.

Software is either downloaded from the default locations set for the specified protocol or from the location specified as part of the command. Always verify software after it has downloaded to assure no errors were encountered. See the “Installing Updated Software” section on page 10-2 for details on verification and making updated software available to the SN 5428.

A maximum of two versions of software can be stored on the SN 5428.

**Examples**

The following example downloads SN 5428 software version 2.2.1 from the default location via standard Hypertext Transfer Protocol (HTTP):

```
[SN5428A]# download software http version 2.2.1
```

The following example downloads a file named *sn5428v311.tar* from the TFTP host named *my\_tftpHost*. The file must exist in the default TFTP directory.

```
[SN5428A]# download software tftp hostname my_tftpHost filename sn5428v311.tar
```

The following file downloads the list of available software from the default location using the SN 5428's proxy configuration:

```
[SN5428A]# download software proxy list
```

**Related Commands**

| Command                        | Description                                                                                                  |
|--------------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>delete software version</b> | Remove the specified version of software from the SN 5428.                                                   |
| <b>software http url</b>       | Specify the default location from which to download updated SN 5428 software via HTTP.                       |
| <b>software http username</b>  | Configure the user name and optional password required to access the default download location.              |
| <b>software proxy</b>          | Configure HTTP proxy information.                                                                            |
| <b>software proxy url</b>      | Specify the default location from which to download updated SN 5428 software via HTTP, using a proxy server. |
| <b>software proxy username</b> | Configure the user name and optional password required to access the proxy URL.                              |
| <b>software tftp</b>           | Specify the default location from which to download updated SN 5428 software via TFTP.                       |
| <b>verify software version</b> | Check the specified software version for problems.                                                           |

# enable

To change the management session from Monitor mode to Administrator mode, use the **enable** command. Monitor mode, which is the default mode, provides view-only access to the SN 5428's management interface. Administrator mode allows the user to create entities and make changes to the configuration of the SN 5428.

**enable**

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Issue the **enable** command after a successful CLI login to change to Administrator mode. You are prompted to enter the Administrator mode password, if required. Use the **exit** command to return to Monitor mode.

**Examples** The following example changes the session from Monitor mode to Administrator mode.

```
[SN5428A]# enable
Enter admin password: ****
[Entering Administrator mode]
```

| Related Commands | Command       | Description                                      |
|------------------|---------------|--------------------------------------------------|
|                  | <b>exit</b>   | Leave Administrator mode and enter Monitor mode. |
|                  | <b>logout</b> | Terminate the management session.                |

# exit

To return the management session to Monitor mode from Administrator mode, use the **exit** command.

**exit**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** None.

---

**Command Modes** Administrator.

---

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

---



---

**Usage Guidelines** Issue the **exit** command to return to Monitor mode after previously issuing the **enable** command.

---

**Examples** The following example returns the CLI session to Monitor mode:

```
[SN5428A]# exit
[Leaving Administrator mode]
```

---

| Related Commands | Command       | Description                       |
|------------------|---------------|-----------------------------------|
|                  | <b>enable</b> | Enter Administrator mode.         |
|                  | <b>logout</b> | Terminate the management session. |

---

# failover scsirouter

To cause the named SCSI routing instance to cease running on this SN 5428 and start running on another SN 5428 in the cluster, use the **failover scsirouter** command.



## Note

If no eligible SN 5428 is found, the SCSI routing instance will start running again on the same SN 5428. If the SN 5428 is configured as a standalone system, failover is not allowed.

```
failover scsirouter name [pri | sec | to systemname]
```

```
failover scsirouter all [to systemname]
```

## Syntax Description

|                      |                                                                                                       |
|----------------------|-------------------------------------------------------------------------------------------------------|
| <i>name</i>          | The name of the SCSI routing instance to be failed over.                                              |
| <b>all</b>           | Failover all instances currently running on this SN 5428.                                             |
| <b>pri</b>           | (Optional) Force failover to the designated primary SN 5428 in the failover list.                     |
| <b>sec</b>           | (Optional) Force failover to the designated secondary SN 5428 in the failover list.                   |
| <b>to systemname</b> | (Optional) Perform the failover to the specified SN 5428. This SN 5428 must be active in the cluster. |

## Defaults

None.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

Use the **all** keyword to failover all SCSI routing instances currently running on this SN 5428. Each SN 5428 can run a maximum of 12 SCSI routing instances; there is a maximum of 12 SCSI routing instances per cluster.

## Examples

The following example causes the SCSI routing instance named *foo* to failover to another SN 5428 in the cluster:

```
[SN5428A]# failover scsirouter foo
```

The following example causes all SCSI routing instances to failover to the SN 5428 named *TestLab1*:

```
[SN5428A] # failover scsirouter all to TestLab1
```

**Related Commands**

| <b>Command</b>             | <b>Description</b>                                                               |
|----------------------------|----------------------------------------------------------------------------------|
| <b>scsirouter enable</b>   | Stop or start the named SCSI routing instance.                                   |
| <b>scsirouter failover</b> | Add the SN 5428 to the HA failover list for the specified SCSI routing instance. |

# halt

To prepare the SN 5428 to be powered down, issue the **halt** command.

**halt** [**force**] [**fast**]

| Syntax Description |                                                                               |
|--------------------|-------------------------------------------------------------------------------|
| <b>fast</b>        | (Optional) Bypassing hardware diagnostics when the SN 5428 is next restarted. |
| <b>force</b>       | (Optional) Force an immediate halt of the SN 5428.                            |

**Defaults** If there are unsaved configuration changes when the command is issued, the default is to save all changes before halting. If the command is issued with the optional **force** keyword, any unsaved configuration changes are discarded.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** The **halt** command prepares the SN 5428 file system to be powered down. If the SN 5428 is participating in a cluster, the **halt** command will cause any SCSI routing instances running on this SN 5428 to failover to another SN 5428 in the cluster.

If the **halt** command is issued with no keywords and there are unsaved changes to the current configuration, you are prompted to save or discard the changes.

Use the **force** keyword to cause an immediate halt of the SN 5428, discarding any unsaved configuration changes. Append the optional **fast** keyword to bypass diagnostics when the SN 5428 is restarted.

When the **halt** command completes, the SN 5428 displays the following system prompt:

```
[HALTED] #
```

The SN 5428 can be safely powered down when the HALTED system prompt appears. The only CLI command that can be issued from the SN 5428 at the HALTED system prompt is the **reboot** command.



**Note**

When the SN 5428 is restarted, the cluster determines any SCSI routing instances that should start on the SN 5428. If the SN 5428 is identified as the preferred SN 5428 for any SCSI routing instance (via the **scsirouter primary** command), that instance will start running on the SN 5428.

**Examples**

The following prompt is received if you issue a **halt** command (without the **force** keyword) when the SN 5428 has unsaved configuration changes.

```
[SN5428A]# halt
*** Warning: This will halt the system.
Do you want to continue? [yes/no (no)] yes

Changes have been made to the current configuration of the system which
have not been saved.
yes - all of the configuration data will be saved,
no - modifications to the configuration data will not be saved.

Save ALL configuration data? [yes/no (yes)] no
Halting system.....!
[HALTED]#
```

The following example halts the SN 5428 (after prompting the user to save any unsaved configuration changes), but bypasses diagnostics when the SN 5428 is restarted.

```
[SN5428A]# halt fast
```

**Related Commands**

| Command | Description                                      |
|---------|--------------------------------------------------|
| reboot  | Cause the SN 5428 to shut down and then restart. |

# help

To display information on how to use the CLI, issue the **help** command.

**help**

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** The **help** command displays information about the various CLI commands that can be issued, based on the mode currently in use. The **help** command also displays information about the special keys that can be used in the CLI.

**Examples** The following example shows the special key information returned as a result of the **help** command:

```
[SN5428A]# help
```

```
Special keys:
? list choices
Backspace delete character backward
Tab complete current word
Ctrl-A go to beginning of line
Ctrl-B or Arrow Left go backward one character
Ctrl-D delete character
Ctrl-E go to end of line
Ctrl-F or Arrow Right go forward one character
Ctrl-K delete from current position to end of line
Ctrl-N or Arrow Down go to next line in history buffer
Ctrl-P or Arrow Up go to previous line in history buffer
Ctrl-T transpose current character and previous character
Ctrl-U delete line
Ctrl-W delete previous word
```

| Related Commands | Command       | Description                                      |
|------------------|---------------|--------------------------------------------------|
|                  | <b>enable</b> | Enter Administrator mode.                        |
|                  | <b>exit</b>   | Leave Administrator mode and enter Monitor mode. |

# hostname

To specify the system name for the SN 5428, use the **hostname** command. The SN 5428 is recognized by this name through the management interface.

This command takes effect immediately, and the new system name is automatically integrated into the prompt string.

**hostname** *sysname*

## Syntax Description

|                |                                                                                                                                                                            |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>sysname</i> | The name of the SN 5428. This may be the fully qualified domain name. Maximum length is 19 characters. The name cannot contain blanks, white space, or control characters. |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Defaults

None.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

All SN 5428s must have a system name.

If you wish to enable network management on the SN 5428 using the facilities of a Domain Name Server (DNS), you must make the SN 5428's system name and IP address known to that DNS. Use the system name specified in this command.

## Examples

The following example shows the SN 5428 name set to *sn5428lab1*.

```
[SN5428A] # hostname sn5428lab1
```

## Related Commands

| Command            | Description                                                 |
|--------------------|-------------------------------------------------------------|
| <b>save all</b>    | Save all configuration information.                         |
| <b>save system</b> | Save selected system configuration information.             |
| <b>show system</b> | Display selected system information, including system name. |

# interface fc devlog

To specify the logging parameters for the switch development log file, use the **interface fc devlog** command.

```
interface fc devlog components component1 [component2...]
```

```
interface fc devlog level notification-level
```

| Syntax Description                                                 |                                                                                                                                                                                                |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>components</b><br><i>component1</i><br>[ <i>component2...</i> ] | At least one of the components described in Table 11-4.                                                                                                                                        |
| <b>level</b> <i>notification-level</i>                             | Limit logging to messages of a specified level or lower. See Table 11-5 in the Usage Guidelines section for a list of valid names that can be used for the <i>notification-level</i> argument. |

**Defaults** Development logging is disabled, by default.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command to limit the amount of information recorded in the switch development log by component and by notification level. To stop all logging for all components, set the notification level to **none**.

**Table 11-4** *interface fc devlog components*

| Component      | Description                                                           |
|----------------|-----------------------------------------------------------------------|
| <b>Cmon</b>    | Monitors internal chassis components and applications.                |
| <b>Diag</b>    | Handles online testing and other diagnostic tasks.                    |
| <b>Ds</b>      | Data services repository for all switch data.                         |
| <b>Fc2</b>     | Class 2 frame handler.                                                |
| <b>MgmtApp</b> | Manages the user interface and internal configuration for the switch. |
| <b>PortApp</b> | Manages the switch ports.                                             |

**Table 11-4** *interface fc devlog components (continued)*

| Component | Description                                                      |
|-----------|------------------------------------------------------------------|
| Swb       | Software bus internal process communications mechanism.          |
| Util      | Utility message interpreter for handling legacy user interfaces. |

**Table 11-5** *interface fc devlog notification-level*

| Notification Level | Description                                                                          |
|--------------------|--------------------------------------------------------------------------------------|
| Critical           | Log all messages from the selected components (critical, warning and informational). |
| Warn               | Log all warning and informational messages for the selected components.              |
| Info               | Log informational messages only for the selected components.                         |
| None               | Log no messages. This setting stops switch development logging.                      |

**Examples**

The following example limits the switch development log file to informational messages only from the management application and the class 2 frame handler:

```
[SN5428A]# interface fc devlog components MgmtApp Fc2
[SN5428A]# interface fc devlog level info
```

The following example stops all switch devlog logging:

```
[SN5428A]# interface fc devlog level none
```

**Related Commands**

| Command                          | Description                                                                        |
|----------------------------------|------------------------------------------------------------------------------------|
| <code>interface fc syslog</code> | Specify logging parameters for the switch system log file.                         |
| <code>show debug fc</code>       | Display internal Fibre Channel interface parameters, including switch log entries. |

# interface fc diag

To set all Fibre Channel interfaces into diagnostic mode for testing purposes, use the **interface fc diag** command.

## interface fc diag

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command to change all FC interfaces to diagnostic mode prior to performing internal or external loopback testing on individual FC interfaces.

- Use the **interface fc enable** command to reenable all FC interfaces. An FC interface must be enabled to run online loopback tests or to allow access to storage targets.
- Use the **no interface fc enable** command to disable all FC interfaces. When you are ready to allow access to the storage targets, you can enable all FC interfaces at once via the **interface fc enable** command, or enable individual interfaces via the **interface fc? enable** command.

**Examples** The following example sets all FC interfaces into a diagnostic state and then performs an internal loopback test on the FC interface named *fc6*:

```
[SN5428A] # interface fc diag
[SN5428A] # interface fc6 loopback internal
```

| Related Commands | Command                       | Description                                                                    |
|------------------|-------------------------------|--------------------------------------------------------------------------------|
|                  | <b>interface fc enable</b>    | Enable all FC interfaces.                                                      |
|                  | <b>interface fc? diag</b>     | Set the named FC interface into diagnostic mode for testing purposes.          |
|                  | <b>interface fc? enable</b>   | Enable the named FC interface.                                                 |
|                  | <b>interface fc? loopback</b> | Initiate a loopback test on the named FC interface.                            |
|                  | <b>show fc</b>                | Display global configuration information for SN 5428 Fibre Channel interfaces. |

# interface fc domainid

To set the SN 5428 Storage Router's domain ID for switched zoned fabric to a unique value, and to prevent the FC fabric from changing that domain ID, use the **interface fc domainid** command. To disable the lock and allow the domain ID to be changed by the switched zoned fabric, use the **no** form of this command.

```
interface fc domainid {domain-id | lock enable}
```

```
no interface fc domainid lock enable
```

## Syntax Description

|                    |                                                                                    |
|--------------------|------------------------------------------------------------------------------------|
| <i>domain-id</i>   | The domain identification number associated with the SN 5428.                      |
| <b>lock enable</b> | Keywords used to disallow changes to the domain ID from the switched zoned fabric. |

## Defaults

The default domain ID for fabric zoning is 1. The domain ID can be changed by the switched zoned fabric, by default.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.3.1   | This command was introduced. |

## Usage Guidelines

Use this command to set the SN 5428 Storage Router's domain identification number for switched zoned fabric to a unique value or to prevent changes to that value by the zoned fabric. Domain IDs allow fabrics to be segmented into different areas.

Domain IDs must be unique among all switch elements within a fabric. If there is a domain ID conflict, the expansion ports (ports operating as E\_Ports) on the two conflicting elements are disabled, isolating each other.

If you are planning to connect to a switched zoned fabric via one or more FC interfaces, complete the appropriate zoning configuration for the SN 5428, as described in Chapter 5, "Configuring for FC Fabric Zoning."

## Examples

The following example sets the switched zoned fabric domain ID for the SN 5428 to 42:

```
[SN5428A]# interface fc domainid 42
```

The following example sets the switched zoned fabric domain ID for the SN 5428 to 5 and enables the lock, which prevents the domain ID from being changed by the zoned fabric.

```
[SN5428A]# interface fc domainid 5
[SN5428A]# interface fc domainid lock enable
```

**Related Commands**

| <b>Command</b>                      | <b>Description</b>                                                                                                 |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>interface fc enable</b>          | Enable all FC interfaces.                                                                                          |
| <b>interface fc interop-credit</b>  | Set the data buffer credit capacity for all FC ports.                                                              |
| <b>interface fc zoning autosave</b> | Configure the SN 5428 to participate in FC switched zones.                                                         |
| <b>interface fc zoning default</b>  | Select the level of communication between the SN 5428 and devices in the fabric where there is no active zone set. |
| <b>interface fc zoning merge</b>    | Set zoning merge compliance.                                                                                       |
| <b>interface fc? diag</b>           | Set the named FC interface into diagnostic mode for testing purposes.                                              |
| <b>interface fc? enable</b>         | Enable the named FC interface.                                                                                     |
| <b>interface fc? loopback</b>       | Initiate a loopback test on the named FC interface.                                                                |
| <b>show fc</b>                      | Display global configuration information for SN 5428 Fibre Channel interfaces.                                     |

# interface fc enable

To enable all Fibre Channel interfaces, use the **interface fc enable** command. To disable all FC interfaces, use the **no** form of this command.

**interface fc enable**

**no interface fc enable**

**Syntax Description** This command has no arguments or keywords.

**Defaults** All FC interfaces are enabled, by default.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** An FC interface must be enabled to allow access to storage targets or perform online loopback testing. Use this command to enable all FC interfaces at one time.

If you experience problems with FC storage, use the **no** form of this command to quickly disable all FC interfaces at once.

**Examples** The following example enables all FC interfaces and then performs an online loopback test for the FC interface named *fc6*:

```
[SN5428A]# interface fc enable
[SN5428A]# interface fc6 loopback online
```

The following example disables all FC interfaces.

```
[SN5428A]# no interface fc enable
```

| Related Commands | Command                       | Description                                                                    |
|------------------|-------------------------------|--------------------------------------------------------------------------------|
|                  | <b>interface fc diag</b>      | Set all FC interfaces into diagnostic mode for testing purposes.               |
|                  | <b>interface fc? diag</b>     | Set the named FC interface into diagnostic mode for testing purposes.          |
|                  | <b>interface fc? enable</b>   | Enable the named FC interface.                                                 |
|                  | <b>interface fc? loopback</b> | Initiate a loopback test on the named FC interface.                            |
|                  | <b>show fc</b>                | Display global configuration information for SN 5428 Fibre Channel interfaces. |

# interface fc interop-credit

To set the buffer-to-buffer credit value for all FC ports, use the **interface fc interop-credit** command.

```
interface fc interop-credit credit
```

|                           |               |                                                                                                                                                                     |
|---------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>credit</i> | The data buffer credit capacity, also known as the buffer-to-buffer credit value. <i>credit</i> is an integer between 0 and 255 inclusive. The default value is 12. |
|---------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |                                                    |
|-----------------|----------------------------------------------------|
| <b>Defaults</b> | The data buffer credit capacity is 12, by default. |
|-----------------|----------------------------------------------------|

|                      |                |
|----------------------|----------------|
| <b>Command Modes</b> | Administrator. |
|----------------------|----------------|

|                        |                |                              |
|------------------------|----------------|------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|                        | 2.3.1          | This command was introduced. |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | Use this command to set the data buffer credit capacity for all the SN 5428's FC ports. The port buffer credit is used to determine how many maximum sized frames can be sent to a recipient before the sending port must wait for an acknowledgement. When the acknowledgement is received, the sending port can continue by sending the next frame. Port buffer credits are required when buffer-to-buffer flow control is in use. Buffer-to-buffer flow control occurs between directly connected FC ports. |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

The data buffer credit capacity must be the same for all switches across the fabric, and should be set to the lowest system-wide setting.

|                 |                                                                   |
|-----------------|-------------------------------------------------------------------|
| <b>Examples</b> | The following example sets the data buffer credit capacity to 15: |
|-----------------|-------------------------------------------------------------------|

```
[SN5428A] # interface fc interop-credit 15
```

|                           |                                                                       |                                                                                                                    |
|---------------------------|-----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Related Commands</b>   | <b>Command</b>                                                        | <b>Description</b>                                                                                                 |
|                           | <b>interface fc domainid</b>                                          | Set the SN 5428's domain ID for FC switch fabric zoning.                                                           |
|                           | <b>interface fc enable</b>                                            | Enable all FC interfaces.                                                                                          |
|                           | <b>interface fc zoning autosave</b>                                   | Configure the SN 5428 to participate in FC switched zones.                                                         |
|                           | <b>interface fc zoning default</b>                                    | Select the level of communication between the SN 5428 and devices in the fabric where there is no active zone set. |
|                           | <b>interface fc zoning merge</b>                                      | Set zoning merge compliance.                                                                                       |
| <b>interface fc? diag</b> | Set the named FC interface into diagnostic mode for testing purposes. |                                                                                                                    |

| <b>Command</b>                | <b>Description</b>                                                             |
|-------------------------------|--------------------------------------------------------------------------------|
| <b>interface fc? enable</b>   | Enable the named FC interface.                                                 |
| <b>interface fc? loopback</b> | Initiate a loopback test on the named FC interface.                            |
| <b>show fc</b>                | Display global configuration information for SN 5428 Fibre Channel interfaces. |

# interface fc syslog

To specify the logging parameters for the switch system log file, use the **interface fc syslog** command.

```
interface fc syslog components component1 [component2...]
```

```
interface fc syslog level notification-level
```

## Syntax Description

|                                                                  |                                                                                                                                                                                                |
|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>components</b><br><i>component1</i><br><i>[component2...]</i> | At least one of the components described in Table 11-6.                                                                                                                                        |
| <b>level</b> <i>notification-level</i>                           | Limit logging to messages of a specified level or lower. See Table 11-7 in the Usage Guidelines section for a list of valid names that can be used for the <i>notification-level</i> argument. |

## Defaults

All components log information into the switch system log, by default. The default notification level is *critical*.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

Use this command to limit the amount of information recorded in the switch system log by component and by notification level. To stop all logging for all components, set the notification level to **none**.

**Table 11-6** *interface fc syslog components*

| Component         | Description                                                                                      |
|-------------------|--------------------------------------------------------------------------------------------------|
| <b>Blade</b>      | Monitors modular circuit boards.                                                                 |
| <b>Chassis</b>    | Monitors chassis hardware components.                                                            |
| <b>Eport</b>      | Monitors all Fibre Channel interfaces where the port is operating as an expansion port (E_Port). |
| <b>NameServer</b> | Monitors name server events.                                                                     |
| <b>MgmtServer</b> | Monitors management server status.                                                               |
| <b>Other</b>      | Monitors miscellaneous events.                                                                   |
| <b>Port</b>       | Monitors all port events.                                                                        |
| <b>Switch</b>     | Monitors switch management events.                                                               |
| <b>Zoning</b>     | Monitors zoning conflict events.                                                                 |

**Table 11-7** *interface fc syslog notification level*

| Notification Level | Description                                                                          |
|--------------------|--------------------------------------------------------------------------------------|
| <b>Critical</b>    | Log all messages from the selected components (critical, warning and informational). |
| <b>Warn</b>        | Log all warning and informational messages for the selected components.              |
| <b>Info</b>        | Log informational messages only for the selected components.                         |
| <b>None</b>        | Log no messages. This setting stops switch system logging.                           |

**Examples**

The following example limits the switch system log file to informational messages only for name server, management server, port and switch management events:

```
[SN5428A]# interface fc syslog components NameServer MgmtServer Port Switch
[SN5428A]# interface fc syslog level info
```

The following example stops all switch syslog logging:

```
[SN5428A]# interface fc syslog level none
```

**Related Commands**

| Command                    | Description                                                                        |
|----------------------------|------------------------------------------------------------------------------------|
| <b>interface fc devlog</b> | Specify logging parameters for the switch development log file.                    |
| <b>show debug fc</b>       | Display internal Fibre Channel interface parameters, including switch log entries. |

# interface fc zoning autosave

To enable the SN 5428 Storage Router to save zoning changes received from switches in the fabric, use the **interface fc zoning autosave** command. To prevent the SN 5428 from saving zoning changes, use the **no** form of this command.

**interface fc zoning autosave enable**

**no interface fc zoning autosave enable**

## Syntax Description

|                        |                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>autosave enable</b> | Enables the SN 5428 to save zoning changes received from switches in the fabric to non-volatile memory. This is the default. |
|------------------------|------------------------------------------------------------------------------------------------------------------------------|

## Defaults

The SN 5428 saves zoning changes by default.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.3.1   | This command was introduced. |

## Usage Guidelines

By default, the SN 5428 Storage Router can merge into existing FC switched fabric zones and participate in the zoning. Use the **no** form of this command, in conjunction with the **interface fc domainid** command with the **lock** keyword to prevent the SN 5428 from participating in FC switched fabric zones.

## Examples

The following example prevents the SN 5428 from participating in FC switched fabric zones. The first command prevents the SN 5428 from saving zoning changes received from switches in the fabric, and the second command locks the domain ID, preventing the FC switch fabric from making changes to that value.

```
[SN5428A]# no interface fc zoning autosave enable
[SN5428A]# interface fc domainid lock enable
```

## Related Commands

| Command                            | Description                                                                                                        |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>interface fc domainid</b>       | Set the SN 5428's domain ID for FC switch fabric zoning.                                                           |
| <b>interface fc enable</b>         | Enable all FC interfaces.                                                                                          |
| <b>interface fc interop-credit</b> | Set the data buffer credit capacity for all FC ports.                                                              |
| <b>interface fc zoning default</b> | Select the level of communication between the SN 5428 and devices in the fabric where there is no active zone set. |

| <b>Command</b>                   | <b>Description</b>                                                             |
|----------------------------------|--------------------------------------------------------------------------------|
| <b>interface fc zoning merge</b> | Set zoning merge compliance.                                                   |
| <b>interface fc? diag</b>        | Set the named FC interface into diagnostic mode for testing purposes.          |
| <b>interface fc? enable</b>      | Enable the named FC interface.                                                 |
| <b>interface fc? loopback</b>    | Initiate a loopback test on the named FC interface.                            |
| <b>show fc</b>                   | Display global configuration information for SN 5428 Fibre Channel interfaces. |

# interface fc zoning default

To select the level of communication between the SN 5428 and devices in the fabric when there is no active zone set, use the **interface fc zoning default** command.

**interface fc zoning default {all | none}**

| Syntax Description | default all                                                                                                                                 | default none                                                                                                    |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
|                    | Enables the SN 5428 to communicate with all switches and other devices in the fabric when there is no active zone set. This is the default. | When there is no active zone set, the SN 5428 cannot communicate with any other switch or device in the fabric. |

**Defaults** If there is no active zone set, the SN 5428 can communicate with all switches and other devices in the fabric, by default.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.3.1   | This command was introduced. |

**Usage Guidelines** By default, the SN 5428 Storage Router can merge into existing FC switched fabric zones and participate in the zoning. Use this command to isolate the SN 5428 and prevent communication with any switch or other device in the fabric, if there is no active zone set.

**Examples** The following example prevents the SN 5428 from communicating with switches and all other devices in the fabric, if there is no active zone set:

```
[SN5428A]# interface fc zoning default none
```

| Related Commands | Command                             | Description                                                                                    |
|------------------|-------------------------------------|------------------------------------------------------------------------------------------------|
|                  | <b>interface fc domainid</b>        | Set the SN 5428's domain ID for FC switch fabric zoning.                                       |
|                  | <b>interface fc enable</b>          | Enable all FC interfaces.                                                                      |
|                  | <b>interface fc interop-credit</b>  | Set the data buffer credit capacity for all FC ports.                                          |
|                  | <b>interface fc zoning autosave</b> | Enable the SN 5428 Storage Router to save zoning changes received from switches in the fabric. |
|                  | <b>interface fc zoning merge</b>    | Set zoning merge compliance.                                                                   |
|                  | <b>interface fc? diag</b>           | Set the named FC interface into diagnostic mode for testing purposes.                          |

| <b>Command</b>                | <b>Description</b>                                                             |
|-------------------------------|--------------------------------------------------------------------------------|
| <b>interface fc? enable</b>   | Enable the named FC interface.                                                 |
| <b>interface fc? loopback</b> | Initiate a loopback test on the named FC interface.                            |
| <b>show fc</b>                | Display global configuration information for SN 5428 Fibre Channel interfaces. |

# interface fc zoning merge

To set zoning merge compliance, use the **interface fc zoning merge** command.

```
interface fc zoning merge {brocade | sw2}
```

| Syntax Description | brocade | Indicates the fabric includes Brocade switches with non-FC-SW-2 compliant firmware. When changes to a zoning database are saved, they will be propagated to all switches on the fabric, even without being activated. This is called a “full zoneset merge.” |
|--------------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | sw2     | Indicates the fabric includes only FC-SW-2 compliant switches. A merge may only occur of active zoning information, ensuring all switches have identical active zone sets. This is the default.                                                              |

**Defaults** The SN 5428 is FC-SW-2 compliant, and is configured to participate in a fabric with only FC-SW-2 compliant switches by default.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.3.1   | This command was introduced. |

**Usage Guidelines** By default, the SN 5428 Storage Router can merge into existing FC switched fabric zones and participate in the zoning. All switches in a fabric should be set to the same merge mode to prevent switches from becoming isolated from each other. By default, the SN 5428 supports the FC-SW-2 compliant merge mode.

If the SN 5428 Storage Router will participate in a fabric that includes Brocade switches with non-FC-SW-2 compliant firmware, use this command to change the merge mode to allow full zoneset merges.

**Examples** The following example changes the merge mode to allow full zoneset merges, because the SN 5428 is participating in a fabric with non-FC-SW-2 compliant switches:

```
[SN5428A]# interface fc zoning merge brocade
```

| Related Commands | Command                            | Description                                              |
|------------------|------------------------------------|----------------------------------------------------------|
|                  | <b>interface fc domainid</b>       | Set the SN 5428’s domain ID for FC switch fabric zoning. |
|                  | <b>interface fc enable</b>         | Enable all FC interfaces.                                |
|                  | <b>interface fc interop-credit</b> | Set the data buffer credit capacity for all FC ports.    |

| Command                             | Description                                                                                                        |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>interface fc zoning autosave</b> | Enable the SN 5428 Storage Router to save zoning changes received from switches in the fabric.                     |
| <b>interface fc zoning default</b>  | Select the level of communication between the SN 5428 and devices in the fabric where there is no active zone set. |
| <b>interface fc? diag</b>           | Set the named FC interface into diagnostic mode for testing purposes.                                              |
| <b>interface fc? enable</b>         | Enable the named FC interface.                                                                                     |
| <b>interface fc? loopback</b>       | Initiate a loopback test on the named FC interface.                                                                |
| <b>show fc</b>                      | Display global configuration information for SN 5428 Fibre Channel interfaces.                                     |

# interface fc? al-fairness

To enable the fairness algorithm (loop priority) on the named Fibre Channel interface, use the **interface fc? al-fairness** command. To disable the fairness algorithm on the named FC interface, use the **no** form of this command.

**interface fc? al-fairness enable**

**no interface fc? al-fairness enable**

## Syntax Description

|               |                                                                                                                                                                                                                                              |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>fc?</i>    | The name of the FC interface for which you are setting this parameter. Valid values are fc1 through fc8. When you type the <b>interface fc?</b> command, the CLI lists the interfaces available. You cannot specify a nonexistent interface. |
| <b>enable</b> | Keyword, required to enable the fairness algorithm on the named FC interface.                                                                                                                                                                |

## Defaults

The fairness algorithm is disabled on all FC interfaces by default, allowing the switch to have priority.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

When the fairness algorithm is not enabled for a specific FC interface, the switch receives priority. Use this command to enable the fairness algorithm for the named interface, removing the switch priority for that interface.



### Note

All SN 5428s in a cluster should be configured with the same interface-specific parameters, allowing failover of SCSI routing instances to provide consistent performance characteristics.

## Examples

The following example enables the fairness algorithm on the FC interface named *fc6*:

```
[SN5428A] # interface fc6 al-fairness enable
```

The following example disables the fairness algorithm on the FC interface named *fc3*. The switch receives priority for traffic on this interface.

```
[SN5428A] # no interface fc3 al-fairness enable
```

**Related Commands**

| <b>Command</b>                      | <b>Description</b>                                                                               |
|-------------------------------------|--------------------------------------------------------------------------------------------------|
| <b>interface fc? default</b>        | Return the named FC interface to its default operational characteristics.                        |
| <b>interface fc?<br/>fan-enable</b> | Enable Fabric Address Notification (FAN) on the named FC interface.                              |
| <b>interface fc? linkspeed</b>      | Set the transfer rate for the named FC interface.                                                |
| <b>interface fc?<br/>mfs-bundle</b> | Enable Multi-Frame Sequence bundling for the named FC interface.                                 |
| <b>interface fc? type</b>           | Set the port type for the named FC interface.                                                    |
| <b>show interface</b>               | Display operational and configuration information for the specified interface or all interfaces. |

# interface fc? default

To return the named Fibre Channel interface to its default operational characteristics, use the **interface fc? default** command.

**interface fc? default**

## Syntax Description

|            |                                                                                                                                                                                                                                                               |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>fc?</i> | The name of the FC interface to be returned to its default operational characteristics. Valid values are fc1 through fc8. When you type the <b>interface fc?</b> command, the CLI lists the interfaces available. You cannot specify a nonexistent interface. |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Defaults

The following are the default operational characteristics for the Fibre Channel interface:

- fairness algorithm is disabled (switch has priority)
- Fabric Address Notification (FAN) is enabled
- transfer rate is automatically negotiated (linkspeed auto)
- Multi-Frame sequence bundling is enabled
- port type is generic loop, indicating the port can function as either a fabric loop port (FL\_Port), an expansion port (E\_Port) or a fabric port (F\_Port).

## Command Modes

Administrator.

## Command History

| Release | Modification                                  |
|---------|-----------------------------------------------|
| 2.2.1   | This command was introduced.                  |
| 2.3.1   | The default port type was changed to GL_Port. |

## Usage Guidelines

Use this command to quickly reset the named FC interface to its default operational characteristics. The results of this command are the same as if each of the following commands were issued for the same named FC interface:

- **no interface fc? al-fairness enable**
- **interface fc? fan-enable enable**
- **interface fc? linkspeed auto**
- **interface fc? mfs-bundle enable timeout 10**
- **interface fc? type gl-port**



### Note

All SN 5428s in a cluster should be configured with the same interface-specific parameters, allowing failover of SCSI routing instances to provide consistent performance characteristics.

**Examples**

The following example returns the operational characteristics to their default settings for the FC interface named *fc6*:

```
[SN5428A]# interface fc6 default
```

**Related Commands**

| Command                              | Description                                                                                      |
|--------------------------------------|--------------------------------------------------------------------------------------------------|
| <b>interface fc?<br/>al-fairness</b> | Enable the fairness algorithm on the named FC interface.                                         |
| <b>interface fc?<br/>fan-enable</b>  | Enable Fabric Address Notification (FAN) on the named FC interface.                              |
| <b>interface fc? linkspeed</b>       | Set the transfer rate for the named FC interface.                                                |
| <b>interface fc?<br/>mfs-bundle</b>  | Enable Multi-Frame Sequence bundling for the named FC interface.                                 |
| <b>interface fc? type</b>            | Set the port type for the named FC interface.                                                    |
| <b>show interface</b>                | Display operational and configuration information for the specified interface or all interfaces. |

# interface fc? diag

To set the named Fibre Channel interface into diagnostic mode for testing purposes, use the **interface fc? diag** command.

**interface fc? diag**

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                       |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>fc?</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | The name of the FC interface to be placed into diagnostic mode. Valid values are fc1 through fc8. When you type the <b>interface fc?</b> command, the CLI lists the interfaces available. You cannot specify a nonexistent interface. |
| <b>Defaults</b>           | None.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                       |
| <b>Command Modes</b>      | Administrator.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                       |
| <b>Command History</b>    | <b>Release</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <b>Modification</b>                                                                                                                                                                                                                   |
|                           | 2.2.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | This command was introduced.                                                                                                                                                                                                          |
| <b>Usage Guidelines</b>   | <p>Use this command to change the named FC interface to diagnostic mode prior to performing an internal or external loopback test.</p> <ul style="list-style-type: none"> <li>• Use the <b>interface fc? enable</b> command to reenble the FC interface. An FC interface must be enabled to run an online loopback test, or to allow access to storage targets.</li> <li>• Use the <b>no interface fc? enable</b> command to disable the FC interface. When you are ready to allow access to the storage targets, you can enable all FC interfaces at once via the <b>interface fc enable</b> command, or enable individual interfaces via the <b>interface fc? enable</b> command.</li> </ul> |                                                                                                                                                                                                                                       |
| <b>Examples</b>           | <p>The following example sets the FC interfaces <i>fc6</i> into a diagnostic state and then performs an internal loopback test:</p> <pre>[SN5428A]# interface fc6 diag [SN5428A]# interface fc6 loopback internal</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                       |
| <b>Related Commands</b>   | <b>Command</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <b>Description</b>                                                                                                                                                                                                                    |
|                           | <b>interface fc diag</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Set all FC interfaces into diagnostic mode for testing purposes.                                                                                                                                                                      |
|                           | <b>interface fc enable</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Enable all FC interfaces.                                                                                                                                                                                                             |
|                           | <b>interface fc? enable</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Enable the named FC interface.                                                                                                                                                                                                        |

| <b>Command</b>                | <b>Description</b>                                                             |
|-------------------------------|--------------------------------------------------------------------------------|
| <b>interface fc? loopback</b> | Initiate a loopback test on the named FC interface.                            |
| <b>show fc</b>                | Display global configuration information for SN 5428 Fibre Channel interfaces. |

# interface fc? enable

To enable the named Fibre Channel interface, use the **interface fc? enable** command. To disable the named FC interface, use the **no** form of this command.

**interface fc? enable**

**no interface fc? enable**

|                           |            |                                                                                                                                                                                                                   |
|---------------------------|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>fc?</i> | The name of the FC interface to be enabled. Valid values are fc1 through fc8. When you type the <b>interface fc?</b> command, the CLI lists the interfaces available. You cannot specify a nonexistent interface. |
|---------------------------|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |       |
|-----------------|-------|
| <b>Defaults</b> | None. |
|-----------------|-------|

|                      |                |
|----------------------|----------------|
| <b>Command Modes</b> | Administrator. |
|----------------------|----------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 2.2.1          | This command was introduced. |

**Usage Guidelines** An FC interface must be enabled to allow access to storage targets or perform online loopback testing. Use this command to enable an individual FC interface.

If you experience a problem with the Fibre Channel interface or a specific storage resource, use the **no** form of this command to disable the named FC interface.

**Examples** The following example enables the FC interface *fc6* and then performs an online loopback test:

```
[SN5428A] # interface fc6 enable
[SN5428A] # interface fc6 loopback online
```

The following example disables the FC interface *fc3*:

```
[SN5428A] # no interface fc3 enable
```

| <b>Related Commands</b> | <b>Command</b>                | <b>Description</b>                                                             |
|-------------------------|-------------------------------|--------------------------------------------------------------------------------|
|                         | <b>interface fc diag</b>      | Set all FC interfaces into diagnostic mode for testing purposes.               |
|                         | <b>interface fc enable</b>    | Enable all FC interfaces.                                                      |
|                         | <b>interface fc? diag</b>     | Set the named FC interface into diagnostic mode for testing purposes.          |
|                         | <b>interface fc? loopback</b> | Initiate a loopback test on the named FC interface.                            |
|                         | <b>show fc</b>                | Display global configuration information for SN 5428 Fibre Channel interfaces. |

# interface fc? fan-enable

To enable Fabric Address Notification (FAN) on the named Fibre Channel interface, use the **interface fc? fan-enable** command. To disable FAN on the named FC interface, use the **no** form of this command.

**interface fc? fan-enable enable**

**no interface fc? fan-enable enable**

## Syntax Description

|               |                                                                                                                                                                                                                                              |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>fc?</i>    | The name of the FC interface for which you are setting this parameter. Valid values are fc1 through fc8. When you type the <b>interface fc?</b> command, the CLI lists the interfaces available. You cannot specify a nonexistent interface. |
| <b>enable</b> | Keyword, required to enable FAN on the named FC interface.                                                                                                                                                                                   |

## Defaults

FAN is enabled on all FC interfaces by default

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

Use this command to enable or disable FAN loop login behavior on the named FC interface.



### Note

All SN 5428s in a cluster should be configured with the same interface-specific parameters, allowing failover of SCSI routing instances to provide consistent performance characteristics.

## Examples

The following example disables FAN on the FC interface named *fc6*:

```
[SN5428A]# no interface fc6 fan-enable enable
```

The following example enables FAN on the FC interface named *fc3*.

```
[SN5428A]# interface fc3 fan-enable enable
```

## Related Commands

| Command                          | Description                                                               |
|----------------------------------|---------------------------------------------------------------------------|
| <b>interface fc? al-fairness</b> | Enable the fairness algorithm on the named FC interface.                  |
| <b>interface fc? default</b>     | Return the named FC interface to its default operational characteristics. |

| <b>Command</b>                      | <b>Description</b>                                                                               |
|-------------------------------------|--------------------------------------------------------------------------------------------------|
| <b>interface fc? linkspeed</b>      | Set the transfer rate for the named FC interface.                                                |
| <b>interface fc?<br/>mfs-bundle</b> | Enable Multi-Frame Sequence bundling for the named FC interface.                                 |
| <b>interface fc? type</b>           | Set the port type for the named FC interface.                                                    |
| <b>show interface</b>               | Display operational and configuration information for the specified interface or all interfaces. |

# interface fc? linkspeed

To set the transfer rate for the named Fibre Channel interface, use the **interface fc? linkspeed** command.

```
interface fc? linkspeed {auto | 1gb | 2gb}
```

| Syntax Description |  |                                                                                                                                                                                                                                              |
|--------------------|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>fc?</i>         |  | The name of the FC interface for which you are setting this parameter. Valid values are fc1 through fc8. When you type the <b>interface fc?</b> command, the CLI lists the interfaces available. You cannot specify a nonexistent interface. |
| <b>auto</b>        |  | Keyword, indicating the transfer rate will be negotiated.                                                                                                                                                                                    |
| <b>1gb</b>         |  | Keyword, indicating the transfer rate will be fixed at 1 Gbps.                                                                                                                                                                               |
| <b>2gb</b>         |  | Keyword, indicating the transfer rate will be fixed at 2 Gbps.                                                                                                                                                                               |

**Defaults** The transfer rate is automatically negotiated to either 1 Gbps or 2 Gbps, by default.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command to change the transfer rate for the named FC interface.



**Note**

All SN 5428s in a cluster should be configured with the same interface-specific parameters, allowing failover of SCSI routing instances to provide consistent performance characteristics.

**Examples** The following example sets the transfer rate for to 2 Gbps for the FC interface named *fc6*:

```
[SN5428A]# interface fc6 linkspeed 2gb
```

| Related Commands | Command                          | Description                                                               |
|------------------|----------------------------------|---------------------------------------------------------------------------|
|                  | <b>interface fc? al-fairness</b> | Enable the fairness algorithm on the named FC interface.                  |
|                  | <b>interface fc? default</b>     | Return the named FC interface to its default operational characteristics. |
|                  | <b>interface fc? fan-enable</b>  | Enable Fabric Address Notification (FAN) on the named FC interface.       |
|                  | <b>interface fc? mfs-bundle</b>  | Enable Multi-Frame Sequence bundling for the named FC interface.          |

| <b>Command</b>            | <b>Description</b>                                                                               |
|---------------------------|--------------------------------------------------------------------------------------------------|
| <b>interface fc? type</b> | Set the port type for the named FC interface.                                                    |
| <b>show interface</b>     | Display operational and configuration information for the specified interface or all interfaces. |

# interface fc? loopback

To initiate a loopback test on the named Fibre Channel interface, use the **interface fc? loopback** command.

```
interface fc? loopback {external | internal | online}
```

## Syntax Description

|                 |                                                                                                                                                                                                                  |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>fc?</i>      | The name of the FC interface to be tested. Valid values are fc1 through fc8. When you type the <b>interface fc?</b> command, the CLI lists the interfaces available. You cannot specify a nonexistent interface. |
| <b>external</b> | Keyword, indicating an external loopback test will be performed. The FC interface must be in a diagnostic state.                                                                                                 |
| <b>internal</b> | Keyword, indicating an internal loopback test will be performed. The FC interface must be in a diagnostic state.                                                                                                 |
| <b>online</b>   | Keyword, indicating an online loopback test will be performed. The FC interface must be enabled.                                                                                                                 |

## Defaults

None.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

Loopback tests are part of standard diagnostic procedures. To display the results or status of a loopback test, use the **show interface fc?** command.

Before performing a loopback test, the named FC interface must be in the correct state.

- For online loopback testing, the FC interface must be enabled. Use the **interface fc? enable** command to enable the FC interface before performing online loopback testing.
- For external or internal loopback testing, the FC interface must be in a diagnostic state. Use the **interface fc? diag** command to set the FC interface into a diagnostic state before performing external or internal loopback testing.

## Examples

The following example sets the FC interface *fc6* into a diagnostic state and then performs an internal loopback test:

```
[SN5428A]# interface fc6 diag
[SN5428A]# interface fc6 loopback internal
```

The following example enables the FC interface *fc3* and then performs an online loopback test:

```
[SN5428A] # interface fc3 enable
[SN5428A] # interface fc3 loopback online
```

**Related Commands**

| Command                     | Description                                                                                      |
|-----------------------------|--------------------------------------------------------------------------------------------------|
| <b>interface fc diag</b>    | Set all FC interfaces into diagnostic mode for testing purposes.                                 |
| <b>interface fc enable</b>  | Enable all FC interfaces.                                                                        |
| <b>interface fc? diag</b>   | Set the named FC interface into diagnostic mode for testing purposes.                            |
| <b>interface fc? enable</b> | Enable the named FC interface.                                                                   |
| <b>show interface</b>       | Display operational and configuration information for the specified interface or all interfaces. |

## interface fc? mfs-bundle

To enable Multi-Frame Sequence (MFS) bundling for the named Fibre Channel interface, use the **interface fc? mfs-bundle** command. To disable MFS bundling for the named FC interface, use the **no** form of this command.

```
interface fc? mfs-bundle enable timeout nn
```

```
no interface fc? mfs-bundle enable
```

### Syntax Description

|                   |                                                                                                                                                                                                                                              |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>fc?</i>        | The name of the FC interface for which you are setting this parameter. Valid values are fc1 through fc8. When you type the <b>interface fc?</b> command, the CLI lists the interfaces available. You cannot specify a nonexistent interface. |
| <b>enable</b>     | Keyword, required to enable MFS bundling on the named FC interface.                                                                                                                                                                          |
| <b>timeout nn</b> | The timeout threshold, in milliseconds. Valid values are 10 through 20480. The default timeout value is 10 msec.                                                                                                                             |

### Defaults

MFS bundling is enabled on all FC interfaces, by default. The default timeout value is 10 msec.

### Command Modes

Administrator.

### Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

### Usage Guidelines

MFS bundling is used to support systems that require frames to be sequenced in a particular order.



#### Note

All SN 5428s in a cluster should be configured with the same interface-specific parameters, allowing failover of SCSI routing instances to provide consistent performance characteristics.

### Examples

The following example enables MFS bundling for the FC interface named *fc6*, and sets the timeout value to 640 msec:

```
[SN5428A]# interface fc6 mfs-bundle enable timeout 640
```

The following example disables MFS bundling for the FC interface named *fc3*:

```
[SN5428A]# no interface fc6 mfs-bundle enable
```

**Related Commands**

| <b>Command</b>                       | <b>Description</b>                                                                               |
|--------------------------------------|--------------------------------------------------------------------------------------------------|
| <b>interface fc?<br/>al-fairness</b> | Enable the fairness algorithm on the named FC interface.                                         |
| <b>interface fc? default</b>         | Return the named FC interface to its default operational characteristics.                        |
| <b>interface fc?<br/>fan-enable</b>  | Enable Fabric Address Notification (FAN) on the named FC interface.                              |
| <b>interface fc? linkspeed</b>       | Set the transfer rate for the named FC interface.                                                |
| <b>interface fc? type</b>            | Set the port type for the named FC interface.                                                    |
| <b>show interface</b>                | Display operational and configuration information for the specified interface or all interfaces. |

# interface fc? type

To set the port type for the named Fibre Channel interface, use the **interface fc? type** command.

```
interface fc? type {auto | f-port | fl-port | g-port | gl-port}
```

```
interface fc? type tl-port mode {autobridge | autolearn}
```

## Syntax Description

|                        |                                                                                                                                                                                                                                              |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>fc?</i>             | The name of the FC interface for which you are setting this parameter. Valid values are fc1 through fc8. When you type the <b>interface fc?</b> command, the CLI lists the interfaces available. You cannot specify a nonexistent interface. |
| <b>auto</b>            | Keyword, indicating the port type is automatically negotiated and functions as a generic loop (GL_Port).                                                                                                                                     |
| <b>f-port</b>          | Keyword, indicating the port type is fabric. F_Ports are fabric ports.                                                                                                                                                                       |
| <b>fl-port</b>         | Keyword, indicating the port type is fabric loop (also known as “public loop”).                                                                                                                                                              |
| <b>g-port</b>          | Keyword, indicating the port type is generic and can function as either an F_Port or an E_Port. An E_Port (also known as an “expansion port”) is used to link multiple FC switches together into a fabric.                                   |
| <b>gl-port</b>         | Keyword, indicating the port type is generic loop and can function as either an F_Port, an FL_Port or an E_Port.                                                                                                                             |
| <b>tl-port</b>         | Keyword, indicating the port type is translated loop.                                                                                                                                                                                        |
| <b>mode autobridge</b> | Keywords, indicating public targets are made visible to the initiator in a private loop.                                                                                                                                                     |
| <b>mode autolearn</b>  | Keywords, indicating targets in a private loop are made visible.                                                                                                                                                                             |

## Defaults

The port type is *generic loop* (GL\_Port), by default.

## Command Modes

Administrator.

## Command History

| Release | Modification                                                                                              |
|---------|-----------------------------------------------------------------------------------------------------------|
| 2.2.1   | This command was introduced.                                                                              |
| 2.3.1   | The default was changed to <b>gl-port</b> , and the <b>g-port</b> and <b>fl-port</b> keywords were added. |

## Usage Guidelines

Select the appropriate port type based on the connected equipment. By default, all of the SN 5428 FC ports are defined as self configuring GL\_Ports.

- A GL\_Port configures as an FL\_Port when connected to a loop of public devices, an F\_Port when connected to a single device, or an E\_Port when connected to another SN 5428 or an FC-SW-2 compliant switch. A GL\_Port may also configure as an E\_Port when connected to a switch running non-FC-SW-2 compliant firmware.

- A G\_Port configures as an F\_Port when connected to a single public device or an E\_Port when connected to another SN 5428 or an FC-SW-2 compliant switch. A G\_Port may also configure as an E\_Port when connected to a switch running non-FC-SW-2 compliant firmware.
- An F\_Port supports connection to a single public device (N\_Port).
- An FL\_Port supports connection to a loop of up to 126 public devices (NL\_Port).
- A TL\_Port supports connection to a loop of up to 126 private devices with the ability to communicate with “off-loop” devices, such as public fabric devices and private devices on other TL\_Ports. TL\_Ports connect to devices that confirm to the Fibre Channel-Private Loop SCSI Direct Attach (FC-PLDA) standard. A TL\_Port acts as a proxy for the off-loop device, translating private frames to and from public frames. Each TL\_Port can proxy up to 64 off-loop devices.

Public devices have full Fibre Channel addressing capability and can communicate with any other public device on the fabric; private devices do not have full FC addressing capability. Private devices have only the Arbitrated Loop Physical Address (ALPA) portion.

**Note**

All SN 5428s in a cluster should be configured with the same interface-specific parameters, allowing failover of SCSI routing instances to provide consistent performance characteristics.

**Examples**

The following example sets the port type to *fabric* for the FC interface named *fc6*:

```
[SN5428A]# interface fc6 type f-port
```

The following example set the port type to translated loop for the FC interface named *fc3*. The mode is *autolearn*, so targets in private loop are made visible.

```
[SN5428A]# interface fc3 type tl-port mode autolearn
```

**Related Commands**

| Command                          | Description                                                                                      |
|----------------------------------|--------------------------------------------------------------------------------------------------|
| <b>interface fc? al-fairness</b> | Enable the fairness algorithm on the named FC interface.                                         |
| <b>interface fc? default</b>     | Return the named FC interface to its default operational characteristics.                        |
| <b>interface fc? fan-enable</b>  | Enable Fabric Address Notification (FAN) on the named FC interface.                              |
| <b>interface fc? linkspeed</b>   | Set the transfer rate for the named FC interface.                                                |
| <b>interface fc? mfs-bundle</b>  | Enable Multi-Frame Sequence bundling for the named FC interface.                                 |
| <b>show interface</b>            | Display operational and configuration information for the specified interface or all interfaces. |

# interface ge?

To set various operational parameters associated with the Gigabit Ethernet interface, such as the size of the maximum transfer unit (MTU) or the use of VLANs, use the **interface ge?** command. To disable the use of VLANs, use the **no** form of this command. To specify that autonegotiation will never be used on this interface, use the **interface ge? no autonegotiation** command.

```
interface ge? {autonegotiation [autodetect] | mtusize {nn | default}}
```

```
interface ge? no autonegotiation
```

```
interface ge? vlan enable
```

```
no interface ge? vlan enable
```

## Syntax Description

|                                   |                                                                                                                                                                                                         |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>ge?</i>                        | The name of the interface for which you are setting this parameter. When you type the <b>interface ge?</b> command, the CLI lists the interfaces available. You cannot specify a nonexistent interface. |
| <b>autonegotiation</b>            | Autonegotiation will always be used on this interface.                                                                                                                                                  |
| <b>autonegotiation autodetect</b> | Automatically detect if autonegotiation should be used for this interface. This is the default setting.                                                                                                 |
| <b>mtusize nn</b>                 | The size of the MTU, in bytes. <i>nn</i> is an integer between 1500 and 9000 inclusive. Gigabit Ethernet interfaces may support jumbo frames.                                                           |
| <b>mtusize default</b>            | Reset the value to the factory default of 1500 bytes.                                                                                                                                                   |
| <b>vlan enable</b>                | Enable VLANs for this interface. This is the default.                                                                                                                                                   |

## Defaults

MTU size defaults to 1500 bytes. Autonegotiation defaults to *autodetect*. For SN 5428s deployed for SCSI routing, the use of VLANs is enabled by default.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

All SN 5428s in a cluster should be configured with the same MTU size and other interface-specific parameters, allowing failover of applications to provide consistent performance characteristics.

Use the **no interface ge? vlan enable** command to quickly restrict VLAN functionality on the SN 5428's Gigabit Ethernet interface for troubleshooting purposes.

---

**Examples**

The following example enables autonegotiation on the Gigabit Ethernet interface, *ge1*.

```
[SN5428A] # interface ge1 autonegotiation
```

The following example disables VLANs for the SN 5428 Gigabit Ethernet interface, *ge2*:

```
[SN5428A] # no interface ge2 vlan enable
```

---

**Related Commands**

| Command                     | Description                                                                                      |
|-----------------------------|--------------------------------------------------------------------------------------------------|
| <code>show interface</code> | Display operational and configuration information for the specified interface or all interfaces. |

---

# interface ha ip-address

To specify the IP address and subnet mask for this system's high availability interface, use the **interface ha ip-address** command.

```
interface ha ip-address {A.B.C.D/bits | A.B.C.D/1.2.3.4}
```

| Syntax Description     |                                                                                                                                                                  |  |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| <i>A.B.C.D/nn</i>      | The IP address of the HA interface. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The <i>/bits</i> specifies the subnet mask in CIDR style.      |  |
| <i>A.B.C.D/1.2.3.4</i> | The IP address of the HA interface. <i>A.B.C.D</i> is the dotted quad notation of the IP address. <i>1.2.3.4</i> is the dotted quad notation of the subnet mask. |  |

| Defaults |  |
|----------|--|
| None.    |  |

| Command Modes  |  |
|----------------|--|
| Administrator. |  |

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

| Usage Guidelines                                                                                                                                                                                                                                   |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| The HA features are used within a cluster of SN 5428s. Each member of the cluster communicates over the HA and management interfaces, exchanging heartbeats and other configuration information, allowing for failover in case of system problems. |  |

The HA interface and the management interface must be on unique IP subnets. In a cluster, the HA interfaces for all SN 5428s should be on the same IP subnet.

After initial system configuration, use the **setup cluster** command to change the configuration of the SN 5428's high availability environment.

For SN 5428s deployed for transparent SCSI routing, or standalone SN 5428s deployed for SCSI routing, the HA interface is optional.

| Examples                                                                                     |  |
|----------------------------------------------------------------------------------------------|--|
| The following example assigns the IP address of 10.1.20.56/24 to the SN 5428's HA interface: |  |

```
[SN5428B]# interface ha ip-address 10.1.20.56/24
```

| Related Commands | Command                          | Description                                                              |
|------------------|----------------------------------|--------------------------------------------------------------------------|
|                  | <b>interface mgmt ip-address</b> | Specify the management interface IP address and subnet mask.             |
|                  | <b>save all</b>                  | Save all configuration information.                                      |
|                  | <b>save system</b>               | Save selected system configuration information, including HA IP address. |

| <b>Command</b>       | <b>Description</b>                                                               |
|----------------------|----------------------------------------------------------------------------------|
| <b>setup cluster</b> | Change the configuration of the SN 5428's high availability environment.         |
| <b>show cluster</b>  | Display cluster-related operational statistics, including heartbeat information. |
| <b>show ha</b>       | Display HA operational statistics for the SN 5428 or for a specific application. |

# interface mgmt ip-address

To specify the IP address and subnet mask of the interface labeled MGMT on the front panel of the SN 5428 Storage Router, use the **interface mgmt ip-address** command. This address is used to manage the SN 5428 via Telnet, the web-based GUI, or SNMP.

**interface mgmt ip-address** {*A.B.C.D/bits* | *A.B.C.D/1.2.3.4*}

| Syntax                 | Description                                                                                                                                                              |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>A.B.C.D/bits</i>    | The IP address of the management interface. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The <i>/bits</i> specifies the subnet mask in CIDR style.      |
| <i>A.B.C.D/1.2.3.4</i> | The IP address of the management interface. <i>A.B.C.D</i> is the dotted quad notation of the IP address. <i>1.2.3.4</i> is the dotted quad notation of the subnet mask. |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** The management and HA interfaces must be on unique IP subnets. In a cluster, the management interfaces for all SN 5428s should be on the same IP subnet.

**Examples** The following example assigns the IP address of *10.1.10.244/24* to the SN 5428's management interface:

```
[SN5428A]# interface mgmt ip-address 10.1.10.244/24
```

| Related Commands | Command                        | Description                                                                                        |
|------------------|--------------------------------|----------------------------------------------------------------------------------------------------|
|                  | <b>interface ha ip-address</b> | Specify the HA interface IP address and subnet mask.                                               |
|                  | <b>ip route</b>                | Add a static route to the SN 5428 Storage Router routing table.                                    |
|                  | <b>save all</b>                | Save all configuration information.                                                                |
|                  | <b>save system</b>             | Save selected system configuration information, including management and HA interface information. |
|                  | <b>setup mgmt</b>              | Run the wizard to configure the management interface.                                              |

| <b>Command</b>        | <b>Description</b>                                                                               |
|-----------------------|--------------------------------------------------------------------------------------------------|
| <b>show cluster</b>   | Display cluster-related operational statistics, including heartbeat information.                 |
| <b>show interface</b> | Display operational and configuration information for the specified interface or all interfaces. |

# ip default-gateway

To add a gateway to the default route in the SN 5428 routing table, use the **ip default-gateway** command. To delete the gateway, use the **no** form of this command.

**ip default-gateway** *E.F.G.H*

**no ip default-gateway** [*A.B.C.D*]

| Syntax         | Description                                                                                |
|----------------|--------------------------------------------------------------------------------------------|
| <i>E.F.G.H</i> | The default gateway IP address.                                                            |
| <i>A.B.C.D</i> | (Optional) The IP address of the default route. The gateway to this route will be removed. |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** All IP interfaces in the SN 5428 use the routing table to reach services and networks outside their local network. Other facilities, such as SNMP and connections to an NTP server or DNS servers, may also use the routing table. Use the **ip default-gateway** command to add a gateway to the default route in this table.

**Examples** The following example adds the gateway *10.3.40.1* to the default route in the SN 5428 routing table:

```
[SN5428A]# ip default-gateway 10.3.40.1
```

| Related Commands | Command           | Description                                                                                                                   |
|------------------|-------------------|-------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>ip route</b>   | Add a static route to the SN 5428 Storage Router routing table.                                                               |
|                  | <b>show ip</b>    | Display entries from the SN 5428 Storage Router routing table and statistics about the protocols used in the SN 5428 network. |
|                  | <b>show route</b> | Display the default routes.                                                                                                   |

# ip domain-name

To specify the name of the SN 5428 domain, use the **ip domain-name** command. To remove a domain name, use the **no** form of this command.

**ip domain-name** *name*

**no ip domain-name**

| Syntax Description | <i>name</i> | The name of the SN 5428 domain. |
|--------------------|-------------|---------------------------------|
|--------------------|-------------|---------------------------------|

| Defaults | None. |
|----------|-------|
|----------|-------|

| Command Modes | Administrator. |
|---------------|----------------|
|---------------|----------------|

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use the **ip domain-name** command in conjunction with the **ip name-server** command. The SN 5428 requires access to a DNS if any IP addresses are entered as host names via any of the SN 5428 management interfaces, or if the SN 5428 management interface IP address is to be correlated with a DNS host name.



**Note**

If the DNS is outside the SN 5428 management subnet, use the **ip route** command to add an appropriate gateway IP address to the SN 5428 routing table.

**Examples** The following example assigns the domain name *abc123z.com* to the SN 5428.

```
[SN5428A] # ip domain-name abc123z.com
```

| Related Commands | Command                   | Description                                                         |
|------------------|---------------------------|---------------------------------------------------------------------|
|                  | <b>ip default-gateway</b> | Configure a gateway for the SN 5428's default route.                |
|                  | <b>ip name-server</b>     | Specify the IP addresses of a primary (and optional secondary) DNS. |
|                  | <b>ip route</b>           | Add a static route to the SN 5428 Storage Router routing table.     |
|                  | <b>setup mgmt</b>         | Run the wizard to configure the management interface.               |

# ip name-server

To specify the IP address of the primary and optional secondary Domain Name Server (DNS), use the **ip name-server** command. To remove the settings for current domain name servers, use the **no** form of this command.

```
ip name-server A.B.C.D [E.F.G.H]
```

```
no ip name-server
```

## Syntax Description

|                |                                                                                                                                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <i>A.B.C.D</i> | The IP address of a primary Domain Name Server, accessible by the SN 5428. <i>A.B.C.D</i> is the dotted quad notation of the IP address. |
| <i>E.F.G.H</i> | (Optional) The IP address of a secondary DNS, accessible by the SN 5428. <i>E.F.G.H</i> is the dotted quad notation of the IP address.   |

## Defaults

None.

## Command Modes

Administrator.

## Command History

| Release | Configuration                |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

The SN 5428 requires access to a DNS if any IP addresses are entered as host names via any of the SN 5428 management interfaces, or if the SN 5428 management interface IP address is to be correlated with a DNS host name. To use the services of a DNS, you must also assign a domain name to the SN 5428 via the **ip domain-name** command.



### Note

If the DNS is outside the SN 5428 management subnet, use the **ip route** command to add an appropriate gateway IP address to the SN 5428 routing table.

## Examples

The following example assigns the domain name *abc123z.com* to the SN 5428, and assigns the IP address of the primary DNS to *10.1.40.243* and the secondary DNS to *10.1.50.249*:

```
[SN5428A]# ip domain-name abc123z.com
[SN5428A]# ip name-server 10.1.40.243 10.1.50.249
```

## Related Commands

| Command                   | Description                                          |
|---------------------------|------------------------------------------------------|
| <b>ip default-gateway</b> | Configure a gateway for the SN 5428's default route. |
| <b>ip domain-name</b>     | Specify the name of the SN 5428's domain.            |

| <b>Command</b>    | <b>Description</b>                                              |
|-------------------|-----------------------------------------------------------------|
| <b>ip route</b>   | Add a static route to the SN 5428 Storage Router routing table. |
| <b>setup mgmt</b> | Run the wizard to configure the management interface.           |

# ip route

To add a static route to the SN 5428 routing table, use the **ip route** command. The specified IP address is accessed via the gateway specified in the command. To remove a static route from the routing table, use the **no** form of this command.

```
ip route {A.B.C.D/bits | A.B.C.D/1.2.3.4} E.F.G.H
```

```
no ip route {A.B.C.D/bits | A.B.C.D/1.2.3.4}
```

## Syntax Description

|                        |                                                                                                                                                                  |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>A.B.C.D/bits</i>    | The IP address of the static route. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The <i>/bits</i> specifies the subnet mask in CIDR style.      |
| <i>A.B.C.D/1.2.3.4</i> | The IP address of the static route. <i>A.B.C.D</i> is the dotted quad notation of the IP address. <i>1.2.3.4</i> is the dotted quad notation of the subnet mask. |
| <i>E.F.G.H</i>         | The gateway IP address through which the static route ( <i>A.B.C.D/bits</i> or <i>A.B.C.D/1.2.3.4</i> ) is accessed.                                             |

## Defaults

None.

## Command Modes

Administrator.

## Command History

| Release | Modification                                                                                                  |
|---------|---------------------------------------------------------------------------------------------------------------|
| 2.2.1   | This command was introduced.                                                                                  |
| 2.3.1   | The <b>interface ha</b> , <b>interface mgmt</b> , <b>interface ge?</b> and <b>vlan</b> keywords were removed. |

## Usage Guidelines

All IP interfaces in the SN 5428 use the routing table to reach services and networks outside their local network. Other facilities, such as SNMP and connections to an NTP server or DNS servers, may also use the routing table. Use the **ip route** command to specify routes for servers or networks outside the local networks associated with the SN 5428's IP interfaces.

Use the **show ip route** command to display the SN 5428 routing table. Use the **show route** command to display all the default routes, included the routes that have been configured but not added to the SN 5428 routing table.



### Note

A route is not added to the routing table until the associated IP address is configured. The CLI displays an informational message if a route is added for an IP address that is not yet configured.

**Examples**

The following command adds a unique route for IP address *10.1.30.0*, specifying the subnet mask in dotted quad notation:

```
[SN5428A]# ip route 10.1.30.0/255.255.255.0 10.1.30.10
```

The following command adds a unique route for IP address 10.1.40.0, which is not yet configured in the SN 5428:

```
[SN5428A]# ip route 10.1.40.0/24 10.1.40.10
Route will be added when a suitable IP address is added
```

**Related Commands**

| Command                   | Description                                                                                                                    |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>ip default-gateway</b> | Configure a gateway for the SN 5428's default route.                                                                           |
| <b>ip domain-name</b>     | Specify the name of the SN 5428's domain.                                                                                      |
| <b>ip name-server</b>     | Specify the IP addresses of a primary (and optional secondary) DNS.                                                            |
| <b>show ip</b>            | Display entries from the SN 5428 Storage Router routing table, and statistics about the protocols used in the SN 5428 network. |
| <b>show route</b>         | Display the default routes.                                                                                                    |

# logging #?

To insert a routing rules entry into the logging table before the specified entry, use the **logging #?** command.

## logging #?

**logging #nn level notification-level from {all | facility-name} to destination1 [destination2...]**

| Syntax Description                       |  |                                                                                                                                                                                                                                                                                             |
|------------------------------------------|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>#?</b>                                |  | Request an indexed list of entries in the logging table.                                                                                                                                                                                                                                    |
| <b>#nn</b>                               |  | The index number from the displayed list of entries. The new routing rule will be inserted before the specified logging table entry.                                                                                                                                                        |
| <i>notification-level</i>                |  | Limit logging to messages of a specified level or lower levels. See Table 11-8 in the Usage Guidelines section for a list of valid names that can be used for the <i>notification-level</i> argument.                                                                                       |
| <b>from all</b>                          |  | Associate the specified level and destinations with all facilities.                                                                                                                                                                                                                         |
| <b>from facility-name</b>                |  | The name of the facility. A facility is the feature area from which the message is received. See Table 11-9 in the Usage Guidelines section for a list of valid facility names. Each facility can have eight notification levels. Each notification level can have up to seven destination. |
| <b>to destination1 [destination2...]</b> |  | At least one of the destinations described in Table 11-10.                                                                                                                                                                                                                                  |

## Defaults

None.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.3.1   | This command was introduced. |

## Usage Guidelines

Event, trace and debug messages can be routed to various destinations, based on the notification level of the message and the application area (facility) that generated the message. When a log message is received by the SN 5428, the logging table rules are searched by facility name and by message level until a match is found. The log message is sent to all the destinations specified by the matching rule.

New routing rules are normally appended to the existing rules in the table. Use this command to insert a routing rule at a specific location within the table.

To display an indexed lists of entries in the logging table, use the number sign (#) character followed by a question mark (?). That action will cause the routing rules in the logging table to be displayed as a numbered (indexed) set of lines. The command is displayed at the prompt below the list to the point of the # keyword. Complete the command by entering the appropriate index number and the desired keywords and variables to compose the new routing rule. The new routing rule will be added to the table before the specified entry.

The level limits logging to messages of the specified notification level or lower levels, based on level number. Table 11-8 describes the available logging levels.

**Table 11-8 Logging Level Notification Levels and Corresponding Numbers**

| Notification Level | Level Number | Description                              |
|--------------------|--------------|------------------------------------------|
| <b>emergency</b>   | 0            | System unusable                          |
| <b>alert</b>       | 1            | Immediate action needed                  |
| <b>critical</b>    | 2            | Critical conditions                      |
| <b>error</b>       | 3            | Error conditions                         |
| <b>warning</b>     | 4            | Non-fatal warning conditions             |
| <b>notice</b>      | 5            | Normal but significant conditions        |
| <b>info</b>        | 6            | Informational messages only              |
| <b>debug</b>       | 7            | Information for troubleshooting purposes |



**Note**

The *debug* notification level should be used for specific troubleshooting purposes only. System performance and HA behavior may be adversely affected by logging at the *debug* notification level.

Each facility can have up to eight notification levels. Each facility and notification level pair can have up to seven destinations. Table 11-9 describes the available facility names.

**Table 11-9 Logging Level Facilities**

| Facility Name   | Description                          |
|-----------------|--------------------------------------|
| <b>AUTH</b>     | AAA authentication.                  |
| <b>CDP</b>      | Cisco Discovery Protocol.            |
| <b>CONF</b>     | Configuration functions.             |
| <b>FC</b>       | SN 5428 Fibre Channel interfaces.    |
| <b>GE</b>       | SN 5428 Gigabit Ethernet interfaces. |
| <b>HA</b>       | SN 5428 high availability clusters.  |
| <b>IF</b>       | Interface manager.                   |
| <b>INVALID</b>  | Generic functions.                   |
| <b>IPROUTER</b> | SN 5428 IP functions.                |
| <b>ISCSI</b>    | iSCSI functions.                     |
| <b>MON</b>      | Hardware monitor.                    |
| <b>SNMP</b>     | Simple Network Management Protocol.  |
| <b>SYSLOG</b>   | Syslog functions.                    |
| <b>UI</b>       | SN 5428 user interface.              |
| <b>VTP</b>      | VTP and VLAN functions.              |

Table 11-10 describes the available logging destinations.

**Table 11-10 Logging Level Destinations**

| Destination    | Description                                                                                                                           |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>all</b>     | Logs to all destinations.                                                                                                             |
| <b>none</b>    | No logging occurs.                                                                                                                    |
| <b>console</b> | Logs to serial console CLI sessions.                                                                                                  |
| <b>logfile</b> | Logs messages to the SN 5428 log file.                                                                                                |
| <b>rslog</b>   | Logs messages to a remote syslog server. Use the <b>logging syslog</b> command to specify the IP address of the remote syslog server. |
| <b>vtty</b>    | Logs to all Telnet or other virtual terminal CLI sessions.                                                                            |

Use the **save system bootconfig** or **save all bootconfig** commands to save the list of log route entries. To delete a log route entry by its index number, use the **delete logging** command.

## Examples

The following example displays an indexed list of the routing rules in the logging table, and then inserts an entry to log anything from the *HA* facility with notification level of *notice* (or lower) to all logging destinations before the third entry. The **show logging** command displays the newly inserted entry.

```
[SN5428A]# logging #?

[SN5428A]# logging #?
Index Level Priority Facility Route
1 critical 2 all console vty logfile
2 debug 7 SNMP rslog
3 warning 4 CDP rslog

[SN5428A]# logging #3 logging level notice from HA to all

[SN5428A]# show logging
Logging is enabled
Logging to syslog host is enabled, ip-address is 10.1.1.144

[SN5428A]# logging #?
Index Level Priority Facility Route
1 critical 2 all console vty logfile
2 debug 7 SNMP rslog
3 notice 5 HA all
4 warning 4 CDP rslog
```

## Related Commands

| Command                    | Description                                                                                                                         |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>clear logging table</b> | Clear the SN 5428 Storage Router logging table of all entries, or to reset the table to factory defaults.                           |
| <b>delete logging</b>      | Delete a rule from the logging table.                                                                                               |
| <b>logging level</b>       | Add rule entries to route SN 5428 event, debug and trace messages to various destinations based on facility and notification level. |

| <b>Command</b>        | <b>Description</b>                                                                       |
|-----------------------|------------------------------------------------------------------------------------------|
| <b>logging on</b>     | Enable or temporarily disable logging of SN 5428 event message.                          |
| <b>logging syslog</b> | Enable remote logging to the specified IP host.                                          |
| <b>save all</b>       | Save all configuration information, including the log route entries list.                |
| <b>save system</b>    | Save selected system configuration information, including log route entries list.        |
| <b>show logging</b>   | Display the routing rules in the logging table and the contents of the SN 5428 log file. |
| <b>show system</b>    | Display selected system information.                                                     |

# logging level

To add a routing rule to the logging table, use the **logging level** command.

**logging level** *notification-level* **from** {**all** | *facility-name*} **to** *destination1* [*destination2...*]

## Syntax Description

|                                                          |                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>notification-level</i>                                | Limit logging to messages of a specified level or lower levels. See Table 11-12 in the Usage Guidelines section for a list of valid names that can be used for the <i>notification-level</i> argument.                                                                                       |
| <b>from all</b>                                          | Associate the specified level and destinations with all facilities.                                                                                                                                                                                                                          |
| <b>from</b> <i>facility-name</i>                         | The name of the facility. A facility is the feature area from which the message is received. See Table 11-11 in the Usage Guidelines section for a list of valid facility names. Each facility can have eight notification levels. Each notification level can have up to seven destination. |
| <b>to</b> <i>destination1</i> [ <i>destination2...</i> ] | At least one of the destinations described in Table 11-13.                                                                                                                                                                                                                                   |

## Defaults

The factory default logging rules are as follows:

- All messages from all facilities at *notice* level or lower levels are logged to all destinations.
- All messages from all facilities at *info* level or lower levels are logged to the SN 5428 log file.
- All messages from all facilities at *debug* level are not logged.

## Command Modes

Administrator.

## Command History

| Release | Modification                                                                 |
|---------|------------------------------------------------------------------------------|
| 2.3.1   | This command was introduced, replacing the <b>logging route add</b> command. |

## Usage Guidelines

Event, trace and debug messages can be routed to various destinations, based on the notification level of the message and the application area (facility) that generated the message. When a log message is received by the SN 5428, the logging table rules are searched by facility name and by notification level until a match is found. The log message is sent to all the destinations specified by the matching rule. When a new routing rule is added, it is appended to the existing list of entries.

Messages are sent in the following format:

```
<timestamp>: %<facility>-<level_number>-<mnemonic>: <message text>
```

The following is an example log message, for the SNMP facility:

```
Mar 18 11:48:05: %SNMP-5-SASAS: SnmpApp starting...
```

Each facility can have up to eight notification levels. Each facility and notification level pair can have up to seven destinations. Table 11-11 describes the available facility names.

**Table 11-11 Logging Level Facilities**

| Facility Name   | Description                          |
|-----------------|--------------------------------------|
| <b>AUTH</b>     | AAA authentication.                  |
| <b>CDP</b>      | Cisco Discovery Protocol.            |
| <b>CONF</b>     | Configuration functions.             |
| <b>FC</b>       | SN 5428 Fibre Channel interfaces.    |
| <b>GE</b>       | SN 5428 Gigabit Ethernet interfaces. |
| <b>HA</b>       | SN 5428 high availability clusters.  |
| <b>IF</b>       | Interface manager.                   |
| <b>INVALID</b>  | Generic functions.                   |
| <b>IPROUTER</b> | SN 5428 IP functions.                |
| <b>ISCSI</b>    | iSCSI functions.                     |
| <b>MON</b>      | Hardware monitor.                    |
| <b>SNMP</b>     | Simple Network Management Protocol.  |
| <b>SYSLOG</b>   | Syslog functions.                    |
| <b>UI</b>       | SN 5428 user interface.              |
| <b>VTP</b>      | VTP and VLAN functions.              |

The notification level limits logging to messages of the specified level or lower levels, based on level number. Table 11-12 describes the available logging levels.

**Table 11-12 Logging Level Notification Levels and Corresponding Numbers**

| Notification Level | Level Number | Description                              |
|--------------------|--------------|------------------------------------------|
| <b>emergency</b>   | 0            | System unusable                          |
| <b>alert</b>       | 1            | Immediate action needed                  |
| <b>critical</b>    | 2            | Critical conditions                      |
| <b>error</b>       | 3            | Error conditions                         |
| <b>warning</b>     | 4            | Non-fatal warning conditions             |
| <b>notice</b>      | 5            | Normal but significant conditions        |
| <b>info</b>        | 6            | Informational messages only              |
| <b>debug</b>       | 7            | Information for troubleshooting purposes |

**Note**

The *debug* notification level should be used for specific troubleshooting purposes only. System performance and HA behavior may be adversely affected by logging at the *debug* notification level.

Table 11-13 describes the available logging destinations.

**Table 11-13 Logging Level Destinations**

| Destination    | Description                                                                                                                           |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>all</b>     | Logs to all destinations.                                                                                                             |
| <b>none</b>    | No logging occurs.                                                                                                                    |
| <b>console</b> | Logs to console CLI sessions.                                                                                                         |
| <b>logfile</b> | Logs messages to the SN 5428 log file.                                                                                                |
| <b>rslog</b>   | Logs messages to a remote syslog server. Use the <b>logging syslog</b> command to specify the IP address of the remote syslog server. |
| <b>vty</b>     | Logs to all Telnet or other virtual terminal CLI sessions.                                                                            |

Use the **save system bootconfig** or **save all bootconfig** commands to save the logging table.

To delete a routing rule from the logging table, use the **delete logging** command.



**Note**

Any message that does not have a matching rule in the logging table is discarded.

**Examples**

The following example logs anything from the *HA* facility with notification level of *notice* (or lower) to all logging destinations.

```
[SN5428A]# logging level notice from HA to all
```

The following example logs messages from all facilities with a notification level of *warning* or lower to all destinations. (If this is the only rule in the logging table, any message with a notification level of *debug*, *info* or *notice* is discarded and not logged.) The log route entries are saved to the SN 5428's bootable configuration.

```
[SN5428A]# logging level warning from all to all
[SN5428A]# save system bootconfig
```

**Related Commands**

| Command                    | Description                                                                                               |
|----------------------------|-----------------------------------------------------------------------------------------------------------|
| <b>clear logging table</b> | Clear the SN 5428 Storage Router logging table of all entries, or to reset the table to factory defaults. |
| <b>delete logging</b>      | Delete a rule from the logging table.                                                                     |
| <b>logging #?</b>          | Insert a routing rule entry into the SN 5428 logging table.                                               |
| <b>logging on</b>          | Enable or temporarily disable logging of SN 5428 event message.                                           |
| <b>logging syslog</b>      | Enable remote logging to the specified IP host.                                                           |
| <b>save all</b>            | Save all configuration information, including the log route entries list.                                 |
| <b>save system</b>         | Save selected system configuration information, including log route entries list.                         |

| <b>Command</b>      | <b>Description</b>                                                                       |
|---------------------|------------------------------------------------------------------------------------------|
| <b>show logging</b> | Display the routing rules in the logging table and the contents of the SN 5428 log file. |
| <b>show system</b>  | Display selected system information.                                                     |

# logging on

To enable logging of SN 5428 event messages based on the rules in the logging table, use the **logging on** command. To temporarily disable logging of all event messages, use the **no logging on** form of this command.

**logging on**

**no logging on**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Logging is enabled by default. The factory default logging rules are as follows:

- All messages from all facilities at *notice* level or lower levels are logged to all destinations.
- All messages from all facilities at *info* level or lower levels are logged to the SN 5428 log file.
- All messages from all facilities at *debug* level are not logged.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.3.1   | This command was introduced. |

**Usage Guidelines** Use the **no** form of this command to quickly disable logging of all messages. For example, if there is an error condition that is overwhelming the console with messages, enter **no logging on** to temporarily disable logging without changing the logging table. Use the **logging on** command to re-enable logging when the problem is resolved.

**Examples** The following example temporarily disables logging of all event messages:

```
[SN5428A] # no logging on
```

| Related Commands | Command                    | Description                                                                                                                         |
|------------------|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>clear logging table</b> | Clear the SN 5428 Storage Router logging table of all entries, or to reset the table to factory defaults.                           |
|                  | <b>delete logging</b>      | Delete a rule from the logging table.                                                                                               |
|                  | <b>logging #?</b>          | Insert a routing rule entry into the SN 5428 logging table.                                                                         |
|                  | <b>logging level</b>       | Add rule entries to route SN 5428 event, debug and trace messages to various destinations based on facility and notification level. |
|                  | <b>logging syslog</b>      | Enable remote logging to the specified IP host.                                                                                     |
|                  | <b>save all</b>            | Save all configuration information, including the log route entries list.                                                           |

| <b>Command</b>      | <b>Description</b>                                                                       |
|---------------------|------------------------------------------------------------------------------------------|
| <b>save system</b>  | Save selected system configuration information, including log route entries list.        |
| <b>show logging</b> | Display the routing rules in the logging table and the contents of the SN 5428 log file. |
| <b>show system</b>  | Display selected system information.                                                     |

# logging syslog

To log messages to a remote syslog host, use the **logging syslog** command. Use the **no** form of this command to disable remote logging.

**logging syslog** *A.B.C.D*

**no logging syslog**

|                           |                |                                                                  |
|---------------------------|----------------|------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>A.B.C.D</i> | The IP address of the syslog host to be used for remote logging. |
|---------------------------|----------------|------------------------------------------------------------------|

|                 |                                        |
|-----------------|----------------------------------------|
| <b>Defaults</b> | Remote logging is disabled by default. |
|-----------------|----------------------------------------|

|                      |                |
|----------------------|----------------|
| <b>Command Modes</b> | Administrator. |
|----------------------|----------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                |
|------------------------|----------------|--------------------------------------------------------------------|
|                        | 2.3.1          | This command was introduced, replacing the <b>logging</b> command. |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | <p>This command identifies a remote syslog host to receive logging messages.</p> <ul style="list-style-type: none"> <li>Use the <b>logging level</b> command with the destination keyword <b>rslog</b> to configure the messages to be logged to the remote host.</li> <li>Use the <b>no logging syslog</b> command to disable remote logging.</li> <li>Use the <b>delete logging</b> command to remove specific logging table entries.</li> <li>Use the <b>show logging</b> command to display the status of remote logging and the IP address of the remote syslog server.</li> </ul> |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |                                                                                                                                                                                                        |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Examples</b> | <p>The following example identifies the IP address of the remote syslog host as <i>10.1.1.144</i> and adds a entry to the logging table to route all emergency level messages to that remote host.</p> |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
[SN5428A]# logging syslog 10.1.1.144
[SN5428A]# logging level emergency from all to rslog
```

| <b>Related Commands</b> | <b>Command</b>             | <b>Description</b>                                                                                                                  |
|-------------------------|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
|                         | <b>clear logging table</b> | Clear the SN 5428 Storage Router logging table of all entries, or to reset the table to factory defaults.                           |
|                         | <b>delete logging</b>      | Delete a rule from the logging table.                                                                                               |
|                         | <b>logging #?</b>          | Insert a routing rule entry into the SN 5428 logging table.                                                                         |
|                         | <b>logging level</b>       | Add rule entries to route SN 5428 event, debug and trace messages to various destinations based on facility and notification level. |

| <b>Command</b>      | <b>Description</b>                                                                    |
|---------------------|---------------------------------------------------------------------------------------|
| <b>logging on</b>   | Enable or temporarily disable logging of SN 5428 event message.                       |
| <b>save all</b>     | Save all configuration information, including the remote logging configuration.       |
| <b>save system</b>  | Save selected system configuration information, including remote logging information. |
| <b>show logging</b> | Display the routing rules in the logging table.                                       |
| <b>show system</b>  | Display selected system information.                                                  |

# logout

To terminate the current CLI management session, use the **logout** command.

**logout**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** None.

---

**Command Modes** Administrator or Monitor.

---

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 2.2.1          | This command was introduced. |

---



---

**Usage Guidelines**

- If a user is connected to the SN 5428 in Administrator mode or Monitor mode via a Telnet session, the **logout** command terminates the CLI management session. No CLI commands can be issued until you log in again.
- If a user is connected to the SN 5428 in Administrator mode via the console interface, the **logout** command returns the session to Monitor mode (like the **exit** command).
- If a user is connected to the SN 5428 in Monitor mode via the console interface, the **logout** command has no effect.

---

| <b>Related Commands</b> | <b>Command</b> | <b>Description</b>                               |
|-------------------------|----------------|--------------------------------------------------|
|                         | <b>enable</b>  | Enter Administrator mode.                        |
|                         | <b>exit</b>    | Leave Administrator mode and enter Monitor mode. |

---

# monitor password

To set the password used for view-only access to the SN 5428 management interface, use the **monitor password** command. Access may be via Telnet (for CLI) or web-based GUI.

**monitor password** *string*

## Syntax Description

|                               |                                                                                                                                          |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>password</b> <i>string</i> | A case-sensitive password associated with view-only access to the SN 5428's management interface. The default password is <i>cisco</i> . |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|

## Defaults

The default password is *cisco*.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

The SN 5428's management interface is password protected. You must enter passwords when accessing the SN 5428 via the CLI or web-based GUI. (Passwords can also be applied to the console interface. See the **restrict console** command for additional information.) The Monitor mode password provides view-only access to the SN 5428's management interface, while the Administrator mode password allows the user to create entities and make changes to the configuration of the SN 5428 system.

Set the password string to "" to clear the password, effectively setting it to nothing.



### Note

The password is displayed in clear text as the command is entered, but it is changed to a series of number signs (#####) when the change is acknowledged.

## Examples

The following example sets the Monitor mode password to *M17g23*. All passwords are case sensitive.

```
[SN5428A] # monitor password M17g23
```

## Related Commands

| Command               | Description                                                                           |
|-----------------------|---------------------------------------------------------------------------------------|
| <b>admin password</b> | Set the login password for administrative access to the SN 5428 management interface. |
| <b>enable</b>         | Enter Administrator mode.                                                             |
| <b>exit</b>           | Leave Administration mode and enter Monitor mode.                                     |
| <b>save all</b>       | Save all configuration information, including the Monitor mode password.              |

| <b>Command</b>      | <b>Description</b>                                                         |
|---------------------|----------------------------------------------------------------------------|
| <b>save system</b>  | Save selected system information, including the Monitor mode password.     |
| <b>setup access</b> | Run the wizard to configure Monitor mode and Administrator mode passwords. |

# ntp peer

To specify the name or IP address of a Network Time Protocol (NTP) server with which the SN 5428 will synchronize date and time, use the **ntp peer** command. To clear the current NTP server setting, use the **no** form of this command.

```
ntp peer{A.B.C.D | server-name}
```

```
no ntp peer
```

## Syntax Description

|                    |                                                                                                                                                                                                              |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>A.B.C.D</i>     | The IP address of the NTP server with which the SN 5428 synchronizes date and time. <i>A.B.C.D</i> is the dotted quad notation of the IP address.                                                            |
| <i>server-name</i> | The name of the NTP server with which the SN 5428 synchronizes date and time. In order to specify a server name, the SN 5428 must be configured to use a DNS server using the <b>ip name-server</b> command. |

## Defaults

None.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

The SN 5428 must provide accurate date and time information for log files and user interfaces. It will use the services of the NTP server to keep the date and time synchronized with the rest of the network. If the NTP server is outside the SN 5428 management subnet, use the **ip route** command to add an appropriate gateway IP address to the SN 5428 routing table.

## Examples

The following example specifies the IP address of the NTP server for the SN 5428 to *10.1.60.86*.

```
[SN5428A] # ntp peer 10.1.60.86
```

## Related Commands

| Command               | Description                                                     |
|-----------------------|-----------------------------------------------------------------|
| <b>clock set</b>      | Set the SN 5428 system clock.                                   |
| <b>clock timezone</b> | Specify the time zone associated with the SN 5428.              |
| <b>ip route</b>       | Add a static route to the SN 5428 Storage Router routing table. |
| <b>save all</b>       | Save all configuration information.                             |
| <b>save system</b>    | Save selected system information, including NTP server name.    |
| <b>setup time</b>     | Run the wizard to configure the system date and time.           |

| <b>Command</b>     | <b>Description</b>                                                        |
|--------------------|---------------------------------------------------------------------------|
| <b>show clock</b>  | Display the current system date and time, including the system time zone. |
| <b>show system</b> | Display selected system information, including NTP server address.        |

# ping

To verify communication with another SN 5428 or system in the network, use the **ping** command.

```
ping {ip-address | servername} [numpkts nn] [size sn]
```

| Syntax Description |  |                                                                                                               |
|--------------------|--|---------------------------------------------------------------------------------------------------------------|
| <i>ip-address</i>  |  | The IP address of another system or SN 5428.                                                                  |
| <i>servername</i>  |  | The name of another server. The SN 5428 must be configured to use the services of a Domain Name Server (DNS). |
| <b>numpkts</b>     |  | (Optional) Keyword indicating the maximum number of pings that may be sent.                                   |
| <i>nn</i>          |  | (Optional) The maximum number of pings. The default value is five.                                            |
| <b>size</b>        |  | (Optional) Keyword indicating the size of each ping packet.                                                   |
| <i>sn</i>          |  | (Optional) The size of each packet, in bytes. The default is 64 bytes; the maximum size is 4096 bytes.        |

**Defaults** The default setting is to attempt five 64-byte pings.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command to verify that there is a TCP/IP communication path to another SN 5428 or system in the network.

**Examples** The following example attempts to verify the communication path to the IP address 10.1.30.17, using the default size and maximum number of packets:

```
[SN5428A] # ping 10.1.30.17
```

The following example attempts to reach the IP address 10.1.30.17 by sending up to three pings, each consisting of a 20-byte packet:

```
[SN5428A] # ping 10.1.30.17 numpkts 3 size 20
```

| Related Commands | Command        | Description                                                                                                                   |
|------------------|----------------|-------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>show ip</b> | Display entries from the SN 5428 Storage Router routing table and statistics about the protocols used in the SN 5428 network. |

## radius-server host

To specify a RADIUS server to be used for AAA authentication services, use the **radius-server host** command. To delete the specified RADIUS server, use the **no** form of this command.

```
radius-server host ip-address [auth-port port-number] [timeout seconds] [retransmit retries]
 [key key-string]
```

```
no radius-server host ip-address [auth-port port-number]
```

### Syntax Description

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>ip-address</i>                   | The IP address of the RADIUS server.                                                                                                                                                                                                                                                                                                                                                               |
| <b>auth-port</b> <i>port-number</i> | (Optional) The UDP destination port for authentication requests. If unspecified, the port number defaults to 1645.                                                                                                                                                                                                                                                                                 |
| <b>key</b> <i>key-string</i>        | (Optional) The authentication and encryption key for all RADIUS communications between the SN 5428 and the RADIUS server. This key must match the encryption used on the RADIUS daemon. If spaces are used in the key, enclose the key in quotation marks. This key overrides the global setting of the <b>radius-server key</b> command. If no key string is specified, the global value is used. |
| <b>timeout</b> <i>seconds</i>       | (Optional) The host-specific time interval that the SN 5428 waits for the RADIUS server to reply before retransmitting. Enter a value in the range of 1 to 1000. This setting overrides the global value of the <b>radius-server timeout</b> command. If no timeout value is specified, the global value is used.                                                                                  |
| <b>retransmit</b> <i>retries</i>    | (Optional) The number of times a RADIUS request is resent to the RADIUS server, if the server is not responding or responding slowly. Enter a value in the range of 1 to 100. This setting overrides the global setting of the <b>radius-server retransmit</b> command. If no retransmit value is specified, the global value is used.                                                             |

### Defaults

No RADIUS server is specified.

### Command Modes

Administrator.

### Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

**Usage Guidelines**

AAA authentication services are used to provide iSCSI authentication for IP hosts requesting access to storage.

- You can use multiple **radius-server host** commands to specify multiple RADIUS servers. The software searches for servers in the order in which you specify them.
- If no host-specific timeout, retransmit, or key values are specified, the global values apply to each RADIUS server.
- If you use spaces in the key, enclose the key in quotation marks.

**Examples**

The following example identifies the server with IP address *10.5.0.53* as the RADIUS server and uses the default port for authentication:

```
[SN5428A] # radius-server 10.5.0.53
```

The following example identifies port 1612 as the destination port for authentication requests on the RADIUS server *10.6.0.61*:

```
[SN5428A] # radius-server host 10.6.0.61 auth-port 1612
```

The following example identifies the server with IP address *10.5.0.53* as the RADIUS server, uses ports 1612 as the authorization port, sets the timeout value to 6, sets the retransmit value to 5, and sets “rad123” as the encryption key, matching the key on the RADIUS server:

```
[SN5428A] # radius-server host 10.5.0.53 auth-port 1612 timeout 6 retransmit 5 key rad123
```

**Related Commands**

| Command                         | Description                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>aaa authentication iscsi</b> | Configure the AAA authentication services to be used for iSCSI authentication.                                             |
| <b>aaa test authentication</b>  | Enable testing of the default AAA authentication list.                                                                     |
| <b>debug aaa</b>                | Enable debugging for the AAA authentication services.                                                                      |
| <b>radius-server key</b>        | Sets the global authentication and encryption key for all RADIUS communications between the SN 5428 and the RADIUS daemon. |
| <b>radius-server retransmit</b> | Specifies how many times the SN 5428 resends the RADIUS request to a server before giving up.                              |
| <b>radius-server timeout</b>    | Sets the interval the SN 5428 waits for a RADIUS server to reply before retransmitting.                                    |
| <b>restore aaa</b>              | Restore AAA authentication services from a saved configuration file.                                                       |
| <b>save aaa</b>                 | Save the current AAA configuration information.                                                                            |
| <b>scsirouter authenticate</b>  | Enable iSCSI authentication for the named SCSI routing instance.                                                           |
| <b>show aaa</b>                 | Display AAA configuration information.                                                                                     |
| <b>tacacs-server host</b>       | Configure remote TACACS+ servers for AAA authentication services.                                                          |

# radius-server key

To set the authentication and encryption key to be used for all RADIUS communications between the SN 5428 Storage Router and the RADIUS daemon, use the **radius-server key** command. To disable the key, use the **no** form of this command.

**radius-server key** *key-string*

**no radius-server key**

|                           |                   |                                                                                                                                                                          |
|---------------------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>key-string</i> | The authentication and encryption key string to be used for all RADIUS communications, in clear text. If spaces are used in the key, enclose the key in quotation marks. |
|---------------------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |       |
|-----------------|-------|
| <b>Defaults</b> | None. |
|-----------------|-------|

|                      |                |
|----------------------|----------------|
| <b>Command Modes</b> | Administrator. |
|----------------------|----------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 2.2.1          | This command was introduced. |

**Usage Guidelines**

After configuring authentication services for iSCSI authentication with the **aaa authentication iscsi** command, use the **radius-server key** command to set the global authentication and encryption key. The key entered as part of the command must match the key used on the RADIUS daemon. If the key includes spaces, enclose the key in quotation marks.

To override the global key for a specific RADIUS server, use the **radius-server host** command with the **key** keyword.

**Examples**

The following example sets the global authentication and encryption key to *my key string*:

```
[SN5428A]# radius-server key "my key string"
```

| <b>Related Commands</b> | <b>Command</b>                  | <b>Description</b>                                                             |
|-------------------------|---------------------------------|--------------------------------------------------------------------------------|
|                         | <b>aaa authentication iscsi</b> | Configure the AAA authentication services to be used for iSCSI authentication. |
|                         | <b>aaa test authentication</b>  | Enable testing of the default AAA authentication list.                         |
|                         | <b>debug aaa</b>                | Enable debugging for the AAA authentication services.                          |
|                         | <b>radius-server host</b>       | Configure remote RADIUS servers for AAA authentication services.               |

| <b>Command</b>                  | <b>Description</b>                                                                            |
|---------------------------------|-----------------------------------------------------------------------------------------------|
| <b>radius-server retransmit</b> | Specifies how many times the SN 5428 resends the RADIUS request to a server before giving up. |
| <b>radius-server timeout</b>    | Sets the interval the SN 5428 waits for a RADIUS server to reply before retransmitting.       |
| <b>restore aaa</b>              | Restore AAA authentication services from a saved configuration file.                          |
| <b>save aaa</b>                 | Save the current AAA configuration information.                                               |
| <b>scsirouter authenticate</b>  | Enable iSCSI authentication for the named SCSI routing instance.                              |
| <b>show aaa</b>                 | Display AAA configuration information.                                                        |
| <b>tacacs-server host</b>       | Configure remote TACACS+ servers for AAA authentication services.                             |

# radius-server retransmit

To specify the number of times the SN 5428 Storage Router resends the RADIUS request to each server in the list of configured RADIUS servers after a timeout occurs, use the **radius-server retransmit** command. To disable retransmission, use the **no** form of this command.

**radius-server retransmit** *retries*

**no radius-server retransmit**

|                           |                |                                                                                             |
|---------------------------|----------------|---------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>retries</i> | The number of times the request can be resent to each server in the list. The default is 3. |
|---------------------------|----------------|---------------------------------------------------------------------------------------------|

**Defaults** The number of possible resends defaults to three.

**Command Modes** Administrator.

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 2.2.1          | This command was introduced. |

**Usage Guidelines** If multiple RADIUS servers are configured for AAA authentication, the SN 5428 attempts to reach each server in the list before incrementing the retransmit count.

To override the global retransmit count for a specific RADIUS server, use the **radius-server host** command with the **retransmit** keyword.

**Examples** The following example sets the retransmit count to six, meaning the request can be resent up to six times for every RADIUS server:

```
[SN5428A] # radius-server retransmit 6
```

| <b>Related Commands</b> | <b>Command</b>                  | <b>Description</b>                                                                                                         |
|-------------------------|---------------------------------|----------------------------------------------------------------------------------------------------------------------------|
|                         | <b>aaa authentication iscsi</b> | Configure the AAA authentication services to be used for iSCSI authentication.                                             |
|                         | <b>aaa test authentication</b>  | Enable testing of the default AAA authentication list.                                                                     |
|                         | <b>debug aaa</b>                | Enable debugging for the AAA authentication services.                                                                      |
|                         | <b>radius-server host</b>       | Configure remote RADIUS servers for AAA authentication services.                                                           |
|                         | <b>radius-server key</b>        | Sets the global authentication and encryption key for all RADIUS communications between the SN 5428 and the RADIUS daemon. |

| <b>Command</b>                     | <b>Description</b>                                                                      |
|------------------------------------|-----------------------------------------------------------------------------------------|
| <b>radius-server timeout</b>       | Sets the interval the SN 5428 waits for a RADIUS server to reply before retransmitting. |
| <b>restore aaa</b>                 | Restore AAA authentication services from a saved configuration file.                    |
| <b>save aaa</b>                    | Save the current AAA configuration information.                                         |
| <b>scsirouter<br/>authenticate</b> | Enable iSCSI authentication for the named SCSI routing instance.                        |
| <b>show aaa</b>                    | Display AAA configuration information.                                                  |
| <b>tacacs-server host</b>          | Configure remote TACACS+ servers for AAA authentication services.                       |

# radius-server timeout

To set the global interval that the SN 5428 Storage Router waits for a RADIUS server to reply, use the **radius-server timeout** command. To restore the default, use the **no** form of this command.

**radius-server timeout** *seconds*

**no radius-server timeout**

|                           |                |                                                                                                 |
|---------------------------|----------------|-------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>seconds</i> | The global timeout value in seconds. Enter a value in the range of 1 to 1000. The default is 5. |
|---------------------------|----------------|-------------------------------------------------------------------------------------------------|

**Defaults** The timeout value defaults to five seconds.

**Command Modes** Administrator.

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 2.2.1          | This command was introduced. |

**Usage Guidelines** Use this command to set the number of seconds the SN 5428 waits for a RADIUS server to reply before timing out.

To override the global timeout value for a specific RADIUS server, use the **radius-server host** command with the **timeout** keyword.

**Examples** The following example sets the global timeout value to 10. You may want to increase the timeout value if you have network problems or if the RADIUS servers are slow to response, which causes consistent timeouts when a lower timeout value is used.

```
[SN5428A] # radius-server timeout 10
```

| <b>Related Commands</b> | <b>Command</b>                  | <b>Description</b>                                                                                                         |
|-------------------------|---------------------------------|----------------------------------------------------------------------------------------------------------------------------|
|                         | <b>aaa authentication iscsi</b> | Configure the AAA authentication services to be used for iSCSI authentication.                                             |
|                         | <b>aaa test authentication</b>  | Enable testing of the default AAA authentication list.                                                                     |
|                         | <b>debug aaa</b>                | Enable debugging for the AAA authentication services.                                                                      |
|                         | <b>radius-server host</b>       | Configure remote RADIUS servers for AAA authentication services.                                                           |
|                         | <b>radius-server key</b>        | Sets the global authentication and encryption key for all RADIUS communications between the SN 5428 and the RADIUS daemon. |

| <b>Command</b>                  | <b>Description</b>                                                                            |
|---------------------------------|-----------------------------------------------------------------------------------------------|
| <b>radius-server retransmit</b> | Specifies how many times the SN 5428 resends the RADIUS request to a server before giving up. |
| <b>restore aaa</b>              | Restore AAA authentication services from a saved configuration file.                          |
| <b>save aaa</b>                 | Save the current AAA configuration information.                                               |
| <b>scsirouter authenticate</b>  | Enable iSCSI authentication for the named SCSI routing instance.                              |
| <b>show aaa</b>                 | Display AAA configuration information.                                                        |
| <b>tacacs-server host</b>       | Configure remote TACACS+ servers for AAA authentication services.                             |

# read

To read and execute the CLI commands in a command file, use the **read** command.

**read script** *command-file* [**force**]

| Syntax Description |                     |                                                                                           |
|--------------------|---------------------|-------------------------------------------------------------------------------------------|
|                    | <i>command-file</i> | The name of the command file. The command file must exist in the <i>script</i> directory. |
|                    | <b>force</b>        | (Optional) Suppress warning prompts and messages.                                         |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use the **show bootconfig** and **show runningconfig** commands with the **to** keyword to create basic files containing many of the CLI commands that were issued to create the SN 5428's bootable or currently running configuration. These files can be modified and used as command files to automate common tasks.

You can also manually create a command file. If you have a set of CLI commands that you run periodically, you can place them in a command file, transfer that file to the SN 5428's script directory and use the **read** command to execute them when needed. Each command should be on a separate line or contain a backslash ( \ ) as the line continuation character at the end of the line. At the end of a continuation sequence, add a blank line as a separator between the sequence and any following command. Any line beginning with an exclamation mark (!) or a number sign (#) is considered to be a comment and will not be executed.

When the command is issued without the **force** keyword, you are reminded that the action may change the configuration of the SN 5428 and are then prompted to confirm your actions.

**Examples** The following example reads and executes the CLI commands in the command file named *myCommands*.

```
[SN5428A]# read script myCommands
*** Warning: this script may change your configuration.
Do you want to continue? [yes/no (yes)] yes
```

**Related Commands**

| <b>Command</b>            | <b>Description</b>                                                                                                    |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>show bootconfig</b>    | Display the SN 5428's bootable configuration, or create a command file based on the SN 5428's bootable configuration. |
| <b>show cli</b>           | Display the syntax of CLI commands.                                                                                   |
| <b>show runningconfig</b> | Display the SN 5428's running configuration, or create a command file based on the SN 5428's running configuration.   |
| <b>show script</b>        | Display the contents of the <i>script</i> directory or the contents of the named command file.                        |

# reboot

To cause the SN 5428 to shut down and then restart, issue the **reboot** command.



## Note

Rebooting may cause the SN 5428 to run a different version of software. See the **software version** command for details.

**reboot [force] [fast]**

## Syntax Description

|              |                                                                                |
|--------------|--------------------------------------------------------------------------------|
| <b>fast</b>  | (Optional) Force a soft reboot of the SN 5428, bypassing hardware diagnostics. |
| <b>force</b> | (Optional) Force an immediate reboot of the SN 5428.                           |

## Defaults

If there are unsaved configuration changes when the command is issued, the default is to save all changes before rebooting. If the command is issued with the optional **force** keyword, any unsaved configuration changes are discarded.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

If the SN 5428 is participating in a cluster, the **reboot** command will cause any SCSI routing instances running on this SN 5428 to failover to another SN 5428 in the cluster. At restart, the cluster determines any SCSI routing instances that should start on the SN 5428. If the SN 5428 is identified as the preferred SN 5428 for any SCSI routing instance (via the **scsirouter primary** command), that instance will start running on the SN 5428.

If the **reboot** command is issued with no keywords and there are unsaved changes to the current configuration, you can choose to either save all changes, save specific areas that have been modified, or reboot without saving any changes.

Use the **force** keyword to cause an immediate reboot of the SN 5428, discarding any unsaved configuration changes. Append the optional **fast** keyword to bypass diagnostics during the reboot sequence.

**Examples**

The following prompt is received if you issue a **reboot** command (without the **force** keyword) when the SN 5428 has unsaved configuration changes.

```
[SN5428A]# reboot
*** Warning: This will reboot the system.
Do you want to continue? [yes/no (no)] yes

Changes have been made to the current configuration of the system which
have not been saved.
yes - all of the configuration data will be saved,
no - modifications to the configuration data will not be saved.

Save ALL configuration data? [yes/no (yes)] yes
Halting system.....
```

The following example reboots the SN 5428 (after prompting the user to save any unsaved configuration changes) but bypasses diagnostics during the reboot process:

```
[SN5428A]# reboot fast
```

**Related Commands**

| <b>Command</b>          | <b>Description</b>                                                    |
|-------------------------|-----------------------------------------------------------------------|
| <b>halt</b>             | Prepare the SN 5428 to be powered down.                               |
| <b>software version</b> | Specify the version of software to run when the SN 5428 is restarted. |

## restore aaa

To cause the AAA authentication configuration to be copied from the specified configuration file into persistent memory, use the **restore aaa** command. The configuration file must exist in the *savedconfig* directory. To display the contents of the *savedconfig* directory, issue the **show savedconfig** command.

**restore aaa from** *filename*

|                           |                             |                                                                                                                                         |
|---------------------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>from</b> <i>filename</i> | The name of the configuration file containing the information to be restored. This file must exist in the <i>savedconfig</i> directory. |
|---------------------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|

|                 |       |
|-----------------|-------|
| <b>Defaults</b> | None. |
|-----------------|-------|

|                      |                |
|----------------------|----------------|
| <b>Command Modes</b> | Administrator. |
|----------------------|----------------|

|                        |                |                              |
|------------------------|----------------|------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|                        | 2.2.1          | This command was introduced. |

**Usage Guidelines** The **restore** command overwrites all existing AAA configuration information, including any user name and passwords in the local username database, RADIUS and TACACS+ configuration information, and the default AAA authentication list used for iSCSI authentication.

**Examples** The following example restores the AAA authentication configuration from the saved configuration file named *aaa\_backup*:

```
[SN5428A]# restore aaa from aaa_backup
```

|                         |                                 |                                                                                |
|-------------------------|---------------------------------|--------------------------------------------------------------------------------|
| <b>Related Commands</b> | <b>Command</b>                  | <b>Description</b>                                                             |
|                         | <b>aaa authentication iscsi</b> | Configure the AAA authentication services to be used for iSCSI authentication. |
|                         | <b>debug aaa</b>                | Enable debugging for the AAA authentication services.                          |
|                         | <b>delete savedconfig</b>       | Remove a saved configuration file from the SN 5428.                            |
|                         | <b>radius-server host</b>       | Configure remote RADIUS servers for AAA authentication services.               |
|                         | <b>save aaa</b>                 | Save the current AAA configuration information.                                |
|                         | <b>scsirouter authenticate</b>  | Enable iSCSI authentication for the named SCSI routing instance.               |
|                         | <b>show aaa</b>                 | Display AAA configuration information.                                         |

| Command                         | Description                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------|
| <code>show savedconfig</code>   | List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file. |
| <code>tacacs-server host</code> | Configure remote TACACS+ servers for AAA authentication services.                                      |

# restore accesslist

To cause the named access list or all access lists to be copied from the specified configuration file into persistent memory, use the **restore accesslist** command. The configuration file must exist in the *savedconfig* directory. To display the contents of the *savedconfig* directory, issue the **show savedconfig** command.



## Note

If the SN 5428 belongs to a cluster, the restored access list information will automatically be propagated to other members of that cluster.

```
restore accesslist {name | all} from filename
```

## Syntax Description

|                             |                                                                                                                                         |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>                 | The name of the access list to be restored.                                                                                             |
| <b>all</b>                  | Keyword to restore all access lists.                                                                                                    |
| <b>from</b> <i>filename</i> | The name of the configuration file containing the information to be restored. This file must exist in the <i>savedconfig</i> directory. |

## Defaults

None.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

If the access list currently exists in some form, the **restore** command does not delete existing information. The **restore** command adds missing entries, or overwrites existing entries of the same name, but never purges or deletes existing access list entries. If necessary, you can delete an access list and all its entries and then restore it from a saved configuration file.



## Note

In a cluster environment, access list management functions are handled by a single SN 5428. To determine which SN 5428 is performing access list management functions, issue the **show cluster** command. If you issue a **restore accesslist** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the SN 5428 that is currently handling those functions. For more information on operating the SN 5428 in a cluster, see Chapter 10, “Maintaining and Managing the SN 5428 Storage Router.”

**Examples**

The following example restores the access list named *fooList* from the saved configuration file named *accessList\_backup*:

```
[SN5428A]# restore accesslist fooList from accessList_backup
```

**Related Commands**

| Command                             | Description                                                                                            |
|-------------------------------------|--------------------------------------------------------------------------------------------------------|
| <b>accesslist</b>                   | Create an access list entity.                                                                          |
| <b>accesslist A.B.C.D/bits</b>      | Add IP addresses to an access list.                                                                    |
| <b>delete accesslist</b>            | Delete a specific access list entry or an entire access list.                                          |
| <b>restore all</b>                  | Restore all the contents of the named configuration file into memory.                                  |
| <b>restore scsirouter</b>           | Restore the named SCSI routing instance from the named configuration file.                             |
| <b>save accesslist</b>              | Save configuration data for the named access list or for all access lists.                             |
| <b>save scsirouter</b>              | Save configuration information for the named SCSI routing instance.                                    |
| <b>save system</b>                  | Save selected system configuration information.                                                        |
| <b>scsirouter target accesslist</b> | Associate an access list with a specific SCSI routing instance target or all targets.                  |
| <b>show accesslist</b>              | Display the contents of the named access list or all access lists.                                     |
| <b>show savedconfig</b>             | List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file. |

# restore all

To cause all the previously saved configuration information to be copied from the specified configuration file into persistent memory, use the **restore all** command. The configuration file must exist in the *savedconfig* directory. Use the **show savedconfig** command to display the contents of the *savedconfig* directory.



## Note

This command may change the running configuration of the SN 5428.

**restore all from** *filename*

## Syntax Description

|                             |                                                                                                                                         |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>from</b> <i>filename</i> | The name of the configuration file containing the information to be restored. This file must exist in the <i>savedconfig</i> directory. |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|

## Defaults

None.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

The **restore all** command restores all information from the named configuration file. Depending on the information that is restored, the running configuration of the SN 5428 will be changed.

A **restore** command may overwrite or delete existing items. However, the **restore** command will not purge or delete existing items from access lists, but will add missing items or overwrite existing items of the same name. If necessary, you may delete access lists, or any other item to be restored, before restoring from a saved configuration file.

The **restore all** command will not restore the SN 5428 route table; use the **restore system ip-route** command to restore a saved route table.

SCSI routing instances must be stopped before they can be restored. Use the **no scsirouter enable** command to stop active SCSI routing instances.



## Note

In a cluster environment, all access list and VLAN management functions are handled by a single SN 5428. To determine which SN 5428 is performing access list and VLAN management functions, issue the **show cluster** command. If you issue the **save all** command from a storage router that is not performing access list and VLAN management functions, the CLI displays an informational message with the name of the SN 5428 that is currently handling those functions. For more information on operating the SN 5428 in a cluster, see Chapter 10, “Maintaining and Managing the SN 5428 Storage Router.”

**Examples**

The following example restores all configuration data contained in the configuration file named *foo\_backup* into persistent memory:

```
[SN5428A]# restore all from foo_backup
```

**Related Commands**

| Command                    | Description                                                                                            |
|----------------------------|--------------------------------------------------------------------------------------------------------|
| <b>failover scsirouter</b> | Cause the named SCSI routing instance to cease running on the SN 5428.                                 |
| <b>restore aaa</b>         | Restore AAA authentication services from a saved configuration file.                                   |
| <b>restore accesslist</b>  | Restore the named access list or all access lists from the named configuration file.                   |
| <b>restore scsirouter</b>  | Restore the named SCSI routing instance from the named configuration file.                             |
| <b>restore system</b>      | Restore selected system information from the named configuration file.                                 |
| <b>restore vlan</b>        | Restore VLAN configuration information from the named configuration file.                              |
| <b>save aaa</b>            | Save the current AAA configuration information.                                                        |
| <b>save accesslist</b>     | Save configuration data for the named access list or all access lists.                                 |
| <b>save all</b>            | Save all configuration information.                                                                    |
| <b>save scsirouter</b>     | Save configuration information for the named SCSI routing instance.                                    |
| <b>save system</b>         | Save selected system configuration information.                                                        |
| <b>save vlan</b>           | Save configuration information for the named VLAN or all VLANs.                                        |
| <b>scsirouter enable</b>   | Stop or start the named SCSI routing instance.                                                         |
| <b>show savedconfig</b>    | List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file. |

## restore scsirouter

To cause the previously saved configuration information related to the named SCSI routing instance to be copied from the specified configuration file into the SN 5428's bootable configuration, use the **restore scsirouter** command. The configuration file must exist in the *savedconfig* directory. Use the **show savedconfig** command to display the contents of the *savedconfig* directory.



### Note

This does not change the running configuration of the SN 5428.

```
restore scsirouter {name | all} from filename
```

### Syntax Description

|                             |                                                                                                                                         |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>                 | The name of the SCSI routing instance to be restored.                                                                                   |
| <b>all</b>                  | Keyword to restore all SCSI routing instances.                                                                                          |
| <b>from</b> <i>filename</i> | The name of the configuration file containing the information to be restored. This file must exist in the <i>savedconfig</i> directory. |

### Defaults

None.

### Command Modes

Administrator.

### Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

### Usage Guidelines

A SCSI routing instance must be inactive before it can be restored. Use the **no scsirouter enable** command to stop an active SCSI routing instance so it can be restored. After the specified SCSI routing instance is restored, issue the **scsirouter enable** command to start the instance and update the SN 5428's running configuration.

A **restore** command never deletes existing SCSI routing instances. The **restore** command will add missing instances and will overwrite configuration information for existing instances of the same name. If necessary, you can delete a SCSI routing instance and then restore it from a saved configuration file.

### Examples

The following example restores the SCSI routing instance *foo1* from the configuration file named *scsi\_backup001*:

```
[SN5428A]# restore scsirouter foo1 from scsi_backup001
```

**Related Commands**

| <b>Command</b>             | <b>Description</b>                                                                                     |
|----------------------------|--------------------------------------------------------------------------------------------------------|
| <b>failover scsirouter</b> | Cause the named SCSI routing instance to cease running on the SN 5428.                                 |
| <b>restore accesslist</b>  | Restore the named access list or all access lists from the named configuration file.                   |
| <b>restore all</b>         | Restore the contents of the named configuration file into memory.                                      |
| <b>save accesslist</b>     | Save configuration data for the named access list or all access lists.                                 |
| <b>save all</b>            | Save all configuration information.                                                                    |
| <b>save scsirouter</b>     | Save configuration information for the named SCSI routing instance.                                    |
| <b>scsirouter enable</b>   | Stop or start the named SCSI routing instance.                                                         |
| <b>scsirouter primary</b>  | Identify a SN 5428 as the preferred SN 5428 to run the named SCSI routing instance.                    |
| <b>show savedconfig</b>    | List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file. |

## restore system

To cause previously saved system configuration information to be copied from the specified configuration file into persistent memory, use the **restore system** command. The configuration file must exist in the *savedconfig* directory. Use the **show savedconfig** command to display the contents of the *savedconfig* directory.

**restore system all from** *filename*

**restore system name from** *filename*

| Syntax Description   |  |                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>all</b>           |  | Restore all restorable system information (except the SN 5428 route table) from the saved configuration file. Restorable system information includes CDP configuration, administrator contact data, DNS and NTP information, configuration for Fibre Channel interfaces, restrict configuration, remote logging data, and the default download location for updated SN 5428 software. |
| <b>name</b>          |  | The named system information to be restored. See Table 11-14 in the Usage Guidelines section for a list of valid names that can be used for the <i>name</i> argument.                                                                                                                                                                                                                 |
| <b>from filename</b> |  | The name of the configuration file containing the information to be restored. This file must exist in the <i>savedconfig</i> directory.                                                                                                                                                                                                                                               |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                                                |
|-----------------|---------|-------------------------------------------------------------|
|                 | 2.2.1   | This command was introduced.                                |
|                 | 2.3.1   | The <b>ip-route</b> and <b>logging</b> keywords were added. |

**Usage Guidelines**

Table 11-14 describes the named system information that can be restored.

**Table 11-14 Restore System Named System Information**

| Named System Configuration | Description                                                                                                                |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>cdp</b>                 | Restore CDP configuration.                                                                                                 |
| <b>contactinfo</b>         | Restore administrator contact information.                                                                                 |
| <b>fc-all</b>              | Restore configuration for all SN 5428 FC interfaces.                                                                       |
| <b>ip-route</b>            | Restore the SN 5428 route table.                                                                                           |
| <b>logging</b>             | Restore the routing rules in the SN 5428 event message logging table. Restored rules are appended to the end of the table. |
| <b>name-server</b>         | Restore DNS configuration.                                                                                                 |
| <b>ntp</b>                 | Restore NTP server configuration.                                                                                          |
| <b>remotelog</b>           | Restore IP address of host used for remote logging.                                                                        |
| <b>restrict</b>            | Restore the SN 5428 restrict configuration.                                                                                |
| <b>snmp</b>                | Restore SNMP configuration.                                                                                                |
| <b>software</b>            | Restore the default software download location and user name and password information for HTTP, proxy, and TFTP.           |

Some system information that is saved when the **save system** command is issued is not available for restoration from a saved configuration file. Use the **show savedconfig** command to display the contents of the specified configuration file. The following configuration information is available for display but cannot be restored:

- Management and HA interface IP addresses
- Gigabit Ethernet interface configuration information
- Administrator mode and Monitor mode passwords
- HA configuration mode

**Examples**

The following example restores all restorable system configuration information (except the SN 5428 route table) from the saved configuration file *system\_backup*:

```
[SN5428A] # restore system all from system_backup
```

The following example restores the SN 5428 route table from the saved configuration file *system\_backup*:

```
[SN5428A] # restore system ip-route from system_backup
```

The following example restores the SNMP configuration information from the saved configuration file *sys\_SN5428A*:

```
[SN5428A] # restore system snmp from sys_SN5428A
```

**Related Commands**

| <b>Commands</b>           | <b>Description</b>                                                                                     |
|---------------------------|--------------------------------------------------------------------------------------------------------|
| <b>delete savedconfig</b> | Remove a saved configuration file from the SN 5428.                                                    |
| <b>restore all</b>        | Restore the contents of the named configuration file into memory.                                      |
| <b>save all</b>           | Save all configuration information.                                                                    |
| <b>save system</b>        | Save selected system configuration information.                                                        |
| <b>show savedconfig</b>   | List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file. |

# restore vlan

To cause the specified VLAN to be copied from the named configuration file into persistent memory, use the **restore vlan** command. The configuration file must exist in the *savedconfig* directory. To display the contents of the *savedconfig* directory, issue the **show savedconfig** command.

```
restore vlan {all | vid} from filename
```

| Syntax Description | all                         | Restore all VLAN definitions.                                                                                                           |
|--------------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
|                    | <i>vid</i>                  | The VLAN identification number.                                                                                                         |
|                    | <b>from</b> <i>filename</i> | The name of the configuration file containing the information to be restored. This file must exist in the <i>savedconfig</i> directory. |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** If the VLAN currently exists, the **restore vlan** command overwrites existing configuration information with the information from the named configuration file. The **restore vlan** command also restores the VTP configuration information.



**Note**

In a cluster environment, VLAN management functions are handled by a single SN 5428. To determine which SN 5428 is performing VLAN management functions, issue the **show cluster** command. If you issue a **restore vlan** command from a storage router that is not performing VLAN management functions, the CLI displays an informational message with the name of the SN 5428 that is currently handling those functions. For more information on operating the SN 5428 in a cluster, see Chapter 10, “Maintaining and Managing the SN 5428 Storage Router.”

**Examples** The following example restores VLAN 100 from the *vlanBackup* file:

```
[SN5428A]# restore vlan 100 from vlanBackup
```

| Related Commands | Command                    | Description                                                                                                |
|------------------|----------------------------|------------------------------------------------------------------------------------------------------------|
|                  | <b>save vlan</b>           | Save configuration information for the named VLAN or all VLANs                                             |
|                  | <b>scsirouter serverif</b> | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |

| Command                 | Description                                                                                            |
|-------------------------|--------------------------------------------------------------------------------------------------------|
| <b>show savedconfig</b> | List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file. |
| <b>show vlan</b>        | Display configuration and operational information for the specified VLAN or all VLANs.                 |
| <b>show vtp</b>         | Display configuration and operational information for VTP.                                             |
| <b>vlan</b>             | Configure a non-VTP VLAN on the SN 5428.                                                               |
| <b>vtp domain</b>       | Assign a VTP domain name to the SN 5428.                                                               |
| <b>vtp mode</b>         | Configure the SN 5428 to operate in client or transparent VTP mode.                                    |

# restrict

To close access to the specified interface via the named service, use the **restrict** command. To allow access via the named service, use the **no** form of this command.

```
restrict all [service]
```

```
restrict interface {all | service}
```

```
no restrict all [service]
```

```
no restrict interface {all | service}
```

| Syntax Description |                  |                                                                                                                                     |
|--------------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------|
|                    | <b>all</b>       | Restrict all interface or all services.                                                                                             |
|                    | <i>interface</i> | Restrict access to the specified interface. See Table 11-15 in the Usage Guidelines section for a list of interface names.          |
|                    | <i>service</i>   | Restrict access via the specified service or protocol. See Table 11-16 in the Usage Guidelines section for a list of service names. |

## Defaults

The following are factory default settings:

- FTP using port 21 is restricted on all interfaces.
- HTTP using port 80 is allowed on the management and HA interfaces. It is restricted on the Gigabit Ethernet interfaces. (HTTP access cannot be restricted on the management or HA interface.)
- Remote login (rlogin) using port 513 is restricted on all interfaces.
- SNMP using port 161 is allowed on the management interface. It is restricted on the HA and Gigabit Ethernet interfaces.
- SSL using port 443 is restricted on all interfaces.
- Telnet using port 23 is allowed on the management interface only. It is restricted on the HA and Gigabit Ethernet interfaces.

## Command Modes

Administrator.

## Command History

| Release | Modification                              |
|---------|-------------------------------------------|
| 2.2.1   | This command was introduced.              |
| 2.3.1   | The <b>SSL</b> service keyword was added. |

## Usage Guidelines

Use the **restrict** command to restrict unauthorized access to SN 5428 interfaces. Use the **show restrict** command to display the current interface and service restrictions.

You can restrict access on the interfaces listed in Table 11-15.

**Table 11-15 restrict interface**

| Interface Keyword | Description                                                                                                                                                                                                                                                 |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ge?</b>        | The SN 5428 Gigabit Ethernet interfaces (including all logical interfaces created by associating a VLAN with a Gigabit Ethernet IP address for a SCSI routing instance). All services are restricted on the SN 5428 Gigabit Ethernet interfaces by default. |
| <b>ha</b>         | The SN 5428 HA interface. This interface is open to HTTP by default. HTTP access cannot be disabled for the HA interface.                                                                                                                                   |
| <b>mgmt</b>       | The SN 5428 management interface. This interface is open to Telnet, SNMP and HTTP by default. HTTP access cannot be disabled for the management interface.                                                                                                  |

You can restrict access to the SN 5428 interfaces by the services or protocols, shown in Table 11-16.

**Table 11-16 restrict interface service**

| Service Keyword | Description                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ftp</b>      | File Transfer Protocol. FTP access is restricted on all interfaces, by default.                                                                                                                                                                                                                                                                                                                          |
| <b>http</b>     | Hypertext Transfer Protocol. HTTP access is available on all interfaces, by default. It cannot be restricted on the management or HA interfaces.                                                                                                                                                                                                                                                         |
| <b>rlogin</b>   | Remote login on port 513. If rlogin is enabled for an interface, the setting is only valid until the storage router is restarted. The rlogin setting is not retained across a storage router restart; rlogin returns to a restricted state for all interfaces.<br><br><b>Note</b> Rlogin is designed for debug purposes and should be used under the guidance of a Cisco Technical Support professional. |
| <b>snmp</b>     | Simple Network Management Protocol. SNMP is enabled on the management interface by default.                                                                                                                                                                                                                                                                                                              |
| <b>ssl</b>      | Secure Socket Layer. SSL is restricted on all interfaces by default.                                                                                                                                                                                                                                                                                                                                     |
| <b>telnet</b>   | Telnet. Telnet access is enabled on the management interface by default; it is restricted on all other interfaces.                                                                                                                                                                                                                                                                                       |

To access the GUI using an SSL connection, enable SSL on the appropriate interface and change the URL to use “https” instead of “http.”

---

**Examples**

The following example restricts HTTP access to the Gigabit Ethernet interface, *ge2*:

```
[SN5428A]# restrict ge2 http
```

The following example restricts Telnet access to the HA interface:

```
[SN5428A]# restrict ha telnet
```

The following example restricts access to all interfaces via FTP.

```
[SN5428A]# restrict all ftp
```

The following example enables SSL on the management interface.

```
[SN5428A]# no restrict mgmt ssl
```

---

**Related Commands**

| Command                 | Description                                                           |
|-------------------------|-----------------------------------------------------------------------|
| <b>restrict console</b> | Enable or disable password checking on the SN 5428 console interface. |
| <b>show restrict</b>    | Display configurable security settings for the SN 5428's interfaces.  |

# restrict console

To enable password checking on the SN 5428 console interface, use the **restrict console** command. The Administrator mode and Monitor mode passwords will be required when accessing the SN 5428 via a console connected to the EIA/TIA-232 port. To disable password checking on the console interface, use the **no** form of this command.

**restrict console**

**no restrict console**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Passwords are disabled on the console interface.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command if you need to restrict access to the SN 5428's console interface.

**Examples** The following example enabled password checking on the SN 5428's console interface:

```
[SN5428A] # restrict console
```

| Related Commands | Command              | Description                                                                   |
|------------------|----------------------|-------------------------------------------------------------------------------|
|                  | <b>restrict</b>      | Secure access to SN 5428 interfaces by communications protocols and services. |
|                  | <b>show restrict</b> | Display configurable security settings for the SN 5428's interfaces.          |

## save aaa

To save the current AAA settings to nonvolatile memory, use the **save aaa** command.

```
save aaa {bootconfig | filename}
```

| Syntax Description | bootconfig      | Save the AAA settings to the SN 5428's bootable configuration, which is used when the SN 5428 Storage Router is restarted.             |
|--------------------|-----------------|----------------------------------------------------------------------------------------------------------------------------------------|
|                    | <i>filename</i> | The name of the file where the AAA configuration information will be written. This file is stored in the <i>savedconfig</i> directory. |

| Defaults | None. |
|----------|-------|
|----------|-------|

| Command Modes | Administrator. |
|---------------|----------------|
|---------------|----------------|

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** You must save configuration data from the running configuration to the bootable configuration for it to be retained in the SN 5428 when it is restarted. Use the *filename* parameter to save the AAA configuration to a file. Configurations saved to a file can be moved between SN 5428s and can be restored at a later time.

The following information is saved:

- The AAA authentication list
- The username database
- All RADIUS server configuration information
- All TACACS+ server configuration information

**Examples** The following example saves the running AAA settings to the bootable configuration, used when the SN 5428 is restarted:

```
[SN5428A]# save aaa bootconfig
```

The following example saves the running AAA settings to a file named *aaa\_SN5428A*:

```
[SN5428A]# save aaa aaa_SN5428A
```

## Related Commands

| Command                         | Description                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------|
| <b>aaa authentication iscsi</b> | Configure the AAA authentication services to be used for iSCSI authentication.                         |
| <b>aaa test authentication</b>  | Enable testing of the default AAA authentication list.                                                 |
| <b>debug aaa</b>                | Enable debugging for the AAA authentication services.                                                  |
| <b>delete savedconfig</b>       | Remove a saved configuration file from the SN 5428.                                                    |
| <b>radius-server host</b>       | Configure remote RADIUS servers for AAA authentication services.                                       |
| <b>restore aaa</b>              | Restore AAA authentication services from a saved configuration file.                                   |
| <b>save accesslist</b>          | Save configuration data for the named access list or for all access lists.                             |
| <b>save all</b>                 | Save all configuration information.                                                                    |
| <b>save scsirouter</b>          | Save configuration information for the named SCSI routing instance.                                    |
| <b>save system</b>              | Save selected system configuration information.                                                        |
| <b>save vlan</b>                | Save configuration information for the named VLAN or all VLANs.                                        |
| <b>scsirouter authenticate</b>  | Enable iSCSI authentication for the named SCSI routing instance.                                       |
| <b>show aaa</b>                 | Display AAA configuration information.                                                                 |
| <b>show savedconfig</b>         | List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file. |
| <b>tacacs-server host</b>       | Configure remote TACACS+ servers for AAA authentication services.                                      |
| <b>username password</b>        | Add a user name and optional password to the local username database.                                  |

# save accesslist

To save configuration data to nonvolatile memory for the named accesslist or for all access lists, use the **save accesslist** command.

```
save accesslist {name | all} {bootconfig | filename}
```

| Syntax Description |                   |                                                                                                                                                 |
|--------------------|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | <i>name</i>       | The name of the access list to be saved.                                                                                                        |
|                    | <b>all</b>        | Save all access lists associated with this SN 5428.                                                                                             |
|                    | <b>bootconfig</b> | Save the access list from the running configuration to the SN 5428's bootable configuration, used when the SN 5428 Storage Router is restarted. |
|                    | <i>filename</i>   | The name of the file where the running access list configuration data will be written. This file is stored in the <i>savedconfig</i> directory. |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** You must save configuration data from the running configuration to the bootable configuration for it to be retained in the SN 5428 when it is restarted. Configurations saved to a file can be moved between SN 5428s, and can be restored at a later time.



**Note**

In a cluster environment, access list management functions are handled by a single SN 5428. To determine which SN 5428 is performing access list management functions, issue the **show cluster** command. If you issue the **save accesslist** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the SN 5428 that is currently handling those functions. For more information on operating the SN 5428 in a cluster, see Chapter 10, “Maintaining and Managing the SN 5428 Storage Router.”

**Examples**

The following example saves the current configuration for all access lists to the bootable configuration, used when the SN 5428 is restarted:

```
[SN5428A]# save accesslist all bootconfig
```

The following example saves the access list *fooList* to a configuration file named *fooList\_SN5428A*:

```
[SN5428A]# save accesslist fooList fooList_SN5428A
```

**Related Commands**

| Command                             | Description                                                                                            |
|-------------------------------------|--------------------------------------------------------------------------------------------------------|
| <b>accesslist</b>                   | Create an access list entity.                                                                          |
| <b>accesslist A.B.C.D/bits</b>      | Add IP addresses to an access list.                                                                    |
| <b>delete accesslist</b>            | Delete a specific access list entry or an entire access list.                                          |
| <b>delete savedconfig</b>           | Remove a saved configuration file from the SN 5428.                                                    |
| <b>restore accesslist</b>           | Restore the named access list or all access lists from the named configuration file.                   |
| <b>save aaa</b>                     | Save the current AAA configuration information.                                                        |
| <b>save all</b>                     | Save all configuration information.                                                                    |
| <b>save scsirouter</b>              | Save configuration information for the named SCSI routing instance.                                    |
| <b>save system</b>                  | Save selected system configuration information.                                                        |
| <b>save vlan</b>                    | Save configuration information for the named VLAN or all VLANs.                                        |
| <b>scsirouter target accesslist</b> | Associate an access list with a specific SCSI routing instance target or all targets.                  |
| <b>show accesslist</b>              | Display the contents of the named access list or all access lists.                                     |
| <b>show savedconfig</b>             | List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file. |

# save all

To save all configuration data for the SN 5428 to nonvolatile memory, use the **save all** command.

```
save all {bootconfig | filename}
```

| Syntax Description | bootconfig      | Save the current running configuration information to the SN 5428's bootable configuration, used when the SN 5428 Storage Router is restarted. |
|--------------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | <i>filename</i> | The name of the file where the configuration data will be written. This file is stored in the <i>savedconfig</i> directory.                    |

| Defaults | None. |
|----------|-------|
|----------|-------|

| Command Modes | Administrator. |
|---------------|----------------|
|---------------|----------------|

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** You must save configuration data from the running configuration to the bootable configuration for it to be retained in the SN 5428 when it is restarted. Depending on the SN 5428 deployment, the **save all** command saves AAA configuration, SCSI routing instances, access lists, VLANs, and selected system configuration information. Configurations saved to a file can be moved between SN 5428s and can be restored at a later time.



### Note

In a cluster environment, all access list and VLAN management functions are handled by a single SN 5428. To determine which SN 5428 is performing access list and VLAN management functions, issue the **show cluster** command. If you issue the **save all** command from a storage router that is not performing access list and VLAN management functions, the CLI displays an informational message with the name of the SN 5428 that is currently handling those functions. For more information on operating the SN 5428 in a cluster, see Chapter 10, “Maintaining and Managing the SN 5428 Storage Router.”

### Examples

The following example saves the current running configuration to the bootable configuration, used when the SN 5428 is restarted:

```
[SN5428A]# save all bootconfig
```

The following example saves the current running configuration to the file named *SN5428A\_03Nov2001*. You may want to do this as a means of archiving the current running configuration of the SN 5428 on a regular basis.

```
[SN5428A]# save all SN5428A_03Nov2001
```

**Related Commands**

| <b>Command</b>            | <b>Description</b>                                                                                     |
|---------------------------|--------------------------------------------------------------------------------------------------------|
| <b>delete savedconfig</b> | Remove a saved configuration file from the SN 5428.                                                    |
| <b>restore all</b>        | Restore the contents of the named configuration file into memory.                                      |
| <b>save aaa</b>           | Save current AAA configuration information.                                                            |
| <b>save accesslist</b>    | Save configuration data for the named access list or for all access lists.                             |
| <b>save scsirouter</b>    | Save configuration information for the named SCSI routing instance.                                    |
| <b>save system</b>        | Save selected system configuration information.                                                        |
| <b>save vlan</b>          | Save configuration information for the named VLAN or all VLANs.                                        |
| <b>show savedconfig</b>   | List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file. |

# save scsirouter

To save all configuration data associated with the named SCSI routing instance to nonvolatile memory, use the **save scsirouter** command.

```
save scsirouter {name | all} {bootconfig | filename}
```

| Syntax Description |  |                                                                                                                                                           |
|--------------------|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>        |  | The name of the SCSI routing instance.                                                                                                                    |
| <b>all</b>         |  | Save configuration data for all SCSI routing instances.                                                                                                   |
| <b>bootconfig</b>  |  | Save the SCSI routing instance from the running configuration to the SN 5428's bootable configuration, used when the SN 5428 Storage Router is restarted. |
| <i>filename</i>    |  | The name of the file where the configuration data will be written. This file is stored in the <i>savedconfig</i> directory.                               |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Maintenance                  |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** You must save configuration data from the running configuration to the bootable configuration for it to be retained in the SN 5428 when it is restarted. Configurations saved to a file can be moved between SN 5428s and can be restored at a later time.

In a cluster environment, the SCSI routing instance can only be saved on the SN 5428 that is the currently running that instance.

**Examples** The following example saves all SCSI routing instances currently running on this SN 5428 to the bootable configuration, used when the SN 5428 is restarted:

```
[SN5428A]# save scsirouter all bootconfig
```

The following example saves the SCSI routing instance named *foo* to the file named *foo\_SN5428A*:

```
[SN5428A]# save scsirouter foo foo_SN5428A
```

**Related Commands**

| <b>Commands</b>            | <b>Description</b>                                                                                         |
|----------------------------|------------------------------------------------------------------------------------------------------------|
| <b>delete savedconfig</b>  | Remove a saved configuration file from the SN 5428.                                                        |
| <b>delete scsirouter</b>   | Delete the named SCSI routing instance or the specified element of the SCSI routing instance.              |
| <b>restore scsirouter</b>  | Restore the named SCSI routing instance from the named configuration file.                                 |
| <b>save aaa</b>            | Save the current AAA configuration information.                                                            |
| <b>save accesslist</b>     | Save configuration data for the named access list or all access lists.                                     |
| <b>save all</b>            | Save all configuration information.                                                                        |
| <b>save system</b>         | Save selected system configuration information.                                                            |
| <b>save vlan</b>           | Save configuration information for the named VLAN or all VLANs.                                            |
| <b>scsirouter</b>          | Create a SCSI routing instance.                                                                            |
| <b>scsirouter enable</b>   | Stop or start the named SCSI routing instance.                                                             |
| <b>scsirouter serverif</b> | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
| <b>setup scsi</b>          | Run the wizard to configure a SCSI routing instance.                                                       |
| <b>show savedconfig</b>    | List the contents of the savedconfig directory or the contents of the named configuration file.            |
| <b>show scsirouter</b>     | Display configuration and operational information for the named SCSI routing instance.                     |

# save system

To save selected system configuration information to nonvolatile memory, use the **save system** command.

```
save system {bootconfig | filename}
```

| Syntax Description | Parameter         | Description                                                                                                                               |
|--------------------|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
|                    | <b>bootconfig</b> | Save the current running system configuration to the SN 5428's bootable configuration, used when the SN 5428 Storage Router is restarted. |
|                    | <i>filename</i>   | The name of the file where the system configuration data will be written. This file is stored in the <i>savedconfig</i> directory.        |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** You must save configuration data from the running configuration to the bootable configuration for it to be retained in the SN 5428 when it is restarted. Configurations saved to a file can be moved between SN 5428s and can be restored at a later time.

The following system configuration data is saved:

- Monitor and Administrator passwords
- Administrative contact information
- Network Time Protocol (NTP) server name
- Primary and optional secondary Domain Name Server (DNS)
- Default location for downloading SN 5428 software
- System and cluster name
- Management and high availability (HA) interface addresses
- Static routes
- SNMP settings
- CDP settings
- Restrict settings
- IP address of remote syslog host for logging
- SN 5428 logging table
- Configuration information for Fibre Channel interfaces

**Examples**

The following example saves the current system configuration to the bootable configuration, used when the SN 5428 is restarted:

```
[SN5428A] # save system bootconfig
```

The following example copies the current system configuration to the file named `sys_SN5428A`:

```
[SN5428A] # save system sys_SN5428A
```

**Related Commands**

| Commands                  | Description                                                                                     |
|---------------------------|-------------------------------------------------------------------------------------------------|
| <b>delete savedconfig</b> | Remove a saved configuration file from the SN 5428.                                             |
| <b>hostname</b>           | Specify the SN 5428's system name.                                                              |
| <b>restore system</b>     | Restore selected system information from the named configuration file.                          |
| <b>save aaa</b>           | Save the current AAA configuration information.                                                 |
| <b>save accesslist</b>    | Save configuration data for the named access list or all access lists.                          |
| <b>save all</b>           | Save all configuration information.                                                             |
| <b>save scsirouter</b>    | Save configuration information for the named SCSI routing instance.                             |
| <b>save vlan</b>          | Save configuration information for the named VLAN or all VLANs.                                 |
| <b>show savedconfig</b>   | List the contents of the savedconfig directory or the contents of the named configuration file. |
| <b>show system</b>        | Display selected system information, including system name.                                     |

# save vlan

To save VLAN and VTP configuration information for the specified VLAN or for all VLANs to nonvolatile memory, use the **save vlan** command.

```
save vlan {vid | all} {bootconfig | filename}
```

| Syntax Description |  |                                                                                                                                          |
|--------------------|--|------------------------------------------------------------------------------------------------------------------------------------------|
| <i>vid</i>         |  | The VLAN identification number of the VLAN configuration to be saved.                                                                    |
| <b>all</b>         |  | Save all VLANs associated with this SN 5428.                                                                                             |
| <b>bootconfig</b>  |  | Save the current VLAN configuration to the system's bootable configuration, to be used when the SN 5428 is restarted.                    |
| <i>filename</i>    |  | The name of the file where the current VLAN configuration data will be written. This file is stored in the <i>savedconfig</i> directory. |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** You must save configuration data from the running configuration to the bootable configuration for it to be retained in the SN 5428 when it is restarted. Configurations saved to a file can be moved between SN 5428s and can be restored at a later time.

VTP mode and domain information is saved, along with the specified VLAN configuration information.



**Note**

In a cluster environment, VLAN management functions are handled by a single SN 5428. To determine which SN 5428 is performing VLAN management functions, issue the **show cluster** command. If you issue the **save vlan** command from a storage router that is not performing VLAN management functions, the CLI displays an informational message with the name of the SN 5428 that is currently handling those functions. For more information on operating the SN 5428 in a cluster, see Chapter 10, "Maintaining and Managing the SN 5428 Storage Router."

**Examples** The following example saves the current configuration for all VLANs to the system's bootable configuration, to be used when the SN 5428 is restarted:

```
[SN5428A]# save vlan all bootconfig
```

The following example saves VLAN 12 to the file named *vlanbackup*:

```
[SN5428A]# save vlan 12 vlanbackup
```

**Related Commands**

| <b>Command</b>          | <b>Description</b>                                                                                     |
|-------------------------|--------------------------------------------------------------------------------------------------------|
| <b>restore vlan</b>     | Restore VLAN configuration information from the named configuration file.                              |
| <b>save aaa</b>         | Save current AAA configuration information.                                                            |
| <b>save accesslist</b>  | Save configuration data for the named access list or all access lists.                                 |
| <b>save all</b>         | Save all configuration information.                                                                    |
| <b>save scsirouter</b>  | Save configuration information for the named SCSI routing instance.                                    |
| <b>save system</b>      | Save selected system configuration information.                                                        |
| <b>show savedconfig</b> | List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file. |
| <b>show vlan</b>        | Display configuration and operational information for the specified VLAN or all VLANs.                 |
| <b>show vtp</b>         | Display configuration and operational information for VTP.                                             |
| <b>vlan</b>             | Configure a non-VTP VLAN on the SN 5428.                                                               |
| <b>vtp domain</b>       | Assign a VTP domain name to the SN 5428.                                                               |
| <b>vtp mode</b>         | Configure the SN 5428 to operate in client or transparent VTP mode.                                    |

# scsirouter

To create a SCSI routing instance, use the **scsirouter** command.

**scsirouter** *name*

| Syntax Description | <i>name</i> | The name of the SCSI routing instance created by this command. Enter a maximum of 31 characters. |
|--------------------|-------------|--------------------------------------------------------------------------------------------------|
|--------------------|-------------|--------------------------------------------------------------------------------------------------|

| Defaults | None. |
|----------|-------|
|----------|-------|

| Command Modes | Administrator. |
|---------------|----------------|
|---------------|----------------|

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** SCSI routing is the routing of SCSI requests and responses between IP hosts in an IP network and storage devices in a Fibre Channel storage network. The SCSI routing instance becomes a binding point for the association of other configuration parameters. A SCSI routing instance provides IP hosts access to Fibre Channel storage.

There can be a maximum of 12 SCSI routing instances defined per SN 5428; if the SN 5428 is a member of a cluster, no more than 12 instances can be defined across the cluster.



**Note**

If the storage router is deployed for transparent SCSI routing, there can be only one SCSI routing instance. The SCSI routing instance is named *transparent* and is automatically created during initial system configuration.

**Examples** The following command creates a SCSI routing entity named *myCompanyWebserver2*.

```
[SN5428A] # scsirouter myCompanyWebserver2
```

| Related Commands | Command                        | Description                                                                                   |
|------------------|--------------------------------|-----------------------------------------------------------------------------------------------|
|                  | <b>accesslist</b>              | Create an access list entity.                                                                 |
|                  | <b>accesslist A.B.C.D/bits</b> | Add IP addresses to an access list.                                                           |
|                  | <b>delete scsirouter</b>       | Delete the named SCSI routing instance or the specified element of the SCSI routing instance. |
|                  | <b>failover scsirouter</b>     | Cause the named SCSI routing instance to cease running on the SN 5428.                        |

| <b>Command</b>                 | <b>Description</b>                                                                                         |
|--------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>restore accesslist</b>      | Restore the named access list or all access lists from the named configuration file.                       |
| <b>restore scsirouter</b>      | Restore the named SCSI routing instance from the named configuration file.                                 |
| <b>save accesslist</b>         | Save configuration data for the named access list or all access lists.                                     |
| <b>save scsirouter</b>         | Save configuration information for the named SCSI routing instance.                                        |
| <b>scsirouter authenticate</b> | Enable iSCSI authentication for the named SCSI routing instance.                                           |
| <b>scsirouter enable</b>       | Stop or start the named SCSI routing instance.                                                             |
| <b>scsirouter serverif</b>     | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
| <b>setup scsi</b>              | Run the wizard to configure a SCSI routing instance.                                                       |
| <b>show scsirouter</b>         | Display configuration and operational information for the named SCSI routing instance.                     |

# scsirouter authenticate

To enable iSCSI authentication using AAA authentication services for the named SCSI routing instance, use the **scsirouter authenticate** command.

**scsirouter** *name* **authenticate** {no | yes}

## Syntax Description

|             |                                                                 |
|-------------|-----------------------------------------------------------------|
| <i>name</i> | The name of this SCSI routing instance.                         |
| <b>no</b>   | Disable AAA authentication for the named SCSI routing instance. |
| <b>yes</b>  | Enable AAA authentication for the named SCSI routing instance.  |

## Defaults

AAA authentication is disabled.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

Use the **scsirouter authenticate** command to enable iSCSI authentication for IP hosts requesting access to storage using the named SCSI routing instance. AAA performs authentication using the services configured on the iSCSI authentication list. Use the **aaa authentication iscsi** command to configure the iSCSI authentication list.



### Note

If authentication is enabled for a SCSI routing instance, but no AAA authentication list is available, AAA attempts to use the “local” authentication method.

## Examples

The following example enables iSCSI authentication for the SCSI routing instance named *foo*:

```
[SN5428A] # scsirouter foo authenticate yes
```

## Related Commands

| Command                         | Description                                                                    |
|---------------------------------|--------------------------------------------------------------------------------|
| <b>aaa authentication iscsi</b> | Configure the AAA authentication services to be used for iSCSI authentication. |
| <b>debug aaa</b>                | Enable debugging for the AAA authentication services.                          |
| <b>radius-server host</b>       | Configure remote RADIUS servers for AAA authentication services.               |
| <b>restore aaa</b>              | Restore AAA authentication services from a saved configuration file.           |
| <b>save aaa</b>                 | Save the current AAA configuration information.                                |
| <b>save scsirouter</b>          | Save configuration information for the named SCSI routing instance.            |

| <b>Command</b>            | <b>Description</b>                                                    |
|---------------------------|-----------------------------------------------------------------------|
| <b>show aaa</b>           | Display AAA configuration information.                                |
| <b>tacacs-server host</b> | Configure remote TACACS+ servers for AAA authentication services.     |
| <b>username password</b>  | Add a user name and optional password to the local username database. |

# scsirouter cdbretrycount

To specify the number of times a failed command should be retried before returning an error on the CDB, use the **scsirouter cdbretrycount** command.

**scsirouter** *name* **cdbretrycount** *nn*

| Syntax Description | <i>name</i> | The name of this SCSI routing instance.                                                                                         |
|--------------------|-------------|---------------------------------------------------------------------------------------------------------------------------------|
|                    | <i>nn</i>   | The number of CDB retries. <i>nn</i> is an integer from 0 to 512. The default value is 30. There is one second between retries. |

**Defaults** The number of CDB retries is 30, by default.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.3.1   | This command was introduced. |

**Usage Guidelines** Use this command to change the number of times a failed CDB will be retried by the SN 5428 before returning an error on the CDB. Retries occur every second. For example, with the default retry count value of 30, it would take 30 seconds before a failed command would be returned with an error.

If an intelligent storage array includes multiple paths between hosts and storage, lowering the CDB retry count value could change the triggering of failover situations.



**Note**

In a high availability cluster, the SN 5428 may fail over a SCSI routing instance when all devices accessed through that instance cannot be reached, before the maximum number of CDB retries occurs.

**Examples** The following example sets the CDB retry count value to 10:

```
[SN5428A] # scsirouter transparent cdbretrycount 10
```

| Related Commands | Command                | Description                                                                            |
|------------------|------------------------|----------------------------------------------------------------------------------------|
|                  | <b>show scsirouter</b> | Display configuration and operational information for the named SCSI routing instance. |

# scsirouter description

To add user-defined identification information to the named SCSI routing instance, use the **scsirouter description** command.

```
scsirouter name description "user text"
```

## Syntax Description

|                                         |                                                                                                                                                                            |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>                             | The name of this SCSI routing instance.                                                                                                                                    |
| <b>description</b> " <i>user text</i> " | User-defined identification information associated with this SCSI routing instance. If the string contains spaces, enclose it in quotes. Enter a maximum of 64 characters. |

## Defaults

None.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

The **scsirouter description** command allows you to add a new description or change an existing description. Descriptions are site-specific.

## Examples

The following example adds the description "Access to WebServer4 WebServer5" to the SCSI routing instance *fool*:

```
[SN5428A]# scsirouter fool description "Access to WebServer4 WebServer5"
```

## Related Commands

| Command                    | Description                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------|
| <b>delete scsirouter</b>   | Delete the named SCSI routing instance or the specified element of the SCSI routing instance.              |
| <b>restore scsirouter</b>  | Restore the named SCSI routing instance from the named configuration file.                                 |
| <b>save scsirouter</b>     | Save configuration information for the named SCSI routing instance.                                        |
| <b>scsirouter</b>          | Create a SCSI routing instance.                                                                            |
| <b>scsirouter enable</b>   | Stop or start the named SCSI routing instance.                                                             |
| <b>scsirouter serverif</b> | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
| <b>setup scsi</b>          | Run the wizard to configure a SCSI routing instance.                                                       |
| <b>show scsirouter</b>     | Display configuration and operational information for the named SCSI routing instance.                     |

# scsirouter enable

To start the named SCSI routing instance on this SN 5428, use the **scsirouter enable** command. To stop the named SCSI routing instance, use the **no** form of this command.

**scsirouter** {*name* | **all**} **enable**

**no scsirouter** {*name* | **all**} **enable**

| Syntax Description |                                                      |
|--------------------|------------------------------------------------------|
| <i>name</i>        | The name of the SCSI routing instance to be started. |
| <b>all</b>         | Start all SCSI routing instances on this SN 5428.    |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** SCSI routing instances that are in a stopped state are not running anywhere in the cluster. To restart a stopped SCSI routing instance, use the **scsirouter enable** command. Use the **all** keyword to start all instances on the SN 5428. All instances previously stopped on this SN 5428 or available instances not running elsewhere in the cluster will start on this SN 5428.

Under normal circumstances, the SCSI routing instance can only be started from the SN 5428 on which it was stopped.

Use the **scsirouter enable** command to bring a restored SCSI routing instance into the running configuration. A restored instance must be started before you can make any additional configuration changes to that instance.



**Note**

SCSI routing instances are automatically started by the SN 5428.

**Examples**

The following example starts the SCSI routing instance named *foo2*. This instance must have been previously stopped.

```
[SN5428A]# scsirouter foo2 enable
```

The following example stops all SCSI routing instances running on the SN 5428:

```
[SN5428A]# no scsirouter all enable
```

**Related Commands**

| Command                    | Description                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------|
| <b>delete scsirouter</b>   | Delete the named SCSI routing instance or the specified element of the SCSI routing instance.              |
| <b>failover scsirouter</b> | Cause the named SCSI routing instance to cease running on the SN 5428.                                     |
| <b>restore scsirouter</b>  | Restore the named SCSI routing instance from the named configuration file.                                 |
| <b>save scsirouter</b>     | Save configuration information for the named SCSI routing instance.                                        |
| <b>scsirouter</b>          | Create a SCSI routing instance.                                                                            |
| <b>scsirouter primary</b>  | Identify the SN 5428 as the preferred SN 5428 to run the named SCSI routing instance.                      |
| <b>scsirouter serverif</b> | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
| <b>setup scsi</b>          | Run the wizard to configure a SCSI routing instance.                                                       |
| <b>show scsirouter</b>     | Display configuration and operational information for the named SCSI routing instance.                     |

# scsirouter failover

To build a list of SN 5428s to be used for failover purposes, use the **scsirouter failover** command.

```
scsirouter name failover {primary | secondary} sysname
```

| Syntax Description              |                                                                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>                     | The name of the SCSI routing instance.                                                                                                                              |
| <b>primary</b> <i>sysname</i>   | The name of the SN 5428 in the cluster. In case of failure, the specified SCSI routing instance will be failed over to this SN 5428.                                |
| <b>secondary</b> <i>sysname</i> | (Optional) The name of the SN 5428 in the cluster. If the primary SN 5428 in the list cannot run the SCSI routing instance, it will be failed over to this SN 5428. |
|                                 | <b>Note</b> Because a high availability cluster consists of two SN 5428 Storage Routers, this parameter is not used.                                                |

**Defaults** None. By default, the HA failover list is not populated.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use the **scsirouter failover** command to build a list of SN 5428s that will be used during the failover process. If the specified SCSI routing instance fails over, the cluster attempts to start running the instance on the SN 5428 designated as the *primary* in the HA failover list. If that SN 5428 cannot run the SCSI routing instance, the cluster will attempt to start the instance on the SN 5428 designated as the *secondary* in the HA failover list.

If there is no primary or secondary SN 5428 on the HA failover list when the SCSI routing instance fails over, the cluster attempts to run the instance on the first SN 5428 that is available.

The SN 5428s specified as primary and secondary should be active in the cluster when the command is issued. If the specified SN 5428 is not currently active in the cluster, the setting will not take affect until the SN 5428 is added to the cluster and the SCSI routing instance is restarted.

Use the **clear scsirouter failover** command to remove the current primary or secondary SN 5428 from the HA failover list.



**Note**

This command causes the SCSI routing instance configuration information to be saved and all nodes in the cluster to be updated.

**Examples**

The following example builds the HA failover list for the SCSI routing instance named *foo*. The primary SN 5428 in the HA failover list is *SN5428A*.

```
[SN5428A]# scsirouter foo failover primary SN5428A
```

**Related Commands**

| Command                          | Description                                                                                                           |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>clear scsirouter failover</b> | Remove the designated primary or secondary SN 5428 from the HA failover list for the specified SCSI routing instance. |
| <b>delete scsirouter</b>         | Delete the named SCSI routing instance or the specified element of the SCSI routing instance.                         |
| <b>failover scsirouter</b>       | Cause the named SCSI routing instance to cease running on the SN 5428.                                                |
| <b>restore scsirouter</b>        | Restore the named SCSI routing instance from the named configuration file.                                            |
| <b>save scsirouter</b>           | Save configuration information for the named SCSI routing instance.                                                   |
| <b>scsirouter</b>                | Create a SCSI routing instance.                                                                                       |
| <b>scsirouter enable</b>         | Stop or start the named SCSI routing instance.                                                                        |
| <b>scsirouter primary</b>        | Identify the SN 5428 as the preferred SN 5428 to run the named SCSI routing instance.                                 |
| <b>scsirouter serverif</b>       | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.            |
| <b>setup scsi</b>                | Run the wizard to configure a SCSI routing instance.                                                                  |
| <b>show scsirouter</b>           | Display configuration and operational information for the named SCSI routing instance.                                |

# scsirouter lun reset

To specify that “LUN reset” rather than “clear task” commands will be sent to the storage resources opened by the specified SCSI routing instance, use the **scsirouter lun reset** command.

**scsirouter** *name* **lun reset** {**yes** | **no**}

| Syntax Description |                                                                                             |  |
|--------------------|---------------------------------------------------------------------------------------------|--|
| <i>name</i>        | The name of the SCSI routing instance. The specified SCSI routing instance must be running. |  |
| <b>yes</b>         | Send “lun reset” to storage resources when they are opened.                                 |  |
| <b>no</b>          | Send “clear task” to storage resources when they are opened.                                |  |

**Defaults** The default is to send “clear task” commands to storage resources.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** It is preferable to send “LUN reset” commands if the device supports them. The specified SCSI routing instance must be running.

**Examples** The following example enables “LUN resets” to all storage resources opened by the SCSI routing instance *foo2*:

```
[SN5428A]# scsirouter foo2 lun reset yes
```

| Related Commands | Command                        | Description                                                                                                                                                |
|------------------|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>delete scsirouter</b>       | Delete the named SCSI routing instance or the specified element of the SCSI routing instance.                                                              |
|                  | <b>restore scsirouter</b>      | Restore the named SCSI routing instance from the named configuration file.                                                                                 |
|                  | <b>save scsirouter</b>         | Save configuration information for the named SCSI routing instance.                                                                                        |
|                  | <b>scsirouter</b>              | Create a SCSI routing instance.                                                                                                                            |
|                  | <b>scsirouter enable</b>       | Stop or start the named SCSI routing instance.                                                                                                             |
|                  | <b>scsirouter primary</b>      | Identify the SN 5428 as the preferred SN 5428 to run the named SCSI routing instance.                                                                      |
|                  | <b>scsirouter reserveproxy</b> | Enable the SCSI reserve/release commands for the specified SCSI routing instance and specify whether these commands are forwarded to the storage resource. |

| Command                    | Description                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------|
| <b>scsirouter serverif</b> | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
| <b>setup scsi</b>          | Run the wizard to configure a SCSI routing instance.                                                       |
| <b>show scsirouter</b>     | Display configuration and operational information for the named SCSI routing instance.                     |

# scsirouter primary

To assign the SN 5428 as the preferred SN 5428 for the named SCSI routing instance, use the **scsirouter primary** command.

```
scsirouter name primary {sysname | none}
```

| Syntax Description |                               |                                                               |
|--------------------|-------------------------------|---------------------------------------------------------------|
|                    | <i>name</i>                   | The name of this SCSI routing instance.                       |
|                    | <b>primary</b> <i>sysname</i> | The system name of the preferred SN 5428.                     |
|                    | <b>primary none</b>           | Indicate no preferred SN 5428 for this SCSI routing instance. |

**Defaults** The default primary attribute is *none*.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** At any given time, a SCSI routing instance can run on only one SN 5428 in a cluster. If a SCSI routing instance has the **primary** attribute set, the specified SN 5428 (upon system restart) will take over running that instance. Use the **scsirouter primary** command if you *always* want the specified SCSI routing instance to run on a specific SN 5428 in a cluster whenever that SN 5428 is available.

If the **primary** attribute is not set (the default condition), the SCSI routing instance continues running on the SN 5428 where it was started until it is explicitly stopped (via a **no scsirouter enable** command), it automatically fails over to another SN 5428 in the cluster because an interface is unavailable or a system failure occurs, or an explicit **failover scsirouter** command is issued.



**Note** Setting the **primary** attribute saves the SN 5428 configuration and circulates those changes to the high availability cluster. It does not immediately change the location of a running SCSI routing instance.

For additional information about HA, cluster configuration, and managing SCSI routing instances in a cluster environment, see Chapter 9, “Configuring a High Availability Cluster,” and Chapter 10, “Maintaining and Managing the SN 5428 Storage Router.”

**Examples**

The following command designates the SN 5428 *LabRouter1* as the SN 5428 on which the SCSI routing instance named *foo* will always, under normal conditions, run.

```
[SN5428A]# scsirouter foo primary LabRouter1
```

The following example resets the primary attribute for the SCSI routing instance named *foo2*. The instance named *foo2* will continue to run on the SN 5428 where it was started until it is explicitly stopped, it automatically fails over, or an explicit **failover scsirouter** command is issued.

```
[SN5428A]# scsirouter foo2 primary none
```

**Related Commands**

| Command                    | Description                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------|
| <b>delete scsirouter</b>   | Delete the named SCSI routing instance or the specified element of the SCSI routing instance.              |
| <b>restore scsirouter</b>  | Restore the named SCSI routing instance from the named configuration file.                                 |
| <b>save scsirouter</b>     | Save configuration information for the named SCSI routing instance.                                        |
| <b>scsirouter</b>          | Create a SCSI routing instance.                                                                            |
| <b>scsirouter enable</b>   | Stop or start the named SCSI routing instance.                                                             |
| <b>scsirouter failover</b> | Add the SN 5428 to the HA failover list for the specified SCSI routing instance.                           |
| <b>scsirouter serverif</b> | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
| <b>setup scsi</b>          | Run the wizard to configure a SCSI routing instance.                                                       |
| <b>show scsirouter</b>     | Display configuration and operational information for the named SCSI routing instance.                     |

# scsirouter reserveproxy

To configure the SCSI routing instance to track SCSI reserve/release commands and to specify whether these commands are forwarded to the storage target, use the **scsirouter reserveproxy** command.

```
scsirouter name reserveproxy {enable passthru {yes | no} | disable}
```

## Syntax Description

|                            |                                                                                                                                                                                                                                         |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>                | The name of the SCSI routing instance.                                                                                                                                                                                                  |
| <b>enable passthru yes</b> | Configure the SCSI routing instance to track SCSI reserve and release commands and enable forwarding of these commands to storage resources.                                                                                            |
| <b>enable passthru no</b>  | Configure the SCSI routing instance to track SCSI reserve and release commands but disable forwarding of these commands to storage resources.                                                                                           |
| <b>disable</b>             | Disable the reserve proxy feature for the named SCSI routing instance. The SN 5428 does not track the SCSI reserve and release commands, which are forwarded to the IP host. The IP host manages the SCSI reserve and release commands. |

## Defaults

Reserve-proxy passthru is disabled.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

The SCSI reserve/release command allows an initiator to reserve the storage for its own use. Attempts to access the storage from other initiators are rejected until the first initiator releases the storage. If the reserve proxy feature is enabled using the **scsirouter reserveproxy** command, the SN 5428 keeps track of the reserved status of target LUNs and returns the appropriate SCSI command status to other initiators that issue SCSI commands to that target LUN.

If passthru is enabled, the SN 5428 forwards the SCSI reserve and release commands to the device. If passthru is not enabled, the SCSI reserve and release commands are not forwarded, but the SN 5428 will respond as if the commands had been forwarded.



### Note

This functionality does not apply to operating systems (such as Windows NT) which do not utilize the SCSI Reserve command.

## Examples

The following example configures the SCSI routing instance *foo2* to track SCSI reserve and release commands and enables forwarding of these commands to storage resources:

```
[SN5428A] # scsirouter foo2 reserveproxy enable passthru yes
```

**Related Commands**

| <b>Command</b>              | <b>Description</b>                                                                                         |
|-----------------------------|------------------------------------------------------------------------------------------------------------|
| <b>delete scsirouter</b>    | Delete the named SCSI routing instance or the specified element of the SCSI routing instance.              |
| <b>restore scsirouter</b>   | Restore the named SCSI routing instance from the named configuration file.                                 |
| <b>save scsirouter</b>      | Save configuration information for the named SCSI routing instance.                                        |
| <b>scsirouter</b>           | Create a SCSI routing instance.                                                                            |
| <b>scsirouter enable</b>    | Stop or start the named SCSI routing instance.                                                             |
| <b>scsirouter failover</b>  | Add the SN 5428 to the HA failover list for the specified SCSI routing instance.                           |
| <b>scsirouter lun reset</b> | Configure the named SCSI routing instance to send a “LUN reset” command when opening all targets.          |
| <b>scsirouter serverif</b>  | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
| <b>setup scsi</b>           | Run the wizard to configure a SCSI routing instance.                                                       |
| <b>show scsirouter</b>      | Display configuration and operational information for the named SCSI routing instance.                     |

## scsirouter serverif

To assign a Gigabit Ethernet interface and IP address to the named SCSI routing instance, use the **scsirouter serverif** command. The specified interface allows IP hosts access to Fibre Channel storage.

```
scsirouter name serverif ge? {A.B.C.D/bits | A.B.C.D/1.2.3.4}
```

```
scsirouter name serverif ge? vlan vid {A.B.C.D/bits | A.B.C.D/1.2.3.4}
```

| Syntax Description         |                                                                                                                                                                                                                                                       |  |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| <i>name</i>                | Name of the SCSI routing instance to which you are adding the Gigabit Ethernet interface.                                                                                                                                                             |  |
| <b>serverif</b> <i>ge?</i> | The name of the interface. When you type the <b>scsirouter serverif</b> command, followed by <b>?</b> , the CLI lists the interfaces available. You cannot specify a nonexistent interface.                                                           |  |
| <i>A.B.C.D/bits</i>        | The IP address of the named interface. If the keyword <b>vlan</b> is used, the IP address is part of the specified VLAN. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The <i>/bits</i> specifies the subnet mask in CIDR style.      |  |
| <i>A.B.C.D/1.2.3.4</i>     | The IP address of the named interface. If the keyword <b>vlan</b> is used, the IP address is part of the specified VLAN. <i>A.B.C.D</i> is the dotted quad notation of the IP address. <i>1.2.3.4</i> is the dotted quad notation of the subnet mask. |  |
| <b>vlan</b> <i>vid</i>     | The keyword and the VLAN identifier.                                                                                                                                                                                                                  |  |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** The specified interface IP address is configured on IP hosts requiring access to storage resources through the SN 5428 Storage Router.

Each SCSI routing instance requires two active elements:

- The *serverif* element assigns an interface and IP address for use by the IP hosts requiring access to storage resources. The instance becomes active when this interface is added.
- The *target* element is a complex item that specifies the mapping between LUNs on the storage devices and the host systems.

The **scsirouter serverif vlan** command is used to associate a VLAN with a SCSI routing instance. All traffic using the specified Gigabit Ethernet interface will be considered as part of the VLAN; all IP hosts accessing storage through the SN 5428 using the specified Gigabit Ethernet interface IP address must connect as part of the specified VLAN.

When the SCSI routing instance is started, a logical interface (for example, ge2VLAN100) is created, which incorporates the physical interface and the VID. This logical interface can be displayed via the **show interface** command.

### Examples

The following command adds the Gigabit Ethernet interface *ge1*, with the IP address 10.1.10.255/24, to the SCSI routing instance named *foo2*.

```
[SN5428A]# scsirouter foo2 serverif ge1 10.1.10.255/24
```

The following command adds the Gigabit Ethernet interface *ge2* and VLAN ID 45, with IP address 10.1.30.255/24, to the SCSI routing instance *fooA*:

```
[SN5428A]# scsirouter fooA serverif ge2 vlan 45 10.1.30.255/24
```

### Related Commands

| Command                   | Description                                                                                   |
|---------------------------|-----------------------------------------------------------------------------------------------|
| <b>delete scsirouter</b>  | Delete the named SCSI routing instance or the specified element of the SCSI routing instance. |
| <b>restore scsirouter</b> | Restore the named SCSI routing instance from the named configuration file.                    |
| <b>save scsirouter</b>    | Save configuration information for the named SCSI routing instance.                           |
| <b>scsirouter</b>         | Create a SCSI routing instance.                                                               |
| <b>scsirouter enable</b>  | Stop or start the named SCSI routing instance.                                                |
| <b>setup scsi</b>         | Run the wizard to configure a SCSI routing instance.                                          |
| <b>show scsirouter</b>    | Display configuration and operational information for the named SCSI routing instance.        |

# scsirouter target accesslist

To associate the named access list with the specified target, use the **scsirouter target accesslist** command.

```
scsirouter name target {name | all} accesslist {name | all | none}
```

| Syntax Description            |  |                                                                                                             |
|-------------------------------|--|-------------------------------------------------------------------------------------------------------------|
| <i>name</i>                   |  | The name of the SCSI routing instance to which this target belongs.                                         |
| <b>target</b> <i>name</i>     |  | The name of the storage target to associate with this access list. The target must already exist.           |
| <b>target</b> all             |  | Associate all targets with the named access list.                                                           |
| <b>accesslist</b> <i>name</i> |  | The name of the access list to associate with this storage target.                                          |
| <b>accesslist</b> none        |  | Prevent any new connections or logins to this target from any IP hosts. This is effectively “no access.”    |
| <b>accesslist</b> all         |  | Allow connections and logins for the specified target from all IP hosts. This is effectively “open access.” |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** An access list identifies the IP hosts allowed to access the associated storage target through the SN 5428. IP hosts can be identified by IP address, CHAP user name, or iSCSI Name. Access lists are associated with specific storage targets.

- Use the **target all** form of this command to create an association between the specified access list and all targets.
- Use the reserved access list name **none** to remove any access list associations for the specified target. This effectively prevents access to this storage target from any IP host.
- Use the reserved access list name **all** to allow access to this storage target from any IP host. This is effectively “open access.”
- Existing connections and logins are not affected by an access list change. However, if there are existing connections, the SN 5428 issues a warning message with that information in response to this command.



**Note**

When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional

details. You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.

### Examples

The following example creates an association between the storage target *webserver4* (accessed via SCSI routing instance *foo*) and the access list *webserver2*.

```
[SN5428A]# scsirouter foo target webserver4 accesslist webserver2
```

The following example provides all IP hosts open access to all targets accessed via SCSI routing instance *LabA*:

```
[SN5428A]# scsirouter LabA target all accesslist all
```

### Related Commands

| Command                         | Description                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>accesslist</b>               | Create an access list entity.                                                                              |
| <b>accesslist A.B.C.D/bits</b>  | Add IP addresses to an access list.                                                                        |
| <b>accesslist chap-username</b> | Add CHAP user name entries to an access list.                                                              |
| <b>accesslist iscsi-name</b>    | Add iSCSI Name entries to an access list.                                                                  |
| <b>delete accesslist</b>        | Delete a specific access list entry or an entire access list.                                              |
| <b>delete scsirouter</b>        | Delete the named SCSI routing instance or the specified element of the SCSI routing instance.              |
| <b>restore accesslist</b>       | Restore the named access list or all access lists from the named configuration file.                       |
| <b>restore scsirouter</b>       | Restore the named SCSI routing instance from the named configuration file.                                 |
| <b>save accesslist</b>          | Save configuration data for the named access list or all access lists.                                     |
| <b>save scsirouter</b>          | Save configuration information for the named SCSI routing instance.                                        |
| <b>scsirouter</b>               | Create a SCSI routing instance.                                                                            |
| <b>scsirouter enable</b>        | Stop or start the named SCSI routing instance.                                                             |
| <b>scsirouter primary</b>       | Identify the SN 5428 as the preferred SN 5428 to run the named SCSI routing instance.                      |
| <b>scsirouter serverif</b>      | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
| <b>setup scsi</b>               | Run the wizard to configure a SCSI routing instance.                                                       |
| <b>show accesslist</b>          | Display the contents of the named access list or all access lists.                                         |
| <b>show scsirouter</b>          | Display configuration and operational information for the named SCSI routing instance.                     |

# scsirouter target description

To add a description to the named target, use the **scsirouter target description** command.

```
scsirouter name target name description "user text"
```

| Syntax Description             |                                                                                                                                                                                  |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>                    | The name of the SCSI routing instance to which this target belongs.                                                                                                              |
| <b>target name</b>             | The name of the storage target.                                                                                                                                                  |
| <b>description "user text"</b> | User-defined identification information associated with this storage target. If the description contains spaces, enclose the string in quotes. Enter a maximum of 64 characters. |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Target description information is an optional attribute of a SCSI routing instance. Use the **show scsirouter** command to display target description information.

**Examples** The following example adds a description to the storage target *webserver4*, accessed through the SCSI routing instance *foo*:

```
[SN5428A] # scsirouter foo target webserver4 description "Web databases"
```

| Related Commands | Command                         | Description                                                                                   |
|------------------|---------------------------------|-----------------------------------------------------------------------------------------------|
|                  | <b>accesslist</b>               | Create an access list entity.                                                                 |
|                  | <b>accesslist A.B.C.D/bits</b>  | Add IP addresses to an access list.                                                           |
|                  | <b>accesslist chap-username</b> | Add CHAP user name entries to an access list.                                                 |
|                  | <b>accesslist iscsi-name</b>    | Add iSCSI Name entries to an access list.                                                     |
|                  | <b>delete accesslist</b>        | Delete a specific access list entry or an entire access list.                                 |
|                  | <b>delete scsirouter</b>        | Delete the named SCSI routing instance or the specified element of the SCSI routing instance. |
|                  | <b>restore accesslist</b>       | Restore the named access list or all access lists from the named configuration file.          |
|                  | <b>restore scsirouter</b>       | Restore the named SCSI routing instance from the named configuration file.                    |

| Command                             | Description                                                                                                |
|-------------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>save accesslist</b>              | Save configuration data for the named access list or all access lists.                                     |
| <b>save scsirouter</b>              | Save configuration information for the named SCSI routing instance.                                        |
| <b>scsirouter</b>                   | Create a SCSI routing instance.                                                                            |
| <b>scsirouter enable</b>            | Stop or start the named SCSI routing instance.                                                             |
| <b>scsirouter primary</b>           | Identify the SN 5428 as the preferred SN 5428 to run the named SCSI routing instance.                      |
| <b>scsirouter serverif</b>          | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
| <b>scsirouter target accesslist</b> | Associate an access list with a specific SCSI routing instance target or all targets.                      |
| <b>setup scsi</b>                   | Run the wizard to configure a SCSI routing instance.                                                       |
| <b>show accesslist</b>              | Display the contents of the named access list or all access lists.                                         |
| <b>show scsirouter</b>              | Display configuration and operational information for the named SCSI routing instance.                     |

## scsirouter target {enabled | disabled}

To allow or disallow connections and logins for the named target, use the **scsirouter target** command.

```
scsirouter name target {name | all} {enabled | disabled}
```

| Syntax Description        |  |                                                                                                                    |
|---------------------------|--|--------------------------------------------------------------------------------------------------------------------|
| <i>name</i>               |  | The name of the SCSI routing instance to which this target belongs.                                                |
| <b>target</b> <i>name</i> |  | The name of the storage target.                                                                                    |
| <b>target all</b>         |  | Allow connections for all targets of this SCSI routing instance to be enabled or disabled.                         |
| <b>enabled</b>            |  | Allow connections and logins for the named target or for all targets of the specified SCSI routing instance.       |
| <b>disabled</b>           |  | Prevent new connections and logins for the named target or for all targets of the specified SCSI routing instance. |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** When you add a target to a SCSI routing instance, it is by default enabled. However, no access list is associated with the target, thus effectively preventing any access to the storage target from any IP hosts. When you associate an access list with a target, the specified connections and logins are allowed. Use the **scsirouter target** command's **enabled** and **disabled** keywords to control access without changing the target access list association.

Existing connections and logins are not affected by the **disabled** keyword, but future connections and logins are not allowed. If existing IP hosts are connected, the SN 5428 issues a warning message with that information in response to this command.

Use the reserved target name **all** to enable or disable connections for all targets of this SCSI routing instance.



**Note**

When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.

**Examples**

The following example enables connections for all targets of the SCSI routing instance *foo*.

```
[SN5428A]# scsirouter foo target all enabled
```

**Related Commands**

| Command                             | Description                                                                                                |
|-------------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>accesslist</b>                   | Create an access list entity.                                                                              |
| <b>accesslist A.B.C.D/bits</b>      | Add IP addresses to an access list.                                                                        |
| <b>accesslist chap-username</b>     | Add CHAP user name entries to an access list.                                                              |
| <b>accesslist iscsi-name</b>        | Add iSCSI Name entries to an access list.                                                                  |
| <b>delete accesslist</b>            | Delete a specific access list entry or an entire access list.                                              |
| <b>delete scsirouter</b>            | Delete the named SCSI routing instance or the specified element of the SCSI routing instance.              |
| <b>restore accesslist</b>           | Restore the named access list or all access lists from the named configuration file.                       |
| <b>restore scsirouter</b>           | Restore the named SCSI routing instance from the named configuration file.                                 |
| <b>save accesslist</b>              | Save configuration data for the named access list or all access lists.                                     |
| <b>save scsirouter</b>              | Save configuration information for the named SCSI routing instance.                                        |
| <b>scsirouter</b>                   | Create a SCSI routing instance.                                                                            |
| <b>scsirouter enable</b>            | Stop or start the named SCSI routing instance.                                                             |
| <b>scsirouter primary</b>           | Identify the SN 5428 as the preferred SN 5428 to run the named SCSI routing instance.                      |
| <b>scsirouter serverif</b>          | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
| <b>scsirouter target accesslist</b> | Associate an access list with a specific SCSI routing instance target or all targets.                      |
| <b>setup scsi</b>                   | Run the wizard to configure a SCSI routing instance.                                                       |
| <b>show accesslist</b>              | Display the contents of the named access list or all access lists.                                         |
| <b>show scsirouter</b>              | Display configuration and operational information for the named SCSI routing instance.                     |

## scsirouter target {serial | lunwwn | wwpn} #?

To use an index method of mapping a logical target or a logical target and LUN combination to storage, use the **scsirouter target {serial | lunwwn | wwpn} #?** command. This command creates an indexed list of storage resources, assigning a unique index number to each LUN available. Specify the storage resources to map by using the appropriate index numbers.

```
scsirouter name target name [lun nn] wwpn #?
```

```
scsirouter name target name lun nn {serial | lunwwn} #?
```

```
scsirouter name target name [lun nn] wwpn #nn [wwpn #nn]
```

```
scsirouter name target name lun nn {serial | lunwwn} #nn
```

| Syntax                    | Description                                                                                                                                                                                                                                      |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>               | Name of the SCSI routing instance to which you are adding the storage target.                                                                                                                                                                    |
| <b>target</b> <i>name</i> | A user-specified name of the logical target. Enter a maximum of 31 characters or a valid iSCSI Name. There is a maximum of 100 targets per SN 5428 or per high availability cluster.                                                             |
| <b>lun</b> <i>nn</i>      | The LUN number associated with the logical target. The LUN number is optional if mapping to a world-wide port number (WWPN) address type. The LUN number is required if mapping to a serial number or LUN world-wide name (LUNWWN) address type. |
| <b>#?</b>                 | Request an indexed list of storage resources available on the Fibre Channel network.                                                                                                                                                             |
| <b>serial</b>             | Use the serial number for the named storage resource.                                                                                                                                                                                            |
| <b>wwpn</b>               | Use the world-wide port number (WWPN) address type for the named storage resource. You can specify a primary and optional secondary WWPN.                                                                                                        |
| <b>lunwwn</b>             | Use the LUN world-wide name (LUNWWN) address type for the named storage resource.                                                                                                                                                                |
| <i>#nn</i>                | The index number from the displayed list. The storage resource listed after the number specified is the physical storage address to which the logical target or logical target and LUN combination is to be mapped.                              |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines**

The `scsirouter target {serial | lunwwn | wwpn} #?` command can be used for target-only or target-and-LUN mapping.

Part of the information included in the indexed list is the address type of each storage resource. The address type indicates what type of physical addressing can be used to access the storage resource: LUN serial number, world-wide port number, or LUN world-wide name. If the list shows more than one address type for a storage resource, specify the address type you prefer for mapping to that storage resource.

**Note**

When you map a target using WWPN and the target needs to be accessed in a high availability cluster, you must specify both the primary WWPN (the WWPN of the storage resource as known to the first SN 5428 in the cluster) and the secondary WWPN (the WWPN of the storage resource as known to the second SN 5428 in the cluster).

To display the indexed list of storage resources, use the number sign (#) character followed by a question mark (?). That action will cause a list of devices discovered on the Fibre Channel network to display as a numbered (indexed) set of lines. The command is displayed at the prompt below the list to the point of the # keyword. Complete the command by entering the appropriate index number.

When a target is added, it is by default enabled. However, it is not associated with any access list (“accesslist none”), effectively disabling access to the target from any IP hosts. Use the `scsirouter target {enabled | disabled}` command to enable access to this storage target for selected IP hosts. See Chapter 6, “Configuring SCSI Routing,” for details on configuring SCSI routing on the SN 5428 Storage Router.

To restore a previously configured target, use the complete iSCSI Name (shown as the *Name* in the `show scsirouter` display) as the target name. The iSCSI Name is a UTF-8 character string based on iSCSI functional requirements. It is a location-independent permanent identifier for an iSCSI node, and is generated when a target is initially created.

**Note**

When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from [Cisco.com](http://Cisco.com).

**Examples**

The following example displays an indexed list of storage resources available to SCSI routing instance *lab2* and maps the logical target *webserver8* to the WWPN storage address represented by index number 3.

```
[SN5428A]# scsirouter lab2 target webserver8 wwpn #?

id interface lunwwn wwpn tgtid lun vendor product
 serial number
1 fc4 20000005ae432e16 21000005ae432e16 n/a 0 SEAGATE ST319451FC
 3EV06X09000081116U2Q
2 fc4 20000005ae431079 21000005ae431079 n/a 0 SEAGATE ST319452FC
 3EV04AFS00008116W8FM
3 fc4 20000005ae036d6e 21000005ae036d6e n/a 0 SEAGATE ST319453FC
 3EV00KD10000820412W7
4 fc4 20000005ae34f99d 21000005ae34f99d n/a 0 SEAGATE ST319452FC
 3EV067QE00007216HAPE
```

```
* [SN5428A] # scsirouter lab2 target webserver8 wwpn #3
```

| Related Commands | Command                             | Description                                                                                                |
|------------------|-------------------------------------|------------------------------------------------------------------------------------------------------------|
|                  | <b>accesslist</b>                   | Create an access list entity.                                                                              |
|                  | <b>accesslist A.B.C.D/bits</b>      | Add IP addresses to an access list.                                                                        |
|                  | <b>accesslist chap-username</b>     | Add CHAP user name entries to an access list.                                                              |
|                  | <b>accesslist iscsi-name</b>        | Add iSCSI Name entries to an access list.                                                                  |
|                  | <b>delete accesslist</b>            | Delete a specific access list entry or an entire access list.                                              |
|                  | <b>delete scsirouter</b>            | Delete the named SCSI routing instance or the specified element of the SCSI routing instance.              |
|                  | <b>restore accesslist</b>           | Restore the named access list or all access lists from the named configuration file.                       |
|                  | <b>restore scsirouter</b>           | Restore the named SCSI routing instance from the named configuration file.                                 |
|                  | <b>save accesslist</b>              | Save configuration data for the named access list or all access lists.                                     |
|                  | <b>save scsirouter</b>              | Save configuration information for the named SCSI routing instance.                                        |
|                  | <b>scsirouter</b>                   | Create a SCSI routing instance.                                                                            |
|                  | <b>scsirouter enable</b>            | Stop or start the named SCSI routing instance.                                                             |
|                  | <b>scsirouter primary</b>           | Identify the SN 5428 as the preferred SN 5428 to run the named SCSI routing instance.                      |
|                  | <b>scsirouter serverif</b>          | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
|                  | <b>scsirouter target accesslist</b> | Associate an access list with a specific SCSI routing instance target or all targets.                      |
|                  | <b>setup scsi</b>                   | Run the wizard to configure a SCSI routing instance.                                                       |
|                  | <b>show accesslist</b>              | Display the contents of the named access list or all access lists.                                         |
|                  | <b>show scsirouter</b>              | Display configuration and operational information for the named SCSI routing instance.                     |

## scsirouter target lun lunwwn

To map a logical target and LUN combination to a LUN world-wide name (LUNWWN) storage address, use the **scsirouter target lun lunwwn** command. The **scsirouter target lun lunwwn** command is a target-and-LUN mapping method of mapping a logical target to storage.

```
scsirouter name target name lun nn lunwwn xx:xx:xx:xx:xx:xx:xx:xx
```

| Syntax Description                              |                                                                                                                                                                        |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>                                     | Name of the SCSI routing instance to which you are adding the storage target.                                                                                          |
| <b>target name</b>                              | A user-specified name of the logical target. Enter a maximum of 31 characters or a valid iSCSI Name. There is a maximum of 100 targets per SN 5428 or SN 5428 cluster. |
| <b>lun nn</b>                                   | The LUN number associated with the logical target. LUNs are integers between 0 and 255.                                                                                |
| <b>lunwwn</b><br><i>xx:xx:xx:xx:xx:xx:xx:xx</i> | The physical LUN world-wide name address.                                                                                                                              |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** The **scsirouter target lun lunwwn** command specifies a logical target name and LUN number combination to be mapped to a physical LUN world-wide name in storage.



### Tips

LUNWWN address notation is represented by 16 hex digits, usually formatted as eight pairs with each pair separated by a colon, *xx:xx:xx:xx:xx:xx:xx:xx*. When entering LUNWWN addresses, colons may be placed anywhere in the address notation, as long as they do not leave one character without a partner character. The entry should be zero-filled from the most significant (the left-most) character position.

The following examples are *correct*:

- 0000:0000:1234:5678
- 0A0F2860:02111750

The following examples are *incorrect*:

- 1:234:567:8:91:23:FF:6
- 12:34:56

When a target is added, it is by default enabled. However, it is not associated with any access list (“accesslist none”), effectively disabling access to the target from any IP hosts. Use the **scsirouter target {enabled | disabled}** command to enable access to this storage target for selected IP hosts.

See Chapter 6, “Configuring SCSI Routing,” for details on configuring SCSI routing instances on the SN 5428 Storage Router.

To restore a previously configured target, use the complete iSCSI Name (shown as the *Name* in the **show scsirouter** display) as the target name. The iSCSI Name is a UTF-8 character string based on iSCSI functional requirements. It is a location-independent permanent identifier for an iSCSI node, and is generated when a target is initially created.



#### Note

When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.

#### Examples

The following example maps a logical target and LUN combination for SCSI router instance *foo*. The logical target and LUN combination, *webserver5* LUN *5*, is mapped to the physical LUNWWN *22:00:00:20:37:19:12:9d*.

```
[SN5428A] # scsirouter foo target webserver5 lun 5 lunwwn 22:00:00:20:37:19:12:9d
```

#### Related Commands

| Command                         | Description                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------|
| <b>accesslist</b>               | Create an access list entity.                                                                 |
| <b>accesslist A.B.C.D/bits</b>  | Add IP addresses to an access list.                                                           |
| <b>accesslist chap-username</b> | Add CHAP user name entries to an access list.                                                 |
| <b>accesslist iscsi-name</b>    | Add iSCSI Name entries to an access list.                                                     |
| <b>delete accesslist</b>        | Delete a specific access list entry or an entire access list.                                 |
| <b>delete scsirouter</b>        | Delete the named SCSI routing instance or the specified element of the SCSI routing instance. |
| <b>restore accesslist</b>       | Restore the named access list or all access lists from the named configuration file.          |
| <b>restore scsirouter</b>       | Restore the named SCSI routing instance from the named configuration file.                    |
| <b>save accesslist</b>          | Save configuration data for the named access list or all access lists.                        |
| <b>save scsirouter</b>          | Save configuration information for the named SCSI routing instance.                           |
| <b>scsirouter</b>               | Create a SCSI routing instance.                                                               |
| <b>scsirouter enable</b>        | Stop or start the named SCSI routing instance.                                                |

| <b>Command</b>                      | <b>Description</b>                                                                                         |
|-------------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>scsirouter primary</b>           | Identify the SN 5428 as the preferred SN 5428 to run the named SCSI routing instance.                      |
| <b>scsirouter serverif</b>          | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
| <b>scsirouter target accesslist</b> | Associate an access list with a specific SCSI routing instance target or all targets.                      |
| <b>setup scsi</b>                   | Run the wizard to configure a SCSI routing instance.                                                       |
| <b>show accesslist</b>              | Display the contents of the named access list or all access lists.                                         |
| <b>show scsirouter</b>              | Display configuration and operational information for the named SCSI routing instance.                     |

# scsirouter target lun serial

To map a logical target and LUN combination to the serial number of the physical LUN, use the **scsirouter target lun serial** command. The **scsirouter target lun serial** command is a target-and-LUN mapping method of mapping a logical target and LUN combination to a physical storage resource by the LUN serial number.

```
scsirouter name target name lun nn serial serialnumber
```

| Syntax Description |                                   |                                                                                                                                                                                      |
|--------------------|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | <i>name</i>                       | Name of the SCSI routing instance to which you are adding the storage target.                                                                                                        |
|                    | <b>target</b> <i>name</i>         | A user-specified name of the logical target. Enter a maximum of 31 characters or a valid iSCSI Name. There is a maximum of 100 targets per SN 5428 or per high availability cluster. |
|                    | <b>lun</b> <i>nn</i>              | The LUN number associated with the <b>target</b> (the iSCSI LUN). iSCSI LUNs are integers between 0 and 255.                                                                         |
|                    | <b>serial</b> <i>serialnumber</i> | The serial number of the physical LUN.                                                                                                                                               |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** The **scsirouter target lun serial** command requires both a logical target and LUN combination and the serial number of the physical LUN.

When a target is added, it is by default enabled. However, it is not associated with any access list (“accesslist none”), effectively disabling access to the target from any IP hosts. Use the **scsirouter target {enabled | disabled}** command to enable access to this storage target for selected IP hosts.

See Chapter 6, “Configuring SCSI Routing,” for details on configuring SCSI routing instances on the SN 5428 Storage Router.

To restore a previously configured target, use the complete iSCSI Name (shown as the *Name* in the **show scsirouter** display) as the target name. The iSCSI Name is a UTF-8 character string based on iSCSI functional requirements. It is a location-independent permanent identifier for an iSCSI node, and is generated when a target is initially created.

**Note**

When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.

**Examples**

The following example maps the logical target and LUN combination for SCSI routing instance *lab2*. The logical target and LUN combination, *webserver9* LUN *1*, is mapped to the physical LUN with a serial number of *ST318451FC3CC05T3N00007116DLWQ*.

```
[SN5428A]# scsirouter lab2 target webserver9 lun 1 serial ST318451FC3CC05T3N00007116DLWQ
```

**Related Commands**

| Command                             | Description                                                                                                |
|-------------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>accesslist</b>                   | Create an access list entity.                                                                              |
| <b>accesslist A.B.C.D/bits</b>      | Add IP addresses to an access list.                                                                        |
| <b>accesslist chap-username</b>     | Add CHAP user name entries to an access list.                                                              |
| <b>accesslist iscsi-name</b>        | Add iSCSI Name entries to an access list.                                                                  |
| <b>delete accesslist</b>            | Delete a specific access list entry or an entire access list.                                              |
| <b>delete scsirouter</b>            | Delete the named SCSI routing instance or the specified element of the SCSI routing instance.              |
| <b>restore accesslist</b>           | Restore the named access list or all access lists from the named configuration file.                       |
| <b>restore scsirouter</b>           | Restore the named SCSI routing instance from the named configuration file.                                 |
| <b>save accesslist</b>              | Save configuration data for the named access list or all access lists.                                     |
| <b>save scsirouter</b>              | Save configuration information for the named SCSI routing instance.                                        |
| <b>scsirouter</b>                   | Create a SCSI routing instance.                                                                            |
| <b>scsirouter enable</b>            | Stop or start the named SCSI routing instance.                                                             |
| <b>scsirouter primary</b>           | Identify the SN 5428 as the preferred SN 5428 to run the named SCSI routing instance.                      |
| <b>scsirouter serverif</b>          | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
| <b>scsirouter target accesslist</b> | Associate an access list with a specific SCSI routing instance target or all targets.                      |
| <b>setup scsi</b>                   | Run the wizard to configure a SCSI routing instance.                                                       |
| <b>show accesslist</b>              | Display the contents of the named access list or all access lists.                                         |
| <b>show scsirouter</b>              | Display configuration and operational information for the named SCSI routing instance.                     |

## scsirouter target lun wwpn lun

To map a logical target and LUN combination to a primary (and optional secondary) storage address where each storage address is specified by world-wide port name (WWPN) and LUN, use the **scsirouter target lun wwpn lun** command. The **scsirouter target lun wwpn lun** command is a target-and-LUN mapping method of mapping a logical target to storage.

```
scsirouter name target name lun nn wwpn xx:xx:xx:xx:xx:xx:xx:xx lun nn
[wwpn xx:xx:xx:xx:xx:xx:xx:xx lun nn]
```

| Syntax Description                     |                                                                                                                                                                                                                                                                                                              |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>                            | Name of the SCSI routing instance to which you are adding the storage target.                                                                                                                                                                                                                                |
| <b>target name</b>                     | A user-specified name of the logical target. Enter a maximum of 31 characters or a valid iSCSI Name. There is a maximum of 100 targets per SN 5428 or per high-availability cluster.                                                                                                                         |
| <b>lun nn</b>                          | The first instance is the LUN number associated with the <b>target</b> (the iSCSI LUN). iSCSI LUNs are integers between 0 and 255. The second instance is the LUN number associated with the primary WWPN (physical device LUN). Physical LUNs may be any physical device number, for example 0x51d1 or 123. |
| <b>wwpn</b><br>xx:xx:xx:xx:xx:xx:xx:xx | Specifies a WWPN for the primary storage address. In a high availability cluster, this is the WWPN for the storage resource as known to the first SN 5428 in the cluster.                                                                                                                                    |
| <b>wwpn</b><br>xx:xx:xx:xx:xx:xx:xx:xx | (Optional) Specifies a WWPN for the secondary storage address, used as an alternate for mapping if the primary is not available. In a high availability cluster, this is the WWPN for the storage resource as known to the second SN 5428 in the cluster.                                                    |
| <b>lun nn</b>                          | (Optional) Specifies the LUN associated with the optional secondary WWPN. Physical LUNs may be any physical device number, for example 0x51d1 or 123.                                                                                                                                                        |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** The **scsirouter target lun wwpn lun** command specifies a logical target name and LUN number combination to be mapped to a physical WWPN and LUN combination in storage.

The secondary WWPN and LUN combination is optional. The secondary combination is mapped to the logical target name and LUN combination as an alternate, if the primary WWPN and LUN combination is not available.

**Note**

When you map a target using WWPN and the target needs to be accessed in a high availability cluster, you must specify both the primary WWPN (the WWPN of the storage resource as known to the first SN 5428 in the cluster) and the secondary WWPN (the WWPN of the storage resource as known to the second SN 5428 in the cluster). The secondary WWPN value may need to be retrieved by issuing the appropriate commands (such as the **show devices** command) from the second SN 5428 in the cluster, or by temporarily attaching the secondary port of the storage device to the first SN 5428.

When a target is added, it is by default enabled. However, it is not associated with any access list (“accesslist none”), effectively disabling access to the target from any IP hosts. Use the **scsirouter target {enabled | disabled}** command to enable access to this storage target for selected IP hosts.

See Chapter 6, “Configuring SCSI Routing,” for details on configuring SCSI routing instances on the SN 5428 Storage Router.

To restore a previously configured target, use the complete iSCSI Name (shown as the *Name* in the **show scsirouter** display) as the target name. The iSCSI Name is a UTF-8 character string based on iSCSI functional requirements. It is a location-independent permanent identifier for an iSCSI node, and is generated when a target is initially created.

**Note**

When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.

**Examples**

The following example maps a logical target and LUN combination for SCSI router instance *lab3*. The logical target and LUN combination, *webserver7* LUN 7, is mapped to the primary WWPN and LUN combination, *22:00:00:20:37:19:15:05* LUN 0.

```
[SN5428A]# scsirouter lab3 target webserver7 lun 7 wwpn 22:00:00:20:37:19:15:05 lun 0
```

The following example maps a logical target and LUN combination to a primary and secondary WWPN: You may need to obtain the secondary WWPN from the SN 5428 Storage Router to which the secondary port of the device is attached, or temporarily attach the storage device’s secondary port to the SN 5428 being configured.

```
[SN5428A]# scsirouter lab4 target webserver8 lun 0 wwpn 22:00:00:20:37:c6:75:6d lun 0 wwpn 21:00:00:20:37:c6:74:7f lun 0
```

**Related Commands**

| Command                         | Description                                                   |
|---------------------------------|---------------------------------------------------------------|
| <b>accesslist</b>               | Create an access list entity.                                 |
| <b>accesslist A.B.C.D/bits</b>  | Add IP addresses to an access list.                           |
| <b>accesslist chap-username</b> | Add CHAP user name entries to an access list.                 |
| <b>accesslist iscsi-name</b>    | Add iSCSI Name entries to an access list.                     |
| <b>delete accesslist</b>        | Delete a specific access list entry or an entire access list. |

| Command                             | Description                                                                                                |
|-------------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>delete scsirouter</b>            | Delete the named SCSI routing instance or the specified element of the SCSI routing instance.              |
| <b>restore accesslist</b>           | Restore the named access list or all access lists from the named configuration file.                       |
| <b>restore scsirouter</b>           | Restore the named SCSI routing instance from the named configuration file.                                 |
| <b>save accesslist</b>              | Save configuration data for the named access list or all access lists.                                     |
| <b>save scsirouter</b>              | Save configuration information for the named SCSI routing instance.                                        |
| <b>scsirouter</b>                   | Create a SCSI routing instance.                                                                            |
| <b>scsirouter enable</b>            | Stop or start the named SCSI routing instance.                                                             |
| <b>scsirouter primary</b>           | Identify the SN 5428 as the preferred SN 5428 to run the named SCSI routing instance.                      |
| <b>scsirouter serverif</b>          | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
| <b>scsirouter target accesslist</b> | Associate an access list with a specific SCSI routing instance target or all targets.                      |
| <b>setup scsi</b>                   | Run the wizard to configure a SCSI routing instance.                                                       |
| <b>show accesslist</b>              | Display the contents of the named access list or all access lists.                                         |
| <b>show scsirouter</b>              | Display configuration and operational information for the named SCSI routing instance.                     |

## scsirouter target wwpn

To map a logical target to a primary (and, optionally, a secondary) storage address specified by world-wide port names (WWPNs), use the **scsirouter target wwpn** command. The **scsirouter target wwpn** command is a target-only method of mapping a logical target specified by WWPNs.

```
scsirouter name target name wwpn xx:xx:xx:xx:xx:xx:xx:xx [wwpn xx:xx:xx:xx:xx:xx:xx:xx]
```

| Syntax Description                     |                                                                                                                                                                                                                                                           |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>                            | Name of the SCSI routing instance to which you are adding the storage target.                                                                                                                                                                             |
| <b>target name</b>                     | A user-specified name of the logical target. Enter a maximum of 31 characters or a valid iSCSI Name. There is a maximum of 100 targets per SN 5428 or per high availability cluster.                                                                      |
| <b>wwpn</b><br>xx:xx:xx:xx:xx:xx:xx:xx | Specifies a WWPN for the primary storage address. In a high availability cluster, this is the WWPN for the storage resource as known to the first SN 5428 in the cluster.                                                                                 |
| <b>wwpn</b><br>xx:xx:xx:xx:xx:xx:xx:xx | (Optional) Specifies a WWPN for the secondary storage address, used as an alternate for mapping if the primary is not available. In a high availability cluster, this is the WWPN for the storage resource as known to the second SN 5428 in the cluster. |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** The **scsirouter target wwpn** command requires only a logical target name to be mapped to a physical target address—no LUNs are specified. However, all LUNs that are part of the physical target address are discovered and made apparent as LUNs belonging to the logical target.



### Tips

WWPN address notation is represented by 16 hex digits, usually formatted as eight pairs with each pair separated by a colon, xx:xx:xx:xx:xx:xx:xx:xx. When entering WWPN addresses, colons can be placed anywhere in the address notation as long as they do not leave one character without a partner character. The entry should be zero-filled from the most significant (the left-most) character position.

The following examples are *correct*:

- 0000:0000:1234:5678
- 0A0F2860:02111750

The following examples are *incorrect*:

- 1:234:567:8:91:23:FF:6
- 12:34:56

**Note**

When you map a target using WWPN and the target needs to be accessed in a high availability cluster, you must specify both the primary WWPN (the WWPN of the storage resource as known to the first SN 5428 in the cluster) and the secondary WWPN (the WWPN of the storage resource as known to the second SN 5428 in the cluster). The secondary WWPN value may need to be retrieved by issuing the appropriate commands (such as the **show devices** command) from the second SN 5428 in the cluster, or by temporarily attaching the secondary port of the storage device to the first SN 5428.

When a target is added, it is by default enabled. However, it is not associated with any access list (“accesslist none”), effectively disabling access to the target from any IP hosts. Use the **scsirouter target {enabled | disabled}** command to enable access to this storage target for selected IP hosts.

See Chapter 6, “Configuring SCSI Routing,” for details on configuring SCSI routing instances on the SN 5428 Storage Router.

To restore a previously configured target, use the complete iSCSI Name (shown as the *Name* in the **show scsirouter** display) as the target name. The iSCSI Name is a UTF-8 character string based on iSCSI functional requirements. It is a location-independent permanent identifier for an iSCSI node, and is generated when a target is initially created.

**Note**

When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.

**Examples**

The following example maps a logical target for SCSI router instance *lab4*. The logical target *webserver1* is mapped to the primary WWPN, *22:00:00:20:37:19:15:05*.

```
[SN5428A]# scsirouter lab4 target webserver1 wwpn 22:00:00:20:37:19:15:05
```

The following example maps a logical target to a primary and secondary WWP. You may need to obtain the secondary WWPN from the SN 5428 Storage Router to which the secondary port of the device is attached, or temporarily attach the storage device’s secondary port to the SN 5428 being configured.

```
[SN5428A]# scsirouter lab5 target webserver9 wwpn 22:00:00:20:37:c6:75:6d wwpn
21:00:00:20:37:c6:74:7f
```

**Related Commands**

| Command                         | Description                                   |
|---------------------------------|-----------------------------------------------|
| <b>accesslist</b>               | Create an access list entity.                 |
| <b>accesslist A.B.C.D/bits</b>  | Add IP addresses to an access list.           |
| <b>accesslist chap-username</b> | Add CHAP user name entries to an access list. |

| Command                             | Description                                                                                                |
|-------------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>accesslist iscsi-name</b>        | Add iSCSI Name entries to an access list.                                                                  |
| <b>delete accesslist</b>            | Delete a specific access list entry or an entire access list.                                              |
| <b>delete scsirouter</b>            | Delete the named SCSI routing instance or the specified element of the SCSI routing instance.              |
| <b>restore accesslist</b>           | Restore the named access list or all access lists from the named configuration file.                       |
| <b>restore scsirouter</b>           | Restore the named SCSI routing instance from the named configuration file.                                 |
| <b>save accesslist</b>              | Save configuration data for the named access list or all access lists.                                     |
| <b>save scsirouter</b>              | Save configuration information for the named SCSI routing instance.                                        |
| <b>scsirouter</b>                   | Create a SCSI routing instance.                                                                            |
| <b>scsirouter enable</b>            | Stop or start the named SCSI routing instance.                                                             |
| <b>scsirouter primary</b>           | Identify the SN 5428 as the preferred SN 5428 to run the named SCSI routing instance.                      |
| <b>scsirouter serverif</b>          | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
| <b>scsirouter target accesslist</b> | Associate an access list with a specific SCSI routing instance target or all targets.                      |
| <b>setup scsi</b>                   | Run the wizard to configure a SCSI routing instance.                                                       |
| <b>show accesslist</b>              | Display the contents of the named access list or all access lists.                                         |
| <b>show scsirouter</b>              | Display configuration and operational information for the named SCSI routing instance.                     |

# setup

To configure the SN 5428 using the setup configuration wizard, use the **setup** command. The setup configuration wizard runs the Management Interface, Date and Time, Network Management, Management Access, and SCSI routing (if applicable) individual wizards in sequence.

## setup

### Syntax Description

This command has no arguments or keywords.

### Defaults

For multiple choice questions, the system presents the choices enclosed in brackets, [ ]. Each multiple choice question has a default answer that is selected when you press Enter or Return. The default is shown in parentheses, ( ). For example:

```
Enable High Availability? [yes/no (no)]
```

For configuration variables, the current value saved in the system is presented in brackets. For example:

```
Network mask ? [255.255.255.0]
```

If the configuration variable does not have a value, the system will present a set of “empty” brackets, [(empty)], or a template that provides the required format of the value. For example:

```
SN5428 system name? [(empty)]
```

### Command Modes

Administrator.

### Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

### Usage Guidelines

Initial system configuration and subsequent reconfiguration can be performed via interactive configuration wizards, either through the console interface or via Telnet (once the management interface has been configured). The configuration wizards prompt you for the necessary information to accomplish the specific configuration task and may invoke multiple commands to complete their functions.

The CLI provides the following configuration wizards:

- Setup—runs the Management Interface, Date and Time, Network Management, Management Access, and SCSI routing (if applicable) individual wizards in sequence.
- Management Interface—configures the management interface with a system name, IP address, and optional DNS server information.
- Date and Time—configures the time zone, use (or non-use) of daylight savings time, the current date and time, and the NTP server address (if one is present).
- Network Management—configures the use of Telnet, web-based GUI, and SNMP for managing the SN 5428 over the network.

- Management Access—configures passwords for monitoring and configuring the SN 5428.
- SCSI Routing—configures the use of the SN 5428 SCSI routing capabilities. The wizard is only available when the SN 5428 is deployed for SCSI routing; it is not available if the storage router is deployed for transparent SCSI routing.

For SN 5428s deployed for SCSI routing, the CLI also provides a Cluster wizard, which configures the SN 5428 to participate in a high availability cluster. Because the initial configuration script configures the SN 5428's high availability environment, the setup configuration wizard does not include the Cluster wizard. (See the “Initial System Configuration Script” section on page 2-6 for details.) However, the Cluster wizard, using the **setup cluster** command, can be run after initial system configuration to change the SN 5428's configuration mode from standalone to clustered, to change membership from one cluster to another, or to resign from a cluster and run as a standalone SN 5428.

During configuration with the setup configuration wizard, operational changes take place and are applied to the currently running system. For example, after the Network Management wizard completes, SNMP network management will be configured for the SN 5428. However, these changes are not saved to the system's bootable configuration until the end of the entire setup configuration wizard. To quit the setup configuration wizard without saving changes, press **Ctrl-C** at any time before the end of the wizard, and then reboot the SN 5428 to restore previous values.




---

**Note**

Some changes may be retained after a reboot. Be sure to review the values provided in the prompts that display if you rerun the setup configuration wizard or run each individual wizard.

---

After entering the setup configuration wizard, several informational messages display, including the following prompt:

```
User level for setup? [novice/expert (expert)]
```

- Enter **novice** to continue with the configuration process. Explanatory text displays before each prompt in the wizard.
- Enter **expert** to continue with the configuration process, suppressing all explanatory text. If you are an experienced user familiar with the setup configuration wizard, you may prefer this option.

At the end of the setup configuration wizard, the following prompt displays:

```
Done with setup.
```

---

**Examples**

The following shows the initial explanatory text for the **setup** command:

```
[SN5428_A]# setup
```

```
You are about to set up the SN5428. Running this wizard will modify
the configuration of this system.
```

```
During setup, operational changes will take place. However, these changes
are not saved until the end of the script. To quit the setup wizard without
saving changes, ** hit CTRL-C at any time **. Reboot to restore previous values.
```

```
For multiple choice questions, the system will present the choices enclosed
in brackets []. Each multiple choice question has a default answer that is
selected when you press return.
```

```
Example: [yes/no (no)].
```

```
Choices are yes and no. No is the default answer.
```

For configuration variables, the current value saved in the system is presented in brackets [varname]. If the configuration variable does not have a value, the system will present a set of brackets [(empty)] or a template that provides the expected format of the value.

Example: [mySN5428] configuration variable has a value

Example: [(empty)] configuration variable does not have a value, no template

Example: [A.B.C.D] template for an IP address.

User level for setup? [novice/expert (expert)]

### Related Commands

| Command                 | Description                                                                |
|-------------------------|----------------------------------------------------------------------------|
| <b>clear conf</b>       | Return most configuration settings to factory defaults.                    |
| <b>setup access</b>     | Run the wizard to configure Monitor mode and Administrator mode passwords. |
| <b>setup cluster</b>    | Change the configuration of the SN 5428's high availability environment.   |
| <b>setup iscsi-port</b> | Run the wizard to manually configure the port used for iSCSI traffic.      |
| <b>setup mgmt</b>       | Run the wizard to configure the management interface.                      |
| <b>setup netmgmt</b>    | Run the wizard to configure network management.                            |
| <b>setup scsi</b>       | Run the wizard to configure a SCSI routing instance.                       |
| <b>setup time</b>       | Run the wizard to configure the system date and time.                      |

## setup access

To configure passwords for monitoring and administering the SN 5428, use the **setup access** configuration wizard. The wizard prompts the user to enter and confirm new passwords.

### setup access

**Syntax Description** This command has no arguments or keywords.

**Defaults** The factory default password for both Administrator mode and Monitor mode is *cisco*.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** The wizard prompts the user to enter (and confirm by re-entering) the new Monitor password, which allows view-only SN 5428 access. The user is also prompted to enter (and confirm by re-entering) the new Administrator password, which allows changes to be made to the SN 5428 configuration.

**Examples** The following example sets the Monitor mode and Administrator mode passwords for the SN 5428, but does not apply them to the console interface. Administrator contact information is also configured. Note that passwords display as asterisks when entered.

```
[SN5428_PR]# setup access
```

```
#####
Management Access Setup
#####
```

The SN5428 CLI and GUI are protected by two passwords. The initial password entered when logging in allows the user to monitor the SN5428, but does not allow changes. The "admin" password allows the user to make configuration changes.

```
** Enter 'q' to skip changing monitor password **
```

```
Enter the current "monitor" password:*****
```

```
** Password Rules **
```

A password can contain any combination of numbers and letters, but should not be something familiar to you and easy to guess.

```
Enter the new "monitor" password: *****
```

```
Enter the new "monitor" password again: *****
```

```
Enter the current "admin" password: *****
```

Enter the new "admin" password: \*\*\*\*\*

Enter the new "admin" password again: \*\*\*\*\*

The new passwords will apply to all telnet and web-based GUI sessions. They will also be applied to the console. If the SN5428 console is in a physically secure location, console passwords are not recommended since they can be lost or forgotten. If the SN5428 is deployed in a less secure environment, the passwords should be applied. If passwords are subsequently lost, contact Cisco Technical Support for information on recovery.

Apply passwords to console ? [yes/no (no)] **no**

The administrative contact is the person or group responsible for configuration and management of the SN5428. The system will store a name, e-mail address, phone number, and pager number for the system administrator. Management applications can retrieve this information and provide it to a support person or directly use it to e-mail or page the administrator.

Input Administrator Info? [yes/no (yes)] **yes**  
 Administrator name? [(empty) ] **Pat Hurley**  
 Phone? [(empty) ] **123.456.7890**  
 Pager number? [(empty)] **12.456.3444 pin 2234**  
 Email? [(empty)] **hurley@abc123z.com**

Done with setup.

#### Related Commands

| Command                 | Description                                                              |
|-------------------------|--------------------------------------------------------------------------|
| <b>clear conf</b>       | Return most configuration settings to factory defaults.                  |
| <b>setup</b>            | Run the setup configuration wizard.                                      |
| <b>setup cluster</b>    | Change the configuration of the SN 5428's high availability environment. |
| <b>setup iscsi-port</b> | Run the wizard to manually configure the port used for iSCSI traffic.    |
| <b>setup mgmt</b>       | Run the wizard to configure the management interface.                    |
| <b>setup netmgmt</b>    | Run the wizard to configure network management.                          |
| <b>setup scsi</b>       | Run the wizard to configure a SCSI routing instance.                     |
| <b>setup time</b>       | Run the wizard to configure the system date and time.                    |

# setup cluster

To configure the high availability (HA) environment for the SN 5428, to add the SN 5428 to a cluster, or to remove it from an existing cluster, use the **setup cluster** configuration wizard. The wizard prompts the user to select the appropriate HA configuration mode, enter a cluster name and (if necessary) an HA interface IP address and subnet mask.

## setup cluster

**Syntax Description** This command has no arguments or keywords.

**Defaults** Defaults or current values are shown in parentheses within the allowable response brackets. In the following example, the allowable responses are *retain* and *delete*, and the default is *delete*.

```
Retain or delete applications ? [retain/delete (delete)]
```

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** The HA features of the SN 5428 Storage Router are designed around a cluster of systems that back each other up in case of failure. A cluster consists of up to four identically configured SN 5428s that continually exchange HA information over their HA and management interfaces.

Clusters are defined by name. The **setup cluster** command prompts the user for the appropriate HA configuration mode and the cluster name.

- Use the **standalone** keyword to identify the SN 5428 as not participating in a high availability cluster. A standalone SN 5428 does not require the management or HA interfaces to be available in order to complete the system configuration. The MGMT and HA ports do not need to be cabled.
- Use the **clustered** keyword to identify the SN 5428 as participating in a high availability cluster. A clustered SN 5428 requires the management and HA interfaces to be available in order to complete the system configuration. The MGMT and HA ports must be correctly cabled.

The command also prompts the user to either retain this SN 5428's configuration, merging it with others in the cluster, or to delete this SN 5428's application configuration data (SCSI routing instances and cluster configuration information) and replace it with cluster data. Retained data is replicated to other SN 5428s in the cluster. When joining an existing cluster, access list information is always deleted and replaced by the cluster's access list information.



### Caution

Retaining configuration data could provide unexpected results.

Changing the SN 5428's cluster name, thereby joining another cluster, has the following effects on its existing configurations and operations:

- All SCSI routing instances are failed-over to another member in the original cluster.
- All applications are stopped.
- The cluster name is changed.
- If the user has chosen to retain data, any unsaved cluster configuration information is saved.
- The system reboots. Configuration information is exchanged. All of the original SCSI routing instances appears in the new cluster, unless the user has chosen to delete rather than retain data.
- Access lists are always deleted. To preserve an existing access list and make it available to the new cluster, the user must save the access list to a configuration file before issuing the **setup cluster** command. Make the saved configuration file available to the SN 5428 currently performing access list maintenance functions for the cluster (via the **copy** command), and then restore the saved access list to the new cluster from that configuration file. See Chapter 9, "Configuring a High Availability Cluster," for details.
- For cases where the names of SCSI routing instances are duplicated within the new cluster (meaning instances of the same name are already running in the new cluster), configuration data from the old cluster is deleted in favor of what is currently running in the new cluster.

## Examples

The following shows example output and input for the **setup cluster** command:

```
[SN5428_PR]# setup cluster
```

```
The system has the ability to run in a standalone or clustered state.
By default, the system will run in a clustered state and communicate
with other SN5428s in the same cluster. If a single SN5428 is deployed
and you don't intend to add a second SN5428 to provide high availability
features in a clustered configuration, you should configure the SN5428 in
standalone mode. Enter CTRL-C at any prompt to cancel changes and return
to the command prompt.
```

```
HA configuration? [standalone/clustered (standalone)] clustered
```

If you select HA configuration mode *clustered*, the wizard prompts you to enter an HA IP address:

```
To determine the health of other SN5428s in a cluster, the SN5428 must send
occasional heartbeat packets on at least two interfaces (in case one interface
has problems). By default, the interfaces used are the 10/100 management
interface (already set up) and the 10/100 HA interface. Please select an IP
address and network mask for the HA interface.
```

```
HA Interface IP address? [10.1.40.230/24]
```

After selecting the HA configuration mode, and optionally setting the HA IP address, the wizard prompts you to enter a cluster name:

```
When you change the cluster that the SN5428 belongs to, you need to
decide if you want the scsirouter instances running on the SN5428 to be
deleted or if you want them to be retained and merged with the new cluster.
```

```
Change cluster to ? [Cluster1]
```

```
For a change from standalone to clustered:
```

```
If you retain the configuration, there may be conflicts when the
scsirouter instances are replicated between this SN5428 and others in the
new cluster.
```

For a change from clustered to standalone:  
 You can retain the configuration without causing any scsirouter instance conflicts for this SN5428 since it will be the only member of the new cluster.  
 Retain or delete scsirouter instances ? [retain/delete (delete)] **retain**

If you choose to retain the SN 5428 configuration, an additional warning displays:

```
#####
Please confirm that you want to retain the configuration.
#####
```

All configuration settings will be saved.  
 The system will REBOOT if you answer "yes"  
 \*\* Enter CTRL-C to cancel. \*\*

Are you sure you want to retain the configuration ? [must type "yes"] **yes**

If you choose to delete your existing configuration, this warning displays:

Retain or delete applications ? [retain/delete (delete)] **delete**

```
#####
Please confirm that you want to delete the configuration.
#####
```

Cluster configuration settings will be saved.  
 The system will REBOOT if you answer "yes"  
 \*\* Enter CTRL-C to cancel and abort the cluster change. \*\*

Are you sure you want to delete the configuration ? [must type "yes"] **yes**

After confirming your selection, the SN 5428 automatically reboots.

## Related Commands

| Command                 | Description                                                                |
|-------------------------|----------------------------------------------------------------------------|
| <b>clear conf</b>       | Return most configuration settings to factory defaults.                    |
| <b>setup</b>            | Run the setup configuration wizard.                                        |
| <b>setup access</b>     | Run the wizard to configure Monitor mode and Administrator mode passwords. |
| <b>setup iscsi-port</b> | Run the wizard to manually configure the port used for iSCSI traffic.      |
| <b>setup mgmt</b>       | Run the wizard to configure the management interface.                      |
| <b>setup netmgmt</b>    | Run the wizard to configure network management.                            |
| <b>setup scsi</b>       | Run the wizard to configure a SCSI routing instance.                       |
| <b>setup time</b>       | Run the wizard to configure the system date and time.                      |

# setup iscsi-port

To change the default listening port used for iSCSI traffic, use the **setup iscsi-port** wizard.

## setup iscsi-port

### Syntax Description

This command has no arguments or keywords.

### Defaults

The default listening port used for iSCSI traffic is 3260. This is the port number assigned by IANA.

### Command Modes

Administrator.

### Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

### Usage Guidelines

If you change the listening port used for iSCSI traffic on the SN 5428, you must make corresponding changes to the IP hosts sending iSCSI traffic to the SN 5428. For example, on a UNIX system, you must update the `/etc/services` file.

After selecting a new port for iSCSI traffic, the SN 5428 will be rebooted.

### Examples

The following shows example output and input for the **show iscsi-port** command:

```
[SN5428A]# setup iscsi-port

#####
iSCSI port Setup Wizard
#####
If you change the iSCSI port number, the SN5428 will reboot itself
for the change to take effect. This will cause all scsirouters to
be stopped.
** Enter CTRL-C to cancel. **

Do you want to change the iSCSI port number?[yes/no (no)] yes

#####
Changing iSCSI port
#####
Now, you will need to enter a new iSCSI port number. The new port
will be used as the iSCSI server listen port. Make sure the new
port is not used by other applications in your network environment.

New port number ? [nn] 5003

#####
Please confirm that you want to change iSCSI port
#####

iscsi port configuration settings will be saved.
```

■ **setup iscsi-port**

The system will REBOOT if you answer "yes".  
 \*\* Enter CTRL-C to cancel. \*\*

Proceed to change the iSCSI port?[yes/no (no)] **yes**

After confirming your intentions, the SN 5428 automatically reboots.

**Related Commands**

| <b>Command</b>       | <b>Description</b>                                                         |
|----------------------|----------------------------------------------------------------------------|
| <b>clear conf</b>    | Return most configuration settings to factory defaults.                    |
| <b>setup</b>         | Run the setup configuration wizard.                                        |
| <b>setup access</b>  | Run the wizard to configure Monitor mode and Administrator mode passwords. |
| <b>setup cluster</b> | Change the configuration of the SN 5428's high availability environment.   |
| <b>setup mgmt</b>    | Run the wizard to configure the management interface.                      |
| <b>setup netmgmt</b> | Run the wizard to configure network management.                            |
| <b>setup scsi</b>    | Run the wizard to configure a SCSI routing instance.                       |
| <b>setup time</b>    | Run the wizard to configure the system date and time.                      |

# setup mgmt

To configure the SN 5428 management interface, use the **setup mgmt** configuration wizard. The wizard prompts the user to enter the SN 5428 system name, management interface IP address and subnet mask, optional default gateway and DNS information.

## setup mgmt

**Syntax Description** This command has no arguments or keywords.

**Defaults** Defaults or current values are shown in parentheses within the allowable response brackets. In the following example, the current SN 5428 system name is *SN5428\_Lab1*.

```
SN5428 system name? [SN5428_Lab1]
```

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** The management interface must be configured before the Telnet interface or web-based GUI can be used for configuration or monitoring tasks. When the wizard is completed, the system displays notification that the management interface is operational.

**Examples** The following shows example output for the **setup mgmt** command:

```
[SN5428A]# setup mgmt
```

```
#####
Management Interface Setup
#####
```

```
Please choose a name for the SN5428. This name is associated with the
SN5428 Management Interface IP address. If you wish to enable network
management on the SN5428, you should add the system name you provide
at this prompt and its IP address to a domain name server (nis, nis+, WINS).
```

```
SN5428 system name? [SN5428A]
```

```
The SN5428 may be managed using telnet, or a web-based GUI, or SNMP via the
10/100 Ethernet interface labeled "mgmt" on the front panel of the system. This
interface must be assigned an IP address.
```

```
Management Interface IP address? [10.1.12.122/24]
```

```
If the SN5428 is to be managed from a subnet other than the one to which it
```

is physically attached, a static route is required. The static route format is "destination/netmask gateway".

Static route for Management Interface? [0.0.0.0/0 10.1.12.1]

If IP addresses are to be entered as host names via any of the SN5428 management interfaces, a Domain Name Server must be specified. A secondary DNS may be specified for use if the primary DNS is not available.

Primary DNS Server? [A.B.C.D]

Secondary DNS Server? [A.B.C.D]

Setting up the management interface ... Done

The management port is now operational. It may be tested using ping or telnet from a host on the network.

Done with setup.

#### Related Commands

| Command                 | Description                                                                |
|-------------------------|----------------------------------------------------------------------------|
| <b>clear conf</b>       | Return most configuration settings to factory defaults.                    |
| <b>setup</b>            | Run the setup configuration wizard.                                        |
| <b>setup access</b>     | Run the wizard to configure Monitor mode and Administrator mode passwords. |
| <b>setup cluster</b>    | Change the configuration of the SN 5428's high availability environment.   |
| <b>setup iscsi-port</b> | Run the wizard to manually configure the port used for iSCSI traffic.      |
| <b>setup netmgmt</b>    | Run the wizard to configure network management.                            |
| <b>setup scsi</b>       | Run the wizard to configure a SCSI routing instance.                       |
| <b>setup time</b>       | Run the wizard to configure the system date and time.                      |

# setup netmgmt

To enable network management via any or all of the available interfaces (Telnet, web-based GUI, or SNMP), use the **setup netmgmt** configuration wizard. The wizard prompts the user to selectively enable the various interfaces and, if SNMP is enabled, will prompt the user to enter the read and write community information, IP addresses for SNMP traps, and additional SNMP configuration information.

## setup netmgmt

### Syntax Description

This command has no arguments or keywords.

### Defaults

Defaults or current values are shown in parentheses within the allowable response brackets. In the following example, the default name for the read community is *public*:

```
Read Community ? [public]
```

### Command Modes

Administrator.

### Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

### Usage Guidelines

All network management interfaces are enabled by default, with SNMP “gets” via the public read community. Run this wizard to disable any of these interfaces, or to change the SNMP read community, configure the SNMP write community for SNMP “sets,” or add addresses for SNMP traps.

### Examples

The following shows example output and input for the **setup netmgmt** command:

```
[SN5428A]# setup mgmt
#####
Network Management Access Setup
#####
```

This wizard will enable you to configure access to telnet, the web-based GUI, and configure SNMP. By default, telnet and the web-based GUI are enabled. SNMP gets via the "public" community are also enabled via the 10/100 management interface. If you want to change these values or configure other SNMP features, please set up the network management.

```
Set up Network Management ? [yes/no (yes)] yes
```

```
Enable telnet on all interfaces? [yes/no (yes)] yes
```

```
Configure SNMP ? [yes/no (yes)] yes
```

If you select to configure SNMP, the wizard prompts you for the following information:

```

Read Community ? [public]

Write Community ? [private] mynetmanagers

First IP address for SNMP traps ? [A.B.C.D] 10.1.30.17

Trap version for first IP address? [1/2 (1)]

Second IP address for SNMP traps ? [A.B.C.D] 10.1.30.18

Trap version for second IP address? [1/2 (1)]

Send auth trap when requester specifies
incorrect community? [yes/no (no)] yes

Modify link up/down traps for one or more interfaces? [yes/no (yes)] yes

Send link up/down traps for MGMT interface? [yes/no (yes)] yes

Send link up/down traps for HA interface? [yes/no (yes)] yes

Send link up/down traps for GE interface? [yes/no (yes)] no

Send link up/down traps for fibre
channel interface? [yes/no (yes)] yes

```

The wizard ends by displaying the following information:

Network Management setup is complete.

By default, these methods of network management will work from any network which is not separated from the SN5428 by a firewall or other traffic-limiting device. To further specify security requirements, please use the normal configuration functions of the CLI or GUI after completing this wizard.

Done with setup.

#### Related Commands

| Command                 | Description                                                                |
|-------------------------|----------------------------------------------------------------------------|
| <b>clear conf</b>       | Return most configuration settings to factory defaults.                    |
| <b>setup</b>            | Run the setup configuration wizard.                                        |
| <b>setup access</b>     | Run the wizard to configure Monitor mode and Administrator mode passwords. |
| <b>setup cluster</b>    | Change the configuration of the SN 5428's high availability environment.   |
| <b>setup iscsi-port</b> | Run the wizard to manually configure the port used for iSCSI traffic.      |
| <b>setup mgmt</b>       | Run the wizard to configure the management interface.                      |
| <b>setup scsi</b>       | Run the wizard to configure a SCSI routing instance.                       |
| <b>setup time</b>       | Run the wizard to configure the system date and time.                      |

# setup scsi

To configure a SCSI routing instance for the SN 5428, use the **setup scsi** configuration wizard. The wizard prompts the user to enter the name of the SCSI routing instance (maximum 32 characters) and to specify the IP address of the Gigabit Ethernet interface for the SCSI routing instance. Then the wizard discovers all Fibre Channel devices connected to the SN 5428. More extensive configuration of SCSI routing instances can be performed via the CLI or the web-based GUI.

## setup scsi

### Syntax Description

This command has no arguments or keywords.

### Defaults

Defaults or current values are shown in parentheses within the allowable response brackets. In the following example, the current default Gigabit Ethernet interface is *ge1*.

```
Scsirouter instance GE interface ? [ge1|ge2 (ge1)]
```

### Command Modes

Administrator.

### Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

### Usage Guidelines

After the wizard finishes the discovery process, it displays a list of accessible storage resources. Targets can be explicitly added by using the web-based GUI or CLI commands.

The **setup scsi** command can only be run when no SCSI routing instance is currently configured on the SN 5428.

### Examples

The following shows example output and input for the **setup scsi** command:

```
[SN5428A]# setup scsi
#####
scsirouter Setup
#####
This wizard will enable you to set up a scsirouter instance, but will not enable you to
specify a VLAN for the IP interface. If a VLAN is required for the scsirouter instance,
please use CLI commands to configure the scsirouter.
Do you want to configure a scsirouter instance ? [yes/no (no)] yes
```

```
scsirouter instance name ? [(empty)] foo
```

The scsirouter instance communicates with IP hosts via the Gigabit Ethernet interface. To enable communication, you need to assign an IP address and network mask to the scsirouter instance for it to use on the Ethernet interface.

```
IP Address ? [A.B.C.D/nn] 10.1.0.45/24
```

Enter the name of the GE interface that you want the scsirouter instance to use.

```
Scsirouter instance GE interface ? [ge1|ge2 (ge1)] ge2
```

```
Please wait ...
```

A scsirouter has been created. A list of accessible FC devices is shown in the table below. Use the "scsirouter" command or the configuration screen via the GUI to define one or more scsirouter targets.

Access to scsirouter targets will be disabled until access is explicitly configured using the the "scsirouter" command or the configuration via the GUI.

```
Fabric Attached Devices detected
```

| Interface | lunwwn           | wwpn             | portId  | lun | vendor  | product    | serial        |
|-----------|------------------|------------------|---------|-----|---------|------------|---------------|
| fc4       | 20000003de432e16 | 21000003de432e16 | 0x104e2 | 0   | SEAGATE | ST318452FC | 3FZ06X0906U2Q |
| fc4       | 20000003de431079 | 21000003de431079 | 0x104e4 | 0   | SEAGATE | ST318452FC | 3FZ04AFS0W8FM |

```
scsirouter setup is complete.
```

```
Done with setup.
```

## Related Commands

| Command                 | Description                                                                |
|-------------------------|----------------------------------------------------------------------------|
| <b>clear conf</b>       | Return most configuration settings to factory defaults.                    |
| <b>setup</b>            | Run the setup configuration wizard.                                        |
| <b>setup access</b>     | Run the wizard to configure Monitor mode and Administrator mode passwords. |
| <b>setup cluster</b>    | Change the configuration of the SN 5428's high availability environment.   |
| <b>setup iscsi-port</b> | Run the wizard to manually configure the port used for iSCSI traffic.      |
| <b>setup mgmt</b>       | Run the wizard to configure the management interface.                      |
| <b>setup netmgmt</b>    | Run the wizard to configure network management.                            |
| <b>setup time</b>       | Run the wizard to configure the system date and time.                      |

# setup time

To set current date and time information and other time-related configuration settings, use the **setup time** configuration wizard. The SN 5428 uses date and time information for log files and the user interface.

## setup time

### Syntax Description

This command has no arguments or keywords.

### Defaults

Defaults or current values are shown in parentheses within the allowable response brackets. In the following example, the current date is *02/05/2002*.

```
Date (mm/dd/yyyy)? [02/05/2002]
```

### Command Modes

Administrator.

### Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

### Usage Guidelines

The wizard prompts the user to enter the appropriate time zone (as an offset from Universal/GMT). The user may also enter an optional IP address of an NTP server, to be used by the SN 5428 for date and time synchronization. Finally, the wizard prompts the user for the current date and time if no NTP server address is provided.

### Examples

The following shows example output and input for the **setup time** command:

```
[SN5428A]# setup time
```

```
#####
Date and Time Setup
#####
```

To provide correct information in log files and user interfaces, the SN5428 must have a reasonably accurate date and time.

To use Daylight Savings Time or specify time zone by geographic region use the "clock timezone" command.

The time zone must be entered as an offset from GMT.

```
0=[0000 GMT] 1=[-0100 WAT] 2=[-0200 AT]
3=[-0300 Brazil] 4=[-0400 AST] 5=[-0500 EST]
6=[-0600 CST] 7=[-0700 MST] 8=[-0800 PST]
9=[-0900 YST] 10=[-1000 AHST] 11=[-1100 NT]
12=[+1200 IDLW] 13=[+1100 WST] 14=[+1000 GST]
15=[+0900 JST] 16=[+0800 CCT] 17=[+0700 WAST]
18=[+0600 ZP6] 19=[+0500 ZP5] 20=[+0400 ZP4]
21=[+0300 BT] 22=[+0200 EET] 23=[+0100 CET]
```

Time Zone? [0-23] 6

If a Network Time Protocol (NTP) server is in use on a network reachable via the SN5428 management interface, it may be used to keep the SN5428 date and time in sync with the rest of the network.

NTP Server IP Address? [A.B.C.D] 10.1.60.86

If you enter the NTP server IP address, the date and time is synchronized with the network and the wizard completes. If you do not enter an NTP server IP address, the wizard prompts you for the current date and time information.

NTP Server IP Address? [A.B.C.D]

Date (mm/dd/yyyy)? [02/05/2002]

Time (hh:mm:ss)? [16:42:38] 10:42:12

Date and time are now configured.

Done with setup.

#### Related Commands

| Command                 | Description                                                                |
|-------------------------|----------------------------------------------------------------------------|
| <b>clear conf</b>       | Return most configuration settings to factory defaults.                    |
| <b>setup</b>            | Run the setup configuration wizard.                                        |
| <b>setup access</b>     | Run the wizard to configure Monitor mode and Administrator mode passwords. |
| <b>setup cluster</b>    | Change the configuration of the SN 5428's high availability environment.   |
| <b>setup iscsi-port</b> | Run the wizard to manually configure the port used for iSCSI traffic.      |
| <b>setup mgmt</b>       | Run the wizard to configure the management interface.                      |
| <b>setup netmgmt</b>    | Run the wizard to configure network management.                            |
| <b>setup scsi</b>       | Run the wizard to configure a SCSI routing instance.                       |

# show aaa

To display AAA configuration information and operational statistics, use the **show aaa** command.

```
show aaa [stats]
```

| Syntax Description | stats | (Optional) Display the number of authentication requests received and sent since the SN 5428 was last rebooted. |
|--------------------|-------|-----------------------------------------------------------------------------------------------------------------|
|--------------------|-------|-----------------------------------------------------------------------------------------------------------------|

| Defaults | None. |
|----------|-------|
|----------|-------|

| Command Modes | Administrator or Monitor. |
|---------------|---------------------------|
|---------------|---------------------------|

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

| Usage Guidelines | Use this command to determine the current AAA configuration for the SN 5428. Use the <b>stats</b> keyword to display usage statistics. |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------|
|------------------|----------------------------------------------------------------------------------------------------------------------------------------|

| Examples | The following example output displays the current AAA authentication configuration for the SN 5428. The authentication list indicates that authentication first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an error and AAA tries to use the local username database for authentication. If a match is found, the user is allowed access; if no match is found, the user is denied access. If this attempt returns an error, the user is not allowed access. |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
[SN5428A]# show aaa
aaa new-model
aaa authentication iscsi default group tacacs+ local
username "fred" password "9 af4f2428498a41a31e237de1c4a9b9fcef"
username "pat" password "9 7ddbccc3d0daf013f4293c3d3bd94539dd"
username "kris" password "9 0607167520058771e66ab1d379d7e6505f"
username "adrian" password "9 0ad24a3b35dc296d894e512416d572b3ee"
radius-server retransmit 12
radius-server host 10.5.0.53 auth-port 1645
tacacs-server timeout 12
tacacs-server host 10.7.0.22 auth-port 49
```

The following is example output from the **show aaa stats** command:

```
[SN5428A]# show aaa stats
authentication requests received = 134
authentication responses sent = 134
authentication requests canceled = 0
authentication requests passed = 130
authentication requests failed = 4

 RADIUS Server Hosts
 IP Address port timeouts bad resps

 10.5.0.53 1645 0 0

 TACACS+ Server Hosts
 IP Address port timeouts bad resps

 10.7.0.22 49 0 0
```

#### Related Commands

| Command                         | Description                                                                    |
|---------------------------------|--------------------------------------------------------------------------------|
| <b>aaa authentication iscsi</b> | Configure the AAA authentication services to be used for iSCSI authentication. |
| <b>debug aaa</b>                | Enable debugging for the AAA authentication services.                          |
| <b>radius-server host</b>       | Configure remote RADIUS servers for AAA authentication services.               |
| <b>restore aaa</b>              | Restore AAA authentication services from a saved configuration file.           |
| <b>save aaa</b>                 | Save the current AAA configuration information.                                |
| <b>tacacs-server host</b>       | Configure remote TACACS+ servers for AAA authentication services.              |
| <b>username password</b>        | Add a user name and optional password to the local username database.          |

# show accesslist

To display a list of access lists or the contents of the named access list (or all access lists), use the **show accesslist** command.

```
show accesslist [name | all] [from {bootconfig | filename | runningconfig}]
```

| Syntax Description        |                                                                                                                                                        |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>               | (Optional) The name of the access list.                                                                                                                |
| <b>all</b>                | (Optional) Display all access list entries.                                                                                                            |
| <b>from bootconfig</b>    | (Optional) Display the access list information from the persistent saved configuration.                                                                |
| <b>from filename</b>      | (Optional) The name of the configuration file where the access list configuration is stored. This file must exist in the <i>savedconfig</i> directory. |
| <b>from runningconfig</b> | (Optional) Display the access list information from the currently running configuration.                                                               |

## Defaults

If no **from** parameters are specified, the display shows information from the currently running configuration.

## Command Modes

Administrator or Monitor.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

- Use the **show accesslist** command to display a list of all access lists from the current running configuration.
- Use the **all** keyword to display the contents of all access lists.
- Use the **from bootconfig** keywords to display the specified access list information as it exists in the current saved configuration, used when the SN 5428 restarts. This may differ from the running configuration.

## Examples

To display a list of access lists, issue this command:

```
[SN5428A] # show accesslist
```

To display the contents of all access lists from the current running configuration, issue this command:

```
[SN5428A] # show accesslist all
```

To display the contents of all access lists as they exist in the current bootable configuration, issue this command:

```
[SN5428A] # show accesslist all from bootconfig
```

To display the contents of the access list named *webserver2* from the current running configuration, issue this command:

```
[SN5428A] # show accesslist webserver2
```

To display the contents of the access list named *webserver2* as it exists in the saved configuration file *backup\_1218*, issue this command:

```
[SN5428A] # show accesslist webserver2 from backup_1218
```

## Related Commands

| Commands                            | Description                                                                           |
|-------------------------------------|---------------------------------------------------------------------------------------|
| <b>accesslist</b>                   | Create an access list entity.                                                         |
| <b>accesslist A.B.C.D/bits</b>      | Add IP addresses to an access list.                                                   |
| <b>accesslist chap-username</b>     | Add CHAP user name entries to an access list.                                         |
| <b>accesslist iscsi-name</b>        | Add iSCSI Name entries to an access list.                                             |
| <b>delete accesslist</b>            | Delete a specific access list entry or an entire access list.                         |
| <b>restore accesslist</b>           | Restore the named access list or all access lists from the named configuration file.  |
| <b>save accesslist</b>              | Save configuration data for the named access list or all access lists.                |
| <b>scsirouter target accesslist</b> | Associate an access list with a specific SCSI routing instance target or all targets. |

# show admin

To display the system administrator contact information, use the **show admin** command.

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** The following information displays:

- Contact name
- E-mail address
- Phone number
- Pager number

**Examples** The following example displays the system administrator contact information:

```
[SN5428A]# show admin
Administrator Contact Information
 Name: Pat Hurley
 Email: phurley@abc123z.com
 Phone: 123.456.7890
 Pager: 123.456.3444 pin 2234
```

| Related Commands | Command                  | Description                                              |
|------------------|--------------------------|----------------------------------------------------------|
|                  | <b>admin contactinfo</b> | Configure the SN 5428 administrator contact information. |

# show boot

To display system boot information and startup file parameters, use the **show boot** command.

**show boot**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** None.

---

**Command Modes** Administrator or Monitor.

---

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

---



---

**Usage Guidelines** Use this command to view system boot information, such as the boot device type, path to the boot image, and path to the file containing the startup commands. The **show boot** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

---

**Examples** The following example displays system boot information:

```
[SN5428A]# show boot
 Boot Device: ata=0,00
 Boot File: /ata0/vxWorks
 Startup File: /ata0/NuSpeed.start
 Flags: 0x0
 Other: fei
```

---

| Related Commands | Command                      | Description                                                                                                                                                                 |
|------------------|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>show software version</b> | Display a list of software versions available on the SN 5428, including the currently running version and the version that will run the next time the SN 5428 is restarted. |

---

# show bootconfig

To display the bootable configuration for the SN 5428, or to save the commands used to create the bootable configuration to a file, use the **show bootconfig** command.

**show bootconfig** [*to filename*]

|                           |                    |                                                                                                                                                                           |
|---------------------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>to filename</b> | (Optional) Save the bootable configuration as a series of CLI commands and descriptive text to the specified file. The file will be saved in the <i>script</i> directory. |
|---------------------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Defaults** None.

**Command Modes** Administrator or Monitor.

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 2.2.1          | This command was introduced. |

**Usage Guidelines** Use the **to** keyword to save the bootable configuration as a series of CLI commands and descriptive text in the specified file. This file is saved in the *script* directory and can be used as a basis to create command scripts to automate common tasks. Use the **read** command to execute a command script.

Table 11-17 describes the significant elements that are displayed:

**Table 11-17 Elements Displayed for the show bootconfig Command**

| <b>Element</b> | <b>Description</b>                                                               |
|----------------|----------------------------------------------------------------------------------|
| AAA            | Authentication, authorization, and accounting method configuration information.  |
| ACCESSLIST     | Access list description and entry information.                                   |
| ADMIN          | The SN 5428 administrator contact information.                                   |
| ADMIN LOGIN    | The Administrator mode password.                                                 |
| CDP            | Cisco Discovery Protocol configuration, including timer and holdtime settings.   |
| CLUSTER        | The name of the cluster to which this SN 5428 belongs.                           |
| DNS            | The name of any defined domain name servers.                                     |
| FC             | Global Fibre Channel attributes.                                                 |
| FC Port(s)     | Operational characteristics of the Fibre Channel interfaces.                     |
| GE             | IP addresses and operational characteristics of the Gigabit Ethernet interfaces. |
| HA             | HA configuration information.                                                    |

**Table 11-17 Elements Displayed for the show bootconfig Command (continued)**

| Element                | Description                                                                                                                                                    |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HA Port                | IP address and operational characteristics of the HA interface.                                                                                                |
| LOGGING ROUTE FACILTIY | The SN 5428 logging table.                                                                                                                                     |
| Mgmt Port              | IP address and operational characteristics of the management interface.                                                                                        |
| MONITOR LOGIN          | The Monitor mode password.                                                                                                                                     |
| REMOTE LOG             | Remote logging configuration information.                                                                                                                      |
| RESTRICT               | Storage router interface restrictions.                                                                                                                         |
| ROUTES                 | SN 5428 static routes table.                                                                                                                                   |
| SCSIROUTER             | Configuration information for each SCSI routing instance, including name, description, server interface and other instance-specific configuration information. |
| SNMP                   | The SNMP settings.                                                                                                                                             |
| SNTP                   | Date and time information, including the address of any associated NTP server.                                                                                 |
| SOFTWARE               | The default download location for SN 5428 software.                                                                                                            |
| SYSTEM                 | SN 5428 Storage Router name.                                                                                                                                   |
| VLAN                   | VLAN configuration information.                                                                                                                                |
| VTP DOMAIN             | VTP domain name.                                                                                                                                               |
| VTP MODE               | VTP configuration mode.                                                                                                                                        |

**Examples**

The following is example output from the **show bootconfig** command, for an SN 5428 deployed for SCSI routing:

```
[SN5428A]$ show bootconfig
!
! CLUSTER
!
! cluster Lab1
!
! ACCESSLIST
!
accesslist aegis
accesslist aegis 10.2.0.23/255.255.255.255
accesslist aegis 10.3.0.36/255.255.255.255
accesslist aegis 10.4.0.49/255.255.255.255
accesslist aegis iscsi-name ign.1987-05.com.cisco.08.80342789af73ebcdef123.xxx
accesslist aegis iscsi-name ign.1987-05.com.cisco.08.7125abc9af73ebcdef123.xxx
accesslist aegis iscsi-name ign.1987-05.com.cisco.08.1234abecf9876bac00034.xxx
accesslist aegis chap-usermane 12h7b.lab2.webservices
accesslist aegis chap-username dorothy
accesslist aegis chap-username lab2servp
!
! VTP DOMAIN
!
vtp domain none
!
```

```
! VTP MODE
!
vtp mode client
!
! VLAN
!
! (no vlan(s) found)
!
! SCSIROUTER
!
scsirouter zeus
scsirouter zeus authenticate "none"
scsirouter zeus primary "none"
scsirouter zeus reserve proxy disable
scsirouter zeus failover primary none
scsirouter zeus failover secondary none
scsirouter zeus lun reset no
scsirouter zeus serverIf gel 10.1.0.45/255.255.255.0
scsirouter zeus target webserver2 wwpn "21:00:00:05:ae:03:6d:6e"
scsirouter zeus target webserver2 enabled
scsirouter zeus target webserver2 accesslist "aegis"
!
! SYSTEM
!
hostname SN5428A
!
! Mgmt Port
!
interface mgmt ip-address 10.1.10.244/255.255.255.0
!
! HA Port
!
interface ha ip-address 10.1.20.56/255.255.255.0
! GE
!
interface ge2 mtusize 1500
interface ge2 autonegotiation autodetect
interface ge2 vlan enable
!
! GE
!
interface gel mtusize 1500
interface gel autonegotiation autodetect
interface gel vlan enable
!!
! ROUTES
!
ip route 10.1.30.0/255.255.255.0 10.1.10.201
ip route 10.1.40.243/255.255.255.255 10.1.10.201
ip route 10.1.50.249/255.255.255.255 10.1.10.201
ip default-gateway 10.1.10.201
!
! ADMIN LOGIN
!
admin password <password>
!
! MONITOR LOGIN
!
monitor password <password>
!
```

```

! SNTP
!
clock timezone CST6CDT
ntp peer 10.1.60.86
!
! SNMP
!
snmp-server community public ro
snmp-server community private rw
no snmp-server host all traps
no snmp-server sendauthtraps
snmp-server linkupdown mgmt
snmp-server linkupdown ge1
snmp-server linkupdown ge2
snmp-server linkupdown fc1
snmp-server linkupdown fc2
snmp-server linkupdown fc3
snmp-server linkupdown fc4
snmp-server linkupdown fc5
snmp-server linkupdown fc6
snmp-server linkupdown fc7
snmp-server linkupdown fc8
!
! DNS
!
ip name-server 10.1.40.243 10.1.50.249
ip domain-name mystoragenet.com
!
! SOFTWARE
!
software http url "http://www.cisco.com"
software http username "ciscocustomer" password "<password>"
software proxy username none
!
! CDP
!
cdp enable
cdp timer 60
cdp holdtime 180
cdp interface mgmt enable
cdp interface ha enable
cdp interface ge1 enable
cdp interface ge2 enable
!
! HA
!
! ha configuration clustered
!
! LOGGING ROUTE FACILITY
!
logging level info from all to console logfile
logging level debug from HA to logfile
!
! RESTRICT
!
restrict mgmt ftp
no restrict mgmt telnet
no restrict mgmt http
no restrict mgmt snmp
restrict mgmt rlogin
restrict mgmt ssl
!

```

```
restrict ha ftp
restrict ha telnet
no restrict ha http
no restrict ha snmp
restrict ha rlogin
restrict ha ssl
!
restrict ge1 ftp
restrict ge1 telnet
restrict ge1 http
restrict ge1 snmp
restrict ge1 rlogin
restrict ge1 ssl
!
restrict ge2 ftp
restrict ge2 telnet
restrict ge2 http
restrict ge2 snmp
restrict ge2 rlogin
restrict ge2 ssl
!
! FC
!
interface fc zoning default all
interface fc zoning autosave enable
interface fc domainid 1
no interface fc domainid lock enable
interface fc interop-credit 12
!
! FC Port(s)
!
interface fc1 enable
no interface fc1 al-fairness enable
interface fc1 fan-enable enable
interface fc1 mfs-bundle enable timeout 10
interface fc1 linkspeed auto
interface fc1 type gl-port
!
interface fc2 enable
no interface fc2 al-fairness enable
interface fc2 fan-enable enable
interface fc2 mfs-bundle enable timeout 10
interface fc2 linkspeed auto
interface fc2 type gl-port
!
interface fc3 enable
no interface fc3 al-fairness enable
interface fc3 fan-enable enable
interface fc3 mfs-bundle enable timeout 10
interface fc3 linkspeed auto
interface fc3 type gl-port
!
interface fc4 enable
no interface fc4 al-fairness enable
interface fc4 fan-enable enable
interface fc4 mfs-bundle enable timeout 10
interface fc4 linkspeed auto
interface fc4 type gl-port
!
```

## show bootconfig

```

interface fc5 enable
no interface fc5 al-fairness enable
interface fc5 fan-enable enable
interface fc5 mfs-bundle enable timeout 10
interface fc5 linkspeed auto
interface fc5 type gl-port
!
interface fc6 enable
no interface fc6 al-fairness enable
interface fc6 fan-enable enable
interface fc6 mfs-bundle enable timeout 10
interface fc6 linkspeed auto
interface fc6 type gl-port
!
interface fc7 enable
no interface fc7 al-fairness enable
interface fc7 fan-enable enable
interface fc7 mfs-bundle enable timeout 10
interface fc7 linkspeed auto
interface fc7 type gl-port
!
interface fc8 enable
no interface fc8 al-fairness enable
interface fc8 fan-enable enable
interface fc8 mfs-bundle enable timeout 10
interface fc8 linkspeed auto
interface fc8 type gl-port
!
! AAA
!
aaa new-model
aaa authentication iscsi default local group radius local-case
username "fred" password "9 af4f2428498a41a31e237de1c4a9b9fcef"
username "pat" password "9 7ddbccc3d0daf013f4293c3d3bd94539dd"
username "kris" password "9 0607167520058771e66ab1d379d7e6505f"
username "adrian" password "9 0ad24a3b35dc296d894e512416d572b3ee"
radius-server retransmit 12
radius-server host 10.5.0.53 auth-port 1645
tacacs-server timeout 12
tacacs-server host 10.7.0.22 auth-port 49

```

The following example creates a command file called *SN5428AScript1* in the *script* directory. It contains many of the CLI commands that were issued to create the SN 5428's current bootable configuration.

```
[SN5428A]# show bootconfig to SN5428AScript1
```

## Related Commands

| Command                   | Description                                                                                                         |
|---------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>read</b>               | Read and execute the CLI commands in the named script file.                                                         |
| <b>restore all</b>        | Restore the contents of the named configuration file into memory.                                                   |
| <b>save all</b>           | Save all configuration information                                                                                  |
| <b>show runningconfig</b> | Display the SN 5428's running configuration, or create a command file based on the SN 5428's running configuration. |
| <b>show savedconfig</b>   | List the contents of the savedconfig directory or the contents of the named configuration file.                     |
| <b>show script</b>        | Display the contents of the script directory or the contents of the named command file.                             |

# show buffers

To display buffer pool information for a variety of areas, use the **show buffers** command.

## show buffers

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** The display includes the number of free memory buffers for each pool, along with those currently allocated to various functions. The **show buffers** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

**Examples** The following is sample output from the **show buffers** command:

```
[SN520A]# show buffers
Pool System:

type number

FREE : 42086
DATA : 0
HEADER : 0
SOCKET : 14
PCB : 21
RTABLE : 31
HTABLE : 0
ATABLE : 0
SONAME : 0
ZOMBIE : 0
SOOPTS : 0
FTABLE : 0
RIGHTS : 0
IFADDR : 18
CONTROL : 0
OOBDATA : 0
IPMOPTS : 1
IPMADDR : 5
IFMADDR : 0
MRTABLE : 0
TOTAL : 42176
LOW WTR : 42082
```

## show buffers

```

number of mbufs: 42176
number of times failed to find headers: 0
number of times failed to find clusters: 0
number of times waited for space: 0
number of times drained protocols for space: 0

```

## CLUSTER POOL TABLE

| size | clusters | free  | usage | low water |
|------|----------|-------|-------|-----------|
| 64   | 44       | 21    | 26    | 21        |
| 128  | 16499    | 16463 | 40599 | 16461     |
| 256  | 461      | 445   | 16    | 445       |
| 512  | 484      | 470   | 40575 | 468       |

## Pool Data:

```

type number

FREE : 16718
DATA : 81
HEADER : 1
SOCKET : 0
PCB : 0
RTABLE : 0
HTABLE : 0
ATABLE : 0
SONAME : 0
ZOMBIE : 0
SOOPTS : 0
FTABLE : 0
RIGHTS : 0
IFADDR : 0
CONTROL : 0
OOBDATA : 0
IPMOPTS : 0
IPMADDR : 0
IFMADDR : 0
MRTABLE : 0
TOTAL : 16800
LOW WTR : 16718
number of mbufs: 16800
number of times failed to find headers: 0
number of times failed to find clusters: 0
number of times waited for space: 0
number of times drained protocols for space: 0

```

## CLUSTER POOL TABLE

| size | clusters | free | usage | low water |
|------|----------|------|-------|-----------|
| 64   | 2832     | 2791 | 4697  | 2791      |
| 128  | 4124     | 4086 | 60309 | 4086      |
| 256  | 901      | 898  | 25583 | 884       |
| 512  | 947      | 947  | 13530 | 939       |
| 1024 | 96       | 96   | 6879  | 77        |
| 2048 | 97       | 97   | 2788  | 95        |

Pool nuevent:

Pool GbE:

| type                                         | number |
|----------------------------------------------|--------|
| FREE                                         | 65616  |
| DATA                                         | 0      |
| HEADER                                       | 0      |
| SOCKET                                       | 0      |
| PCB                                          | 0      |
| RTABLE                                       | 0      |
| HTABLE                                       | 0      |
| ATABLE                                       | 0      |
| SONAME                                       | 0      |
| ZOMBIE                                       | 0      |
| SOOPTS                                       | 0      |
| FTABLE                                       | 0      |
| RIGHTS                                       | 0      |
| IFADDR                                       | 0      |
| CONTROL                                      | 0      |
| OOBDATA                                      | 0      |
| IPMOPTS                                      | 0      |
| IPMADDR                                      | 0      |
| IFMADDR                                      | 0      |
| MRTABLE                                      | 0      |
| TOTAL                                        | 65616  |
| LOW WTR                                      | 65614  |
| number of mbufs:                             | 65616  |
| number of times failed to find headers:      | 0      |
| number of times failed to find clusters:     | 0      |
| number of times waited for space:            | 0      |
| number of times drained protocols for space: | 0      |

CLUSTER POOL TABLE

| size  | clusters | free  | usage | low water |
|-------|----------|-------|-------|-----------|
| ----- | -----    | ----- | ----- | -----     |
| ----- | -----    | ----- | ----- | -----     |

Pool iSCSI:

| type    | number |
|---------|--------|
| FREE    | 3240   |
| DATA    | 0      |
| HEADER  | 0      |
| SOCKET  | 0      |
| PCB     | 0      |
| RTABLE  | 0      |
| HTABLE  | 0      |
| ATABLE  | 0      |
| SONAME  | 0      |
| ZOMBIE  | 0      |
| SOOPTS  | 0      |
| FTABLE  | 0      |
| RIGHTS  | 0      |
| IFADDR  | 0      |
| CONTROL | 0      |
| OOBDATA | 0      |
| IPMOPTS | 0      |
| IPMADDR | 0      |
| IFMADDR | 0      |
| MRTABLE | 0      |

## ■ show buffers

```

TOTAL : 3240
LOW WTR : 3240
number of mbufs: 3240
number of times failed to find headers: 0
number of times failed to find clusters: 0
number of times waited for space: 0
number of times drained protocols for space: 0

```

---

 CLUSTER POOL TABLE
 

---

| size  | clusters | free  | usage | low water |
|-------|----------|-------|-------|-----------|
| ----- | -----    | ----- | ----- | -----     |
| ----- | -----    | ----- | ----- | -----     |

## Net Buffers:

```

type number

FREE : 12798
USED : 2
TOTAL : 12800

```

---

**Related Commands**

| Command                  | Description                                                                                   |
|--------------------------|-----------------------------------------------------------------------------------------------|
| <b>show stack</b>        | Display the SN 5428 memory stack on a per-task basis.                                         |
| <b>show tech-support</b> | Display a variety of diagnostic information for use by Cisco Technical Support professionals. |

---

# show cdp

To display global Cisco Discovery Protocol (CDP) configuration information for the SN 5428, including timer and holdtime information, use the **show cdp** command.

```
show cdp
```

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** This command displays current CDP configuration. Use this command to determine if CDP is enabled, and view packet timing and holdtime information. CDP allows network applications to learn device-type information and the SNMP agent address of neighboring devices.

**Examples** The following example displays CDP configuration information for the SN 5428. It shows that CDP is enabled and packets are sent every minute. The SN 5428 directs its neighbors to hold its CDP advertisements for 3 minutes (the default CDP **holdtime** value). The SN 5428 is also enabled to send CDP version 2 advertisements.

```
[SN5428A]# show cdp
Global CDP information:
 CDP is enabled
 Sending CDP packets every 60 seconds
 Sending a holdtime value of 180 seconds
 Sending CDPv2 advertisements are enabled
```

Table 11-18 describes the significant fields shown in the display.

**Table 11-18 Description of Fields in the show cdp Command Output**

| Field                                       | Definition                                                                                                                       |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Sending CDP packets every <i>nn</i> seconds | The interval (in seconds) between transmissions of CDP advertisements. This field is controlled by the <b>cdp timer</b> command. |

**Table 11-18 Description of Fields in the show cdp Command Output (continued)**

| Field                                         | Definition                                                                                                                                                                      |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sending a holdtime value of <i>nn</i> seconds | The amount of time (in seconds) the SN 5428 directs a neighbor to hold the CDP advertisement before discarding it. This field is controlled by the <b>cdp holdtime</b> command. |
| Sending CDPv2 advertisements are enabled      | Indicates that CDP version 2 advertisements are enabled.                                                                                                                        |

**Related Commands**

| Command                   | Description                                                                                                                    |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>cdp enable</b>         | Enable or disable CDP on the SN 5428 Storage Router.                                                                           |
| <b>cdp holdtime</b>       | Specify the amount of time the receiving device should hold a CDP packet from the SN 5428 Storage Router before discarding it. |
| <b>cdp interface</b>      | Switch CDP on or off for the specified interface.                                                                              |
| <b>cdp timer</b>          | Specify the amount of time between transmissions of CDP packets from the SN 5428 Storage Router.                               |
| <b>show cdp entry</b>     | Display information about a specific neighbor device listed in the CDP neighbors table.                                        |
| <b>show cdp interface</b> | Display information about the SN 5428 interfaces on which CDP is enabled.                                                      |
| <b>show cdp neighbors</b> | Display detailed information about neighboring devices discovered using CDP.                                                   |
| <b>show cdp traffic</b>   | Display information about traffic between devices gathered using CDP.                                                          |

# show cdp entry

To display information about a specific neighboring device or all neighboring devices discovered using CDP, use the **show cdp entry** command.

```
show cdp entry { * | all | device-id }
```

| Syntax Description |           |                                                                     |
|--------------------|-----------|---------------------------------------------------------------------|
|                    | *         | Display all CDP neighbors.                                          |
|                    | all       | Display all CDP neighbors.                                          |
|                    | device-id | The device ID of the CDP neighbor about which you want information. |

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command to display operational information about the SN 5428's CDP neighbors. Use **show cdp neighbors** command to display the device ID for the neighbor about which you want additional information.

**Examples** The following is sample output from the **show cdp entry** command. Information about all neighboring devices is displayed, including device ID, address and protocol, platform, interface, holdtime, and version.

```
[SN5428A]# show cdp entry *

Device ID: SCA0428017Q(lab-sn5428A.mylab.com)
Entry address(es):
 IP address: 10.2.1.28
Platform: WS-C6509, Capabilities: Trans-Bridge Switch IGMP
Interface: ge2, Port ID (outgoing port): 4/13
Holdtime : 176 sec

Version :
WS-C6509 Software, Version McpSW: 6.1(1b) NmpSW: 6.1(1b)
 Copyright (c) 1995-2000 by
Cisco Systems

advertisement version: 2
VTP Management Domain: 'LAB-SN5428A'
Native VLAN: 220
Duplex: full
```

**Related Commands**

| <b>Command</b>            | <b>Description</b>                                                                                                             |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>cdp enable</b>         | Enable or disable CDP on the SN 5428 Storage Router.                                                                           |
| <b>cdp holdtime</b>       | Specify the amount of time the receiving device should hold a CDP packet from the SN 5428 Storage Router before discarding it. |
| <b>cdp interface</b>      | Switch CDP on or off for the specified interface.                                                                              |
| <b>cdp timer</b>          | Specify the amount of time between transmissions of CDP packets from the SN 5428 Storage Router.                               |
| <b>show cdp</b>           | Display global CDP configuration information for the SN 5428.                                                                  |
| <b>show cdp interface</b> | Display information about the SN 5428 interfaces on which CDP is enabled.                                                      |
| <b>show cdp neighbors</b> | Display detailed information about neighboring devices discovered using CDP.                                                   |
| <b>show cdp traffic</b>   | Display information about traffic between devices gathered using CDP.                                                          |

# show cdp interface

To display information about the SN 5428 Storage Router interfaces on which CDP is enabled, use the **show cdp interface** command.

```
show cdp interface [if-name]
```

|                           |                |                                                                                                                                                 |
|---------------------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>if-name</i> | Display CDP status and operational information for the specified SN 5428 interface. The following are valid interface names: mgmt, ha, and ge2. |
|---------------------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |       |
|-----------------|-------|
| <b>Defaults</b> | None. |
|-----------------|-------|

|                      |                           |
|----------------------|---------------------------|
| <b>Command Modes</b> | Administrator or Monitor. |
|----------------------|---------------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 2.2.1          | This command was introduced. |

**Usage Guidelines** CDP can be enabled for all SN 5428 interfaces, including the management, high availability, and Gigabit Ethernet interfaces. Use the **show cdp interface** command to display a brief summary of all SN 5428 interfaces on which CDP is enabled. To display status and operational information for a specific interface, add the interface name argument.

**Examples** The following is example output from the **show cdp interface** command:

```
[SN5428A]# show cdp interface
Port CDB Status
----- -
mgmt enabled
ha enabled
ge1 enabled
ge2 enabled
```

The following is example output for the management interface (*mgmt*):

```
[SN5428A]# show cdp interface mgmt
Port CDB Status
----- -
mgmt enabled
```

| <b>Related Commands</b> | <b>Command</b>      | <b>Description</b>                                                                                                             |
|-------------------------|---------------------|--------------------------------------------------------------------------------------------------------------------------------|
|                         |                     | <b>cdp enable</b>                                                                                                              |
|                         | <b>cdp holdtime</b> | Specify the amount of time the receiving device should hold a CDP packet from the SN 5428 Storage Router before discarding it. |

## ■ show cdp interface

| <b>Command</b>            | <b>Description</b>                                                                               |
|---------------------------|--------------------------------------------------------------------------------------------------|
| <b>cdp interface</b>      | Switch CDP on or off for the specified interface.                                                |
| <b>cdp timer</b>          | Specify the amount of time between transmissions of CDP packets from the SN 5428 Storage Router. |
| <b>show cdp</b>           | Display global CDP configuration information for the SN 5428.                                    |
| <b>show cdp entry</b>     | Display information about a specific neighbor device listed in the CDP neighbors table.          |
| <b>show cdp neighbors</b> | Display detailed information about neighboring devices discovered using CDP.                     |
| <b>show cdp traffic</b>   | Display information about traffic between devices gathered using CDP.                            |

# show cdp neighbors

To display detailed information about neighboring devices discovered using CDP, use the **show cdp neighbors** command.

**show cdp neighbors** [*interface if-name*] [*detail*]

| Syntax Description              |                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>interface</b> <i>if-name</i> | (Optional) Keyword and name of the SN 5428 interface connected to the neighbors for which you want information.                                       |
| <b>detail</b>                   | (Optional) Display detailed information about a neighbor (or neighbors) including network address, enabled protocols, holdtime, and software version. |

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use the **show cdp neighbors** command to display brief or detailed information about neighboring devices discovered using CDP. Add the **interface** keyword and the interface name to limit the display to neighbors connected to that specific interface.

Use the **detail** keyword to display detailed information about all devices, or devices connected to the specified interface.

**Examples** The following is example output from the **show cdp neighbors** command:

```
[SN5428A]# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
 S - Switch, H - Host, I - IGMP, r - Repeater
Device-ID Capability Platform Remote Port

SCA05600126 (kal6-lab-swa.cm TSI WS-C6509 4/16
SCA05600126 (kal6-lab-swa.cm TSI WS-C6509 4/12
JAB04140GZC (kal6-lab-z4-swa TS WS-C2948 1/23
```

Table 11-19 describes the significant fields shown in the display.

**Table 11-19 Description of Fields in the show cdp neighbors Command Output**

| Field            | Description                                                                                                                                                                                                                                                                                         |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Capability Codes | The type of device that can be discovered.                                                                                                                                                                                                                                                          |
| Device-ID        | The name of the neighbor device and either the MAC address or the serial number of this device. This field is truncated after 27 characters.                                                                                                                                                        |
| Capability       | The type of the device listed in the CDP Neighbors table. Possible values are: <ul style="list-style-type: none"> <li>• R—Router</li> <li>• T—Transparent bridge</li> <li>• B—Source-routing bridge</li> <li>• S—Switch</li> <li>• H—Host</li> <li>• I—IGMP device</li> <li>• r—Repeater</li> </ul> |
| Platform         | The product number of the device. This field is truncated after 21 characters.                                                                                                                                                                                                                      |
| Remote Port      | The port number of the remove device.                                                                                                                                                                                                                                                               |

The following is sample output for one neighbor from the **show cdp neighbors detail** command. The output includes additional information about the neighbor, including network address, enabled protocols, and software version.

```
[SN5428A]# show cdp neighbors detail

Device ID: TRC0448016Q(lab-sn5428a.mlab.com)
Entry address(es):
 IP address: 10.2.0.83
Platform: WS-C6509, Capabilities: Trans-Bridge Switch IGMP
Interface: mgmt, Port ID (outgoing port): 7/48
Holdtime : 138 sec

Version :
WS-C6509 Software, Version McpSW: 6.1(1b) NmpSW: 6.1(1b)
 Copyright (c) 1995-2000 by Cisco Systems

advertisement version: 2
VTP Management Domain: 'LAB-SN5428A'
Native VLAN: 220
Duplex: half

Device ID: 000421b45a00(lab32)
Entry address(es):
 IP address: 10.2.0.185
Platform: SN5428, Capabilities: Router
Interface: mgmt, Port ID (outgoing port): fei0
Holdtime : 174 sec

Version :
Cisco SN5428 Software Version 2.3.1
```

```
advertisement version: 2
Duplex: half
sysObjectID: 1.3.6.1.4.1.9.1.407
```

Table 11-20 describes the significant fields shown in the display.

**Table 11-20 Description of Fields in the show cdp neighbors detail Command Output**

| Field                 | Description                                                                                                                                                             |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device-ID             | The name of the neighbor device and either the MAC address or the serial number of this device.                                                                         |
| Entry address(es)     | A list of network addresses of neighbor devices.                                                                                                                        |
| IP address            | The IP address of the neighboring device.                                                                                                                               |
| Platform              | The product number of the device.                                                                                                                                       |
| Capability            | The device type of the neighbor. This device can be a router, a bridge, a transparent bridge, a source-routing bridge, a switch, a host, an IGMP device, or a repeater. |
| Interface             | The protocol and port number of the port on the current device.                                                                                                         |
| Holdtime              | The remaining amount of time (in seconds) the current device will hold the CDP advertisement from a sending router before discarding it.                                |
| Version               | The software version of the neighbor device.                                                                                                                            |
| advertisement version | The CDP advertisement version.                                                                                                                                          |
| VTP Management Domain | The name of the VTP management domain.                                                                                                                                  |
| Native VLAN           | The native VLAN identification number.                                                                                                                                  |
| Duplex                | The duplex state of connection between the SN 5428 and the neighbor device.                                                                                             |
| sysObjectID           | The system object identifier.                                                                                                                                           |

#### Related Commands

| Command                   | Description                                                                                                                    |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>cdp enable</b>         | Enable or disable CDP on the SN 5428 Storage Router.                                                                           |
| <b>cdp holdtime</b>       | Specify the amount of time the receiving device should hold a CDP packet from the SN 5428 Storage Router before discarding it. |
| <b>cdp interface</b>      | Switch CDP on or off for the specified interface.                                                                              |
| <b>cdp timer</b>          | Specify the amount of time between transmissions of CDP packets from the SN 5428 Storage Router.                               |
| <b>show cdp</b>           | Display global CDP configuration information for the SN 5428.                                                                  |
| <b>show cdp entry</b>     | Display information about a specific neighbor device listed in the CDP neighbors table.                                        |
| <b>show cdp interface</b> | Display information about the SN 5428 interfaces on which CDP is enabled.                                                      |
| <b>show cdp traffic</b>   | Display information about traffic between devices gathered using CDP.                                                          |

# show cdp traffic

To display information about traffic between devices gathered using Cisco Discovery Protocol (CDP), use the **show cdp traffic** command.

**show cdp traffic**

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command to view statistics about CDP traffic between the SN 5428 and other devices.

**Examples** The following is example output from the show cdp traffic command.

```
[SN5428A]# show cdp traffic
CDP counters :
 Total packets output: 4968, Input: 22329
 Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
 No memory: 0, Invalid packet: 0, Fragmented: 0
 CDP version 1 advertisements output: 1242, Input: 9911
 CDP version 2 advertisements output: 3726, Input: 12418
```

Table 11-21 describes the fields shown in the display.

**Table 11-21 Description of Fields in the show cdp traffic Command Output**

| Field                | Description                                                                                                                                                                  |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Total packets output | The number of CDP advertisements sent by the SN 5428. This value is the sum of the “CDP version 1 advertisements output” and “CDP version 2 advertisements output” fields    |
| Input                | The number of CDP advertisements received by the SN 5428. This value is the sum of the “CDP version 1 advertisements input” and “CDP version 2 advertisements input” fields. |
| Hdr syntax           | The number of CDP advertisements with bad headers received by the SN 5428.                                                                                                   |
| Chksum error         | The number of times the verification operation failed on incoming CDP advertisements.                                                                                        |

**Table 11-21 Description of Fields in the show cdp traffic Command Output (continued)**

| Field                               | Description                                                                                                                                                                                                                                         |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Encaps failed                       | The number of times CDP failed to send advertisements on an interface because of a failure caused by the bridge port of the SN 5428.                                                                                                                |
| No memory                           | The number of times the SN 5428 did not have sufficient memory to store the CDP advertisements in the advertisement cache table when the SN 5428 attempted to assemble advertisement packets for transmission or to parse them when receiving them. |
| Invalid packet                      | The number of invalid CDP advertisements received and sent by the SN 5428.                                                                                                                                                                          |
| Fragmented                          | The number of times fragments or portions of a single CDP advertisement were received by the SN 5428 instead of the complete advertisement.                                                                                                         |
| CDP version 1 advertisements output | The number of CDP version 1 advertisements sent by the SN 5428.                                                                                                                                                                                     |
| Input                               | The number of CDP version 1 advertisements received by the SN 5428.                                                                                                                                                                                 |
| CDP version 2 advertisements output | The number of CDP version 2 advertisements sent by the SN 5428.                                                                                                                                                                                     |
| Input                               | The number of CDP version 2 advertisements received by the SN 5428.                                                                                                                                                                                 |

**Related Commands**

| Command                   | Description                                                                                                                    |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>cdp enable</b>         | Enable or disable CDP on the SN 5428 Storage Router.                                                                           |
| <b>cdp holdtime</b>       | Specify the amount of time the receiving device should hold a CDP packet from the SN 5428 Storage Router before discarding it. |
| <b>cdp interface</b>      | Switch CDP on or off for the specified interface.                                                                              |
| <b>cdp timer</b>          | Specify the amount of time between transmissions of CDP packets from the SN 5428 Storage Router.                               |
| <b>show cdp</b>           | Display global CDP configuration information for the SN 5428.                                                                  |
| <b>show cdp entry</b>     | Display information about a specific neighbor device listed in the CDP neighbors table.                                        |
| <b>show cdp interface</b> | Display information about the SN 5428 interfaces on which CDP is enabled.                                                      |
| <b>show cdp neighbors</b> | Display detailed information about neighboring devices discovered using CDP.                                                   |

# show cli

To display information about the SN 5428 CLI, use the **show cli** command.

**show cli** [*command-keyword*] [*command-keyword ... command keyword ...*]

|                           |                        |                                                                                                              |
|---------------------------|------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>command-keyword</i> | (Optional) The first keyword in the command displays the CLI command tree for all varieties of that command. |
|---------------------------|------------------------|--------------------------------------------------------------------------------------------------------------|

|                 |       |
|-----------------|-------|
| <b>Defaults</b> | None. |
|-----------------|-------|

|                      |                           |
|----------------------|---------------------------|
| <b>Command Modes</b> | Administrator or Monitor. |
|----------------------|---------------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 2.2.1          | This command was introduced. |

**Usage Guidelines** Use the **show cli** command to display the complete CLI command tree, along with helpful information about command parameters and arguments. Use the *command-keyword* arguments to display information about a specific set of commands, such as *scsirouter* or *cdp* commands. Only valid commands and keywords will be displayed.



**Note**

The set of CLI commands and keywords that will be available to you depend on the level of authority associated with your CLI management session and the deployment option selected for the SN 5428 during initial configuration.

**Examples** The following is example output from the **show cli** command, showing the CLI command tree information for the **ping** command.

```
[SN5428A]# show cli ping
ping
 <A.B.C.D | servername>
 numpkts
 <npkts>
 size
 <sn>
 size
 <sn>
```

Send ICMP pings to a host  
IP address or hostname to ping  
Number of packets to attempt  
Integer (Default is 5)  
Size of packet  
Integer (Default is 64)  
Size of packet  
Integer (Default is 64)

| <b>Related Commands</b> | <b>Command</b> | <b>Description</b>                            |
|-------------------------|----------------|-----------------------------------------------|
|                         | <b>help</b>    | Display information about how to use the CLI. |

# show clock

To display the current system date and time, use the **show clock** command.

**show clock**

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command to display the SN 5428 date and time setting.

**Examples** The following is example output from the **show clock** command:

```
[SN5428A]# show clock
Thurs Mar 21 15:54:25 CST 2002
```

| Related Commands | Command               | Description                                                                                                             |
|------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------|
|                  | <b>clock set</b>      | Set the system clock to the given date and time.                                                                        |
|                  | <b>clock timezone</b> | Specify the SN 5428 time zone information.                                                                              |
|                  | <b>ntp peer</b>       | Specify the name or IP address of the NTP server with which the SN 5428 will synchronize date and time.                 |
|                  | <b>setup time</b>     | Run the wizard to configure date and time information (including NTP server and time zone) associated with the SN 5428. |

# show cluster

To display operational information related to the SN 5428 cluster, use the **show cluster** command.

**show cluster**

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command to display cluster information for the SN 5428 whether it is in standalone or clustered mode.

**Examples** The following example displays cluster information. The SN 5428 belongs to a cluster.

```
[SN5428A]# show cluster
Cluster Name: Weblab
Cluster Changes: 2
Last Change: Tue Mar 19 04:12:51 GMT+6 2002
IP Multicast Address: 224.0.0.101

Local Node: SN5428A
HA Configuration: CLUSTERED
HA: up MGMT Port: up HA Port: up
Sent 19240 heartbeats
Rcvd 19238 heartbeats

Cluster Node List:
System Name MGMT IP HA IP Last Heard From
SN5428A 10.1.10.244 10.1.20.56 Self
SN5428B 10.1.10.223 10.1.20.98 Tue Mar 18 05:17:43

Application List:
Application Name Master on State Last Config Update
scsirouter/scsi1 SN5428A Master Mar 18 21:23:45
scsirouter/scsi2 SN5428B Master Mar 18 23:21:10

Access List and Vlan Management is on SN5428A
```

The following example displays cluster information about a standalone SN 5428:

```
[SN5428A]# show cluster
Cluster Name: 630041D
Cluster Changes: 0
Last Change: Mon Nov 19 14:09:18 GMT+6 2001
IP Multicast Address: 224.0.0.101

Local Node: SN5428A
HA Configuration: STANDALONE
HA: down MGMT Port: up HA Port: down
Sent 0 heartbeats
Rcvd 0 heartbeats

Cluster Node List:
System Name MGMT IP HA IP Last Heard From
SN5428A 10.1.10.244 Self

Application List:
Application Name Master on State Last Config Update
scsirouter/foo SN5428A Master Jan 19 13:05:33
Access List and Vlan Management is on SN5428A
```

Table 11-22 describes the fields shown in the display.

**Table 11-22 Description of Fields in the show cluster Command Output**

| Field Name            | Data Format | Description                                                                                                                                                                               |
|-----------------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cluster Name          | string      | The name of the SN 5428 cluster.                                                                                                                                                          |
| Cluster Changes       | decimal     | The number of cluster changes made to this SN 5428 since it was initially configured, or since the last <b>clear conf</b> command was issued.                                             |
| Last Change           | date        | The date and time of the last cluster configuration change.                                                                                                                               |
| IP Multicast Address  | IP address  | The IP address used for multicast communications. IANA has assigned the multicast IP address 224.0.0.101 to the Cisco SN 5428 Storage Router.                                             |
| Local Node            | string      | The name of the SN 5428.                                                                                                                                                                  |
| HA Configuration      | string      | Indicates the configuration of HA in the SN 5428. Valid configurations are STANDALONE or CLUSTERED.                                                                                       |
| HA                    | string      | Indicates the state of the HA application in the SN 5428. Valid states are <i>up</i> or <i>down</i> . If the SN 5428 HA configuration is STANDALONE, the HA state should be <i>down</i> . |
| MGMT Port             | string      | Indicates the state of the SN 5428's physical management port. Valid states are <i>up</i> or <i>down</i> .                                                                                |
| HA Port               | string      | Indicates the state of the SN 5428's physical HA port. Valid states are <i>up</i> or <i>down</i> .                                                                                        |
| Sent . . . heartbeats | decimal     | Number of heartbeats transmitted on the HA network.                                                                                                                                       |
| Rcvd . . . heartbeats | decimal     | Number of heartbeats received on the HA network.                                                                                                                                          |
| Cluster Node List     | string      | A list of SN 5428s in the cluster.                                                                                                                                                        |

**Table 11-22 Description of Fields in the show cluster Command Output (continued)**

| Field Name                      | Data Format | Description                                                                                    |
|---------------------------------|-------------|------------------------------------------------------------------------------------------------|
| System Name                     | string      | The name of the SN 5428.                                                                       |
| MGMT IP                         | IP address  | The IP address of the SN 5428's management interface.                                          |
| HA IP                           | IP address  | The IP address of the SN 5428's HA interface.                                                  |
| Last Heard From                 | date        | The date and time the SN 5428 was last heard from.                                             |
| Application List                | string      | A list of applications running on the SN 5428.                                                 |
| Application Name                | string      | A list of all SCSI routing instances in the cluster.                                           |
| Master on                       | string      | The name of the SN 5428 currently running this SCSI routing instance.                          |
| State                           | string      | The state of the SCSI routing instance.                                                        |
| Last Config Update              | date        | The date and time of the last configuration change to this SCSI routing instance.              |
| Access List and Vlan Management | string      | The name of the SN 5428 in the cluster that currently handles access list and VLAN management. |

**Related Commands**

| Command              | Description                                                                      |
|----------------------|----------------------------------------------------------------------------------|
| <b>save all</b>      | Save all configuration information.                                              |
| <b>save system</b>   | Save selected system configuration information.                                  |
| <b>setup cluster</b> | Change the configuration of the SN 5428's high availability environment.         |
| <b>show ha</b>       | Display HA operational statistics for the SN 5428 or for a specific application. |
| <b>show system</b>   | Display selected system information, including system name.                      |

# show cpu

To display CPU utilization information, use the **show cpu** command.

**show cpu**

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command to view the percentage of CPU utilization for the last five seconds, the last minute, and the last five minutes. The **show cpu** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

**Examples** The following is example output from the show cpu command:

```
[SN5428A]# show cpu
CPU Utilization for last 5 seconds: 1%; last 1 minute: 2%; last 5 minutes: 2%
```

| Related Commands | Command                  | Description                                                                                   |
|------------------|--------------------------|-----------------------------------------------------------------------------------------------|
|                  | <b>show buffers</b>      | Display information about SN 5428 buffer pools.                                               |
|                  | <b>show memory</b>       | Display information about SN 5428 memory and related resources.                               |
|                  | <b>show stack</b>        | Display the SN 5428 memory stack on a per-task basis.                                         |
|                  | <b>show tech-support</b> | Display a variety of diagnostic information for use by Cisco Technical Support professionals. |

# show crash

To display saved crash trace information or current crash trace information, use the **show crash** command.

**show crash [current]**

| Syntax Description | current | (Optional) Returns the current crash trace information for the running SN 5428. |
|--------------------|---------|---------------------------------------------------------------------------------|
|--------------------|---------|---------------------------------------------------------------------------------|

| Defaults | None. |
|----------|-------|
|----------|-------|

| Command Modes | Administrator or Monitor. |
|---------------|---------------------------|
|---------------|---------------------------|

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines**

The default crash trace file is `crash.txt` in the `log` directory. This file is created if the SN 5428 unexpectedly restarts. Use the **current** keyword to display the trace information as it exists for the currently running SN 5428. To save the **show crash** command output, redirect the output of your console using the logging facilities for your specific console interface. Depending on your console interface and scroll buffer size, you may also be able to copy and paste the contents from your console into an ASCII text file.

The **show crash** command is designed for debug purposes and should only be used under the guidance of a Cisco Technical Support professional.

**Examples**

The following example displays the beginning of current crash trace information:

```
[SN5428A]# show crash current
Current running system crash information

Cisco Systems Crash Trace
Time Stamp: Thu Mar 21 16:04:35 CST 2002
System Model: SN5428
Software Version: 2.3.1

#####
#
Exception Info
#
#####
intContext: -1
Task: 0xffffffff
Param 1: 0xffffffff
Param 2: 0xffffffff
Panic Msg: NULL
```

```
#####
#
Boot Info
#
#####
VxWorks (for Galileo GT64260/MPC7410) version 5.4.1.
Kernel: WIND version 2.5.
Made on Mar 20 2002, 15:35:30.
Boot line:
ata=0,00(0,0):/ata0/vxWorks e=10.1.10.244:ffffff00 tn=lab2 s=/ata0/NuSpeed.start o=fei

#####
#
Software Info
#
#####
2.3.1
```

In the following example, no saved crash trace information exists. This condition occurs when the command is issued and the SN 5428 has never unexpectedly restarted.

```
show crash
No crash information available
```

#### Related Commands

| Command                  | Description                                                                                   |
|--------------------------|-----------------------------------------------------------------------------------------------|
| <b>show buffers</b>      | Display information about SN 5428 buffer pools.                                               |
| <b>show memory</b>       | Display information about SN 5428 memory and related resources.                               |
| <b>show stack</b>        | Display the SN 5428 memory stack on a per-task basis.                                         |
| <b>show tech-support</b> | Display a variety of diagnostic information for use by Cisco Technical Support professionals. |

# show debug

To display a variety of debug information or perform specific troubleshooting activities, use the **show debug** command.

```
show debug {forcecfwdump | lldrestartfcfw | mailboxtrace | rawlunatabase} fci?
```

```
show debug portarray fci?
```

| Syntax Description |                       |                                                                                                                                                                                                                                |
|--------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | <i>fci?</i>           | The name of the internal FC interface. Valid values are fci1 and fci2. When you type <b>fci?</b> , the CLI lists the interfaces available. You cannot specify a nonexistent interface.                                         |
|                    | <b>forcecfwdump</b>   | Force a dump of firmware. A file named <i>qlclifwdump0n.txt</i> is created in the <i>/ata4</i> partition, where <i>0n</i> starts at “01” and increments for each firmware dump (for example, <i>/ata4/qlclifwdump01.txt</i> ). |
|                    | <b>lldrestartfcfw</b> | Restart the Fibre Channel firmware. Any existing connections may be dropped.                                                                                                                                                   |
|                    | <b>mailboxtrace</b>   | Display mailbox trace data.                                                                                                                                                                                                    |
|                    | <b>portarray</b>      | Display all active virtual ports. This command is only available in systems deployed for transparent SCSI routing.                                                                                                             |
|                    | <b>rawlunatabase</b>  | Display raw LUN database information for all discovered targets.                                                                                                                                                               |

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                            |
|-----------------|---------|-----------------------------------------|
|                 | 2.2.1   | This command was introduced.            |
|                 | 2.3.1   | The <b>portarray</b> keyword was added. |

**Usage Guidelines** Use this command to display debugging information for internal Fibre Channel interfaces.



**Caution**

Some **show debug** commands may perform actions that drop existing connections or otherwise impact normal SN 5428 performance. The **show debug** command is designed for debug purposes and should only be used under the guidance of a Cisco Technical Support professional.

**Examples**

The following example displays raw lun database information for all targets discovered on the internal FC interface *fc11*:

```
[SN5428_PR]# show debug rawlunatabase fc11

Entry Address = 0xd047ab4
fabricLoginFailureCode=0x0,fabricLoginExtendedCode=0x0,fabricLoginTimeoutCode=0x0
ReportLunsLLDStatus=0x0,ReportLunsLLDStatusModifier=0x0,ReportLunsSCSIStatus=0x0,ReportLun
sASCASCQ=0x0,ReportLunsLunCount=1
InquiryLLDStatus=0x0,InquiryLLDStatusModifier=0x0,InquiryLastLunWithLLDLError=0x0,
InquirySCSIStatus=0x0,InquiryASCASCQ=0x0,InquiryLastLunWithSCSIStatusError=0x0
boolLunsNotSupported=0x0,InquiryLastLunNotSupported=0x0
loopId=0x0,masterState=0x6,slaveState=0x7,loggedIn=1,roles=1,valid=1,portId=0x104e1,scanLu
ns=0x0
numberLuns=0x1,reportAsyncEvent=0x0,node_wwn=0x20000004 0xae4122a6, port_wwn=0x21000004
0xae4322a6

lun=0, wwnn=0x20000020 0x37559b0e, reportAsyncEvent=0x0
stdInquiry data for lun=0x0
bytes0-7=0x00000332 0x8b00700a
vendorId=SEAGATE , product=ST318451FC , revision=0001 device Type=0x0
DeviceIdPage:bytes0-3= 0x0083000c,bytes4-7= 0x01030008,bytes8-11= 0x20000020
:bytes12-15= 0x37559b0e,bytes16-19=0x00800014,bytes20-23=0x33434330
S/N Page:bytes0-3= 0x00800014 s/n=3CC01M4K0000710367CX

Entry Address = 0xab1603c
fabricLoginFailureCode=0x0,fabricLoginExtendedCode=0x0,fabricLoginTimeoutCode=0x0
ReportLunsLLDStatus=0x0,ReportLunsLLDStatusModifier=0x0,ReportLunsSCSIStatus=0x0,ReportLun
sASCASCQ=0x0,ReportLunsLunCount=1
InquiryLLDStatus=0x0,InquiryLLDStatusModifier=0x0,InquiryLastLunWithLLDLError=0x0,
InquirySCSIStatus=0x0,InquiryASCASCQ=0x0,InquiryLastLunWithSCSIStatusError=0x0
boolLunsNotSupported=0x0,InquiryLastLunNotSupported=0x0
loopId=0x1,masterState=0x6,slaveState=0x7,loggedIn=1,roles=1,valid=1,portId=0x101e2,scanLu
ns=0x0
numberLuns=0x1,reportAsyncEvent=0x0,node_wwn=0x20000004 0xae4304cd, port_wwn=0x22000004
0xae4304cd

lun=0, wwnn=0x20000004 0xae4304cd, reportAsyncEvent=0x0
stdInquiry data for lun=0x0
bytes0-7=0x00000312 0x8b00700a
vendorId=SEAGATE , product=ST318452FC , revision=0002 device Type=0x0
DeviceIdPage:bytes0-3= 0x0083000c,bytes4-7= 0x01030008,bytes8-11= 0x20000004
:bytes12-15= 0xae4304cd,bytes16-19=0x00700014,bytes20-23=0x43465630
S/N Page:bytes0-3= 0x00800014 s/n=3FZ0647A00a06216DVJ7

Entry Address = 0xcb1974c
fabricLoginFailureCode=0x0,fabricLoginExtendedCode=0x0,fabricLoginTimeoutCode=0x0
ReportLunsLLDStatus=0xbfc0,ReportLunsLLDStatusModifier=0x3801,ReportLunsSCSIStatus=0x7fcb,
ReportLunsASCASCQ=0x8c13,ReportLunsLunCou7
InquiryLLDStatus=0x5179,InquiryLLDStatusModifier=0x8492,InquiryLastLunWithLLDLError=0x7a90,
InquirySCSIStatus=0xacea,InquiryASCASCQ=0x800b,InquiryLastLunWithSCSIStatusError=0xffe3
boolLunsNotSupported=0x38da7321,InquiryLastLunNotSupported=0xfc51
loopId=0x7e,masterState=0x6,slaveState=0x7,loggedIn=1,roles=0,valid=1,portId=0xfffffe,scan
Luns=0x1
numberLuns=0x0,reportAsyncEvent=0x0,node_wwn=0x10000002 0x3d071161, port_wwn=0x20000002
0x3a171241
```

**Related Commands**

| <b>Command</b>                     | <b>Description</b>                                                                |
|------------------------------------|-----------------------------------------------------------------------------------|
| <b>debug scsirouter</b>            | Enable debugging for the named SCSI routing instance                              |
| <b>debug scsirouter<br/>target</b> | Enable debugging for a specific SCSI routing instance target and LUN combination. |

# show debug fc

To display internal Fibre Channel interface parameters, use the **show debug fc** command.

**show debug fc {all | brief}**

| Syntax Description | all          | Description                                                                                                                        |
|--------------------|--------------|------------------------------------------------------------------------------------------------------------------------------------|
|                    | <b>all</b>   | Display all interface parameters for internal FC interfaces fc0, fc15, fci1 and fci2, including all switch log entries.            |
|                    | <b>brief</b> | Display all interface parameters for internal FC interfaces fc0, fc15, fci1 and fci2. Includes only the last 5 switch log entries. |

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command to display initiator WWPN information (fci1 is initiator WWPN1 and fci2 is initiator WWPN2) and other parameters related to internal FC interfaces for the SN 5428. The **show debug fc** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

**Examples** The following example displays various configuration parameters for the internal FC interfaces, and the last five switch log entries:

```
[SN5428_PR]# show debug fc brief

Interface WWPN switch port

fc0 200000021e071161
fc15 200f00021e071161

Interface WWPN internal

fci1 280000021e071160
fci2 290000021e071160

Global attributes Value

Switch Name SN5428
Node WWN 100000021e071151
DomainID 1
SysLogLevel Critical
SysLogComp NameServer MgmtServer Zoning Switch Chassis Blade Port Eport Other
DevLogLevel Critical
DevLogComp None
```

```

AlarmEntries 1

Display last 5 of 45 syslog entries
[41][Tue Mar 19 05:08:44.280 2002][C][Switch Management:0x3e061163.304.4][User interface
session 3 user cisco@OB-session3 has been]

[42][Tue Mar 19 05:08:44.290 2002][C][Switch Management:0x3e061163.304.4][User interface
session <4> user <cisco@OB-session4> has t]

[43][Tue Mar 19 05:08:44.290 2002][C][Switch Management:0x3e061163.304.4][User interface
session 4 user cisco@OB-session4 has been]

[44][Tue Mar 19 05:33:13.792 2002][C][Switch Management:0x3e061163.304.4][Successful login
user cisco@OB-session3 admin 1 address U]

[45][Tue Mar 19 05:33:13.793 2002][C][Switch Management:0x3e061163.304.4][User interface
session 3 has been opened]

Display 4 devlog entries
[1][Tue Mar 19 03:10:11.057 2002][DI][Switch Log Client/0:0x3e061163.0.5][requesting
logging oper data]

[2][Tue Mar 19 03:10:11.059 2002][DI][Switch Log Client/0:0x3e061163.0.5][received,
DS_RESP_STATUS msg,id = -987127616, status = 0x]

[3][Tue Mar 19 03:10:36.797 2002][DI][Switch Log Client/0:0x3e061163.0.5][updating logging
oper data]

[4][Tue Mar 19 03:10:38.713 2002][DC][Management Server:0x3e0671163.314.6][pltdb.cc.620:
database version '2' does not match code ve]

```

**Related Commands**

| Command                        | Description                                                                       |
|--------------------------------|-----------------------------------------------------------------------------------|
| <b>debug scsirouter</b>        | Enable debugging for the named SCSI routing instance                              |
| <b>debug scsirouter target</b> | Enable debugging for a specific SCSI routing instance target and LUN combination. |

# show debug scsirouter

To display a variety of debug information or perform specific troubleshooting activities for SCSI routing instances, use the **show debug** command.

```
show debug scsirouter {name | all} {scsitrace | tfestatus}
```

```
show debug scsirouter name tfestatus verbose
```

```
show debug scsirouter name target name [lun nn [scsitrace]]
```

## Syntax Description

|                               |                                                                                                      |
|-------------------------------|------------------------------------------------------------------------------------------------------|
| <b>scsirouter</b> <i>name</i> | The name of the SCSI routing instance.                                                               |
| <b>all</b>                    | Display information for all SCSI routing instances.                                                  |
| <b>scsitrace</b>              | Display raw trace information for the specified SCSI routing instance or target and LUN combination. |
| <b>tfestatus</b>              | Display the status of the trace configuration for the specified SCSI routing instance.               |
| <b>target</b> <i>name</i>     | The name of the target associated with the specified SCSI routing instance.                          |
| <b>lun</b> <i>nn</i>          | The target LUN number.                                                                               |

## Defaults

None.

## Command Modes

Administrator or Monitor.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

To enable trace facilities for debugging SCSI routing instances, use the **debug scsirouter** command. The **show debug scsirouter** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

## Examples

The following example displays TFE status data for the SCSI routing instance named *foo*:

```
[SN5428_PR]# show debug scsirouter foo tfestatus
```

## Related Commands

| Command                        | Description                                                                       |
|--------------------------------|-----------------------------------------------------------------------------------|
| <b>debug scsirouter</b>        | Enable debugging for the named SCSI routing instance                              |
| <b>debug scsirouter target</b> | Enable debugging for a specific SCSI routing instance target and LUN combination. |

# show devices

To display a list of devices found on the SN 5428 Fibre Channel network, use the **show devices** command.

**show devices** [*fc?* | **rediscover**]

| Syntax Description |                                                                                                                                                                                                                                          |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>fc?</i>         | (Optional) Limit the display to devices on the named FC interface. Valid values are fc1 through fc8. When you type the <b>interface fc?</b> command, the CLI lists the interfaces available. You cannot specify a nonexistent interface. |
| <b>rediscover</b>  | (Optional) Begin a new discovery process on the Fibre Channel network                                                                                                                                                                    |

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command to display information about all devices discovered on the named SN 5428 Fibre Channel interface, or all FC interfaces. This information can be used when assigning targets to SCSI routing instances. The storage information includes the LUN world-wide name, WWPN, port ID, LUN number, vendor, product name, and LUN serial number.

Use the **rediscover** keyword to clear the existing list of devices and begin a new discovery process on the SN 5428 FC network. Issue the **show devices** command again to display all discovered devices.



**Caution**

The **show devices rediscover** command flushes existing tables and forces a PLOGI to each device. If IP hosts are accessing a device, they will be required to wait until this process completes.

**Examples** The following is example output from the **show devices rediscover** command, followed by the **show devices** command:

```
[SN5428A]# show devices rediscover
Fibre channel discovery kicked off!

[SN5428A]# show devices
Interface lunwwn wwpn portId lun vendor product serial

fc4 20000003ad432e16 21000003ad432e16 0x104e2 0 SEAGATE ST319452FC 3FZ06X0906U2Q
fc4 20000003ad431079 2100000ead431079 0x104e4 0 SEAGATE ST319452FC 3FZ04AFS7W8FM
```

Table 11-23 describes the fields shown in the display.

**Table 11-23 Description of Fields in the show devices Command Output**

| Field     | Description                                   |
|-----------|-----------------------------------------------|
| Interface | The FC interface associated with the storage. |
| lunwwn    | LUN world-wide name (LUNWWN) address.         |
| wwpn      | World-wide port name (WWPN) address.          |
| portId    | The port and domain ID.                       |
| lun       | The physical LUN associated with the storage. |
| vendor    | The vendor of the storage resource.           |
| serial    | The serial number of the storage resource.    |

#### Related Commands

| Command                | Description                                                                                        |
|------------------------|----------------------------------------------------------------------------------------------------|
| <b>show interface</b>  | Display operational and configuration information about the specified interface or all interfaces. |
| <b>show scsirouter</b> | Display configuration and operational information about the named SCSI routing instance.           |

# show diagnostics

To show that the hardware passed diagnostic tests on startup, use the **show diagnostics** command.

**show diagnostics**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** None.

---

**Command Modes** Administrator or Monitor.

---

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

---



---

**Usage Guidelines** The **show diagnostics** command is designed for debug purposes and should be used under the guidance of a Cisco Technical Support professional.

---

**Examples** The following is example output from the **show diagnostics** command:

```
[SN5428A]# show diagnostics
SN5428 Hardware Diagnostics Passed.
```

---

| Related Commands | Command                  | Description                                                                                   |
|------------------|--------------------------|-----------------------------------------------------------------------------------------------|
|                  | <b>show tech-support</b> | Display a variety of diagnostic information for use by Cisco Technical Support professionals. |

---

# show fc

To display global configuration information for SN 5428 Fibre Channel interfaces, use the **show fc** command.

```
show fc
```

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** This command displays global configuration information, including error detect timeout value and resource allocation timeout value, for all SN 5428 FC interfaces.

**Examples** The following example displays global configuration information for all FC interfaces:

```
SN5428A1# show fc
Global attributes Value

Domain ID 1
Domain ID lock disabled
Active Zone None
Zoning Merge SW2
Zoning Default All
Zoning Autosave enabled
Error Detect timeout (edtov) 2000
Resource Allocation timeout (ratov) 10000
Buffer to Buffer Credit (interop) 12
```

| Related Commands | Command                             | Description                                                                                    |
|------------------|-------------------------------------|------------------------------------------------------------------------------------------------|
|                  | <b>interface fc domainid</b>        | Set the SN 5428's domain ID for FC switch fabric zoning.                                       |
|                  | <b>interface fc enable</b>          | Enable all FC interfaces.                                                                      |
|                  | <b>interface fc interop-credit</b>  | Set the data buffer credit capacity for all FC ports.                                          |
|                  | <b>interface fc zoning autosave</b> | Enable the SN 5428 Storage Router to save zoning changes received from switches in the fabric. |

| Command                            | Description                                                                                                        |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>interface fc zoning default</b> | Select the level of communication between the SN 5428 and devices in the fabric where there is no active zone set. |
| <b>interface fc zoning merge</b>   | Set zoning merge compliance.                                                                                       |
| <b>show interface</b>              | Display operational and configuration information for the specified interface or all interfaces.                   |

# show ha

To display HA configuration and status information and HA statistics for the SN 5428 or selected applications and SCSI routing instances running in the HA environment, use the **show ha** command.

```
show ha all
```

```
show ha app {all | list} stats
```

```
show ha app nn {stats | failover list}
```

```
show ha node stats
```

| Syntax Description | all                                | Description                                                                                        |
|--------------------|------------------------------------|----------------------------------------------------------------------------------------------------|
|                    | <b>all</b>                         | Display brief HA status and configuration information.                                             |
|                    | <b>app all stats</b>               | Show HA statistics for all applications.                                                           |
|                    | <b>app list stats</b>              | Display a list of HA applications and brief HA statistics. This list includes application numbers. |
|                    | <b>app <i>nn</i> stats</b>         | Display HA statistics for the specified application number.                                        |
|                    | <b>app <i>nn</i> failover list</b> | Display the failover list for the specified SCSI routing instance.                                 |
|                    | <b>node stats</b>                  | Generate a display of HA statistics for the SN 5428 node.                                          |

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command to help determine if there are communications problems within the SN 5428 cluster. The **show ha all** command displays the state of the management and HA interfaces.

To display statistics about all applications, issue this command:

```
[SN5428A]# show ha app all stats
```

To display a list of SCSI routing instances and other HA applications, with their creation dates and last failover times, issue this command:

```
[SN5428A]# show ha app list stats
```

**Examples**

The following is example output from the **show ha** command, using the **app list** keywords to display a list of applications and SCSI routing instances:

```
[SN5428A]# show ha app list stats

-----HA APPLICATION LIST-----

Type = cluster Created = Tue Mar 19 17:08:02 CDT 2002
 (Number 1) cluster/myCluster Created = Tue Mar 19 17:08:03 CDT 2002
 Activated = Tue Mar 19 17:08:03 CDT 2002
 Last Failover = no failover yet

Type = scsirouter Created = Tue Mar 19 17:08:02 CDT 2002
 (Number 2) scsirouter/myScsi1 Created = Wed Mar 20 16:36:02 CDT 2002
 Activated = Wed Mar 20 16:36:07 CDT 2002
 Last Failover = no failover yet
 (Number 3) scsirouter/myScsi1 Created = Wed Mar 20 18:20:14 CDT 2002
 Activated = Thu Mar 21 07:45:01 CDT 2002
 Last Failover = Thu Mar 21 11:15:33 CDT 2002

```

Table 11-24 describes the significant fields shown in the display.

**Table 11-24 Description of Fields in the show ha Command Output**

| Field         | Description                                                                                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type          | The type of HA application or service.                                                                                                                                                 |
| Created       | The date and time that the application or service type was created.                                                                                                                    |
| Number        | The HA application or service number. This number is used in the <b>show ha</b> command with the <b>app</b> keyword to display information about that specific application or service. |
| Created       | The date and time that the specific application or service was created.                                                                                                                |
| Activated     | The date and time that the specific application or service became active.                                                                                                              |
| Last Failover | The date and time that the specific application or service last failed over.                                                                                                           |

The following is example output from the **show ha** command, using the **app nn stats** keyword and parameter to display operational statistics about the SCSI routing instance named *foo*:

```
[SN5428A]# show ha app 2 stats

-----HA APPLICATION Number 2-----
Application Name = scsirouter/foo
Type = scsirouter Master Specifics: DataBase:
AppId = 0759e950 Node Id = 0042f1a7 ID = 597099c8
State = Master Preferred Slave = No Status = Up to Date
 Permanent Master = No Last Update =
 Mon Apr 8 21:03:55 GMT 2002
```

```

HA Message Transmission Summary:
Total = 00000005 Broadcasts = 00000002 Unicasts = 00000003
HA Message Reception Summary:
Total = 00000004

```

```

-----Message Breakdown-----
 Message Types Received Message Types Transmitted
Master Requests = 00000002 Master Requests = 00000001
Master Acks = 00000001 Master Acks = 00000002
Elections = 00000001 Elections = 00000001
Refusals = 00000000 Refusals = 00000000
Conflicts = 00000000 Conflicts = 00000000
Resolves = 00000000 Resolves = 00000000
Quits = 00000000 Quits = 00000000
Resignations = 00000000 Resignations = 00000001
Doas = 00000000 Doas = 00000000

```

Table 11-25 describes the significant fields shown in the display.

**Table 11-25 Description of Fields in the show ha app Command Output**

| Field                           | Description                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Application Name                | The complete name of the HA application. The syntax is <i>application-type/application name</i> .                                        |
| Type                            | The HA application type.                                                                                                                 |
| AppId                           | The HA application identification number.                                                                                                |
| State                           | The state of the HA application.                                                                                                         |
| Master Specifics: Node Id       | The ID of the node that is currently running the HA application.                                                                         |
| Preferred Slave                 | Indicates if the SN 5428 is the first SN 5428 on the failover list for this HA application.                                              |
| Permanent Master                | Indicates if the SN 5428 is defined as the primary for the HA application.                                                               |
| Database: ID                    | The ID of the internal database entry associated with this HA application.                                                               |
| Status                          | Indicates if the database is current or if there is an outstanding configuration update pending.                                         |
| Last Update                     | The date and time of the last update to this HA application.                                                                             |
| HA Message Transmission Summary | The number of HA messages that have been transmitted by this application. The Total value is the sum of the Broadcasts and the Unicasts. |

**Table 11-25 Description of Fields in the show ha app Command Output (continued)**

| Field                        | Description                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HA Message Reception Summary | The total number of HA messages received by this application.                                                                                                                                                                                                                                                                                                                  |
| Message Breakdown            | The number of each type of HA message that has been received and transmitted by this HA application. The following are HA message types: <ul style="list-style-type: none"> <li>• Master Requests</li> <li>• Master Acks</li> <li>• Elections</li> <li>• Refusals</li> <li>• Conflicts</li> <li>• Resolves</li> <li>• Quits</li> <li>• Resignations</li> <li>• Doas</li> </ul> |

**Related Commands**

| Command                        | Description                                                                                      |
|--------------------------------|--------------------------------------------------------------------------------------------------|
| <b>interface ha ip-address</b> | Specify the HA interface IP address and subnet mask.                                             |
| <b>setup cluster</b>           | Change the configuration of the SN 5428's high availability environment.                         |
| <b>show cluster</b>            | Display cluster-related operational statistics, including heartbeat information.                 |
| <b>show interface</b>          | Display operational and configuration information for the specified interface or all interfaces. |

# show hosts

To display information about Fibre Channel hosts, use the **show hosts** command.

**show hosts**

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Host information is useful when troubleshooting situations where the attached devices cannot be seen. This may be caused by the addition of a target with a WWPN or LUNWWN that does not match any of the known initiators.

**Examples** The following example displays FC host information:

```
[SN5428A]# show hosts
Fibre Channel Host Information

Interface Host wwpn wwnn portId

fc3 200000024e070ae1 200000064e070af1 0x204ae
```

Table 11-26 describes the signification fields shown in the display.

**Table 11-26 Description of Fields in the show hosts Command Output**

| Field     | Description                                            |
|-----------|--------------------------------------------------------|
| Interface | The name of the FC interface associated with the host. |
| Host wwpn | The host world-wide port name.                         |
| wwnn      | The host world-wide node name.                         |
| portId    | The host port ID.                                      |

| Related Commands | Command      | Description                                                                         |
|------------------|--------------|-------------------------------------------------------------------------------------|
|                  | show devices | Display a list of devices discovered on the storage router Fibre Channel interface. |

# show interface

To display operational characteristics and statistics for interfaces configured for the SN 5428, use the **show interface** command. Statistics are cumulative since the last time the system was started.

**show interface**

**show interface brief** [*expression*]

**show interface all** [**stats**]

**show interface** [*if-name*] [**hosts** | **stats**]

**show interface** *if-name* **iscsilogins**

| Syntax             | Description                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>brief</b>       | Show basic operational characteristics for all interfaces, including status, IP address, and selected options.                                         |
| <i>expression</i>  | (Optional) Limit the display to selected options that matches this expression.                                                                         |
| <i>if-name</i>     | (Optional) Show basic operational characteristics and configuration data for the specified interface. Valid interface names are listed in Table 11-27. |
| <b>all</b>         | (Optional) Display operational and configuration data for all interfaces.                                                                              |
| <b>stats</b>       | (Optional) Show operational statistics, such as number of input and output packets, for the specified interface.                                       |
| <b>hosts</b>       | (Optional) For FC interfaces, display FC host information.                                                                                             |
| <b>iscsilogins</b> | Show iSCSI host logins for the specified interface. This keyword is only valid when the SN 5428 is deployed for transparent SCSI routing.              |

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                                                                  |
|-----------------|---------|-------------------------------------------------------------------------------|
|                 | 2.2.1   | This command was introduced.                                                  |
|                 | 2.3.1   | The <i>expression</i> argument and the <b>iscsilogins</b> keyword were added. |

## Usage Guidelines

- Use the **show interface** command with no parameters to display the basic operational characteristics and configuration data for all interfaces defined for the SN 5428.
- Use the **show interface brief** command to display basic operational characteristics for each of the SN 5428 interfaces. This display includes status (up or down) information for the interface and selected operational options such as type of interface, MTU size, and speed. Use the *expression* argument to limit the display to options that match the expression.

- Use the **show interface *if-name* stats** command to display operational statistics related to the specified interface. This information can include packets received and transmitted, collisions, octets, multicast packets, dropped and unsupported protocol, exception status IOCBs (such as LIP reset aborts, port unavailable or logged out, DMA errors, port configuration changed, command timeout, data overrun, write or read data underrun, and queue full), Fibre Channel errors, and other general events.

**Table 11-27 Valid Interface Names**

| Interface Name | Description                                                             |
|----------------|-------------------------------------------------------------------------|
| <b>fc?</b>     | The SN 5428 Fibre Channel interface, for example fc1 or fc5.            |
| <b>fci?</b>    | The internal SN 5428 Fibre Channel interface, for example fci1 or fci2. |
| <b>ge?</b>     | The SN 5428 Gigabit Ethernet interface, for example, ge1 or ge2.        |
| <b>ha</b>      | The SN 5428 high availability interface.                                |
| <b>mgmt</b>    | The SN 5428 management interface.                                       |

**Examples**

The following is example output from the **show interface** command:

```
[SN5428A]# show interface
Operational Data
Interface Stat IP/Netmask MAC Options

lo0 up 127.0.0.1/ff000000 000000000000 type Loopback
 mtu 32768
 speed 0
 flags UP LOOPBK RUNNING MLTCST
mgmt up 10.1.10.244/ffffff00 00023d070cc0 type Ethernet
 mtu 1500
 speed 100000000
 flags UP BRDCST RUNNING MLTCST
ha up 10.1.20.56/ffffff00 00023d070cc1 type Ethernet
 mtu 1500
 speed 100000000
 flags UP BRDCST RUNNING MLTCST
fc1 up
 type Fibre Channel
 OperState enabled
 PortID 010100
 WWN 200100c0aa00bc30
 LinkSpeed 1Gb/s
 LinkState Active
 SyncState SyncAcquired
 LoginStatus LoggedIn
 Loopback Status Not Running
 MaxCredit 12
 RunningType fl-port
 PendingType gl-port
 SFPType 100-M5-SN-1
 SFPVendor PICOLIGHT
 SFPVendorID 850400
 SFPPartNumber PL-XPL-00-S23-00
 SFPRev
fc2 down
 type Fibre Channel
 OperState disabled
 PortID 010200
 WWN 200200c0cc00ac30
 LinkSpeed auto
 LinkState Inactive
```



```

PortID 010600
WWN 200600c0ad00cc30
LinkSpeed auto
LinkState Inactive
SyncState SyncLost
LoginStatus NotLoggedIn
Loopback Status Not Running
MaxCredit 12
RunningType Unknown
PendingType gl-port
SFPTYPE NotInstalled
SFPVendor Unknown
SFPVendorID 0
SFPPartNumber Unknown
SFPRev 0
fc7 down
type Fibre Channel
OperState disabled
PortID 010700
WWN 200700c0bd00ac30
LinkSpeed 2Gb/s
LinkState Inactive
SyncState SyncLost
LoginStatus NotLoggedIn
Loopback Status Not Running
MaxCredit 12
RunningType Unknown
PendingType gl-port
SFPTYPE NotInstalled
SFPVendor Unknown
SFPVendorID 0
SFPPartNumber Unknown
SFPRev 0
fc8 down
type Fibre Channel
OperState disabled
PortID 010800
WWN 200800c0dd00bc30
LinkSpeed auto
LinkState Inactive
SyncState SyncLost
LoginStatus NotLoggedIn
Loopback Status Not Running
MaxCredit 12
RunningType Unknown
PendingType gl-port
SFPTYPE NotInstalled
SFPVendor Unknown
SFPVendorID 0
SFPPartNumber Unknown
SFPRev 0
ge1 up 10.1.10.45/ffffff00 02023da80a51 type Gigabit Ethernet
mtu 1500
speed 1000000000
flags UP BRDCST RUNNING MLTCST
signal signal detect
duplex full
auto-negotiate complete
flow control rx pause
SFPVendor Tyco Electronics
SFPVendor unknown
SFPPartNumber 1382350-1
SFPRev 0000350-1
ge2 up 10.3.10.25/ffffff00 02045aa80a51 type Gigabit Ethernet
mtu 1500
speed 1000000000

```

```

flags UP BRDCST RUNNING MLTCST
signal signal detect
duplex full
auto-negotiate complete
flow control rx pause
SFPVendor Tyco Electronics
SFPVendor unknown
SFPPartNumber 1382350-1
SFPRev 0000350-1

Configuration Data

Interface IP Address Netmask

mgmt 10.1.10.244
ha 10.1.20.56

Interface Status Al- Fan- Link Loopback Mfs- Time Port-
----- ----- ----- ----- ----- ----- ----- -----
fc1 enabled disabled enabled auto None enabled 10 gl-port
fc2 enabled disabled enabled auto None enabled 10 gl-port
fc3 enabled disabled enabled auto None enabled 10 g-port
fc4 enabled disabled enabled auto None enabled 10 fl-port
fc5 enabled disabled enabled auto None enabled 10 fl-port
fc6 enabled disabled enabled auto None enabled 10 gl-port
fc7 enabled disabled enabled auto None enabled 10 gl-port
fc8 enabled disabled enabled auto None enabled 10 gl-port

Interface MTU Size AutoNegotiation Vlan IP Address Netmask

ge1 1500 autodetect enabled
ge2 1500 autodetect enabled

```

Table 11-28 describes the fields shown in the display.

**Table 11-28 Description of Fields in the show interface Command Output**

| Field              | Description                                                                                                                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operational Data   | Operational characteristics.                                                                                                                                                                               |
| Interface          | The interface name.                                                                                                                                                                                        |
| Stat               | The status of the interface.                                                                                                                                                                               |
| IP/Netmask         | The IP address and subnet mask of the interface.                                                                                                                                                           |
| MAC                | The MAC address of the interface.                                                                                                                                                                          |
| Options            | Configuration and operational information for the interface, including interface type, MTU size, speed, Small Form-factor Pluggable (SFP) module, running and pending port type, and activity information. |
| Configuration Data | Configuration information. Not all fields are applicable to all interfaces.                                                                                                                                |
| Interface          | The interface name.                                                                                                                                                                                        |
| IP Address         | The IP address of the interface.                                                                                                                                                                           |
| Netmask            | The subnet mask of the interface.                                                                                                                                                                          |
| Status             | For FC interfaces, the status of the interface (enabled or disabled).                                                                                                                                      |
| Al-fairness        | For FC interfaces, the status of the fairness algorithm (enabled or disabled).                                                                                                                             |

**Table 11-28 Description of Fields in the show interface Command Output (continued)**

| Field           | Description                                                                           |
|-----------------|---------------------------------------------------------------------------------------|
| Fan-enable      | For FC interfaces, the status of Fabric Address Notification (enabled or disabled).   |
| Link speed      | For FC interfaces, the transfer rate.                                                 |
| Loopback type   | For FC interfaces, the type of loopback test enabled for the interface.               |
| Mfs-bundle      | For FC interfaces, the status of Multi-Frame Sequence bundling (enabled or disabled). |
| Timeout         | For FC interfaces, the MFS-bundle timeout value.                                      |
| Port-type       | For FC interfaces, the pending port type.                                             |
| MTU Size        | For Gigabit Ethernet interfaces, the size of the maximum transfer unit, in bytes.     |
| AutoNegotiation | For Gigabit Ethernet interfaces, the autonegotiation setting.                         |
| Vlan            | For Gigabit Ethernet interfaces, the status of VLAN support (enabled or disabled).    |

The following is example output from the **show interface brief** command, using the match expression *type* to limit the options displayed:

```
[SN5428A]# show interface brief type
Interface Stat IP/Netmask MAC Options

lo0 up 127.0.0.1/ff000000 000000000000 type Loopback
mgmt up 10.1.10.244/ffffff00 00012d071160 type Ethernet
fc1 up type Fibre Channel
fc2 down type Fibre Channel
fc3 down type Fibre Channel
fc4 up type Fibre Channel
fc5 down type Fibre Channel
fc6 down type Fibre Channel
fc7 down type Fibre Channel
fc8 down type Fibre Channel
ge1 up 10.1.10.45/ffffff00 02012d020304 type Gigabit Ethernet
ge2 up 10.3.10.23/ffffff00 02034d030405 type Gigabit Ethernet
```

The following is example output from the **show interface stats** command, for the FC interface *fc4*:

```
[SN5428A]# show interface fc4 stats

Port Attribute Value Port Attribute Value

BytePerf 0 FramePerf 0
TxBytePerf 0 TxFramePerf 0
RxBytePerf 0 RxFramePerf 0
ErrorRates 16

Login Count 0x6 Logout Count 0x5
Total Errors 0xb Invalid Dest Addr 0x0

Class2 Frames In 0x0 Class2 Frames Out 0x0
Class3 Frames In 0x93 Class3 Frames Out 0x68
Total Rx Frames 0x93 Total Tx Frames 0x68

Class2 Words In 0x0 Class2 Words Out 0x0
Class3 Words In 0x0 Class3 Words Out 0x87
Total Rx Words 0x0 Total Tx Words 0x87
```

```

Decode Error Count 0xb Loss of Sync Count 0x1
Invalid CRC Count 0x0 Tx Wait Count 0x34
Class3 Toss Count 0x0 FReject Count 0x0
FBusy Count 0x0 Link Failures 0x0
Flow Error Count 0x0 LP_TOV Timeout Count 0x0
Primitive Seq Errors 0x0

Rx Link Resets 0x0 Rx Offline Seq 0x0
Tx Link Resets 0x0 Tx Offline Seq 0xc
Total Link Resets 0x0 Total Offline Seq 0xc

AL Init Count 0x9 AL Init Error Count 0x1
LIP_F7_F7_Count 0x8 LIP_F7_AL_PS Count 0x1
LIP_F8_F7_Count 0x0 LIP_F8_AL_PS Count 0x0
Total LIPS Received 0x9 LIP_AL_PD_AL_PS Count 0x0

```

Table 11-29 describes the port attributes shown in the display:

**Table 11-29 Description of Port Attributes in the show interface stats Command Output**

| Port Attribute     | Description                                       |
|--------------------|---------------------------------------------------|
| BytePerf           | Total number of bytes processed by this port.     |
| TxBytePerf         | Total number of bytes transmitted by this port.   |
| RxBytePerf         | Total number of bytes received by this port.      |
| ErrorRates         | The error rate for this port.                     |
| FramePerf          | Total number of frames processed by this port.    |
| TxFramePerf        | Total number of frames transmitted by this port.  |
| RxFramePerf        | Total number of frames received by this port.     |
| Login Count        | Incremented when a user logs in.                  |
| Total Errors       | Total number of errors detected.                  |
| Logout Count       | Incremented when a user logs out.                 |
| Invalid Dest Add   | Number of invalid destination addresses received. |
| Class2 Frames In   | Number of class 2 frames received by this port.   |
| Class3 Frames In   | Number of class 3 frames received by this port.   |
| Total Rx Frames    | Total number of frames received by this port.     |
| Class2 Frames Out  | Number of class 2 frames sent by this port.       |
| Class3 Frames Out  | Number of class 3 frames sent by this port.       |
| Total Tx Frames    | Total number of frames issued by this port.       |
| Class2 Words In    | Number of class 2 words received by this port.    |
| Class3 Words In    | Number of class 3 words received by this port.    |
| Total Rx Words     | Total number of words received by this port.      |
| Class2 Words Out   | Number of class 2 words sent by this port.        |
| Class3 Words Out   | Number of class 3 words sent by this port.        |
| Total Tx Words     | Total number of words issued by this port.        |
| Decode Error Count | Number of decoding errors detected.               |

**Table 11-29 Description of Port Attributes in the show interface stats Command Output (continued)**

| Port Attribute       | Description                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Invalid CRC Count    | Number of invalid CRCs detected.                                                                                                                                                                                                                                                                                                                                                                                        |
| Class3 Toss Count    | Number of class 3 frames tossed.                                                                                                                                                                                                                                                                                                                                                                                        |
| FBusy Count          | The number of times the switch sent a P_BSY because a Class 2 frame could not be delivered within a specified time period; the number of class 2 and class 3 fabric busy (F_BSY) frames generated by this port in response to incoming frames. This usually indicates a busy condition on the fabric that is preventing delivery of this frame.                                                                         |
| Flow Error Count     | Number of flow errors.                                                                                                                                                                                                                                                                                                                                                                                                  |
| Primitive Seq Errors | Primitive sequence errors detected.                                                                                                                                                                                                                                                                                                                                                                                     |
| Loss of Sync Count   | Number of synchronization losses detected by this port. A loss of synchronization (greater than 100 ms) is detected by the receipt of an invalid transmission word.                                                                                                                                                                                                                                                     |
| Tx Wait Count        | Time waiting to transmit when blocked with no credit. Measured in FC Word times.                                                                                                                                                                                                                                                                                                                                        |
| FReject Count        | Number of frames from devices that were rejected.                                                                                                                                                                                                                                                                                                                                                                       |
| Link Failures        | Number of optical link failures detected by this port. A link failure is a loss of synchronization for a period of time greater than the timeout value or by loss of signal while not in the offline state. A loss of signal causes the switch to attempt to re-establish the link. If the link is not re-established by the time specified, a link failure is counted. A link reset is performed after a link failure. |
| LP_TOV Timeout Count | Number of times the timeout value on the local port has been triggered.                                                                                                                                                                                                                                                                                                                                                 |
| Rx Link Resets       | Number of link reset primitives received from an attached device.                                                                                                                                                                                                                                                                                                                                                       |
| Tx Link Resets       | Number of link resets issued by this port.                                                                                                                                                                                                                                                                                                                                                                              |
| Total Link Reset     | Total number of link reset primitives.                                                                                                                                                                                                                                                                                                                                                                                  |
| Rx Offline Seq       | Number of offline sequences received. An OLS is issued for link initialization, an NOS state, or to enter the offline state.                                                                                                                                                                                                                                                                                            |
| Tx Offline Seq       | Number of offline sequences issued by this port.                                                                                                                                                                                                                                                                                                                                                                        |
| Total Offline Seq    | Total number of offline sequences issues by this port.                                                                                                                                                                                                                                                                                                                                                                  |
| AL Init Count        | Incremented each time the port begins AL initialization.                                                                                                                                                                                                                                                                                                                                                                |

**Table 11-29 Description of Port Attributes in the show interface stats Command Output (continued)**

| Port Attribute        | Description                                                                                                                                              |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| LIP_F7_F7_Count       | A loop initialization primitive frame used to acquire a valid AL_PA.                                                                                     |
| LIP_F8_F7_Count       | A loop initialization primitive frame used to indicate that a loop failure has been detected at the receiver.                                            |
| Total LIPS Received   | Total number of loop initialization primitives received.                                                                                                 |
| AL Init Error Count   | Number of times the port entered initialization and the initialization failed.                                                                           |
| LIP_F7_AL_PS Count    | This LIP is used to reinitialize the loop. An L_port, identified by AL_PS, may have noticed a performance degradation and is trying to restore the loop. |
| LIP_F8_AL_PS Count    | This LIP denotes a loop failure detected by the L_port identified by AL_PS.                                                                              |
| LIP_AL_PD_AL_PS Count | Number of F7, AL_PS LIPs, or AL_PD (vendor specific) resets performed.                                                                                   |

**Related Commands**

| Command                          | Description                                                                              |
|----------------------------------|------------------------------------------------------------------------------------------|
| <b>interface ge?</b>             | Configure various operational parameters associated with the Gigabit Ethernet interface. |
| <b>interface ha ip-address</b>   | Specify the HA interface IP address and subnet mask.                                     |
| <b>interface mgmt ip-address</b> | Specify the management interface IP address and subnet mask.                             |
| <b>setup mgmt</b>                | Run the wizard to configure the management interface.                                    |
| <b>setup cluster</b>             | Change the configuration of the SN 5428's high availability environment.                 |

# show ip

To display information about the SN 5428 Storage Router network, including a variety of protocol stack statistics, use the **show ip** command.

```
show ip {arp | hosts | route | tcp | udp}
```

```
show ip [icmp | route | tcp | udp] stats
```

## Syntax Description

|                    |                                                    |
|--------------------|----------------------------------------------------|
| <b>arp</b>         | Display the ARP table.                             |
| <b>hosts</b>       | Display all known hosts on the SN 5428 IP network. |
| <b>route</b>       | Display the system route table.                    |
| <b>tcp</b>         | Display active TCP connections.                    |
| <b>udp</b>         | Display system UDP activity.                       |
| <b>icmp stats</b>  | Display ICMP-related network statistics.           |
| <b>route stats</b> | Display route-related network statistics.          |
| <b>tcp stats</b>   | Display TCP-related network statistics.            |
| <b>udp stats</b>   | Display UDP-related network statistics.            |
| <b>stats</b>       | Display all IP-related network statistics.         |

## Defaults

None.

## Command Modes

Administrator or Monitor.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

- Use the **show ip** command with the **stats** keyword to display operational network statistics related to the specified protocol. The information displayed depends on the type of protocol specified.
- Use the **arp** keyword to display the ARP table.
- Use the **hosts** keyword to display all known IP hosts on the SN 5428 IP network.
- Use the **route** keyword to display the SN 5428 system routing table, including network and host routes. *0.0.0.0/32* is the default route.
- Use the **tcp** keyword to display active TCP connections, including the SN 5428 web server and other server tasks.
- Use the **udp** keyword to display User Datagram Protocol (UDP) activity on the system.

**Examples**

The following is example output from the **show ip stats** command:

```
[SN5428A]# show ip stats
 Total Packets 131784
 Bad Checksum 0
 Packet too Short 0
 Not Enough Data 0
 Bad Header Length 0
 Bad Packet Length 0
 Fragments Received 0
 Fragments Dropped 0
 Fragments Timed Out 0
 Packets Forwarded 0
 Destination Unreachable 1604
 Redirected Packets 0
 Unknown Protocol 17
 Out of Buffers 0
 Packets Reassembled 0
 Fragments Sent 0
 No Route 0
 Generic Drop 0
```

**Related Commands**

| Command         | Description                                                     |
|-----------------|-----------------------------------------------------------------|
| <b>ip route</b> | Add a static route to the SN 5428 Storage Router routing table. |

# show logging

To display the logging table routing rules or to display contents of the SN 5428 log file, use the **show logging** command.

```
show logging [[all | last nn] [match string] | size]
```

| Syntax Descriptions        |                                                                                                    |  |
|----------------------------|----------------------------------------------------------------------------------------------------|--|
| <b>all</b>                 | (Optional) Display all log file entries.                                                           |  |
| <b>last <i>nn</i></b>      | (Optional) Display the last <i>nn</i> lines from the current SN 5428 log file.                     |  |
| <b>match <i>string</i></b> | (Optional) Display all entries that match the specified string. String matching is case-sensitive. |  |
| <b>size</b>                | (Optional) Display the number of messages in the log file and the size of the log file, in bytes.  |  |

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                          |
|-----------------|---------|---------------------------------------|
|                 | 2.2.1   | This command was introduced.          |
|                 | 2.3.1   | The <b>route</b> keyword was removed. |

- Usage Guidelines**
- Use the **show logging** command to display the routing rules in the logging table, which is used to route event messages to the appropriate destinations based on the message level and facility.
  - Use the **match *string*** parameters to display messages in the SN 5428 log file that match the specified string. You can search the entire log file for matching messages or restrict the search to the last *nn* number of messages.

**Examples** The following is example output from the **show logging** command:

```
[SN5428A]# show logging
Logging is enabled
Logging to syslog host is enabled, ip-address is 10.1.1.144

Index Level Priority Facility Route
1 info 6 all console logfile
2 debug 7 HA logfile rslog
```

The following is example output from the **show logging last 20 match "Successful"** command:

```
[SN5428A]# show logging last 20 match "Successful"
Apr 10 20:48:13: %UI-5-NSCL: Successful CLI login from [10.1.68.196]
Apr 10 22:15:12: %UI-5-NSCL: Successful CLI login from [10.1.42.120]
May 29 21:43:05: %UI-5-NSCL: Successful CLI login from [console]
```

**Related Commands**

| <b>Command</b>             | <b>Description</b>                                                                                                                  |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>clear logging table</b> | Clear the SN 5428 Storage Router logging table of all entries, or to reset the table to factory defaults.                           |
| <b>delete logging</b>      | Delete a rule from the logging table.                                                                                               |
| <b>logging #?</b>          | Insert a routing rule entry into the SN 5428 logging table.                                                                         |
| <b>logging level</b>       | Add rule entries to route SN 5428 event, debug and trace messages to various destinations based on facility and notification level. |
| <b>logging on</b>          | Enable or temporarily disable logging of SN 5428 event message.                                                                     |
| <b>logging syslog</b>      | Enable remote logging to the specified IP host.                                                                                     |

# show memory

To display information about memory and related resources in the SN 5428, use the **show memory** command.

**show memory**

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command to display information about the SN 5428 memory usage. The **show memory** command is designed for debug purposes and should be used under the guidance of a Cisco Technical Support professional.

**Examples** The following is example output from the **show memory** command:

```
[SN5428A]# show memory
Memory: 226341288 Available: 34174208
 Free Blocks: 430 Max Free Block Size: 26066888
 File Descriptors: 256 Available: 233

Buffer Memory:

Buffer Total Free Total Free
Pool Blocks Blocks Mbufs Mbufs Warnings
System 17488 17401 42176 42089
Data 8997 8997 16800 16800
GbE 65536 63494 65616 65616
iSCSI 3000 3000 3240 3240
```

| Related Commands | Command             | Description                                                             |
|------------------|---------------------|-------------------------------------------------------------------------|
|                  | <b>show buffers</b> | Display information about SN 5428 buffer pools.                         |
|                  | <b>show modules</b> | Display addressing information related to the SN 5428 software modules. |
|                  | <b>show stack</b>   | Display the SN 5428 memory stack on a per-task basis.                   |

| <b>Command</b>           | <b>Description</b>                                                                            |
|--------------------------|-----------------------------------------------------------------------------------------------|
| <b>show task</b>         | Display information about the tasks running in the SN 5428.                                   |
| <b>show tech-support</b> | Display a variety of diagnostic information for use by Cisco Technical Support professionals. |

# show modules

To display addressing information about the modules included in the SN 5428, use the **show modules** command.

## show modules

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command to display the memory locations for each module of the SN 5428 software. The **show modules** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

**Examples** The following is example output from the **show modules** command:

```
[SN5428A]# show modules

MODULE NAME MODULE ID GROUP # TEXT START DATA START BSS START

 sysInit.out 0xd6f12c8 2 0xd6e5040 0xd6efd20 0xd6efe08
 crashDump.out 0xd5c76b8 3 0xd5c15a0 0xd5c6030 0xd5c60a0
 snmp_util.out 0xd5c00d8 4 0xd5bf300 0xd5bfa90 0xd5bfac8
 nuUtils.out 0xd5becc0 5 0xd574b60 0xd58bd70 0xd58c948
 nuEvents.out 0xd5b8160 6 0xd5afd90 0xd5b60f0 0xd5b6ab8
 ha.out 0xd5add30 7 0xd59d5d0 0xd5ac410 0xd5ac708
 confNode.out 0xd574928 8 0xd56fa40 0xd5737d0 0xd573828
 authServer.out 0xd5746f8 9 0xd564a70 0xd56dc40 0xd56ddb8
 drv.out 0xd5744b0 10 0xd514ee0 0xd524140 0xd52422c
 qlptic.out 0xd53b460 11 0xd324a20 0xd378d50 0xd40a220
 qlpt.out 0xd514ca8 12 0xd4b3d30 0xd4c5e80 0xd4d8418
 i82543.out 0xd510d10 13 0xd49a760 0xd4b3b20 0xd4b3d28
 smlApi.out 0xd509b48 14 0xd4dcf80 0xd4e97f0 0xd4e9a60
 vtp.out 0xd504dd0 15 0xd4fd970 0xd5037f0 0xd503910
scsiTargetFE.out 0xd504b70 16 0xd42d9f0 0xd451b90 0xd4594e8
scsiTargetBE.out 0xd49a520 17 0xd414010 0xd42af30 0xd42d8e8
 virtdev.out 0xd4948d8 18 0xd494580 0xd494580 0xd4945a8
scsiTcpAuth.out 0xd4942b8 19 0xd48fe70 0xd493610 0xd493668
scsiTcpServer.out 0xd494070 20 0xd461690 0xd48e870 0xd48ea24
scsiTcpClient.out 0xd3247e0 21 0xd116980 0xd136ba0 0xd136fe8
 ttcp.out 0xd31d388 22 0xd2f1c70 0xd2f8ec0 0xd2f95e8
 confMgmt.out 0xd31a300 23 0xd317000 0xd319490 0xd319610
 hdwmon.out 0xd31a0b8 24 0xd310810 0xd314fd0 0xd31560c
```

## show modules

```

diag.out 0xd319e58 25 0xd0bb3e0 0xd0dce50 0xd0ddd48
confXML.out 0xd116748 26 0xd09fee0 0xd0bb300 0xd0bb3d8
confObj.out 0xd116498 27 0xcfcfa20 0xd01b5c0 0xd01bbb8
clusterApp.out 0xd09fca8 28 0xd094350 0xd09dc70 0xd09dcec
 cdp.out 0xd090c08 29 0xd0844a0 0xd08e740 0xd08ed08
 systemApp.out 0xd07d2e0 30 0xcfa3cc0 0xcfcfa90 0xcfcfa0c
 ipRouter.out 0xd06e5c8 31 0xd066980 0xd06c980 0xd06ca1c
 scsiRouter.out 0xd06e250 32 0xd045fe0 0xd060430 0xd06057c
 frameRacer.out 0xd06de58 33 0xd030b30 0xd03a770 0xd03a83c
authServerApp.out 0xd06dac8 34 0xd025850 0xd030ab0 0xd030b1c
 fcSwApp.out 0xd045e28 35 0xd070150 0xd07be40 0xd07cddc
 fdisk.out 0xd041808 36 0xd10b690 0xd110a40 0xd110e6c
 openssl.out 0xd041650 37 0xcd3d640 0xce240b0 0xce2dc18
 ui.out 0xcfa3a90 38 0xc570ec0 0xc89f9b0 0xc8c91e4
 ifx.out 0xcd3d410 39 0xcd39850 0xcd3bcc0 0xcd3c3d8
 ether.out 0xcd388b0 40 0xcd37040 0xcd37ae0 0xcd37fa8
 mau_if.out 0xcd36810 41 0xcd34810 0xcd358e0 0xcd35cf8
 mau_neg.out 0xcd33b50 42 0xcd32750 0xcd33020 0xcd332f8
 entity.out 0xcd31f38 43 0xcd03790 0xcd05e40 0xcd11fc8
entity_sensor.out 0xcd2f5b8 44 0xcd2cec0 0xcd2e2b0 0xcd2e978
 cdp_snmp.out 0xcd2c038 45 0xcd28950 0xcd2ab20 0xcd2afd8
 fcmgmt_fcsw.out 0xcd2be08 46 0xcd1b320 0xcd22d20 0xcd257f8
 iscsi_mib.out 0xcd03558 47 0xccde150 0xcce6a40 0xcce8278
 snmpApp.out 0xccfd1d0 48 0xccf9d80 0xccfc0e0 0xccfc23c

```

## Related Commands

| Command                  | Description                                                                                   |
|--------------------------|-----------------------------------------------------------------------------------------------|
| <b>show buffers</b>      | Display information about SN 5428 buffer pools.                                               |
| <b>show memory</b>       | Display information about SN 5428 memory and related resources.                               |
| <b>show stack</b>        | Display the SN 5428 memory stack on a per-task basis.                                         |
| <b>show task</b>         | Display information about the tasks running in the SN 5428.                                   |
| <b>show tech-support</b> | Display a variety of diagnostic information for use by Cisco Technical Support professionals. |

# show restrict

To display current restrictions on the use of the SN 5428 Storage Router console, interfaces, and ports, use the **show restrict** command.

## show restrict

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command to identify the current SN 5428 interface access restrictions.

## Examples

The following is example output from the **show restrict** command. The output shows that passwords are not enabled for the SN 5428 console. All interfaces are closed to FTP and SSL. The HA and Gigabit Ethernet interfaces are also closed to Telnet. The Gigabit Ethernet interfaces are closed to HTTP. All interfaces are open to SNMP.

```
[SN5428A]# show restrict

Interface Port Status Protocol
----- -
mgmt 21 closed ftp
 23 open telnet
 80 open http (static)
 161 open snmp
 443 closed ssl

ha 21 closed ftp
 23 closed telnet
 80 open http (static)
 161 open snmp
 443 closed ssl

ge1 21 closed ftp
 23 closed telnet
 80 closed http
 161 open snmp
 443 closed ssl
```

## ■ show restrict

```

ge2 21 closed ftp
 23 closed telnet
 80 closed http
 161 open snmp
 443 closed ssl

```

```

Console Passwords: disabled

```

**Related Commands**

| <b>Command</b>          | <b>Description</b>                                                            |
|-------------------------|-------------------------------------------------------------------------------|
| <b>restrict</b>         | Secure access to SN 5428 interfaces by communications protocols and services. |
| <b>restrict console</b> | Enable or disable password checking on the SN 5428 console interface.         |

# show route

To display all routes that have been configured, including those that have not been added to the routing table because the associated interface is not yet configured, use the **show route** command.

## show route

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command to display all routes that have been configured for the SN 5428, including routes that have been configured but have not been added to the routing table. Use the **show ip route** command to display the entire SN 5428 routing table.



**Note** A route is not added to the routing table until the associated interface is configured.

**Examples** The following is example output from the **show route** command:

```
[SN5428A]# show route
ip route default 10.1.10.201
```

| Related Commands | Command                   | Description                                                                                                                   |
|------------------|---------------------------|-------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>ip default-gateway</b> | Configure a gateway for the SN 5428's default route.                                                                          |
|                  | <b>ip route</b>           | Add a static route to the SN 5428 Storage Router routing table.                                                               |
|                  | <b>show ip</b>            | Display entries from the SN 5428 Storage Router routing table and statistics about the protocols used in the SN 5428 network. |

# show runningconfig

To display the current running configuration of the SN 5428, or save the commands used to create the running configuration to a file, use the **show runningconfig** command.

```
show runningconfig [to filename]
```

|                           |                    |                                                                                                                                                                                    |
|---------------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>to filename</b> | (Optional) Save the SN 5428's running configuration as a series of CLI commands and descriptive text in the specified file. The file will be saved in the <i>script</i> directory. |
|---------------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |       |
|-----------------|-------|
| <b>Defaults</b> | None. |
|-----------------|-------|

|                      |                           |
|----------------------|---------------------------|
| <b>Command Modes</b> | Administrator or Monitor. |
|----------------------|---------------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 2.2.1          | This command was introduced. |

**Usage Guidelines**

Use the **show runningconfig** command to display the current system configuration information as it would be saved to a configuration file. Use the **to** keyword to save the running configuration as a series of CLI commands and descriptive text in the specified file. This file is saved in the *script* directory and can be used as a basis to create command scripts to automate common tasks. Use the **read** command to execute a command script.

Table 11-30 describes the significant elements that are displayed.

**Table 11-30 Elements Displayed for the show runningconfig Command**

| <b>Element</b> | <b>Description</b>                                                              |
|----------------|---------------------------------------------------------------------------------|
| AAA            | Authentication, authorization, and accounting method configuration information. |
| ACCESSLIST     | Access list description and entry information.                                  |
| ADMIN          | The SN 5428 administrator contact information.                                  |
| ADMIN LOGIN    | The Administrator mode password.                                                |
| CDP            | Cisco Discovery Protocol configuration, including timer and holdtime settings.  |
| CLUSTER        | The name of the cluster to which this SN 5428 belongs.                          |
| DNS            | The name of any defined domain name servers.                                    |
| FC             | Global Fibre Channel attributes.                                                |
| FC Port(s)     | Operational characteristics of the Fibre Channel interfaces.                    |

**Table 11-30 Elements Displayed for the show runningconfig Command (continued)**

| Element                | Description                                                                                                                                                    |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GE                     | IP addresses and operational characteristics of the Gigabit Ethernet interfaces.                                                                               |
| HA                     | HA configuration information.                                                                                                                                  |
| HA Port                | IP address and operational characteristics of the HA interface.                                                                                                |
| LOGGING ROUTE FACILITY | The SN 5428 logging table.                                                                                                                                     |
| Mgmt Port              | IP address and operational characteristics of the management interface.                                                                                        |
| MONITOR LOGIN          | The Monitor mode password.                                                                                                                                     |
| REMOTE LOG             | Remote logging configuration information.                                                                                                                      |
| RESTRICT               | Storage router interface restrictions.                                                                                                                         |
| SCSIROUTER             | Configuration information for each SCSI routing instance, including name, description, server interface and other instance-specific configuration information. |
| SNMP                   | The SNMP settings.                                                                                                                                             |
| SNTP                   | Date and time information, including the address of any associated NTP server.                                                                                 |
| SOFTWARE               | The default download location for SN 5428 software.                                                                                                            |
| SYSTEM                 | SN 5428 Storage Router name.                                                                                                                                   |
| VLAN                   | VLAN configuration information.                                                                                                                                |
| VTP DOMAIN             | VTP domain name.                                                                                                                                               |
| VTP MODE               | VTP configuration mode.                                                                                                                                        |

**Examples**

The following is an example of output from the **show runningconfig** command, for an SN 5428 deployed for SCSI routing:

```
[SN5428A]# show runningconfig
!
! CLUSTER
!
! cluster Lab1
!
! ACCESSLIST
!
accesslist aegis
accesslist aegis 10.2.0.23/255.255.255.255
accesslist aegis 10.3.0.36/255.255.255.255
accesslist aegis 10.4.0.49/255.255.255.255
accesslist aegis iscsi-name ign.1987-05.com.cisco.08.80342789af73ebcdef123.xxx
accesslist aegis iscsi-name ign.1987-05.com.cisco.08.7125abc9af73ebcdef123.xxx
accesslist aegis iscsi-name ign.1987-05.com.cisco.08.1234abecf9876bac00034.xxx
accesslist aegis chap-usermane 12h7b.lab2.webservices
accesslist aegis chap-username dorothy
accesslist aegis chap-username lab2servp
!
```

```

! VTP DOMAIN
!
vtp domain none
!
! VTP MODE
!
vtp mode client
!
! VLAN
!
! (no vlan(s) found)
!
! SCSIROUTER
!
scsirouter zeus
scsirouter zeus authenticate "none"
scsirouter zeus primary "none"
scsirouter zeus reserve proxy disable
scsirouter zeus failover primary none
scsirouter zeus failover secondary none
scsirouter zeus lun reset no
scsirouter zeus serverIf ge1 10.1.0.45/255.255.255.0
scsirouter zeus target webserver2 wwpn "21:00:00:05:ae:03:6d:6e"
scsirouter zeus target webserver2 enabled
scsirouter zeus target webserver2 accesslist "aegis"
!
! SYSTEM
!
hostname SN5428A
!
! Mgmt Port
!
interface mgmt ip-address 10.1.10.244/255.255.255.0
!
! HA Port
!
interface ha ip-address 10.1.20.56/255.255.255.0
! GE
!
interface ge2 mtusize 1500
interface ge2 autonegotiation autodetect
interface ge2 vlan enable
!
! GE
!
interface ge1 mtusize 1500
interface ge1 autonegotiation autodetect
interface ge1 vlan enable
!!
! ROUTES
!
ip route 10.1.30.0/255.255.255.0 10.1.10.201
ip route 10.1.40.243/255.255.255.255 10.1.10.201
ip route 10.1.50.249/255.255.255.255 10.1.10.201
ip default-gateway 10.1.10.201
!
! ADMIN LOGIN
!
admin password <password>
!
! MONITOR LOGIN
!
monitor password <password>
!

```

```
! SNTP
!
clock timezone CST6CDT
ntp peer 10.1.60.86
!
! SNMP
!
snmp-server community public ro
snmp-server community private rw
no snmp-server host all traps
no snmp-server sendauthtraps
snmp-server linkupdown mgmt
snmp-server linkupdown ge1
snmp-server linkupdown ge2
snmp-server linkupdown fc1
snmp-server linkupdown fc2
snmp-server linkupdown fc3
snmp-server linkupdown fc4
snmp-server linkupdown fc5
snmp-server linkupdown fc6
snmp-server linkupdown fc7
snmp-server linkupdown fc8
!
! DNS
!
ip name-server 10.1.40.243 10.1.50.249
ip domain-name mystoragenet.com
!
! SOFTWARE
!
software http url "http://www.cisco.com"
software http username "ciscocustomer" password "<password>"
software proxy username none
!
! CDP
!
cdp enable
cdp timer 60
cdp holdtime 180
cdp interface mgmt enable
cdp interface ha enable
cdp interface ge1 enable
cdp interface ge2 enable
!
! HA
!
! ha configuration clustered
!
! LOGGING ROUTE FACILITY
!
logging level info from all to console logfile
logging level debug from HA to logfile
!
! RESTRICT
!
restrict mgmt ftp
no restrict mgmt telnet
no restrict mgmt http
no restrict mgmt snmp
restrict mgmt rlogin
no restrict mgmt ssl
!
```

```

restrict ha ftp
restrict ha telnet
no restrict ha http
no restrict ha snmp
restrict ha rlogin
restrict ha ssl
!
restrict ge1 ftp
restrict ge1 telnet
restrict ge1 http
restrict ge1 snmp
restrict ge1 rlogin
restrict ge1 ssl
!
restrict ge2 ftp
restrict ge2 telnet
restrict ge2 http
restrict ge2 snmp
restrict ge2 rlogin
restrict ge2 ssl
!
!
! FC
!
interface fc zoning default all
interface fc zoning autosave enable
interface fc domainid 1
no interface fc domainid lock enable
interface fc interop-credit 12
!
! FC Port(s)
!
interface fc1 enable
no interface fc1 al-fairness enable
interface fc1 fan-enable enable
interface fc1 mfs-bundle enable timeout 10
interface fc1 linkspeed auto
interface fc1 type gl-port
!
interface fc2 enable
no interface fc2 al-fairness enable
interface fc2 fan-enable enable
interface fc2 mfs-bundle enable timeout 10
interface fc2 linkspeed auto
interface fc2 type gl-port
!
interface fc3 enable
no interface fc3 al-fairness enable
interface fc3 fan-enable enable
interface fc3 mfs-bundle enable timeout 10
interface fc3 linkspeed auto
interface fc3 type gl-port
!
interface fc4 enable
no interface fc4 al-fairness enable
interface fc4 fan-enable enable
interface fc4 mfs-bundle enable timeout 10
interface fc4 linkspeed auto
interface fc4 type gl-port
!

```

```

interface fc5 enable
no interface fc5 al-fairness enable
interface fc5 fan-enable enable
interface fc5 mfs-bundle enable timeout 10
interface fc5 linkspeed auto
interface fc5 type gl-port
!
interface fc6 enable
no interface fc6 al-fairness enable
interface fc6 fan-enable enable
interface fc6 mfs-bundle enable timeout 10
interface fc6 linkspeed auto
interface fc6 type gl-port
!
interface fc7 enable
no interface fc7 al-fairness enable
interface fc7 fan-enable enable
interface fc7 mfs-bundle enable timeout 10
interface fc7 linkspeed auto
interface fc7 type gl-port
!
interface fc8 enable
no interface fc8 al-fairness enable
interface fc8 fan-enable enable
interface fc8 mfs-bundle enable timeout 10
interface fc8 linkspeed auto
interface fc8 type gl-port

! AAA
!
aaa new-model
aaa authentication iscsi default local group radius local-case
username "fred" password "9 af4f2428498a41a31e237de1c4a9b9fcef"
username "pat" password "9 7dbccc3d0daf013f4293c3d3bd94539dd"
username "kris" password "9 0607167520058771e66ab1d379d7e6505f"
username "adrian" password "9 0ad24a3b35dc296d894e512416d572b3ee"
radius-server retransmit 12
radius-server host 10.5.0.53 auth-port 1645
tacacs-server timeout 12
tacacs-server host 10.7.0.22 auth-port 49

```

The following example creates a command file called *SN5428A\_script2* in the *script* directory. It contains many of the CLI commands that were issued to create the SN 5428's current running configuration.

```
[SN5428A]# show runningconfig to SN5428A_script2
```

### Related Commands

| Command                 | Description                                                                                                           |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>read</b>             | Read and execute the CLI commands in the named script file.                                                           |
| <b>restore all</b>      | Restore the contents of the named configuration file into memory.                                                     |
| <b>save all</b>         | Save all configuration information                                                                                    |
| <b>show bootconfig</b>  | Display the SN 5428's bootable configuration, or create a command file based on the SN 5428's bootable configuration. |
| <b>show savedconfig</b> | List the contents of the savedconfig directory or the contents of the named configuration file.                       |
| <b>show script</b>      | Display the contents of the script directory or the contents of the named command file.                               |

# show savedconfig

To list the available files in the *savedconfig* directory or to view the contents of a specific configuration file, use the **show savedconfig** command. Configuration files are stored in the *savedconfig* directory.

```
show savedconfig [filename]
```

|                           |                 |                                                                                                                                                      |
|---------------------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>filename</i> | (Optional) The name of the configuration file to display. This file must exist in the <i>savedconfig</i> directory and be in the appropriate format. |
|---------------------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |       |
|-----------------|-------|
| <b>Defaults</b> | None. |
|-----------------|-------|

|                      |                           |
|----------------------|---------------------------|
| <b>Command Modes</b> | Administrator or Monitor. |
|----------------------|---------------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 2.2.1          | This command was introduced. |

**Usage Guidelines**

Use this command to display a list of configuration files in the *savedconfig* directory before attempting a restore. Use the *filename* parameter to view the contents of the specified configuration file. You can also use the **show scsirouter from** or **show accesslist from** commands to display specific objects from the named configuration file, allowing you to verify that the object of your **restore** command exists in the selected file.

**Examples**

The following is example output from the **show savedconfig** command:

```
[SN5428A]# show savedconfig
Config_Nov122001
Config_Jul172001
Special_Config
AccessList_Config
```

The following is example output from the **show savedconfig** command using the *filename* parameter:

```
[SN5428A]# show savedconfig AccessList_Config
!
! CLUSTER
!
cluster Lab1
!
! ACCESSLIST
!
accesslist aegis
accesslist aegis 10.2.0.23/255.255.255.255
accesslist aegis 10.3.0.36/255.255.255.255
accesslist aegis 10.4.0.49/255.255.255.255
```

**Related Commands**

| <b>Command</b>            | <b>Description</b>                                                                                                          |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>copy</b>               | Copy the named configuration or script file from a remote location to the SN 5428 or from the SN 5428 to a remote location. |
| <b>delete savedconfig</b> | Remove a saved configuration file from the SN 5428.                                                                         |
| <b>restore aaa</b>        | Restore AAA authentication services from a saved configuration file.                                                        |
| <b>restore accesslist</b> | Restore the named access list or all access lists from the named configuration file.                                        |
| <b>restore all</b>        | Restore the contents of the named configuration file into memory.                                                           |
| <b>restore scsirouter</b> | Restore the named SCSI routing instance from the named configuration file.                                                  |
| <b>restore system</b>     | Restore selected system information from the named configuration file.                                                      |
| <b>restore vlan</b>       | Restore VLAN configuration information from the named configuration file.                                                   |
| <b>save aaa</b>           | Save the current AAA configuration information.                                                                             |
| <b>save accesslist</b>    | Save configuration data for the named access list or all access lists.                                                      |
| <b>save all</b>           | Save all configuration information.                                                                                         |
| <b>save scsirouter</b>    | Save configuration information for the named SCSI routing instance.                                                         |
| <b>save system</b>        | Save selected system configuration information.                                                                             |
| <b>save vlan</b>          | Save configuration information for the named VLAN or all VLANs.                                                             |
| <b>show bootconfig</b>    | Display the SN 5428's bootable configuration, or create a command file based on the SN 5428's bootable configuration.       |
| <b>show runningconfig</b> | Display the SN 5428's running configuration, or create a command file based on the SN 5428's running configuration.         |

# show script

To list the available files in the *script* directory or to view the contents of a specific command file, use the **show script** command. Configuration files are stored in the *script* directory.

```
show script [filename]
```

|                           |                 |                                                                                                          |
|---------------------------|-----------------|----------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>filename</i> | (Optional) The name of the command file to display. This file must exist in the <i>script</i> directory. |
|---------------------------|-----------------|----------------------------------------------------------------------------------------------------------|

|                 |       |
|-----------------|-------|
| <b>Defaults</b> | None. |
|-----------------|-------|

|                      |                           |
|----------------------|---------------------------|
| <b>Command Modes</b> | Administrator or Monitor. |
|----------------------|---------------------------|

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

|                         |                                                                                                                                                                                                                                                         |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | Use this command to display a list of files in the <i>script</i> directory before attempting to execute the commands in the script using the <b>read</b> command. Use the <i>filename</i> parameter to view the contents of the specified command file. |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |                                                                      |
|-----------------|----------------------------------------------------------------------|
| <b>Examples</b> | The following is example output from the <b>show script</b> command: |
|-----------------|----------------------------------------------------------------------|

```
[SN5428A]# show script
MyScriptFile
Lab1_Script
Test_12Nov
MyBoot
```

| Related Commands | Command     | Description                                                                                                                 |
|------------------|-------------|-----------------------------------------------------------------------------------------------------------------------------|
|                  | <b>copy</b> | Copy the named configuration or script file from a remote location to the SN 5428 or from the SN 5428 to a remote location. |
|                  | <b>read</b> | Read and execute the CLI commands in the named script file.                                                                 |

# show scsirouter

To display configuration information and operational statistics related to the named SCSI routing instance or all instances, use the **show scsirouter** command.

**show scsirouter**

**show scsirouter** *name* **all**

**show scsirouter** {*name* | **all**} [**from** {**bootconfig** | **runningconfig** | *filename*}]

**show scsirouter** {*name* | **all**} **brief**

**show scsirouter** {*name* | **all**} **connection** [**stats** | **tcp**]

**show scsirouter** {*name* | **all**} **serverif** [**from** {**bootconfig** | **runningconfig** | *filename*}]

**show scsirouter** {*name* | **all**} **failover**

**show scsirouter** {*name* | **all**} **host** [**stats** | **table**]

**show scsirouter** {*name* | **all**} **stats**

**show scsirouter** {*name* | **all**} **target** {*name* | **all**} [**from** {**bootconfig** | **runningconfig** | *filename*} | **stats**]

**show scsirouter** {*name* | **all**} **target table**

## Syntax Description

|                           |                                                                                                                                                                                                                                                                                          |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>               | The name of the SCSI routing instance or the name of the target.                                                                                                                                                                                                                         |
| <i>name</i> <b>all</b>    | Display all configuration information for the specified SCSI routing instance.                                                                                                                                                                                                           |
| <b>all</b>                | Display the requested information for all SCSI routing instances or all targets.                                                                                                                                                                                                         |
| <b>from bootconfig</b>    | (Optional) Display the requested configuration information from the persistent saved configuration. Use this keyword string to display complete configuration information for a SCSI routing instance from any SN 5428 in a cluster, even if the instance is not active on that SN 5428. |
| <b>from runningconfig</b> | (Optional) Display the requested configuration information from the currently running configuration.                                                                                                                                                                                     |
| <b>from filename</b>      | (Optional) The name of the saved configuration file containing the specified SCSI routing instance information. This file must exist in the <i>savedconfig</i> directory.                                                                                                                |
| <b>brief</b>              | (Optional) Display brief configuration information.                                                                                                                                                                                                                                      |
| <b>connection</b>         | (Optional) Display connection information for the named SCSI routing instance.                                                                                                                                                                                                           |
| <b>failover</b>           | (Optional) Display the HA failover list for the named SCSI routing instance.                                                                                                                                                                                                             |
| <b>host</b>               | (Optional) Display status and other operational data for IP hosts currently connected to the named SCSI routing instance.                                                                                                                                                                |
| <b>host table</b>         | (Optional) Display information about all IP hosts that have attempted to connect to the named SCSI routing instance.                                                                                                                                                                     |

|                     |                                                                                                                                                                                                                                                |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>serverif</b>     | (Optional) Display configuration information for the Gigabit Ethernet interface associated with the named SCSI routing instance.                                                                                                               |
| <b>stats</b>        | (Optional) Display accumulated operational information for the SCSI routing instance. This display shows statistics accumulated since the named SCSI routing instance became active or statistics were last cleared, whichever is more recent. |
| <b>target</b>       | (Optional) Display configuration information related to targets (including the iSCSI Name) associated with the named SCSI routing instance.                                                                                                    |
| <b>target table</b> | Display all targets, target status, and access list associations for the specified SCSI routing instance or all instances, in table format.                                                                                                    |
| <b>tcp</b>          | (Optional) Display current and maximum TCP window size for each connected IP host.                                                                                                                                                             |

### Defaults

The **show scsirouter** command with no parameters displays the name of each SCSI routing instance running on this SN 5428. When no **from** parameters are specified, the information displayed is from the currently running configuration.

### Command Modes

Administrator or Monitor

### Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

### Usage Guidelines

In a cluster environment, a SCSI routing instance can only be active on one SN 5428 at a time. Issue the appropriate **show** commands from the SN 5428 that is running the instance to display complete configuration information and operational statistics. If you issue **show** commands from an SN 5428 that is not running the instance, operational statistics are not available and configuration information is truncated.



#### Timesaver

To display complete configuration information for a SCSI routing instance from any SN 5428 in a cluster, even if that SCSI routing instance is not active on that SN 5428, use the command **show scsirouter name from bootconfig**.

Use the optional **target** or **serverif** keyword to restrict the display to configuration information related to those objects. For example:

- The command **show scsirouter name target** displays current configuration information, including access list and iSCSI Name, for all targets associated with the named SCSI routing instance.
- The command **show scsirouter all serverif** displays current configuration information for the Gigabit Ethernet interfaces associated with all SCSI routing instances.

Use the **connection** or **host** keyword to display specific operational data for the named SCSI routing instance.

- The command **show scsirouter name host stats** displays IP host status and operational statistics for currently connected IP hosts for the named SCSI routing instance.

- The command **show scsirouter name host table** displays iSCSI Name, alias, IP address and CHAP user name (if any) for all IP hosts that have attempted to access the named SCSI routing instance. If you are going to use iSCSI Name entries for access control, you can use this command to obtain or verify the iSCSI Name of your IP hosts.
- The command **show scsirouter name stats** displays accumulated operational information about all IP hosts that have been connected since the named instance became active. Operational statistics include login information, information about the version of compatible iSCSI drivers, and other status information.
- The command **show scsirouter all connection stats** displays connection statistics for all SCSI routing instances.
- The **show scsirouter all stats** command is useful for determining quick operational status of all instances running in the SN 5428.
- Use the **show scsirouter all** command to display configuration information for all SCSI routing instances, including descriptions, targets and associated access lists.

## Examples

The following is example output from the **show scsirouter** command:

```
[SN5428A]# show scsirouter
foo
foo2
```

The following is example output from the **show scsirouter stats** command. The status of SCSI routing instance *jdb1* indicates that it is running on another SN 5428 in the cluster.

```
[SN5428A]# show scsirouter all stats

router status started iSCSI ver (Min/Max) logins active
foo2 ACTIVE Jan 09 22:17:28 2/2 10 7
jdb1 INACTIVE-slave
```

Table 11-31 describes the significant fields in the display.

**Table 11-31 Description of Fields in the show scsirouter stats Command Output**

| Field               | Description                                                                                                                                                                                                                                                                           |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| router              | The name of the SCSI routing instance.                                                                                                                                                                                                                                                |
| status              | Indicates if the instance is active or inactive. If the SCSI routing instance was explicitly disabled, the status will be “INACTIVE”, with no additional information shown. If the SCSI routing instance is running on another node in the cluster, the status will “INACTIVE-slave.” |
| started             | The date and time the SCSI routing instance was last started.                                                                                                                                                                                                                         |
| iSCSI ver (Min/Max) | The iSCSI draft version information (minimum and maximum version that can be used with the SCSI routing instance).                                                                                                                                                                    |
| logins              | Total number of logins attempted.                                                                                                                                                                                                                                                     |
| active              | Total number of active connections.                                                                                                                                                                                                                                                   |

The following is example output from the **show scsirouter all host table** command. If you are going to use iSCSI Name entries for access control, you can configure your IP hosts and attempt to access the desired SCSI routing instance. Then issue this command to display the iSCSI Name information, which can be used to populate the desired access list.

```
[SN5428A]# show scsirouter all host table
Name: iqn.1987-05.com.cisco.01.27a2410eaed4affa82a81143d70ce10
Alias: lab1
IP: 10.2.0.23
CHAP username: 742Nlab1
```

### Related Commands

| Command                          | Description                                                                                                |
|----------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>accesslist</b>                | Create an access list entity.                                                                              |
| <b>accesslist A.B.C.D/bits</b>   | Add IP addresses to an access list.                                                                        |
| <b>clear counters scsirouter</b> | Reset accumulated operational statistics for the specified SCSI routing instance.                          |
| <b>delete scsirouter</b>         | Delete the named SCSI routing instance or the specified element of the SCSI routing instance.              |
| <b>restore accesslist</b>        | Restore the named access list or all access lists from the named configuration file.                       |
| <b>restore scsirouter</b>        | Restore the named SCSI routing instance from the named configuration file.                                 |
| <b>save accesslist</b>           | Save configuration data for the named access list or all access lists.                                     |
| <b>save scsirouter</b>           | Save configuration information for the named SCSI routing instance.                                        |
| <b>save system</b>               | Save selected system configuration information.                                                            |
| <b>scsirouter enable</b>         | Stop or start the named SCSI routing instance.                                                             |
| <b>scsirouter failover</b>       | Add the SN 5428 to the HA failover list for the specified SCSI routing instance.                           |
| <b>scsirouter serverif</b>       | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
| <b>setup scsi</b>                | Run the wizard to configure a SCSI routing instance.                                                       |

# show sessions

To display information about active Telnet or GUI sessions to the SN 5428, use the **show sessions** command.

```
show sessions {all | cli | gui}
```

| Syntax Description | all | Description                                                   |
|--------------------|-----|---------------------------------------------------------------|
|                    | all | Display all active SN 5428 Telnet or GUI management sessions. |
|                    | cli | Display only active CLI sessions.                             |
|                    | gui | Display only active GUI sessions.                             |

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** There are a maximum of 16 concurrent CLI management sessions per SN 5428.

**Examples** The following is example output from the **show sessions** command. The asterisk designates the CLI management session from which the command was issued.

```
[SN5428A]# show sessions all
```

```

 Id Auth From Login
 --- -
 1 monitor console Mar 22 17:19:10 [TELNET]
 * 2 admin 10.1.40.212 Mar 22 11:44:46 [TELNET]
 3 admin 10.3.12.222 Mar 22 11:47:12 [GUI]
```

| Related Commands | Command                 | Description                                                                           |
|------------------|-------------------------|---------------------------------------------------------------------------------------|
|                  | <b>admin password</b>   | Set the login password for administrative access to the SN 5428 management interface. |
|                  | <b>monitor password</b> | Set the login password for view-only access to the SN 5428 management interface.      |

# show snmp

To display SNMP management configuration information for the SN 5428, use the **show snmp** command.

## show snmp

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use the **show snmp** command to review the SNMP configuration settings before changing those settings with the **snmp-server** command.

The command displays IP addresses of the destination hosts used for notifications (traps), the name of the SNMP community having read access to the SN 5428 network (get-community), and the name of the community having write access to the SN 5428 network (set-community), the version of traps to be sent, and configuration information for Send Authentication and Link Up/Down traps.

**Examples** The following is example output from the **show snmp** command:

```
[SN5428A]$ show snmp
First Trap Host: 10.1.30.17, will be sent version 1 traps
Second Trap Host: <none found or defined>
Get Community String: public
Set Community String: mynetmanagers
Send Authentication Traps: enabled
Link Up/Down Enable for mgmt: enabled
Link Up/Down Enable for ha: disabled
Link Up/Down Enable for fc1: enabled
Link Up/Down Enable for fc2: enabled
Link Up/Down Enable for fc3: disabled
Link Up/Down Enable for fc4: enabled
Link Up/Down Enable for fc5: disabled
Link Up/Down Enable for fc6: enabled
Link Up/Down Enable for fc7: enabled
Link Up/Down Enable for fc8: disabled
Link Up/Down Enable for ge1: enabled
Link Up/Down Enable for ge2: enabled
```

| Related Commands | Command       | Description                                     |
|------------------|---------------|-------------------------------------------------|
|                  | setup netmgmt | Run the wizard to configure network management. |
|                  | snmp-server   | Configure the SN 5428 for SNMP management.      |

# show software version

To display a list of software versions available on the SN 5428, use the **show software version** command.

**show software version {all | boot | current | x.x.y}**

| Syntax Description |                |                                                                                                   |
|--------------------|----------------|---------------------------------------------------------------------------------------------------|
|                    | <b>all</b>     | Display information about all versions of software available on the SN 5428.                      |
|                    | <b>boot</b>    | Display only information about the version of software that will run when the system is rebooted. |
|                    | <b>current</b> | Display only information about the version of software that is currently running on the SN 5428.  |
|                    | <i>x.x.y</i>   | Display information about the specified software version.                                         |

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use the **show software version all** command to display the size of each version of software and the date and time it was built. The display also shows the version of software currently running and the version which will be booted when the system is reset. It includes the protocol and default location from which new software is available for download and the amount of disk space currently available for new software.



**Note** A maximum of two versions of software can be stored on the SN 5428.

**Examples**

The following is example output from the **show software version all** command:

```
[SN5428A]# show software version all

Version Boot Hash Sign Crash Size Date

2.3.1 OK OK N/A 1 19456240 May 10 09:57 CDT 2002

 Http Url: http://www.cisco.com
 Http Username: phurley
 Http Password: *****

 Proxy Address:
 Proxy Port:
 Proxy Url:
 Proxy Username:
 Proxy Password:

 Tftp Hostname:
 Tftp Directory:

Disk Space Available: 13357.0 KB
Current Version: 2.3.1
Boot Version: 2.3.1
```

**Related Commands**

| Command                        | Description                                                                                                    |
|--------------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>delete software version</b> | Remove the specified version of software from the SN 5428.                                                     |
| <b>download software</b>       | Download the list of available software versions or the specified version of software from the named location. |
| <b>save all</b>                | Save all configuration information.                                                                            |
| <b>save system</b>             | Save selected system configuration information.                                                                |
| <b>software version</b>        | Specify the version of software to run when the SN 5428 is restarted.                                          |
| <b>verify software version</b> | Check the specified software version for problems.                                                             |

# show stack

To display usage of the stack on a per-task basis, use the **show stack** command.

## show stack

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator and Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** The **show stack** command is designed for debug purposes and should be used under the guidance of a Cisco Technical Support professional.

**Examples** The following is example output from the **show stack** command:

```
[techpubs2]# show stack
Stack Usage by Task
```

| NAME          | ENTRY        | TID     | SIZE  | CUR  | HIGH  | MARGIN |
|---------------|--------------|---------|-------|------|-------|--------|
| tRootTask     | usrRoot      | e7ffdf8 | 19440 | 192  | 2368  | 17072  |
| tExcTask      | excTask      | dfef3b8 | 7984  | 240  | 936   | 7048   |
| tLogTask      | logTask      | dffba30 | 4984  | 224  | 968   | 4016   |
| tCrashDump    | crashDumpTas | d5c7320 | 4080  | 160  | 224   | 3856   |
| utilMonitor   | 0x000d57d3c4 | c9e68c8 | 9984  | 296  | 816   | 9168   |
| tShell        | shell        | d6fbca0 | 39056 | 464  | 1000  | 38056  |
| tWdbTask      | 0x00000af940 | d6fded8 | 7912  | 456  | 656   | 7256   |
| qlFc1         | QlogicFC::sc | cb0fde8 | 9992  | 200  | 1432  | 8560   |
| qlFc2         | QlogicFC::sc | caa4de8 | 9992  | 200  | 1432  | 8560   |
| tAuthServ     | authServerTa | c970bb8 | 15984 | 432  | 872   | 15112  |
| tFtpdTask     | 0x00000d3114 | d718740 | 11984 | 336  | 400   | 11584  |
| wancomTask    | wancomTask   | d7e2de8 | 1984  | 160  | 432   | 1552   |
| wancomTask    | wancomTask   | d6e4e28 | 1984  | 160  | 408   | 1576   |
| wancomTask    | wancomTask   | cd2f328 | 1984  | 160  | 408   | 1576   |
| HA_main       | HA_main_task | ca34878 | 9992  | 376  | 648   | 9344   |
| tEventManager | 0x000d5b0830 | ccf8bf0 | 16368 | 568  | 10536 | 5832   |
| tNuLogWatche  | tNuLogWatche | ccf49d8 | 16368 | 592  | 1176  | 15192  |
| VTP           | Vtp::task(vo | c979ee0 | 9992  | 256  | 696   | 9296   |
| tSnmpd        | 0x0000049fe4 | ca10d38 | 28664 | 1920 | 2472  | 26192  |
| tProtoCDP     | cdp_prot(voi | c97e758 | 16368 | 272  | 3304  | 13064  |
| HA_newcfg     | HA_newcfg_ta | ca3e330 | 15984 | 200  | 280   | 15704  |
| HA_monitor    | HA_monitor_t | ca3a298 | 5984  | 184  | 672   | 5312   |
| HA_appctrl    | HA_appctrl_t | ca38910 | 15984 | 240  | 6040  | 9944   |

```

hdwMonitor 0x000d313acc ca46de8 9984 144 928 9056
sensorMntr entitySensor ca09b20 9984 152 216 9768
tSnmpTmr 0x0000049d50 ca11f50 4080 248 312 3768
tSMLMgr 0x000d4e6300 ca06e98 9992 3736 4528 5464
tfeTask ScsiTargetGl c920d80 9992 176 720 9272
scsiTcp ScsiTcpServe c91e2a0 9992 512 1040 8952
ReadOneSecto 0x00000371c4 dff8028 19984 200 448 19536
WriteOneSect 0x0000037460 dff2ff0 19984 200 352 19632
tNetTask netTask d7f19e0 9984 208 1688 8296
ui tEmWeb c9eeae0 32760 1472 16016 16744
tFcSwMon FcSwApp: :fcs c96b0d0 7984 344 4200 3784
idleTask 0x000d57d6b8 c9e3d98 9984 168 512 9472
INTERRUPT 5000 0 696 4304

```

Table 11-32 describes the fields in the display.

**Table 11-32 Description of Fields in the show stack Command Output**

| Field  | Description                                                             |
|--------|-------------------------------------------------------------------------|
| NAME   | The name of the task.                                                   |
| ENTRY  | The task entry point.                                                   |
| TID    | The task ID.                                                            |
| SIZE   | The maximum size of the task, in bytes.                                 |
| CUR    | The current size of the task.                                           |
| HIGH   | The largest size of the task since the SN 5428 was last started.        |
| MARGIN | The margin between the size of the task and the size in the HIGH field. |

#### Related Commands

| Command                  | Description                                                                                   |
|--------------------------|-----------------------------------------------------------------------------------------------|
| <b>show buffers</b>      | Display information about SN 5428 buffer pools.                                               |
| <b>show memory</b>       | Display information about SN 5428 memory and related resources.                               |
| <b>show modules</b>      | Display addressing information related to the SN 5428 software modules.                       |
| <b>show task</b>         | Display information about the tasks running in the SN 5428.                                   |
| <b>show tech-support</b> | Display a variety of diagnostic information for use by Cisco Technical Support professionals. |

# show system

To display a variety of system information about the SN 5428, including system name and deployment option, use the **show system** command. A table of information about SN 5428 network interfaces also displays.

## show system

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use the **show system** command to quickly display information about the SN 5428 system configuration, including system name, current software version, date and time, NTP server, name server and domain information.

**Examples** The following is example output from the **show system** command:

```
[SN5428A]# show system
 System Name: SN5428A
 System Deployed For: SCSI routing
 Software Capacity: 37888.0 KB
 Free Software Space: 13357.0 KB
 Configuration Capacity: 8128.0 KB
 Free Configuration Space: 7904.0 KB
 Log Capacity: 8128.0 KB
 Free Log Space: 7866.0 KB
 Software Version: 2.3.1
 Last Reset: Tue May 14 20:40:53 GMT 2002
 Current Time: Tue May 14 22:30:57 GMT 2002
 Time Zone: GMT
 NTP Server: 10.1.60.86
 Name Servers: 10.1.40.243 (Pri) 10.1.50.249 (Sec)
 Domain: mystoragenet.com

 Model Number Rev Serial Number
 System SN5428 01 MGV0620026H-05
 Processor RAINMAKER 01 SAP0620026H
```

```

Device IP/Netmask MAC
lo0 127.0.0.1/8 00:00:00:00:00:00
mgmt 10.1.10.244/24 00:01:2c:06:13:70
ha 10.1.20.56/24 00:01:64:40:ef:c1
ge1
ge2 10.1.0.45/24 02:02:3d:01:1c:a5

```

Table 11-33 describes the fields in the display.

**Table 11-33 Description of Fields in the show system Command Output**

| Field                    | Description                                                                                        |
|--------------------------|----------------------------------------------------------------------------------------------------|
| System Name              | The name of the SN 5428.                                                                           |
| Software Capacity        | The amount of space allocated for SN 5428 software, in kilobytes.                                  |
| Free Software Space      | Total software capacity currently available, in kilobytes.                                         |
| Configuration Capacity   | The amount of space allocated for SN 5428 configuration files, in kilobytes.                       |
| Free Configuration Space | Total configuration capacity currently available, in kilobytes.                                    |
| Log Capacity             | The amount of space allocated for SN 5428 log files, in kilobytes.                                 |
| Free Log Space           | Total log capacity currently available, in kilobytes.                                              |
| Software Version         | The version of software that is currently running, such as 2.3.1.                                  |
| Last Reset               | The date and time the system was last reset.                                                       |
| Current Time             | The current date and time.                                                                         |
| Time Zone                | The time zone in which this SN 5428 is located.                                                    |
| NTP Server               | The IP address of the time server.                                                                 |
| Name Server              | The IP address of the primary and secondary DNS servers.                                           |
| Domain                   | The domain to which the SN 5428 belongs.                                                           |
| Model Number             | The model number for the SN 5428, processor, and Fibre Channel and Gigabit Ethernet interfaces.    |
| Rev                      | The revision number for the SN 5428, processor, and Fibre Channel and Gigabit Ethernet interfaces. |
| Serial Number            | The serial number for the SN 5428, processor, and Fibre Channel and Gigabit Ethernet interfaces.   |
| Device                   | The name of the SN 5428 interface.                                                                 |
| IP/Netmask               | The IP address and subnet mask associated with the named interface.                                |
| MAC                      | The machine address associated with the named interface.                                           |

#### Related Commands

| Commands              | Description                                                                                             |
|-----------------------|---------------------------------------------------------------------------------------------------------|
| <b>hostname</b>       | Specify the SN 5428 system name.                                                                        |
| <b>ip name-server</b> | Specify the IP addresses of a primary (and optional secondary) DNS.                                     |
| <b>logging #?</b>     | Enable remote logging to the specified IP host.                                                         |
| <b>ntp peer</b>       | Specify the name or IP address of the NTP server with which the SN 5428 will synchronize date and time. |

| <b>Commands</b>                | <b>Description</b>                                                    |
|--------------------------------|-----------------------------------------------------------------------|
| <b>save all</b>                | Save all configuration information.                                   |
| <b>software version</b>        | Specify the version of software to run when the SN 5428 is restarted. |
| <b>verify software version</b> | Check the specified software version for problems.                    |

# show task

To display information about tasks running in the SN 5428, issue the **show task** command.

```
show task {all | task-id}
```

| Syntax Description | all            | Display information about all running tasks.                                 |
|--------------------|----------------|------------------------------------------------------------------------------|
|                    | <i>task-id</i> | The TID for a specific task, obtained from the <b>show task all</b> display. |

**Defaults** None.

**Command Modes** Administrator and Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use the **show task** command to view priority, status, and error information for all tasks, and register and stack trace information for a specific task. The **show task** command is designed for debug purposes and should be used under the guidance of a Cisco Technical Support professional.

**Examples** The following is example output from the **show task all** command:

```
[SN5428A]# show task all
Running Tasks
```

| NAME         | ENTRY        | TID     | PRI | STATUS | PC     | SP       | ERRNO  | DELAY |
|--------------|--------------|---------|-----|--------|--------|----------|--------|-------|
| tRootTask    | usrRoot      | e7ffdf8 | 0   | DELAY  | bd414  | e7ffdf38 | 30065  | 40    |
| tExcTask     | excTask      | dfef3b8 | 0   | PEND   | 117534 | dfef2c8  | 3006b  | 0     |
| tLogTask     | logTask      | dfbfa30 | 0   | PEND   | 117534 | dfb950   | 0      | 0     |
| tCrashDump   | crashDumpTa  | d5c7320 | 0   | PEND   | b8a08  | d5c7280  | 0      | 0     |
| utilMonitord | 57d3c4       | c9e68c8 | 1   | DELAY  | bd414  | c9e67a0  | 0      | 39    |
| tShell       | shell        | d6fbca0 | 1   | PEND   | 117534 | d6fbad0  | d0003  | 0     |
| tWdbTask     | af940        | d6fded8 | 3   | PEND   | b8a08  | d6fdd10  | 0      | 0     |
| qlFc1        | scsiTask__8Q | cb0fde8 | 45  | PEND+T | b8a08  | cb0fd20  | 3d0004 | 72    |
| qlFc2        | scsiTask__8Q | caa4de8 | 45  | PEND+T | b8a08  | caa4d20  | 3d0004 | 72    |
| tAuthServ    | authServerTa | c970bb8 | 50  | PEND   | b8a08  | c970a08  | 0      | 0     |
| tFtpdTask    | d3114        | d718740 | 55  | PEND   | b8a08  | d7185f0  | 0      | 0     |
| wancomTask   | wancomTask   | d7e2de8 | 60  | PEND   | b8a08  | d7e2d48  | 0      | 0     |
| wancomTask   | wancomTask   | d6e4e28 | 60  | PEND   | b8a08  | d6e4d88  | 0      | 0     |
| wancomTask   | wancomTask   | cd2f328 | 60  | PEND   | b8a08  | cd2f288  | 0      | 0     |
| HA_main      | HA_main_task | ca34878 | 77  | PEND   | b8a08  | ca34700  | 0      | 0     |
| tEventMgr    | d5b0830      | ccf8bf0 | 78  | PEND   | 117534 | ccf89b8  | 3d0004 | 0     |
| tNuLogWatch  | tNuLogWatche | ccf49d8 | 78  | PEND   | 117534 | ccf4788  | c0002  | 0     |
| VTP          | task__3Vtp   | c979ee0 | 80  | PEND   | 117534 | c979de0  | 0      | 0     |
| tSnpmd       | 49fe4        | ca10d38 | 150 | PEND   | b8a08  | ca105b8  | 0      | 0     |

## show task

```

tProtoCDP cdp_prot__Fv c97e758 150 PEND 117534 c97e648 0 0
HA_newcfg HA_newcfg_ta ca3e330 160 DELAY bd414 ca3e268 0 129
HA_monitor HA_monitor_t ca3a298 160 DELAY bd414 ca3a1e0 0 129
HA_appctrl HA_appctrl_t ca38910 160 PEND 117534 ca38820 380003 0
hdwMonitor d313acc ca46de8 180 DELAY bd414 ca46d58 0 12030
sensorMntr entitySensor ca09b20 180 PEND b8a08 ca09a88 0 0
tSnmpTmr 49d50 ca11f50 200 PEND 117534 calle58 0 0
tSMLMgr d4e6300 ca06e98 200 PEND+T b8a08 ca06000 3d0004 34
tfeTask tfeTask__19S c920d80 200 DELAY bd414 c920cd0 0 38
scsiTcp task__13Scsi c91e2a0 201 PEND b8a08 c91e0a0 0 0
ReadOneSect 371c4 dff8028 202 PEND b8a08 dff7f60 0 0
WriteOneSec 37460 dff2ff0 202 PEND b8a08 dff2f28 0 0
tNetTask netTask d7f19e0 202 PEND b8a08 d7f1910 0 0
ui tEmWeb c9eeae0 203 READY bde84 c9ed9c8 0 0
tFcSwMon fcswMon_Task c96b0d0 248 READY bd414 c96af78 0 0
idleTask d57d6b8 c9e3d98 249 READY b9440 c9e3d08 0 0

```

The following is example output from the **show task** command for TID bfb490:

```

[SN5428A]# show task bfb490
Registers

NAME ENTRY TID PRI STATUS PC SP ERRNO DELAY

tLogTask logTask bfb490 0 PEND 2cd38c bfb3b0 0 0

stack: base 0xbfb490 end 0xbfa108 size 4984 high 1048 margin 3936

options: 0x6
VX_UNBREAKABLE VX_DEALLOC_STACK

r0 = 0 sp = bfb3b0 r2 = 0 r3 = 0
r4 = 0 r5 = 0 r6 = 0 r7 = 0
r8 = 0 r9 = 0 r10 = 0 r11 = 0
r12 = 0 r13 = 0 r14 = 0 r15 = 0
r16 = 0 r17 = 0 r18 = 0 r19 = 0
r20 = 310000 r21 = 310000 r22 = 300000 r23 = 310000
r24 = 310000 r25 = 310000 r26 = 310000 r27 = ffffffff
r28 = 10000003 r29 = 10000010 r30 = bfb6ac r31 = 0
msr = b030 lr = 0 ctr = 0 pc = 2cd38c
cr = 42000020 xer = 0

Stack Trace

2b3324 vxTaskEntry +60 : logTask ()
25c4e0 logTask +30 : msgQReceive ()
2743f0 msgQReceive +298: qJobGet ()

```

## Related Commands

| Command                  | Description                                                                                   |
|--------------------------|-----------------------------------------------------------------------------------------------|
| <b>show buffers</b>      | Display information about SN 5428 buffer pools.                                               |
| <b>show memory</b>       | Display information about SN 5428 memory and related resources.                               |
| <b>show modules</b>      | Display addressing information related to the SN 5428 software modules.                       |
| <b>show stack</b>        | Display the SN 5428 memory stack on a per-task basis.                                         |
| <b>show tech-support</b> | Display a variety of diagnostic information for use by Cisco Technical Support professionals. |

# show tech-support

To display the results of several CLI **show** commands useful for debugging purposes, use the **show tech-support** command.

## show tech-support

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command to display the output of the following commands:

- show system
- show clock
- show software version all
- show cluster
- show admin
- show interface brief
- show interface all
- show interface all stats
- show ip arp
- show ip hosts
- show ip route
- show ip tcp
- show ip udp
- show ip stats
- show ip icmp stats
- show ip route stats
- show ip tcp stats
- show ip udp stats
- show snmp

- show devices
- show accesslist all
- show scsirouter all
- show bootconfig
- show runningconfig
- show ha node stats
- show ha app list stats
- show ha app all stats
- show diagnostics
- show boot
- show memory
- show task all
- show stack
- show modules
- show buffers
- show debug scsirouter all tfestatus
- show debug fc all

The **show tech-support** command is designed for debug purposes and should be used under the guidance of a Cisco Technical Support professional.

### Examples

The following is abbreviated example output from the **show tech-support** command:

```
[SN5428A]# show tech-support

*
* show tech
*

 Generated: Fri Mar 22 22:05:20 GMT 2002
 System Name: SN5428A

*
* show system
*

```

### Related Commands

| Command                | Description                                                                                                           |
|------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>show accesslist</b> | Display the contents of the named access list or all access lists.                                                    |
| <b>show admin</b>      | Display system administrator contact information.                                                                     |
| <b>show boot</b>       | Display system boot information and startup file parameters.                                                          |
| <b>show bootconfig</b> | Display the SN 5428's bootable configuration, or create a command file based on the SN 5428's bootable configuration. |

| <b>Command</b>               | <b>Description</b>                                                                                                                                                          |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>show buffers</b>          | Display information about SN 5428 buffer pools.                                                                                                                             |
| <b>show clock</b>            | Display the current system date and time, including the system time zone.                                                                                                   |
| <b>show cluster</b>          | Display cluster-related operational statistics, including heartbeat information.                                                                                            |
| <b>show debug</b>            | Display debug trace information for the specified SCSI routing instance.                                                                                                    |
| <b>show devices</b>          | Display a list of devices discovered on the SN 5428 Fibre Channel interface.                                                                                                |
| <b>show diagnostics</b>      | Display hardware diagnostic test results.                                                                                                                                   |
| <b>show ha</b>               | Display HA operational statistics for the SN 5428 or for a specific application.                                                                                            |
| <b>show interface</b>        | Display operational and configuration information for the specified interface or all interfaces.                                                                            |
| <b>show ip</b>               | Display entries from the SN 5428 Storage Router routing table, and statistics about the protocols used in the SN 5428 network.                                              |
| <b>show memory</b>           | Display information about SN 5428 memory and related resources.                                                                                                             |
| <b>show modules</b>          | Display addressing information related to the SN 5428 software modules.                                                                                                     |
| <b>show runningconfig</b>    | Display the SN 5428's running configuration, or create a command file based on the SN 5428's running configuration.                                                         |
| <b>show scsirouter</b>       | Display configuration and operational information for the named SCSI routing instance.                                                                                      |
| <b>show snmp</b>             | Display the SN 5428's SNMP management configuration information.                                                                                                            |
| <b>show software version</b> | Display a list of software versions available on the SN 5428, including the currently running version and the version that will run the next time the SN 5428 is restarted. |
| <b>show stack</b>            | Display the SN 5428 memory stack on a per-task basis.                                                                                                                       |
| <b>show system</b>           | Display selected system information, including system name.                                                                                                                 |
| <b>show task</b>             | Display information about the tasks running in the SN 5428.                                                                                                                 |

# show version

To display version information for system-level software and applications, use the **show version** command.

**show version**

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use the **show version** command for version information about the SN 5428 operating system software, system bootstrap, application software, and CLI.

**Examples** The following is example output from the **show version** command:

```
[SN5428A]# show version

CISCO SN 5428 Storage Router

Operating System Software Ver: 2.3.1
System Bootstrap Ver: 2.3.1
Application Software Ver: 2.3.1
CLI Version 2.1

Copyright (c) 1986-2002 by Cisco Systems, Inc
```

| Related Commands | Command                      | Description                                                                                                                                                                 |
|------------------|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>show software version</b> | Display a list of software versions available on the SN 5428, including the currently running version and the version that will run the next time the SN 5428 is restarted. |

# show vlan

To view configuration and operational information about the specified VLAN, use the **show vlan** command.

```
show vlan [id vid] [brief | config]
```

| Syntax Description | id vid | (Optional) ID of the VLAN to be displayed.                                                 |
|--------------------|--------|--------------------------------------------------------------------------------------------|
|                    | brief  | (Optional) Display name, status, and ports for each VLAN.                                  |
|                    | config | (Optional) Display detailed configuration information for the specified VLAN or all VLANs. |

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** A VLAN is a group of independent devices that communicate as if they are on the same physical LAN segment but can actually be located anywhere on the network. The SN 5428 dynamically obtains VLAN information from the switch attached to the Gigabit Ethernet interface. Use the **show vlan** command to learn of any VLANs configured on the attached network.

**Examples** The following is example output from the **show vlan** command, followed by example output from the **show vlan config** command for the VLAN ID *101*:

```
[SN5428A]# show vlan
VLAN Name Status Ports

101 vlanfoo1 active ge1, ge2
102 vlanfoo2 active ge2

VLAN Type MTU Interfaces

101 enet 1500 ge2VLAN101
102 enet 1500 ge2VLAN102

[SN5428A]# show vlan id 101 config
vlan 101 name vlanfoo1 mtu 1500
```

| Related Commands | Command                    | Description                                                                                                |
|------------------|----------------------------|------------------------------------------------------------------------------------------------------------|
|                  | <b>restore vlan</b>        | Restore VLAN configuration information from the named configuration file.                                  |
|                  | <b>save all</b>            | Save all configuration information, including VLAN information.                                            |
|                  | <b>save scsirouter</b>     | Save configuration information for the named SCSI routing instance.                                        |
|                  | <b>save system</b>         | Save selected system configuration information, including VLAN information.                                |
|                  | <b>save vlan</b>           | Save configuration information for the named VLAN or all VLANs.                                            |
|                  | <b>scsirouter serverif</b> | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
|                  | <b>show vtp</b>            | Display configuration and operational information for VTP.                                                 |
|                  | <b>vlan</b>                | Configure a non-VTP VLAN on the SN 5428.                                                                   |
|                  | <b>vtp domain</b>          | Assign a VTP domain name to the SN 5428.                                                                   |
|                  | <b>vtp mode</b>            | Configure the SN 5428 to operate in client or transparent VTP mode.                                        |

# show vtp

To display general configuration and status information about the VLAN Trunking Protocol (VTP), use the **show vtp** command.

**show vtp [config | stats]**

| Syntax Description | config | (Optional) Display mode and domain information. |
|--------------------|--------|-------------------------------------------------|
|                    | stats  | (Optional) Display operational statistics.      |

**Defaults** None.

**Command Modes** Administrator or Monitor.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** VTP must be in transparent mode to configure VLANs. Use the **show vtp** command to view the current VTP configuration.

**Examples** The following is example output from the **show vtp** command, with the SN 5428 in VTP Client mode:

```
[SN5428A]# show vtp
Configuration Revision : 0
Number of existing VLANs : 2
VTP Operating Mode : Client
VTP Domain Name : lab1
```

The following is example output from the **show vtp** command, with the SN 5428 in VTP Transparent mode:

```
[SN5428A]# show vtp
Configuration Revision : 0
Number of existing VLANs : 2
VTP Operating Mode : Transparent
VTP Domain Name :
```

The following is example output from the **show vtp config** command:

```
[SN5428A]# show vtp config
vtp mode client
vtp domain lab1
```

The following is example output from the **show vtp stats** command:

```
[SN5428A]# show vtp stats
Summary advertisements received : 3
Subset advertisements received : 2
Request advertisements received : 5
Request advertisements transmitted : 5
```

#### Related Commands

| Command                    | Description                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------|
| <b>restore vlan</b>        | Restore VLAN configuration information from the named configuration file.                                  |
| <b>save all</b>            | Save all configuration information, including VLAN information.                                            |
| <b>save scsirouter</b>     | Save configuration information for the named SCSI routing instance.                                        |
| <b>save system</b>         | Save selected system configuration information, including VLAN information.                                |
| <b>save vlan</b>           | Save configuration information for the named VLAN or all VLANs.                                            |
| <b>scsirouter serverif</b> | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
| <b>show vlan</b>           | Display configuration and operational information for the specified VLAN or all VLANs.                     |
| <b>vlan</b>                | Configure a non-VTP VLAN on the SN 5428.                                                                   |
| <b>vtp domain</b>          | Assign a VTP domain name to the SN 5428.                                                                   |
| <b>vtp mode</b>            | Configure the SN 5428 to operate in client or transparent VTP mode.                                        |

# snmp-server

To configure SNMP management on the SN 5428, use the **snmp-server** command. To disable SNMP management or specific host or traps, use the **no** forms of this command.

```
snmp-server community community-name {ro | rw}

snmp-server host A.B.C.D [version version-number] traps

snmp-server linkupdown {all | if-name}

snmp-server sendauthtraps

no snmp-server host {all | A.B.C.D} traps

no snmp-server linkupdown {all | if-name}

no snmp-server sendauthtraps
```

| Syntax Description                   |  |                                                                                                                                                                                                                                                                                                       |
|--------------------------------------|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>community-name</i>                |  | The name of the community having the specified access (read or write) to the SN 5428. Enclose the string in quotation marks.                                                                                                                                                                          |
| <b>ro</b>                            |  | Read-only access. The SN 5428 will respond to this community's GET commands. The default SNMP getcommunity is <i>public</i> .                                                                                                                                                                         |
| <b>rw</b>                            |  | Read-write access. The SN 5428 will respond to this community's SET commands. The default SNMP setcommunity is <i>private</i> .                                                                                                                                                                       |
| <i>A.B.C.D</i>                       |  | The IP address of the first destination host used for notifications (traps). <i>A.B.C.D</i> is the dotted quad notation of the IP address. If the command is issued twice, the second IP address becomes the second destination host used for notifications. Version 1 traps will be sent by default. |
| <b>version</b> <i>version-number</i> |  | (Optional) The SNMP version for the traps. Use 1 to specify version 1 traps; use 2 to specify version 2 traps.                                                                                                                                                                                        |
| <b>traps</b>                         |  | Keyword, indicating the specified version of traps will be sent to the designated host.                                                                                                                                                                                                               |
| <b>host all</b>                      |  | Remove all destination hosts used for SNMP notifications (traps).                                                                                                                                                                                                                                     |
| <b>linkupdown all</b>                |  | Enable or disable SNMP link up/down traps for all interfaces.                                                                                                                                                                                                                                         |
| <b>linkupdown</b> <i>if-name</i>     |  | Enable or disable SNMP link up/down traps for the specified interface. See Table 11-34 for a list of valid interface names.                                                                                                                                                                           |
| <b>sendauthtraps</b>                 |  | Enable or disable authentication failure traps sent when an SNMP request is received with an incorrect community name.                                                                                                                                                                                |

## Defaults

The default read-only community name is *public*. This is also known as the *getcommunity*. The default read-write community name is *private*. This is also known as the *setcommunity*. SNMP notifications are disabled by default.

## Command Modes

Administrator.

**Command History**

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

**Usage Guidelines**

A variety of network management methods may be used with the SN 5428, including SNMP. All management methods are enabled by default.

The first issuance of the **snmp-server host** command sets an initial destination host used for traps; the second issuance of the command sets an additional destination host. Version 1 traps are sent by default. To send other trap versions, use the **snmp-server host** command with the **version** keyword.

Link up/down traps can be sent for any valid SN 5428 interface.

**Table 11-34 Valid Interface Names**

| Interface Name | Description                                              |
|----------------|----------------------------------------------------------|
| <b>mgmt</b>    | The management interface.                                |
| <b>ha</b>      | The HA interface.                                        |
| <b>fc?</b>     | The Fibre Channel interface, for example, fc1 or fc5.    |
| <b>ge?</b>     | The Gigabit Ethernet interface, for example, ge1 or ge2. |

**Examples**

The following command identifies the IP address *10.3.4.200* as a destination host for SNMP Version 1 traps. You can configure two destination hosts for traps.

```
[SN5428A]# snmp-server host 10.3.4.200 traps
```

The following command enables the SN 5428 to send authentication failure traps to the SNMP destination host:

```
[SN5428A]# snmp-server sendauthtraps
```

The following command enables the SN 5428 to send SNMP link up/down traps for all interfaces to the SNMP destination host :

```
[SN5428A]# snmp-server linkupdown all
```

**Related Commands**

| Command              | Description                                                      |
|----------------------|------------------------------------------------------------------|
| <b>setup mgmt</b>    | Run the wizard to configure the management interface.            |
| <b>setup netmgmt</b> | Run the wizard to configure network management.                  |
| <b>show snmp</b>     | Display the SN 5428's SNMP management configuration information. |

# software http url

To configure the default location from which to download updated SN 5428 software to the SN 5428 via HTTP protocol, use the **software http url** command.

```
software http url {http://servername/path | default | none}
```

| Syntax Description            |                                                                                                                                 |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <i>http://servername/path</i> | The complete URL identifying the location from which to download SN 5428 software.                                              |
| <b>default</b>                | Return setting to the default download location. The default location is set to <code>http://www.cisco.com</code> .             |
| <b>none</b>                   | Delete the current download location and leave the URL blank. Use this keyword to prevent software downloads via HTTP protocol. |

**Defaults** The default download location is `http://www.cisco.com`.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Updated SN 5428 software is available from the Cisco.com website. It can also be downloaded and stored locally, then transferred to the SN 5428 when necessary via the **software http url** command.

To see the location defined as the current default download location, issue the **show software version all** command.

**Examples** The following command sets the default download location to the URL `http://www.lab-foo.com/~sn5428`:

```
[SN5428A] # software http url http://www.lab-foo.com/~sn5428
```

| Related Commands | Command                  | Description                                                                                                       |
|------------------|--------------------------|-------------------------------------------------------------------------------------------------------------------|
|                  | <b>download software</b> | Download the list of available software versions or the specified version of software from the named location.    |
|                  | <b>save all</b>          | Save all configuration information, including default download location for updated SN 5428 software.             |
|                  | <b>save system</b>       | Save selected system configuration information, including default download location for updated SN 5428 software. |

| <b>Command</b>                 | <b>Description</b>                                                                                                                                                          |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>show software version</b>   | Display a list of software versions available on the SN 5428, including the currently running version and the version that will run the next time the SN 5428 is restarted. |
| <b>software http username</b>  | Configure the user name and optional password required to access the default download location.                                                                             |
| <b>software proxy</b>          | Configure HTTP proxy information.                                                                                                                                           |
| <b>software proxy url</b>      | Specify the default location from which to download updated SN 5428 software via HTTP, using a proxy server.                                                                |
| <b>software proxy username</b> | Configure the user name and optional password required to access the proxy URL.                                                                                             |
| <b>software tftp</b>           | Specify the default location from which to download updated SN 5428 software via TFTP.                                                                                      |
| <b>software version</b>        | Specify the version of software to run when the SN 5428 is restarted.                                                                                                       |
| <b>verify software version</b> | Check the specified software version for problems.                                                                                                                          |

# software http username

To configure an optional user name and password used to retrieve updated SN 5428 software from the HTTP download location, use the **software http username** command.

```
software http username {webservice-username | none} [password webservice-password]
```

| Syntax Description         |                                                                                                                    |  |
|----------------------------|--------------------------------------------------------------------------------------------------------------------|--|
| <i>webservice-username</i> | The user name required to retrieve SN 5428 software from the download location.                                    |  |
| <b>none</b>                | Indicates user name and password are not required. Sets these values to <i>none</i> . This is the default setting. |  |
| <i>webservice-password</i> | (Optional) The password required to retrieve SN 5428 software from the download location.                          |  |

**Defaults** By default, the user name and password are set to *none*.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use the **show software version all** command to display the current user name configured for retrieval of updated SN 5428 software from the HTTP download location.

Use the keyword **none** to indicate that the web server does not require a user name and password to download software, effectively changing the user name and password values to *none*. This is the default setting.

See the **software http url** command for details on setting the location from which to download software.

**Examples** The following example sets the user name for HTTP download to *FooAdmin* and the password to *foo*:

```
[SN5428A] # software http username FooAdmin password foo
```

| Related Commands | Command                  | Description                                                                                                       |
|------------------|--------------------------|-------------------------------------------------------------------------------------------------------------------|
|                  | <b>download software</b> | Download the list of available software versions or the specified version of software from the named location.    |
|                  | <b>save all</b>          | Save all configuration information, including default download location for updated SN 5428 software.             |
|                  | <b>save system</b>       | Save selected system configuration information, including default download location for updated SN 5428 software. |

| <b>Command</b>                 | <b>Description</b>                                                                                                                                                          |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>show software version</b>   | Display a list of software versions available on the SN 5428, including the currently running version and the version that will run the next time the SN 5428 is restarted. |
| <b>software http url</b>       | Specify the default location from which to download updated SN 5428 software via HTTP.                                                                                      |
| <b>software proxy</b>          | Configure HTTP proxy information.                                                                                                                                           |
| <b>software proxy url</b>      | Specify the default location from which to download updated SN 5428 software via HTTP, using a proxy server.                                                                |
| <b>software proxy username</b> | Configure the user name and optional password required to access the proxy URL.                                                                                             |
| <b>software tftp</b>           | Specify the default location from which to download updated SN 5428 software via TFTP.                                                                                      |
| <b>software version</b>        | Specify the version of software to run when the SN 5428 is restarted.                                                                                                       |
| <b>verify software version</b> | Check the specified software version for problems.                                                                                                                          |

# software proxy

To configure the address and port of a proxy server to be used when downloading updated SN 5428 software to the SN 5428 via HTTP protocol, use the **software proxy** command.

**software proxy address** *address* [**port** *nn*]

**software proxy port** *nn*

| Syntax Description | <i>address</i> | The IP address or URL of the proxy server. To remove a proxy server address, set the address string to blank, using “ ”. |
|--------------------|----------------|--------------------------------------------------------------------------------------------------------------------------|
|                    | <i>nn</i>      | (Optional) The port number of the proxy server.                                                                          |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** The proxy server will be used to access the proxy URL for HTTP download of software for the SN 5428. To change the port specification without changing the address, use the **software proxy port** command. Use the **software proxy url** command to configure the default download location.

**Examples** The following example configures the proxy address as *10.1.10.126* and port as *32*:

```
[SN5428A]# software proxy address 10.1.10.126 port 32
```

| Related Commands | Command                      | Description                                                                                                                                                                 |
|------------------|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>download software</b>     | Download the list of available software versions or the specified version of software from the named location.                                                              |
|                  | <b>save all</b>              | Save all configuration information, including default download location for updated SN 5428 software.                                                                       |
|                  | <b>save system</b>           | Save selected system configuration information, including default download location for updated SN 5428 software.                                                           |
|                  | <b>show software version</b> | Display a list of software versions available on the SN 5428, including the currently running version and the version that will run the next time the SN 5428 is restarted. |
|                  | <b>software http url</b>     | Specify the default location from which to download updated SN 5428 software via HTTP.                                                                                      |

| <b>Command</b>                 | <b>Description</b>                                                                                           |
|--------------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>software http username</b>  | Configure the user name and optional password required to access the default download location.              |
| <b>software proxy url</b>      | Specify the default location from which to download updated SN 5428 software via HTTP, using a proxy server. |
| <b>software proxy username</b> | Configure the user name and optional password required to access the proxy URL.                              |
| <b>software tftp</b>           | Specify the default location from which to download updated SN 5428 software via TFTP.                       |
| <b>software version</b>        | Specify the version of software to run when the SN 5428 is restarted.                                        |
| <b>verify software version</b> | Check the specified software version for problems.                                                           |

# software proxy url

To configure the default location from which to download updated SN 5428 software to the SN 5428 via HTTP protocol using the configured proxy server, use the **software proxy url** command.

**software proxy url** {*http://servername/path* | **default** | **none**}

| Syntax Description            |                                                                                                                                          |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <i>http://servername/path</i> | The complete URL identifying the location from which to download SN 5428 software via the configured proxy server.                       |
| <b>default</b>                | Return setting to the default proxy download location. The default location is <i>http://www.cisco.com</i> .                             |
| <b>none</b>                   | Delete the current proxy download location and leave the URL blank. Use this keyword to prevent software downloads via the proxy server. |

**Defaults** The proxy URL is set to *none*.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** If you use a proxy server to access locations on the Internet, configure the proxy server address and port number using the **software proxy address** command. The proxy server will be used to access the proxy URL when downloading updated SN 5428 software.

**Examples** The following example configures the proxy address as *10.1.10.126* and port as *32* and then sets the proxy download URL to *http://www.foo-a.com*:

```
[SN5428A] # software proxy address 10.1.10.126 port 32
[SN5428A] # software proxy url http://www.foo-a.com
```

| Related Commands | Command                  | Description                                                                                                       |
|------------------|--------------------------|-------------------------------------------------------------------------------------------------------------------|
|                  | <b>download software</b> | Download the list of available software versions or the specified version of software from the named location.    |
|                  | <b>save all</b>          | Save all configuration information, including default download location for updated SN 5428 software.             |
|                  | <b>save system</b>       | Save selected system configuration information, including default download location for updated SN 5428 software. |

| <b>Command</b>                 | <b>Description</b>                                                                                                                                                          |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>show software version</b>   | Display a list of software versions available on the SN 5428, including the currently running version and the version that will run the next time the SN 5428 is restarted. |
| <b>software http url</b>       | Specify the default location from which to download updated SN 5428 software via HTTP.                                                                                      |
| <b>software http username</b>  | Configure the user name and optional password required to access the default download location.                                                                             |
| <b>software proxy</b>          | Configure HTTP proxy information.                                                                                                                                           |
| <b>software proxy username</b> | Configure the user name and optional password required to access the proxy URL.                                                                                             |
| <b>software tftp</b>           | Specify the default location from which to download updated SN 5428 software via TFTP.                                                                                      |
| <b>software version</b>        | Specify the version of software to run when the SN 5428 is restarted.                                                                                                       |
| <b>verify software version</b> | Check the specified software version for problems.                                                                                                                          |

# software proxy username

To configure a user name and an optional password to be used to retrieve updated SN 5428 software from the proxy download location, use the **software proxy username** command.

```
software proxy username {webservice-username | none} [password webservice-password]
```

| Syntax Description         |                                                                                                                    |  |
|----------------------------|--------------------------------------------------------------------------------------------------------------------|--|
| <i>webservice-username</i> | The user name required to retrieve SN 5428 software from the proxy download location.                              |  |
| <b>none</b>                | Indicates user name and password are not required. Sets these values to <i>none</i> . This is the default setting. |  |
| <i>webservice-password</i> | (Optional) The password required to retrieve SN 5428 software from the proxy download location.                    |  |

## Defaults

By default, the user name and password are set to *none*.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

Use the **show software version all** command to display the current user name used to retrieve updated SN 5428 software from the proxy download location.

Use the keyword **none** to indicate that the web server does not require a user name and password to download software, effectively changing the user name and password values to *none*. This is the default setting.

See the **software proxy url** command for details on setting the location from which to download software.

## Examples

The following example sets the user name for proxy download to *FooAdmin* and the password to *foo*:

```
[SN5428A] # software proxy username FooAdmin password foo
```

## Related Commands

| Command                  | Description                                                                                                    |
|--------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>download software</b> | Download the list of available software versions or the specified version of software from the named location. |
| <b>save all</b>          | Save all configuration information, including default download location for updated SN 5428 software.          |

| <b>Command</b>                 | <b>Description</b>                                                                                                                                                          |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>save system</b>             | Save selected system configuration information, including default download location for updated SN 5428 software.                                                           |
| <b>show software version</b>   | Display a list of software versions available on the SN 5428, including the currently running version and the version that will run the next time the SN 5428 is restarted. |
| <b>software http url</b>       | Specify the default location from which to download updated SN 5428 software via HTTP.                                                                                      |
| <b>software http username</b>  | Configure the user name and optional password required to access the default download location.                                                                             |
| <b>software proxy</b>          | Configure HTTP proxy information.                                                                                                                                           |
| <b>software proxy url</b>      | Specify the default location from which to download updated SN 5428 software via HTTP, using a proxy server.                                                                |
| <b>software tftp</b>           | Specify the default location from which to download updated SN 5428 software via TFTP.                                                                                      |
| <b>software version</b>        | Specify the version of software to run when the SN 5428 is restarted.                                                                                                       |
| <b>verify software version</b> | Check the specified software version for problems.                                                                                                                          |

# software tftp

To configure host and directory information to be used when downloading updated SN 5428 software to the SN 5428 via the Trivial File Transfer Protocol (TFTP), use the **software tftp** command.

**software tftp directory** {*directory\_name* | none}

**software tftp hostname** *hostname* [**directory** *directory\_name*]

| Syntax Description |                       |                                                                                                            |
|--------------------|-----------------------|------------------------------------------------------------------------------------------------------------|
|                    | <i>directory_name</i> | The name of the TFTP base directory.                                                                       |
|                    | none                  | Remove the directory setting, effectively disabling the use of TFTP protocol.                              |
|                    | <i>hostname</i>       | The name of the remote TFTP host. To remove the TFTP configuration, set the host name to blank, using “ ”. |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command to set the required TFTP parameters for downloading software updates via TFTP protocol.

Use the **show software version all** command to display the current TFTP settings.

**Examples** The following example sets the TFTP hostname to *TFTPHost1* and the directory to */tftpboot*:

```
[SN5428A]# software tftp hostname TFTPHost1 directory /tftpboot
```

| Related Commands | Command                  | Description                                                                                                       |
|------------------|--------------------------|-------------------------------------------------------------------------------------------------------------------|
|                  | <b>download software</b> | Download the list of available software versions or the specified version of software from the named location.    |
|                  | <b>save all</b>          | Save all configuration information, including default download location for updated SN 5428 software.             |
|                  | <b>save system</b>       | Save selected system configuration information, including default download location for updated SN 5428 software. |

| <b>Command</b>                 | <b>Description</b>                                                                                                                                                          |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>show software version</b>   | Display a list of software versions available on the SN 5428, including the currently running version and the version that will run the next time the SN 5428 is restarted. |
| <b>software http url</b>       | Specify the default location from which to download updated SN 5428 software via HTTP.                                                                                      |
| <b>software http username</b>  | Configure the user name and optional password required to access the default download location.                                                                             |
| <b>software proxy</b>          | Configure HTTP proxy information.                                                                                                                                           |
| <b>software proxy url</b>      | Specify the default location from which to download updated SN 5428 software via HTTP, using a proxy server.                                                                |
| <b>software proxy username</b> | Configure the user name and optional password required to access the proxy URL.                                                                                             |
| <b>software version</b>        | Specify the version of software to run when the SN 5428 is restarted.                                                                                                       |
| <b>verify software version</b> | Check the specified software version for problems.                                                                                                                          |

# software version

To specify the version of software to run the next time the SN 5428 is restarted, use the **software version** command. This command forces a system reset and changes the running version of SN 5428 software.

**software version** v.x.y

|                           |                |                                                                     |
|---------------------------|----------------|---------------------------------------------------------------------|
| <b>Syntax Description</b> | v.x.y          | The version of SN 5428 software to be run when the system is reset. |
| <b>Defaults</b>           | None.          |                                                                     |
| <b>Command Modes</b>      | Administrator. |                                                                     |
| <b>Command History</b>    | <b>Release</b> | <b>Modification</b>                                                 |
|                           | 2.2.1          | This command was introduced.                                        |

## Usage Guidelines

This command performs necessary system modifications to assure that the new software version can be run. It causes a system reset, and the new version of software will be run when the reset is complete.

In a cluster environment, this command may temporarily suspend normal HA communications, causing a failover of any SCSI routing instances active on the SN 5428. Any instances with the **primary** attribute set to the IP address of the SN 5428 will resume running on the SN 5428 after it is rebooted.

Use the **show software version all** command to display the list of available versions, the currently running version, and the boot version that will run when the system is reset.

## Examples

The following is example output from the **software version** command:

```
[SN5428A]# software version 2.3.1

Module Size Status MD5 Digest

vxWorks 2869748 OK 1182ea6bfbe784e639d5766d829a385f
vxWorks.sym 209560 OK 69b153a735f0797fd7f4230dfe632e7c
bootrom_uncmp.hex 1369179 OK fc8c1d6288cc04c44c393fff7532553c
sysInit.out 67548 OK 1d4d1269ce46c6b223830101346bd63d
crashDump.out 13652 OK c2c8db951adfaf32c57975ff272fff23
snmp_util.out 2076 OK 6c3ebddf5ef2bd50c7b2d9e695424c7e
nuUtils.out 43638 OK 25f68962b1ce5ed3fdaa1ed71cb64033
nuEvents.out 19472 OK f8baf4bb1b609ace0e2a8fc5c9b176e7
ha.out 33341 OK d98cb57e4dbd8741b560b38463f6b446
confNode.out 10844 OK 6b8382753fdd97a94472a329f876cbff
authServer.out 16434 OK 555b12d11e64d67191fefaf0e6320776c
drv.out 29807 OK f1d3d36436c66f102e9804887ac85ac8
qlogic.out 394985 OK 833f8ede2ce87e232eb302aa93767fd5
i82543.out 48295 OK 87f8ee5988971078b5e77394bebb7263
vtp.out 16885 OK a641ccc2d4a16596cc452cc58d8d8ac7
scsiTargetFE.out 73894 OK 710ef047015ab3e4e3ef7ed5d0692661
```

```

scsiTargetBE.out 47793 OK fa3179ebe054b72ca039f8384698dbe8
scsiTcpAuth.out 8355 OK dc822106573c22a2831230ad783cfdca
scsiTcpServer.out 93938 OK 8563e5f5bc803a04ef2f3bec8891192e
scsiTcpClient.out 62874 OK 2d72e6315eed5f9cc4fc70a3dc8753d4
ttcp.out 22137 OK 5d596240993cbf6de71df41dbe3bd0dd
confMgmt.out 6133 OK 7f1b773360d5a68a2bb3a747a7feb87c
diag.out 42043 OK c0ea00c3d4452263bb1396e3a4c91016
confXML.out 47288 OK 63ba6d8469fe203cf6be46ae68301f67
confObj.out 137416 OK f442bcf82590e81d7189bcd6b9a273e9
clusterApp.out 20771 OK 037dba9b65c1f67d27ffa35a3f6938c8
cdp.out 26665 OK 61a9e079b88a0f91bef5d5d7bec7945b
systemApp.out 69688 OK de391acd10f93c7c6be50d0fd884a81c
ipRouter.out 15913 OK 6dafefeac98c0361a84614f22cad90d4
scsiRouter.out 57422 OK e85eed1292842ac83aad4a86b92cbdb4
authServerApp.out 22846 OK 6162dbc884936a6fb21586dedb6f0334
ui.out 1443381 OK 1068c0e2f9481cd0c3eccecc0b04354f7
ifx.out 7810 OK 950d73c7e9238120d75a9f5a643928be
ether.out 3356 OK 9dd0e464be634d6ef09e73ad54e88021
mau_if.out 4269 OK b37cfaa6ceed5c19800553a29840306e
mau_neg.out 2671 OK 8f663c04951779edc13440aa8a9f0841
entity.out 8011 OK 52bcd95dd9630030c943e9f3148e50cf
cdp_snmp.out 5839 OK 40158423a55a46d6765e209704038a0e
fcmgmt.out 21742 OK caeb77cfe1c3a6d73936b0f307110628
iscsi_mib.out 20691 OK 344577311ae32b994532938a18b596b1
snmpApp.out 6515 OK cb81c2f37b1b05f1de1d3db5183618ae

```

Disk Space (required/available): 3146856/8716288 bytes

Please do **\*NOT\*** shutdown or reboot the system until the software update process completes. A fatal error could occur if you shutdown or reboot the system before the software update process completes.

Attempt 1:

```

 Gathering system files... OK
 Verifying checksums... OK
 Updating system files... OK
 Updating flash device... File [/ata0/software/2.3.1/bootrom_uncmp.hex]

```

opened successfully.

Done reading and converting image file.

Erasing Entire FLASH device...Done

Programming FLASH...Done

Verifying

FLASH...Done

OK

The software update process was successful. You must reboot the system in-order for the new software version to take effect.

## Related Commands

| Command                        | Description                                                                                                       |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>delete software version</b> | Remove the specified version of software from the SN 5428.                                                        |
| <b>download software</b>       | Download the list of available software versions or the specified version of software from the named location.    |
| <b>save all</b>                | Save all configuration information, including default download location for updated SN 5428 software.             |
| <b>save system</b>             | Save selected system configuration information, including default download location for updated SN 5428 software. |

| Command                        | Description                                                                                                                                                                 |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>show software version</b>   | Display a list of software versions available on the SN 5428, including the currently running version and the version that will run the next time the SN 5428 is restarted. |
| <b>software http url</b>       | Specify the default location from which to download updated SN 5428 software via HTTP.                                                                                      |
| <b>software http username</b>  | Configure the user name and optional password required to access the default download location.                                                                             |
| <b>software proxy</b>          | Configure HTTP proxy information.                                                                                                                                           |
| <b>software proxy url</b>      | Specify the default location from which to download updated SN 5428 software via HTTP, using a proxy server.                                                                |
| <b>software proxy username</b> | Configure the user name and optional password required to access the proxy URL.                                                                                             |
| <b>software tftp</b>           | Specify the default location from which to download updated SN 5428 software via TFTP.                                                                                      |
| <b>verify software version</b> | Check the specified software version for problems.                                                                                                                          |

# tacacs-server host

To specify a TACACS+ server to be used for AAA authentication services, use the **tacacs-server host** command. Use the **no** form of this command to delete the specified host.

**tacacs-server host** *ip-address* [**auth-port** *port-number*] [**timeout** *seconds*] [**key** *key-string*]

**no tacacs-server host** *ip-address* [**auth-port** *nn*]

## Syntax Description

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>ip-address</i>                   | The IP address of the TACACS+ server.                                                                                                                                                                                                                                                                                                                                                                                |
| <b>auth-port</b> <i>port-number</i> | (Optional) The server port number. Valid port numbers range from 1 to 65535. If unspecified, the port number defaults to 49.                                                                                                                                                                                                                                                                                         |
| <b>timeout</b> <i>seconds</i>       | (Optional) The amount of time the SN 5428 should wait for a reply from a TACACS+ server before timing out. This setting overrides the global setting of the <b>tacacs-server timeout</b> command. If no timeout value is specified, the global value is used.                                                                                                                                                        |
| <b>key</b> <i>key-string</i>        | (Optional) The authentication and encryption key for all TACACS+ communication between the SN 5428 and this TACACS+ server. The character string must match the key used by the TACACS+ daemon. This key overrides the global setting of the <b>tacacs-server key</b> command. If no key string is specified, the global value is used. If spaces are part of the key string, enclose the string in quotation marks. |

## Defaults

No TACACS+ server is specified.

## Command Modes

Administrator.

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 2.2.1   | This command was introduced. |

## Usage Guidelines

AAA authentication services are used to provide iSCSI authentication for IP hosts requesting access to storage resources.

- You can use multiple **tacacs-server host** commands to specify multiple TACACS+ servers. The software searches for servers in the order in which you specify them.
- If no server-specific timeout or key values are specified, the global values apply to each TACACS+ server.
- If you use spaces in the key, enclose the key in quotation marks.

**Examples**

The following example specifies the server with IP address 172.29.39.46 as the TACACS+ server and uses the default port for authentication:

```
[SN5428A] # tacacs-server host 172.29.39.46
```

The following example specifies port 52 as the destination port for authentication requests on the TACACS+ server 172.29.39.46:

```
[SN5428A] # tacacs-server host 172.29.39.46 auth-port 52
```

The following example specifies the server with IP address 172.29.39.46 as the TACACS server, uses ports 52 as the authorization port, sets the timeout value to 6, and sets *tac123* as the encryption key, matching the key on the TACACS+ server:

```
[SN5428A] # tacacs-server host 172.29.39.46 auth-port 52 timeout 6 key tac123
```

**Related Commands**

| Command                         | Description                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>aaa authentication iscsi</b> | Configure the AAA authentication services to be used for iSCSI authentication.                                               |
| <b>aaa test authentication</b>  | Enable testing of the default AAA authentication list.                                                                       |
| <b>debug aaa</b>                | Enable debugging for the AAA authentication services.                                                                        |
| <b>radius-server host</b>       | Configure remote RADIUS servers for AAA authentication services.                                                             |
| <b>restore aaa</b>              | Restore AAA authentication services from a saved configuration file.                                                         |
| <b>save aaa</b>                 | Save the current AAA configuration information.                                                                              |
| <b>scsirouter authenticate</b>  | Enable iSCSI authentication for the named SCSI routing instance.                                                             |
| <b>show aaa</b>                 | Display AAA configuration information.                                                                                       |
| <b>tacacs-server key</b>        | Sets the global authentication and encryption key for all TACACS+ communications between the SN 5428 and the TACACS+ daemon. |
| <b>tacacs-server timeout</b>    | Sets the interval the SN 5428 waits for a TACACS+ server to reply.                                                           |

## tacacs-server key

To set the authentication and encryption key used for all TACACS+ communications between the SN 5428 and the TACACS+ daemon, use the **tacacs-server key** command. To disable the key, use the **no** form of this command.

**tacacs-server key** *key-string*

**no tacacs-server key**

|                           |                   |                                                                                                                                                                                           |
|---------------------------|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>key-string</i> | The authentication and encryption key string to be used for all TACACS+ communications, in unencrypted text. If spaces are part of the key string, enclose the string in quotation marks. |
|---------------------------|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |       |
|-----------------|-------|
| <b>Defaults</b> | None. |
|-----------------|-------|

|                      |                |
|----------------------|----------------|
| <b>Command Modes</b> | Administrator. |
|----------------------|----------------|

|                        |                |                              |
|------------------------|----------------|------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|                        | 2.2.1.         | This command was introduced. |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | <p>After using the <b>aaa authentication iscsi</b> command to configure the iSCSI default authentication list to use TACACS+ authentication services, use the <b>tacacs-server key</b> command to set the global authentication and encryption key. The key entered as part of the command must match the key used on the TACACS+ daemon. If spaces are part of the key string, enclose the key string in quotation marks.</p> <p>To override the global key for a specific TACACS+ server, use the <b>tacacs-server host</b> command with the <b>key</b> keyword.</p> |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |                                                                                                                                                                               |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Examples</b> | <p>The following example sets the global authentication and encryption key to <i>my TACACS key string</i>:</p> <pre>[SN5428A]# radius-server key "my TACACS key string"</pre> |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                         |                                 |                                                                                |
|-------------------------|---------------------------------|--------------------------------------------------------------------------------|
| <b>Related Commands</b> | <b>Command</b>                  | <b>Description</b>                                                             |
|                         | <b>aaa authentication iscsi</b> | Configure the AAA authentication services to be used for iSCSI authentication. |
|                         | <b>aaa test authentication</b>  | Enable testing of the default AAA authentication list.                         |
|                         | <b>debug aaa</b>                | Enable debugging for the AAA authentication services.                          |
|                         | <b>radius-server host</b>       | Configure remote RADIUS servers for AAA authentication services.               |
|                         | <b>restore aaa</b>              | Restore AAA authentication services from a saved configuration file.           |

| <b>Command</b>                     | <b>Description</b>                                                 |
|------------------------------------|--------------------------------------------------------------------|
| <b>save aaa</b>                    | Save the current AAA configuration information.                    |
| <b>scsirouter<br/>authenticate</b> | Enable iSCSI authentication for the named SCSI routing instance.   |
| <b>show aaa</b>                    | Display AAA configuration information.                             |
| <b>tacacs-server host</b>          | Configure remote TACACS+ servers for AAA authentication services.  |
| <b>tacacs-server timeout</b>       | Sets the interval the SN 5428 waits for a TACACS+ server to reply. |

## tacacs-server timeout

To set the global interval that the SN 5428 Storage Router waits for a TACACS+ server to reply, use the **tacacs-server timeout** command. To restore the default, use the **no** form of this command.

**tacacs-server timeout** *seconds*

**no tacacs-server timeout**

|                           |                |                                                                                                 |
|---------------------------|----------------|-------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>seconds</i> | The global timeout value, in seconds. Enter a value in the range of 1 to 300. The default is 5. |
|---------------------------|----------------|-------------------------------------------------------------------------------------------------|

|                 |                                             |
|-----------------|---------------------------------------------|
| <b>Defaults</b> | The timeout value defaults to five seconds. |
|-----------------|---------------------------------------------|

|                      |                |
|----------------------|----------------|
| <b>Command Modes</b> | Administrator. |
|----------------------|----------------|

|                        |                |                              |
|------------------------|----------------|------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|                        | 2.2.1          | This command was introduced. |

**Usage Guidelines** Use this command to set the number of seconds the SN 5428 waits for a TACACS+ server to reply before timing out.

To override the global timeout value for a specific TACACS+ server, use the **tacacs-server host** command with the **timeout** keyword.

**Examples** The following example sets the global timeout value to 10. You may want to increase the timeout value if you have network problems or if TACACS+ servers are slow to respond, causing persistent timeouts when a lower timeout value is used.

```
[SN5428A]# tacacs-server timeout 10
```

|                         |                                 |                                                                                |
|-------------------------|---------------------------------|--------------------------------------------------------------------------------|
| <b>Related Commands</b> | <b>Command</b>                  | <b>Description</b>                                                             |
|                         | <b>aaa authentication iscsi</b> | Configure the AAA authentication services to be used for iSCSI authentication. |
|                         | <b>aaa test authentication</b>  | Enable testing of the default AAA authentication list.                         |
|                         | <b>debug aaa</b>                | Enable debugging for the AAA authentication services.                          |
|                         | <b>radius-server host</b>       | Configure remote RADIUS servers for AAA authentication services.               |
|                         | <b>restore aaa</b>              | Restore AAA authentication services from a saved configuration file.           |
|                         | <b>save aaa</b>                 | Save the current AAA configuration information.                                |

| <b>Command</b>                     | <b>Description</b>                                                                                                           |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>scsirouter<br/>authenticate</b> | Enable iSCSI authentication for the named SCSI routing instance.                                                             |
| <b>show aaa</b>                    | Display AAA configuration information.                                                                                       |
| <b>tacacs-server host</b>          | Configure remote TACACS+ servers for AAA authentication services.                                                            |
| <b>tacacs-server key</b>           | Sets the global authentication and encryption key for all TACACS+ communications between the SN 5428 and the TACACS+ daemon. |

# username password

To build a local user name database for use with the local method of AAA authentication services, use the **username password** command. Use the **no** form of this command to delete the specified user name.

**username** *user-name* **password** *password-string*

**no username** *user-name*

| Syntax Description     |                                                       |
|------------------------|-------------------------------------------------------|
| <i>user-name</i>       | A valid user name.                                    |
| <i>password-string</i> | The password associated with the specified user name. |

| Defaults |       |
|----------|-------|
|          | None. |

| Command Modes |                |
|---------------|----------------|
|               | Administrator. |

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines**

Use the **username password** command to build the local username database. Use the **aaa authentication iscsi** command to configure the iSCSI default authentication list to use *local* or *local-case* authentication services. The AAA authentication service, *local-case*, performs a case-sensitive user name match; the *local* service user name match is not case-sensitive. Both *local* and *local-case* use case-sensitive password matching for authentication.

To display the contents of the local username database, issue the **show aaa** command.

**Examples**

The following example configures two user names (*foo* and *foo2*) and password (*foopassword* and *foo2password*):

```
[SN5428A]# username foo password foopassword
[SN5428A]# username foo2 password foo2password
```

To display the user name database, issue the **show aaa** command. The following is example output from the **show aaa** command:

```
[SN5428A]# show aaa
aaa new-model
aaa authentication iscsi default group tacacs+ local none
username foo password <password>
username foo2 password <password>
```

**Related Commands**

| <b>Command</b>                  | <b>Description</b>                                                             |
|---------------------------------|--------------------------------------------------------------------------------|
| <b>aaa authentication iscsi</b> | Configure the AAA authentication services to be used for iSCSI authentication. |
| <b>aaa test authentication</b>  | Enable testing of the default AAA authentication list.                         |
| <b>debug aaa</b>                | Enable debugging for the AAA authentication services.                          |
| <b>restore aaa</b>              | Restore AAA authentication services from a saved configuration file.           |
| <b>save aaa</b>                 | Save the current AAA configuration information.                                |
| <b>scsirouter authenticate</b>  | Enable iSCSI authentication for the named SCSI routing instance.               |
| <b>show aaa</b>                 | Display AAA configuration information.                                         |

# verify software version

To check the specified software version for problems, issue the **verify software version** command.

```
verify software version {all | boot | current | version-id}
```

| Syntax Description | all               | Verify all software versions available to the SN 5428.                  |
|--------------------|-------------------|-------------------------------------------------------------------------|
|                    | <b>boot</b>       | The software version that is set to boot at the next system restart.    |
|                    | <b>current</b>    | The software version that is currently running.                         |
|                    | <i>version-id</i> | A specific version of software, which must be available to the SN 5428. |

**Defaults** None.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** Use this command after downloading software to verify that the download completed successfully and that the downloaded software is bootable. The size and the status of each module is verified.

**Examples** The following is example output from the **verify software version** command:

```
[SN5428A]# verify software version 2.3.1
```

| Module            | Size    | Status | MD5 Digest                       |
|-------------------|---------|--------|----------------------------------|
| vxWorks           | 3119913 | OK     | 420ba55287add359f02f0932415c3203 |
| vxWorks.sym       | 245049  | OK     | 062154305d71e60499cbba710e091b77 |
| bootrom_uncmp.hex | 1966930 | OK     | 79bb147b9f057ecf4766004a7a8f0be7 |
| sysInit.out       | 72076   | OK     | f756574e1d760411fc3c13d9590e6c31 |
| crashDump.out     | 13462   | OK     | 609c6defda14130d71255f1b26c128b3 |
| snmp_util.out     | 2077    | OK     | 88f1b160932133aab07da25cbd5c520b |
| nuUtils.out       | 52957   | OK     | 2f0271fb8282bd9a38d32e4f142109b6 |
| nuEvents.out      | 18508   | OK     | b215633efbf9c4d737b516f5ad712c48 |
| ha.out            | 36012   | OK     | a8f83208eb83316aa679408721b8d52e |
| confNode.out      | 10679   | OK     | cd0152297bcc3fc737d1dae9c55263af |
| authServer.out    | 18906   | OK     | b66f197036ef74ffb204c481045b04ad |
| drv.out           | 30620   | OK     | 1d8774cd9d9853d980d95840e03cdc79 |
| qlogic.out        | 478010  | OK     | f2d0b13bf88bc3e140d2712de6bfce4e |
| qlpt.out          | 80798   | OK     | 1cdfc3bfeffb44cd97eb5601034956d4 |
| i82543.out        | 58694   | OK     | 614a7ce789e3d7d42952086fdef4d91c |
| smlApi.out        | 30453   | OK     | 79203a80401b7334542e82e23f52b6f0 |
| vtp.out           | 17172   | OK     | e8b5a7acecbf766660278857acd80551 |
| scsiTargetFE.out  | 77934   | OK     | b7cf617bb2d4d6723e2e8ec59b7ddcc7 |
| scsiTargetBE.out  | 50189   | OK     | 250f4020e7613b0122b2d12067ee4064 |
| virtdev.out       | 303     | OK     | ce37770b184c0a2bdbc47fb3e5658843 |

|                   |         |    |                                  |
|-------------------|---------|----|----------------------------------|
| scsiTcpAuth.out   | 8424    | OK | 9d9616ddde0314abc9ad2650c1b22846 |
| scsiTcpServer.out | 91533   | OK | d77cef22fc961cc5b3a4ca914659a6e4 |
| scsiTcpClient.out | 68519   | OK | 62033f5866b1fb08d801fed755a69290 |
| ttcp.out          | 22137   | OK | 5d596240993cbf6de71df41dbe3bd0dd |
| confMgmt.out      | 6767    | OK | 8e67403acedb64fc3a68f252c628936a |
| hdwmon.out        | 12935   | OK | 66e60a605d91b0fe85e62c1e5c3a71e6 |
| diag.out          | 74801   | OK | ac75b19301f3491c58b8790b6cf1b644 |
| confXML.out       | 47412   | OK | f802d1480f8af4dbec911598ad659f3d |
| confObj.out       | 154851  | OK | 618e72d69b97ab8a86f9c9d2a9be9023 |
| clusterApp.out    | 24504   | OK | a523036efceefbbf95852c3710bb9de0 |
| cdp.out           | 27041   | OK | 78778c0c7c95191938e7dbef2288135f |
| systemApp.out     | 93654   | OK | 2d6729d36329c6c3805b4c0022088110 |
| ipRouter.out      | 16201   | OK | bc35cff58b73084eea26fc3c9091bc87 |
| scsiRouter.out    | 63549   | OK | 4c5c554b22da14171b70da39026dc327 |
| frameRacer.out    | 24764   | OK | 2f0ae5bfcc0a41d41cfe691608d15ff9 |
| authServerApp.out | 23736   | OK | 44417351837641ae951b8eeb8a418884 |
| fcSwApp.out       | 31924   | OK | cc95921345ccef8e91f2efff618aeb3a |
| fdisk.out         | 14196   | OK | c10ad63180733cf0bc6979d1cd24d0e3 |
| openssl.out       | 515026  | OK | 1109b92a3efcbf26689f25a1bf7993a0 |
| ui.out            | 1730553 | OK | cb56a8458b0ea9e26c0f7d3559546946 |
| ifx.out           | 7890    | OK | 262b2ef1a13b1052a7276280316cbda  |
| ether.out         | 3356    | OK | 1db2ce56be21368a2bfea2887d3882e6 |
| mau_if.out        | 4297    | OK | 99e5ffe6bf83669d84da9757bc147cd9 |
| mau_neg.out       | 2688    | OK | 50a1b135c3999da5f1d05f3b173f3f69 |
| entity.out        | 8244    | OK | 592d0560447e2857375d893883a44bf7 |
| entity_sensor.out | 5073    | OK | d192a6a5ef7bf58a9a7db003dfb10a73 |
| cdp_snmp.out      | 6745    | OK | 71c0b033b43be82ff16ce46520fd75f6 |
| fcmgmt_fcsww.out  | 24031   | OK | 1bb0ac4fb3a69527b5495545a989406c |
| iscsi_mib.out     | 20853   | OK | 2a2a82b3810a8047cbb939e550054b99 |
| snmpApp.out       | 7412    | OK | 9e0e661793fe789129313aff49e128dd |

**Related Commands**

| Command                        | Description                                                                                                                                                                 |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>delete software version</b> | Remove the specified version of software from the SN 5428.                                                                                                                  |
| <b>download software</b>       | Download the list of available software versions or the specified version of software from the named location.                                                              |
| <b>show software version</b>   | Display a list of software versions available on the SN 5428, including the currently running version and the version that will run the next time the SN 5428 is restarted. |

# vlan

To configure a VLAN on the SN 5428 Storage Router, use the **vlan** command. To delete a VLAN, use the **no** form of this command.

```
vlan vid [name vlan_name] [mtusize nn]
```

```
no vlan vid
```

| Syntax Description           |                                                                                                                                                                                                                                         |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>vid</i>                   | VLAN identification (VID) number. Enter an integer from 1 to 4095.                                                                                                                                                                      |
| <b>name</b> <i>vlan_name</i> | (Optional) The name of the VLAN, which can be up to 32 characters in length. If not specified, the default VLAN name has <i>VLAN</i> as the prefix followed by the VID, left padded to four bytes (for example, VLAN0002, or VLAN0045). |
| <b>mtusize</b> <i>nn</i>     | The size of the maximum transfer unit, in bytes. <i>nn</i> is an integer from 1500 to 9000. The default MTU is 1500.                                                                                                                    |

**Defaults** The default VLAN name is comprised of the prefix *VLAN* and the VID, left padded to four bytes. The default MTU size is 1500.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** In a cluster environment, VLAN management functions are handled by a single SN 5428. To determine which SN 5428 is performing VLAN management functions, issue the **show cluster** command. If you issue the **vlan** command from a storage router that is not performing VLAN management functions, the CLI displays an informational message with the name of the SN 5428 that is currently handling those functions. For more information on operating the SN 5428 in a cluster, see Chapter 10, “Maintaining and Managing the SN 5428 Storage Router.”

VLANs are a cluster-wide configuration item. When configured and copied to the boot configuration file, HA communications will propagate the VLAN information to all SN 5428s in the cluster. A maximum of 16 VLANs can be configured in a cluster.

VLAN information can only be configured when the SN 5428 is in VTP Transparent mode. In transparent mode, received VTP packets are ignored and VLAN configuration information is retrieved from the SN 5428 cluster.

The SN 5428 uses 802.1Q VLAN encapsulation to carry VLAN information on packets sent and received on the Gigabit Ethernet interface. The 802.1Q packet tag is a four-byte field inserted between the source MAC address and ether-type fields in the layer 2 header. It consists of a two-byte Tag Protocol Identifier (TPID) field and a two-byte Tag Control Information (TCI) field. The TPID contains the “protocol type” field (0x8100), which identifies the packet as a valid 802.1Q tagged packet. The TCI contains the 12-bit VLAN Identifier (VID) field and a 3-bit User Priority (UP) field.

Use the **vlan** command to locally configure VLANs when the SN 5428 is connected to a switched network that does not support VTP but does support 802.1Q VLANs.

### Examples

The following set of commands places the SN 5428 in VTP Transparent mode and configures a VLAN named *weblan001* on the SN 5428. The VID is 45.

```
[SN5428A]# vtp mode transparent
[SN5428A]# Jul 30 15:24:02:Vtp:AS_NOTICE :VTP changed to transparent mode
[SN5428A]# vlan 45 name weblan001
[SN5428A]# Jul 30 15:25:45:Vtp:AS_NOTICE :VLAN 45 added (name=VLAN0045, mtu=1500)
```

### Related Commands

| Command                    | Description                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------|
| <b>restore vlan</b>        | Restore VLAN configuration information from the named configuration file.                                  |
| <b>save all</b>            | Save all configuration information, including VLAN information.                                            |
| <b>save scsirouter</b>     | Save configuration information for the named SCSI routing instance.                                        |
| <b>save system</b>         | Save selected system configuration information, including VLAN information.                                |
| <b>save vlan</b>           | Save configuration information for the named VLAN or all VLANs.                                            |
| <b>scsirouter serverif</b> | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
| <b>show vlan</b>           | Display configuration and operational information for the specified VLAN or all VLANs.                     |
| <b>show vtp</b>            | Display configuration and operational information for VTP.                                                 |
| <b>vtp domain</b>          | Assign a VTP domain name to the SN 5428.                                                                   |
| <b>vtp mode</b>            | Configure the SN 5428 to operate in client or transparent VTP mode.                                        |

# vtp domain

To assign a VLAN Trunking Protocol (VTP) domain name to the SN 5428 Storage Router, use the **vtp domain** command. VLAN information will not be accepted from a switch which is in a different domain.

**vtp domain** {*domain\_name* | none}

| Syntax Description |                                                                                                                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>domain_name</i> | The name of the domain to which the SN 5428 belongs.                                                                                                                                         |
| none               | The SN 5428 is not assigned to a specific domain. If the SN 5428 is in VTP Client mode, it will assign itself to the first domain from which it receives a VTP message. This is the default. |

**Defaults** None. The SN 5428 will assign itself to the first domain from which it receives a VTP message.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** In a cluster environment, VTP configuration functions are handled by a single SN 5428. To determine which SN 5428 is performing VTP configuration functions, issue the **show cluster** command. The SN 5428 that is performing VLAN management also performs VTP configuration. If you issue the **vtp domain** command from a storage router that is not performing VTP configuration functions, the CLI displays an informational message with the name of the SN 5428 that is currently handling those functions. For more information on operating the SN 5428 in a cluster, see Chapter 10, “Maintaining and Managing the SN 5428 Storage Router.”

The VTP domain name applies to all SN 5428s participating in a cluster. The VTP domain name is a cluster-wide configuration setting. When the VTP domain name is set using the **vtp domain** command and saved to the boot configuration file (via a **save all** or **save system** command), an HA exchange occurs and the VTP domain name will become active on all SN 5428s in the cluster.

**Examples** The following example sets the VTP domain name to *Lab\_Network*:

```
[SN5428A]# vtp domain Lab_Network
```

| Related Commands | Command             | Description                                                               |
|------------------|---------------------|---------------------------------------------------------------------------|
|                  | <b>restore vlan</b> | Restore VLAN configuration information from the named configuration file. |
|                  | <b>save all</b>     | Save all configuration information, including VLAN information.           |

| <b>Command</b>             | <b>Description</b>                                                                                         |
|----------------------------|------------------------------------------------------------------------------------------------------------|
| <b>save scsirouter</b>     | Save configuration information for the named SCSI routing instance.                                        |
| <b>save system</b>         | Save selected system configuration information, including VLAN information.                                |
| <b>save vlan</b>           | Save configuration information for the named VLAN or all VLANs.                                            |
| <b>scsirouter serverif</b> | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
| <b>show vlan</b>           | Display configuration and operational information for the specified VLAN or all VLANs.                     |
| <b>show vtp</b>            | Display configuration and operational information for VTP.                                                 |
| <b>vlan</b>                | Configure a non-VTP VLAN on the SN 5428.                                                                   |
| <b>vtp mode</b>            | Configure the SN 5428 to operate in client or transparent VTP mode.                                        |

# vtp mode

To assign the VTP mode in which the SN 5428 Storage Router operates, use the **vtp mode** command.

**vtp mode {client | transparent}**

| Syntax Description | client                                                                                                                                                                                                  | transparent                                                                                                                                                                                  |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | The SN 5428 will operate in VTP Client mode. The SN 5428 will exchange VTP packets with an externally attached switch to learn about the VLANs that are accessible in the network. This is the default. | The SN 5428 will operate in VTP Transparent mode. The SN 5428 will not exchange VTP packets and will only learn about VLANs from explicit SN 5428 configuration via the <b>vlan</b> command. |

**Defaults** Client.

**Command Modes** Administrator.

| Command History | Release | Modification                 |
|-----------------|---------|------------------------------|
|                 | 2.2.1   | This command was introduced. |

**Usage Guidelines** In a cluster environment, VTP configuration functions are handled by a single SN 5428. To determine which SN 5428 is performing VTP configuration functions, issue the **show cluster** command. The SN 5428 that is performing VLAN management also performs VTP configuration. If you issue the **vtp mode** command from a storage router that is not performing VTP configuration functions, the CLI displays an informational message with the name of the SN 5428 that is currently handling those functions. For more information on operating the SN 5428 in a cluster, see Chapter 10, “Maintaining and Managing the SN 5428 Storage Router.”

VTP operates in either client or transparent mode. In client mode, the SN 5428 exchanges VTP packets with a locally connected switch to learn about the VLANs available in the network. In transparent mode, VTP packets are ignored and VLAN information is pulled directly from the SN 5428 cluster configuration.

When operating as a VTP client, the SN 5428 sends a VTP advertisement when one of the following events occur:

- The Gigabit Ethernet interface on any SN 5428 in the cluster transitions to the *up* state and a valid domain name has either been configured or previously learned.
- The VTP domain name changes.
- A VTP summary advertisement is received with a higher configuration revision.

The switch replies to the SN 5428 with a summary advertisement, followed by one or more subset advertisements.

When operating in transparent mode, the SN 5428 ignores any VTP packets it may receive. VLANs are configured using the GUI or the CLI **vlan** command. Use transparent mode when the SN 5428 is connected to a switched network that does not support VTP but does support 802.1Q VLANs.

### Examples

The following example places the SN 5428 in VTP Transparent mode:

```
[SN5428A] # vtp mode transparent
```

### Related Commands

| Command                    | Description                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------|
| <b>restore vlan</b>        | Restore VLAN configuration information from the named configuration file.                                  |
| <b>save all</b>            | Save all configuration information, including VLAN information.                                            |
| <b>save scsirouter</b>     | Save configuration information for the named SCSI routing instance.                                        |
| <b>save system</b>         | Save selected system configuration information, including VLAN information.                                |
| <b>save vlan</b>           | Save configuration information for the named VLAN or all VLANs.                                            |
| <b>scsirouter serverif</b> | Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance. |
| <b>show vlan</b>           | Display configuration and operational information for the specified VLAN or all VLANs.                     |
| <b>show vtp</b>            | Display configuration and operational information for VTP.                                                 |
| <b>vlan</b>                | Configure a non-VTP VLAN on the SN 5428.                                                                   |
| <b>vtp domain</b>          | Assign a VTP domain name to the SN 5428.                                                                   |





---

## Symbols

\* (asterisk), meaning of in prompt **2-9**

---

## Numerics

802.1Q

trunk port setting **4-1**

VLAN encapsulation **1-15, 4-1, 11-360**

---

## A

AAA

about **1-17, 8-2**

*See also* authentication

aaa authentication iscsi command **8-7, 11-3**

aaa new-model command **11-5**

aaa test authentication command **8-8, 11-6**

access, configuring for SCSI routing **6-11**

access control

SCSI routing and **1-6**

transparent SCSI routing and **1-12**

accessing iSCSI targets

access lists **6-11**

denying **6-12**

access list **6-10**

CHAP user name **6-9**

IP address **6-9**

iSCSI Name **6-9**

accesslist A.B.C.D/bits command **11-10**

accesslist chap-username command **11-12**

accesslist command **6-10, 6-11, 11-8**

accesslist description command **6-10, 11-14**

accesslist iscsi-name command **11-16**

access lists

adding entries **11-10, 11-12, 11-16**

associating with iSCSI target **6-11, 11-191**

cluster environment

creating in **6-11**

maintaining in **6-11**

clusters and **10-11, 11-10, 11-12, 11-16**

configuring **6-11**

creating **6-9, 11-8**

function of **1-7**

adding

access list entries **6-10, 11-10, 11-12, 11-16**

iSCSI target description **11-193**

iSCSI targets **6-7, 11-205, 11-208**

routes **11-108, 11-112**

SN 5428s to cluster **9-2**

admin contactinfo command **3-6, 11-18**

administrator contact information, configuring **3-6, 11-18**

administrator password, configuring **3-6**

admin password command **3-6, 11-20**

angle brackets **xi**

asterisk (\*), meaning of in CLI **2-9**

audience **ix**

authentication

configuration elements (figure) **8-3**

configuring **8-1**

creating list **8-7**

enabling **8-8**

example configuration (figure) **8-4**

overview **1-17**

saving configuration **8-9**

testing **8-8**

verifying configuration 8-9  
 automating tasks with scripts 10-24

---

## B

backing up system configuration 10-8  
 backups, restoring from 10-9  
 boldface font xi  
 boldface screen font xi  
 braces xi  
 buffer-to-buffer credit 11-75

---

## C

capturing configuration 10-33  
 CDB retry count 11-177  
 CDP  
   about 10-23  
   disabling 10-24  
   enabling 11-22  
   managing 10-23  
   modifying  
     holdtime 10-24  
     timeout value 10-24  
 cdp enable command 11-22  
 cdp holdtime command 11-23  
 cdp interface command 11-24  
 cdp timer command 11-25  
 Challenge Handshake Authentication Protocol  
   *See* CHAP  
 CHAP 1-17, 8-2  
 character case sensitivity in CLI 2-9  
 checklist, first-time configuration (table) 2-5  
 CIDR style xi  
 Cisco Discovery Protocol  
   *See* CDP  
 classless interdomain routing style  
   *See* CIDR style

clear conf {all | system} command 11-28  
 clear conf command 2-6, 10-16, 10-17, 11-26  
 clear counters interface command 11-30  
 clear counters scsirouter command 11-31  
 clear fc command 11-32  
 clearing  
   accumulated operational statistics 11-30, 11-31  
   failover list 11-36  
   Fibre Channel switch log entries 11-32  
   log file entries 11-34  
   logging table rules 11-35  
   system configuration 11-26, 11-28  
 clear log command 11-34  
 clear logging table command 11-35  
 clear scsirouter failover command 11-36

## CLI

  about commands 11-1  
   administrator mode 2-9  
   automating tasks with scripts 10-24  
   character case sensitivity 2-9  
   command modes 2-9  
   command prompt  
     about 2-9  
     asterisk (\*), meaning of 2-9  
   monitor mode 2-9  
   overview 2-8  
   reserved words 2-9  
   special keys 2-10  
   starting management session 2-10  
   usage tips 11-1  
 clock, configuring 3-4  
 clock set command 3-4, 11-38  
 clock timezone command 3-4, 11-39  
 clusters  
   access lists and 3-7, 6-11, 10-11, 11-8, 11-10, 11-12, 11-16  
   adding SN 5428s to 9-2  
   automatic failover 10-21  
   configuration requirements 11-102  
   configuring 9-1 to 9-5

- controlling SCSI routing instances **10-18**
- failing over SCSI routing instances **10-21**
- joining
  - different cluster **9-5**
  - existing cluster **3-7**
- manual failover **10-21**
- maximum number of SCSI routing instances **11-173**
- overview **1-17**
- precautions for setting boot version **10-7**
- resetting system and **10-15**
- retaining configuration data **11-216**
- shared configuration settings **9-2**
- VLANs and **4-4, 10-12, 11-360**
- VTP and **11-362, 11-364**
- See also* high availability
- collecting configuration information **2-2**
- command modes
  - administrator **2-9**
  - monitor **2-9**
- command prompt in CLI
  - about **2-9**
  - asterisk (\*), meaning of **2-9**
- command scripts **10-24**
- command syntax conventions **xi**
- configuration
  - capturing **10-33**
  - collecting information **2-2**
- configuration checklist, first-time (table) **2-5**
- configuration script, initial system **2-6**
- configuration wizard, setup **2-7**
- connecting a console **2-6**
- console, connecting **2-6**
- conventions **xi**
- copy command **9-4, 10-8, 10-9, 11-40**
- crash log **10-27**
- creating
  - access lists **6-9, 11-8**
  - authentication list **8-7**
  - SCSI routing instances **6-6, 11-173**

---

## D

- data buffer credit capacity **11-75**
- date, configuring **3-4**
- debug aaa command **11-42**
- debug cmd command **11-44**
- debug facilities **10-33**
- debug scsirouter command **11-45**
- debug scsirouter target command **11-46**
- default FC interface configuration **11-87**
- delete accesslist command **11-47**
- delete logging command **11-50**
- delete savedconfig command **10-17, 11-53**
- delete script command **11-54**
- delete scsirouter command **11-56**
- delete software version command **10-5, 10-6, 11-58**
- deleting
  - access list **11-47**
  - access list elements **11-47**
  - command file **11-54**
  - logging table rule **11-50**
  - saved configuration file **11-53**
  - script **11-54**
  - SCSI routing instance elements **11-56**
  - software version **11-58**
- diagnostics, understanding **10-30**
- disabling connections **10-19**
- displaying available software **10-2, 10-5**
- DNS **3-3, 11-109, 11-110**
- document conventions **xi**
- document organization (table) **x**
- domain ID **1-16, 5-2**
  - configure **5-2, 11-72**
- domain name, configuring **3-3**
- downloading software **10-5**
- download software command **10-2, 10-5, 10-6, 11-59**

---

**E**E\_Port **1-3, 1-15**    resetting **5-2**

EIA/TIA-232 console interface

    requiring password **3-6**enable command **2-10, 11-61**enable FC interfaces **11-74, 11-91**

enabling access

    FTP **11-157**    HTTP **11-157**    rlogin **11-157**    SNMP **11-157**    SSL **11-157**    Telnet **11-157**enabling connections **10-19**event information **10-26**

event messages

    about **10-30**    filtering **10-32**    routing **10-32**exit command **11-62**

---

**F**failover **10-21**    *See also* clusters; high availabilityfailover command **10-22, 10-23**failover scsirouter command **9-3, 9-4, 10-7, 11-63**FAN loop login behavior **11-92**FC hosts, displaying information **11-279**FC interfaces **6-2**    default values **6-14**    diagnostic mode **11-71**    displaying internal configuration **11-267**    enabling **11-74, 11-91**    Fabric Address Notification **11-92**    fairness algorithm **11-85**    global configuration information **11-273**linkspeed **11-94**loopback testing **11-96**Multi-frame sequence bundling **11-98**naming **1-18**no active zoneset **11-81**operational characteristics **6-14**port types **6-14, 11-100**returning to default configuration **11-87**save zoning changes **11-79**set data buffer credit capacity **11-75**set zoning merge compliances **11-83**specify domain ID for zoned fabric **5-2, 11-72**testing **11-89**transfer rate **11-94**FC storage **1-3**filtering event messages **10-32**first-time configuration checklist (table) **2-5**FTP **10-28**

---

**G**

Gigabit Ethernet interface

    naming **1-18**    *See* server interfaceGUI, about **2-11**

---

**H**

HA

*See* high availabilityhalt command **10-15, 11-65**hardware interface naming **1-18**help command **11-67**

high availability

    cluster name, configuring **3-7**    configuration mode, selecting **3-7**    deleting current configuration **3-7**    failover **10-21**

- automatic **10-21**
- handling **10-21**
- HA interface, configuring **3-7, 11-104**
- heartbeats **10-21**
- retaining current configuration **3-7**
- shared configuration settings **9-2**
- See also* clusters
- high availability clusters
  - See* clusters
- hostname command **3-3, 11-68**
- HTTPS
  - See* SSL

---

**I**

- IEEE 802.1Q
  - See* 802.1Q
- IETF **1-2**
- initial system configuration script **2-6**
- initiator WWPN1 **1-16, 5-2**
- initiator WWPN2 **1-16, 5-2**
- installing updated software **10-2**
- interface
  - Fibre Channel naming **1-18**
  - naming **1-18**
  - settings, configuring **11-102**
- interface fc? al-fairness command **11-85**
- interface fc? default command **11-87**
- interface fc? diag command **11-89**
- interface fc? enable command **11-91**
- interface fc? fan-enable command **11-92**
- interface fc? linkspeed command **11-94**
- interface fc? loopback command **11-96**
- interface fc? mfs-bundle command **11-98**
- interface fc? type command **11-100**
- interface fc devlog command **11-69**
- interface fc diag command **11-71**
- interface fc domainid command **5-2, 11-72**
- interface fc enable command **11-74**
- interface fc interop-credit command **11-75**
- interface fc syslog command **11-77**
- interface fc zoning autosave command **11-79**
- interface fc zoning default command **11-81**
- interface fc zoning merge command **11-83**
- interface ge? command **11-102**
- interface ha ip-address command **11-104**
- interface mgmt ip-address command **3-3, 11-106**
- Internet Engineering Task Force
  - See* IETF
- Inter-Switch Link (ISL) **4-1**
- ip default-gateway command **11-108**
- ip domain-name command **3-3, 11-109**
- ip name-server command **3-3, 11-110**
- ip route command **3-3, 3-4, 4-4, 11-112**
- iSCSI authentication
  - See* authentication
- iSCSI CHAP
  - See* CHAP
- iSCSI driver **1-4, 1-5, 1-6, 6-2, 8-1, 8-2, 8-6, 10-7, 10-18**
  - TOE **1-1**
- iSCSI drivers **1-1, 1-19**
  - configuring **ix**
  - example configuration files, obtaining **ix**
  - installing **ix**
  - port for iSCSI traffic **11-219**
  - readme file, obtaining **ix**
  - transparent SCSI routing and **1-10**
- iSCSI Name
  - adding to access list **11-16**
  - determining **11-16, 11-309**
  - using to identify IP host **11-16**
- iSCSI port **11-219**
- iSCSI protocol **1-2**
- iSCSI targets
  - access list control **6-11**
  - allowing connections **11-195**
  - configuring **6-7, 11-198, 11-200, 11-205, 11-208**
  - configuring access **6-11**

disabling **11-195**  
 enabling **11-195**  
 SCSI routing and **1-5**  
 transparent SCSI routing and **1-11**  
 italic font **xi**

---

## L

local username database  
   about **8-2**  
   configuring **8-6**  
 log file  
   clearing **10-26**  
   filtering event messages **10-32**  
   managing **10-26**  
   routing event messages **10-32**  
   saving **10-33**  
   viewing **10-33**  
 logging  
   adding routing rules **11-118**  
   destinations **11-114, 11-118**  
   disabling **11-122**  
   enabling **11-122**  
   facilities **11-114, 11-118**  
   filtering event messages **10-32**  
   insert routing rule **11-114**  
   notification levels **11-114, 11-118**  
   remote syslog host **11-124**  
   routing event messages **10-32**  
   understanding **10-30**  
 logging #? command **11-114**  
 logging level command **11-118**  
 logging on command **11-122**  
 logging syslog command **11-124**  
 logging table  
   building **11-50, 11-114, 11-118**  
 logical targets  
   *See* iSCSI targets  
 logout command **11-126**

---

## M

maintaining  
   access lists **6-11**  
   storage router **10-1**  
 management interface  
   clusters and **3-3**  
   configuring **3-3, 11-106**  
 management session, starting **2-10**  
 management station  
   SCSI routing and **1-5**  
   transparent SCSI routing and **1-11**  
 managing the storage router **10-1 to 10-33**  
 mapping storage  
   SCSI routing and **1-5**  
   target-and-LUN examples (table) **1-6**  
   target-and-LUN using LUNWWN addressing **6-8**  
   target-and-LUN using serial number addressing **6-8**  
   target-and-LUN using WWPN addressing **6-7**  
   target-only examples (table) **1-6**  
   target-only using WWPN addressing **6-9**  
   transparent SCSI routing and **1-11**  
 merging cluster configuration data **11-216**  
 message notification levels **10-30**  
 messages  
   about **10-30**  
   filtering **10-32**  
   routing **10-32**  
 monitor password, configuring **3-6**  
 monitor password command **3-6, 11-127**  
 MTU size  
   specifying for GbE interfaces **11-102**  
   specifying for VLAN **4-4**  
   verifying **4-6**

---

## N

network management access  
   configuring **3-5**

SNMP, configuring 3-5

no aaa authentication iscsi default command 11-3

no aaa new-model command 11-5

no cdp enable command 11-22

no cdp holdtime command 11-23

no cdp interface command 11-24

no cdp timer command 11-25

no debug aaa command 11-42

no debug scsirouter command 11-45

no debug scsirouter target command 11-46

no interface fc? al-fairness command 11-85

no interface fc? enable command 11-91

no interface fc? fan-enable command 11-92

no interface fc? mfs-bundle command 11-98

no interface fc domainid command 11-72

no interface fc enable command 5-2, 11-74

no interface fc zoning autosave command 11-79

no interface ge? vlan enable command 11-102

no ip default-gateway command 11-108

no ip domain-name command 11-109

no ip name-server command 11-110

no ip route command 11-112

no logging on command 11-122

no logging syslog command 11-124

no ntp peer command 11-129

no radius-server host command 11-132

no radius-server key command 11-134

no radius-server retransmit command 11-136

no radius-server timeout command 11-138

no restrict command 11-157

no restrict console command 11-160

no tacacs-server host command 11-350

no tacacs-server key command 11-352

no tacacs-server timeout command 11-354

notification levels 10-30

no username command 11-356

no vlan command 11-360

ntp peer command 3-4, 11-129

NTP server, configuring 3-4, 11-129

---

## O

operational statistics, viewing 10-21

organization of document (table) x

---

## P

passwords

- about 8-6
- configuring
  - administrator 3-6
  - for authentication 8-6
  - monitor 3-6
- default admin 11-20
- default monitor 11-127
- encrypted format 8-7
- factory defaults 2-9
- recovering 10-18
- rules 8-6

ping command 11-131

powering down 10-15

prompt in CLI

- about 2-9
- asterisk (\*), meaning of 2-9

---

## R

RADIUS

- about 8-2
- configuring 8-5, 11-132
- global encryption key 11-134
- global retransmit count 11-136
- global timeout value 11-138

radius-server host command 8-5, 11-132

radius-server key command 8-5, 11-134

radius-server retransmit command 11-136

radius-server timeout command 11-138

read command 11-140

reboot command 10-7, 11-142

recovering passwords **10-18**  
 related documentation **xii**  
 reserved words in CLI **2-9**  
 reserve proxy feature  
     passthru commands to IP host **11-187**  
     track SCSI reserve/release commands **11-187**  
 resetting logging table **11-35**  
 resetting system  
     clusters and **10-15**  
     removing saved configuration files **10-17**  
     retaining system settings **10-17**  
     to factory defaults **10-15**  
 restore aaa command **10-12, 11-144**  
 restore accesslist command **9-5, 10-11, 11-146**  
 restore all **10-17**  
 restore all command **11-148**  
 restore scsirouter command **10-9, 11-150**  
 restore system command **10-14, 11-152**  
 restore vlan command **10-12, 11-155**  
 restoring  
     AAA authentication information **10-12**  
     access list **10-10**  
     deleted SCSI routing instance **10-9**  
     existing SCSI routing instance **10-10**  
     from backups **10-9**  
     system configuration **10-13**  
     VLANs **10-12**  
 restrict command **3-5, 11-157**  
 restrict console command **3-6, 11-160**  
 restricting access  
     FTP **11-157**  
     HTTP **11-157**  
     rlogin **11-157**  
     SNMP **11-157**  
     SSL **11-157**  
     Telnet **11-157**  
 routing event messages **10-32**

---

## S

save aaa command **11-161**  
 save accesslist command **11-163**  
 save all command **3-8, 10-8, 11-165**  
 save scsirouter command **10-8, 10-9, 11-167**  
 save system command **3-8, 11-169**  
 save vlan command **11-171**  
 screen font **xi**  
 screen font, boldface **xi**  
 script directory **10-24**  
 scripts, automating tasks **10-24**  
 scsirouter authenticate command **8-8, 11-175**  
 scsirouter cdbretrycount command **11-177**  
 scsirouter command **6-6, 11-173**  
 scsirouter description command **11-178**  
 scsirouter enable command **10-9, 11-179**  
 scsirouter failover command **11-181**  
 scsirouter lun reset command **11-183**  
 scsirouter primary command **9-4, 10-23, 11-185**  
 scsirouter reserveproxy command **11-187**  
 scsirouter serverif command **6-6, 11-189**  
 scsirouter target {enabled | disabled} command **11-195**  
 scsirouter target {serial | lunwwn | wwpn} #?  
     command **11-197**  
 scsirouter target accesslist command **6-11, 11-191**  
 scsirouter target description command **11-193**  
 scsirouter target disabled command **10-19**  
 scsirouter target enabled command **10-19**  
 scsirouter target lun lunwwn command **6-8, 11-200**  
 scsirouter target lun serial command **6-8, 11-203**  
 scsirouter target lun wwpn lun command **6-7, 11-205**  
 scsirouter target wwpn command **6-9, 11-208**  
 SCSI routing  
     access control **1-6**  
     basic network structure **1-5**  
     configuration elements (figure) **6-3**  
     configuring **6-1 to 6-12**  
     example configuration (figure) **6-4**

- instances, about **1-8**
- mapping storage **1-5**
- overview **1-3 to 1-8**
- routing SCSI requests and responses **1-4**
- saving configuration **6-13**
- troubleshooting **11-269**
- verifying configuration **6-13 to 6-14**
- SCSI routing instances
  - adding iSCSI target description **11-193**
  - allowing connections to iSCSI target **11-195**
  - assigning preferred SN 5428 **11-185**
  - changing configuration **10-18**
  - configuring
    - CDB retry count **11-177**
    - iSCSI targets **6-7**
    - server interface **6-6**
  - controlling **10-18**
  - creating **6-6, 11-173**
  - disabling
    - connections **10-19**
    - iSCSI targets **11-195**
    - reserve proxy feature **11-187**
  - enabling
    - connections **10-19**
    - iSCSI targets **11-195**
    - reserve proxy feature **11-187**
  - failover **10-21**
  - maximum number **11-173**
  - starting **10-20**
  - stopping **10-20**
  - troubleshooting **11-269**
  - VLAN access to storage devices via (figure) **6-5**
- Secure Sockets Layer Support
  - See* SSL
- security services
  - See* authentication
- sequencing FC frames **11-98**
- server interface
  - SCSI routing instance, configuring for **6-6, 11-189**
  - setting software boot version **10-7**
  - setup access command **9-4, 11-214**
  - setup cluster command **3-7, 9-3, 9-5, 11-216**
  - setup command **2-8, 11-211**
  - setup configuration wizard **2-7, 11-211**
  - setup iscsi-port command **11-219**
  - setup mgmt command **11-221**
  - setup netmgmt command **9-4, 11-223**
  - setup scsi command **11-225**
  - setup time command **9-4, 11-227**
  - show aaa command **8-9, 11-229**
  - show accesslist command **6-13, 11-231**
  - show admin command **3-8, 11-233**
  - show boot command **11-234**
  - show bootconfig command **11-235**
  - show buffers command **11-241**
  - show cdp command **11-245**
  - show cdp entry command **11-247**
  - show cdp interface command **11-249**
  - show cdp neighbors command **11-251**
  - show cdp traffic command **11-254**
  - show cli command **2-9, 11-256**
  - show clock command **11-257**
  - show cluster command **3-7, 3-8, 9-2, 9-3, 11-258**
  - show cpu command **11-261**
  - show crash command **11-262**
  - show debug command **11-264**
  - show debug fc brief **5-2**
  - show debug fc command **11-267**
  - show debug scsirouter command **11-269**
  - show device command **5-3**
  - show devices command **7-4, 11-270**
  - show diagnostics command **11-272**
  - show fc command **11-273**
  - show ha command **11-275**
  - show hosts command **11-279**
  - show interface command **7-3, 11-280**
  - show ip command **11-289**
  - show ip route command **3-8**

- show logging command **11-291**
- show memory command **11-293**
- show modules command **11-295**
- show restrict command **11-297**
- show route command **11-299**
- show runningconfig command **11-300**
- show savedconfig command **10-9, 11-306**
- show script command **11-308**
- show scsirouter command **6-14, 7-2, 10-9, 11-309**
- show scsirouter stats command **10-21**
- show sessions command **11-313**
- show snmp command **3-8, 11-314**
- show software version command **10-2, 11-316**
- show software version command, example **10-3**
- show stack command **11-318**
- show system command **3-8, 11-320**
- show task command **11-323**
- show tech-support command **11-325**
- show version command **11-328**
- show vlan command **4-6, 11-329**
- show vtp command **4-5, 11-331**
- shutting down **10-15**
- site-specific contact information, configuring **11-18**
- SNMP messages **10-23**
- snmp-server command **3-5, 11-333**
- software
  - available versions **10-2, 10-5**
  - boot version, setting **10-7**
  - downloading **10-5**
  - overview **1-2**
  - updating **10-2**
- software http url command **10-4, 11-335**
- software http username command **10-4, 11-337**
- software proxy command **10-4, 11-339**
- software proxy url command **10-4, 11-341**
- software proxy username command **10-4, 11-343**
- software tftp command **10-5, 11-345**
- software version command **10-7, 11-347**
- special keys in CLI **2-10**
- square brackets **xi**
- SSL **1-3**
- starting
  - CLI management session **2-10**
  - SCSI routing instances **10-20**
- static route table **11-108, 11-112**
- stopping, SCSI routing instances **10-20**
- storage router software overview **1-2**
- strings, user-defined text
  - case sensitivity **2-9**
  - command syntax convention **xi**
- switch interconnect
  - See also* E\_Port
- switch log files
  - clearing **11-32**
  - configure devlog logging parameters **11-69**
  - configure syslog logging parameters **11-77**
- syntax conventions (table) **xi**
- system clock, configuring **11-38**
- system configuration, verifying **3-8**
- system configuration script, initial **2-6**
- system management **10-1 to 10-33**
- system messages, capturing **10-30**
- system name
  - CLI command prompt and **2-9**
  - configuring **3-3**
- system parameters
  - configuring **3-1 to 3-7**
  - restoring **10-13**
  - verifying **3-8**

---

## T

- TACACS+
  - about **8-2**
  - configuring **8-6, 11-350**
  - global encryption key **11-352**
  - global timeout value **11-354**
- tacacs-server host command **8-6, 11-350**

tacacs-server key command **8-6, 11-352**  
 tacacs-server timeout command **11-354**  
 target-and-LUN mapping examples (table) **1-6**  
 target-only mapping examples (table) **1-6**  
 targets  
     *See* iSCSI targets  
 TCP/IP Offload Engine  
     *See* TOE  
 Telnet, starting CLI management session **2-10**  
 terminal emulation, configuring **2-6**  
 testing FC interfaces **11-71, 11-89, 11-96**  
 text strings, user-defined  
     case sensitivity **2-9**  
     command syntax convention **xi**  
 time, configuring **3-4**  
 time zone, specifying **3-4**  
 TOE **1-1**

transparent SCSI routing  
     access control **1-12**  
     basic network structure **1-11**  
     configuring **7-1 to 7-2**  
     discovering new targets **7-2**  
     instances, about **1-14, 7-1**  
     iSCSI drivers and **1-10**  
     mapping storage **1-11**  
     overview **1-8 to 1-14**  
     routing SCSI requests and responses **1-10**  
     verifying configuration **7-2 to 7-4**  
 troubleshooting  
     debugging OS commands **11-44**  
     gathering information for **10-27**

## U

updating software  
     about **10-2**  
     downloading **10-5**  
     setting boot version **10-7**

user-defined text strings  
     case sensitivity **2-9**  
     command syntax convention **xi**  
 username database, local  
     about **8-2**  
     configuring **8-6**  
 username password command **8-6, 11-356**

## V

verify software version command **11-358**  
 vertical bars **xi**  
 VID **1-2, 1-6, 1-15, 4-4**  
 viewing  
     available software **10-2, 10-5**  
     operational statistics **10-21**  
 VLAN access, overview **1-14 to 1-15**  
 vlan command **4-4, 11-360**  
 VLAN encapsulation **1-15, 4-1, 11-360**  
 VLAN identifier number  
     *See* VID  
 VLANs  
     802.1Q **4-1**  
     assigning  
         to SCSI routing instance **4-6, 6-6**  
         unique name **4-4**  
     clusters and **4-4, 10-12, 11-360**  
     configuring for **4-1 to 4-4**  
     IP route, configuring **4-4**  
     MTU size, specifying **4-4**  
     server interface, configuring **4-6, 6-6**  
     switch port setting for Cisco switch **4-1**  
     verifying configuration **4-5 to 4-6**  
     VID **4-4**  
 VTP  
     client mode **4-3**  
     clusters and **11-362, 11-364**  
     domain name, assigning **4-3**  
     transparent mode **4-4**

- verifying
  - configured settings **4-5**
  - operational information **4-5**
- vtp domain command **4-3, 11-362**
- vtp mode command **4-3, 4-4, 11-364**

---

## W

- web-based GUI, about **2-11**
- wizards
  - setup **2-7, 11-211**
  - setup access **11-214**
  - setup cluster **11-216**
  - setup iscsi-port **11-219**
  - setup mgmt **11-221**
  - setup netmgmt **11-223**
  - setup scsi **11-225**
  - setup time **11-227**
- WWPN
  - zoning **1-16**
- WWPN1
  - initiator **1-16, 5-2**
- WWPN2
  - initiator **1-16, 5-2**

---

## Z

- zones
  - clearing saved configuration information **5-1, 11-32**
  - default behavior with no active zoneset **11-81**
  - saving changes **11-79**
  - set merge compliance **11-83**
  - specify domain ID **5-2, 11-72**
- zoning **1-3, 1-15, 5-1**
  - configuring **5-1**
  - fabric participation **1-16**
  - initiators WWPN1 and WWPN2 **1-16, 5-2**
  - WWPN **1-16**