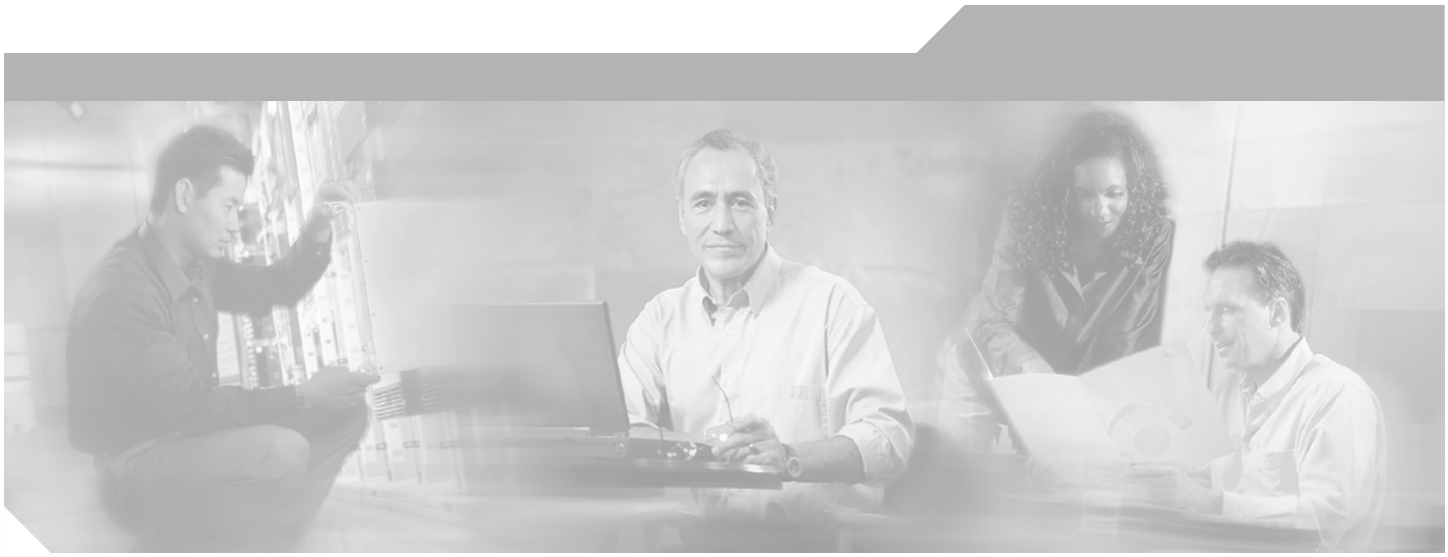
Cisco Systems

Send documentation comments to mdsfeedback-doc@cisco.com.



Cisco MDS 9000 Family Command Reference

Cisco MDS SAN-OS Release 3.0(1) through 3.0(2)
May 2006

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

Text Part Number: OL-8413-02

Cisco MDS 9000 Family Command Reference

CONTENTS

New and Changed Information

Table 1 summarizes the new and changed commands for Cisco MDS SAN-OS Release 3.x, and tells you where they are documented in the *Cisco MDS 9000 Family Command Reference*.

Table 1 New and Changed Commands in the Cisco MDS 9000 Family Command Reference

Feature	Description	Where Documented
New and Changed Commands for Cisco SAN-OS Release 3.0(2)		
Fibre Channel domains	**fcdomain** command (**optimize fast-restart** option)	F Commands
FICON enhancements	**ficon port default-state prohibit-all** command	F Commands
	show ficon command (**port default-state** option)	Show Commands
New and Changed Commands for Cisco SAN-OS Release 3.0(1)		
AAA enhancements	**aaa authentication login** command (**mschap** option)	A Commands

Table 1 New and Changed Commands in the Cisco MDS 9000 Family Command Reference

Feature	Description	Where Documented
	deadtime (radius group configuration) command **deadtime (tacacs+ group configuration)** command	D Commands
	debug radius command (**server-monitor** and **server-monitor-errors** options) **debug tacacs+** command (**server-monitor** and **server-monitor-errors** options)	Debug Commands
	radius-server deadtime command **radius-server directed-request** command **radius-server host** command (*ipv6-address* argument and **test** option)	R Commands
	server (radius configuration) command (*ipv6-address* argument) **server (tacacs+ configuration)** command (*ipv6-address* argument)	S Commands
	show aaa authentication command (**mschap** option) **show radius-server** command (*server-name*, *ipv4-address*, and *ipv6-address* arguments; **directed-request** and **statistics** options) **show tacacs-server** command (*server-name*, *ipv4-address*, and *ipv6-address* arguments; **directed-request** and **statistics** options)	Show Commands
	tacacs-server deadtime command **tacacs-server directed-request** command **tacacs-server host** command (*ipv6-address* argument and **test** option)	T Commands
	username command (**ssh-cert-dn**, **dsa**, and **rsa** options)	U Commands
boot auto-copy command enabled by default	**boot** command (**auto-copy** default state changed to enabled)	B Commands
Call Home	**alert-group** command	A Commands
	show callhome command (**user-def-cmds** option)	Show Commands

Table 1 New and Changed Commands in the Cisco MDS 9000 Family Command Reference

Feature	Description	Where Documented
Certificate authorities and digital certificates	**crypto ca authenticate** command **crypto ca crl request** command **crypto ca enroll** command **crypto ca export** command **crypto ca import** command **crypto ca test verify** command **crypto ca trustpoint** command **crypto key generate rsa** command **crypto key zeroize rsa** command	C Commands
	delete ca-certificate command **delete certificate** command	D Commands
	debug cert-enroll command	Debug Commands
	enrollment terminal command	E Commands
	ocsp url command	O Commands
	revocation-check command **rsakeypair** command	R Commands
	show crypto ca certificates command **show crypto ca crl** command **show crypto ca trustpoints** command **show crypto key mypubkey rsa** command	Show Commands
CFS support for allowed domain ID list	**fcdomain abort vsan** command **fcdomain commit vsan** command **fcdomain distribute** command	F Commands
	show fcdomain command (**pending**, **pending-diff**, **session-status**, and **status** options)	Show Commands
CFS over IP	**cfs ipv4 distribute** command **cfs ipv4 mcast-address** command **cfs ipv6 distribute** command **cfs ipv6 mcast-address** command	C Commands

Table 1 New and Changed Commands in the Cisco MDS 9000 Family Command Reference

Feature	Description	Where Documented
CFS support for RSCN	**clear rscn session vsan** command	C Commands
	rscn abort vsan command **rscn commit vsan** command **rscn distribute** command **rscn event-tov** command	R Commands
	show rscn command (**event-tov**, **pending**, and **pending-diff** options)	Show Commands
CLI Enhancements	**cli alias name** command **cli var name (EXEC)** command **cli var name (configuration)** command	C Commands
	show cli alias command **show cli variables** command	Show Commands
	pwc command	P Commands
	run-script command (added example showing user-defined variable)	R Commands
Cloud Discovery	**cloud discover** command **cloud discovery** command **cloud-discovery enable** command	C Commands
	debug cloud command	Debug Commands
	show cloud discovery command **show cloud membership** command **show debug** command (**cloud** option)	Show Commands
Configuration Check	**show incompatibility system** command (added example showing that the command output provides the commands to disable incompatible features)	Show Commands
Crossbar graceful shutdown	**out-of-service module** command **out-of-service xbar** command	O Commands
Deprecated Commands	**fcid-last-byte** command	F Commands
EPLD enhancements for the MDS 9513	**install clock-module** command	I Commands
	show version command (**clock-module** option)	Show Commands

Table 1 New and Changed Commands in the Cisco MDS 9000 Family Command Reference

Feature	Description	Where Documented
FICON Port Numbering	**ficon enable** command	F Commands
	ficon logical-port assign port-numbers command	
	ficon slot assign port-numbers command	
	ficon swap command (**interface** option)	
	show ficon command (**port-numbers** and **stat** options; **pib** and **portnumber** keywords)	Show Commands
Generation 2 Module Support	**channel-group** command	C Commands
	debug port-resources command	Debug Commands
	out-of-service command	O Commands
	switchport command (**fcbbscn** option, **ST** option to **mode** keyword, **4000** option to **speed** keyword, **auto max 2000** option to **speed** keyword, **rate-mode** keyword; added Gigabit Ethernet interface syntax and management interface syntax)	S Commands
	show interface command (**fc capabilities** option)	Show Commands
	show module command (**recovery-steps** and **x-bar** options)	
	show port index-allocation command	
	show port-resources module command	
IKE Enhancements	**authentication** command	A Commands
	identity command	I Commands
	keycommand(**hostname** keyword)	K Commands

Table 1 New and Changed Commands in the Cisco MDS 9000 Family Command Reference

Feature	Description	Where Documented
IPv6	**clear ips stats** command **clear ipv6 access-list** command **clear ipv6 neighbors** command **clear vrrp** command (**ipv4** and **ipv6** options)	C Commands
	deny (IPv6-ACL configuration) command	D Commands
	ipv6 access-list command **ipv6 address** command **ipv6 address autoconfig** command **ipv6 enable** command **ipv6 nd** command **ipv6 route** command **ipv6 routing** command **ipv6 traffic-filter** command	I Commands
	permit (IPv6-ACL configuration) command **ping** command(**ipv6** option)	P Commands
	show ip arp command **show ip interface** command **show ip traffic** command **show ips ipv6** command **show ipv6 access-list** command **show ipv6 interface** command **show ipv6 neighbours** command **show ipv6 route** command **show ipv6 routing** command **show ipv6 traffic** command **show vrrp** command (**ipv6** option)	Show Commands
	traceroute command (**ipv6** option)	T Commands
	vrrp command(**ipv6** option; **address** and **advertisement-interval** options specific to IPv6)	V Commands
iSCSI Server Load Balancing (iSLB)	**clear islb session** command	C Commands
	debug ips command (**iSLB** and **iSNS** options)	Debug Commands

Table 1 New and Changed Commands in the Cisco MDS 9000 Family Command Reference

Feature	Description	Where Documented
	iscsi dynamic initiator command **islb abort** command **islb commit** command **islb distribute** command **islb initiator** command **islb save-initiator** command **islb virtual-target name** command **islb vrrp** command **islb zoneset activate** command	I Commands
	member (zone configuration and zoneset-zone configuration submode) command (*ipv6* argument) **metric (iSLB initiator configuration)** command **mutual-chap username (iSCSI initiator configuration and iSLB initiator configuration)** command (added iSLB initiator configuration submode)	M Commands
	show islb cfs-session status command **show islb initiator** command **show islb merge status** command **show islb pending** command **show islb pending-diff** command **show islb session** command **show islb status** command **show islb virtual-target** command **show islb vrrp** command	Show Commands
	static (iSCSI initiator configuration and iSLB initiator configuration) command (added iSLB initiator configuration submode)	S Commands
	target (iSLB initiator configuration) command	T Commands
	username (iSCSI initiator configuration and iSLB initiator configuration) command (added iSLB initiator configuration submode)	U Commands
	vsan (iSCSI initiator configuration and iSLB initiator configuration) command (added iSLB initiator configuration submode)	V Commands
	zonename (iSLB initiator configuration) command	Z Commands

Table 1 New and Changed Commands in the Cisco MDS 9000 Family Command Reference

Feature	Description	Where Documented
IVR	**clear ivr service-group database** command	C Commands
	ivr copy active-service-group user-configured-service-group command **ivr copy active-topology user-configured-topology** command **ivr copy active-zoneset full-zoneset** command **ivr service-group activate** command **ivr zone rename** command **ivr zoneset rename** command	I Commands
	show ivr service-group command **show ivr virtual-switch-wwn** command	Show Commands
Lossless InOrder Delivery (IOD)	**debug rib** command (**liod_error**, **liod_event**, and **liod_trace** options)	Debug Commands
McData Interoperability Support	**show wwn** command (**vsan-wwn** option)	Show Commands
	vsan database command (increased the interop mode range to 4)	V Commands
	wwn vsan command	W Commands
Message logging	**logging timestamp** command	L Commands
N-port identifier virtualization (NPIV)	**npiv enable** command	N Commands
Onboard Failure Logging (OBFL)	**clear logging** command (**onboard**, **module** and **session,** options)	C Commands
	hw-module logging onboard command	H Commands
	show logging command (**onboard** logging)	Show Commands
Online Health Management System	**system health** command (**frame-length** and **auto** options to the **loopback** keyword) **system health external-loopback** command (**source** and **destination** keywords and the **frame-count** and **frame-length** options **system health internal-loopback** command (**frame-count** and **frame-length** options) **system health module** command (Added note about frequency range for bootflash) **system health serdes-loopback** command	S Commands
SAN tuner extension	**tape-read command-id** command **tape-write command-id** command	T Commands

Table 1 New and Changed Commands in the Cisco MDS 9000 Family Command Reference

Feature	Description	Where Documented
SANTap	**clear santap module** command	C Commands
	santap module command (**cvt-name**, **dvt**, **target-pwwn**, **target-vsan**, **dvt-name**, **dvt-vsan**, **dvt-port**, **lun-size-handling**, and **io-timeout** options)	S Commands
Troubleshooting	**show tech-support** command (**fcdomain**, **port-channel**, and **zone** options)	Show Commands
Zoning	**clear zone** command (**lock** option)	C Commands
	system default zone default-zone permit command **system default zone distribute full** command	S Commands
	show system command (**zone** option) **show zone analysis** command	Show Commands
	zone compact vsan command **zone default-zone** command (added Usage Guidelines) **zoneset (configuration mode)** command (added Usage Guidelines)	Z Commands

Preface

This preface describes the audience, organization, and conventions of the *Cisco MDS 9000 Family Command Reference*. It also provides information on how to obtain related documentation.

Audience

This guide is for experienced network operators and administrators who are responsible for configuring and maintaining the Cisco MDS 9000 family of multilayer directors and fabric switches.

Organization

This guide is organized as follows:

Chapter	Title	Description
Chapter 1	CLI Overview	Describes the CLI (command-line interface).
Chapter 2	A Commands	Describes all commands beginning with the letter “a.”
Chapter 3	B Commands	Describes all commands beginning with the letter “b.”
Chapter 4	C Commands	Describes all commands beginning with the letter “c.”
Chapter 5	D Commands	Describes all commands beginning with the letter “d.”
Chapter 6	Debug Commands	Describes all the **debug** commands.
Chapter 7	E Commands	Describes all commands beginning with the letter “e.”
Chapter 8	F Commands	Describes all commands beginning with the letter “f.”
Chapter 9	G Commands	Describes all commands beginning with the letter “g.”
Chapter 10	H Commands	Describes all commands beginning with the letter “h.”
Chapter 11	I Commands	Describes all commands beginning with the letter “i.”
Chapter 12	J Commands	Describes all commands beginning with the letter “j.”
Chapter 13	K Commands	Describes all commands beginning with the letter “k.”
Chapter 14	L Commands	Describes all commands beginning with the letter “l.”
Chapter 15	M Commands	Describes all commands beginning with the letter “m.”
Chapter 16	N Commands	Describes all commands beginning with the letter “n.”

Chapter	Title	Description
Chapter 17	O Commands	Describes all commands beginning with the letter “o.”
Chapter 18	P Commands	Describes all commands beginning with the letter “p.”
Chapter 19	Q Commands	Describes all commands beginning with the letter “q.”
Chapter 20	R Commands	Describes all commands beginning with the letter “r.”
Chapter 21	S Commands	Describes all commands beginning with the letter “s” except for the **show** commands.
Chapter 22	Show Commands	Describes all the **show** commands.
Chapter 23	T Commands	Describes all commands beginning with the letter “t.”
Chapter 24	U Commands	Describes all commands beginning with the letter “u.”
Chapter 25	V Commands	Describes all commands beginning with the letter “v.”
Chapter 26	W Commands	Describes all commands beginning with the letter “w.”
Chapter 27	Z Commands	Describes all commands beginning with the letter “z.”
Chapter 28	Caching Services Module Commands	Describes all commands pertaining to the Caching Services Module (CSM).

Document Conventions

Command descriptions use these conventions:

Convention	Indication
boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use these conventions:

Convention	Indication
`screen` font	Terminal sessions and information the switch displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
`italic screen` font	Arguments for which you supply values are in *`italic screen`* font.
< >	Nonprinting characters, such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

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

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

Send documentation comments to mdsfeedback-doc@cisco.com.

Related Documentation

The documentation set for the Cisco MDS 9000 Family includes the following documents. To find a document online, use the Cisco MDS SAN-OS Documentation Locator at: http://www.cisco.com/en/US/products/ps5989/products_documentation_roadmap09186a00804500c1.html. For information on IBM TotalStorage SAN Volume Controller Storage Software for the Cisco MDS 9000 Family, refer to the IBM TotalStorage Support website: http://www.ibm.com/storage/support/2062-2300/

Release Notes

- *Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Releases*
- *Cisco MDS 9000 Family Release Notes for Storage Services Interface Images*
- *Cisco MDS 9000 Family Release Notes for Cisco MDS SVC Releases*
- *Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images*

Compatibility Information

- *Cisco MDS 9000 SAN-OS Hardware and Software Compatibility Information*
- *Cisco MDS 9000 Family Interoperability Support Matrix*
- *Cisco MDS SAN-OS Release Compatibility Matrix for IBM SAN Volume Controller Software for Cisco MDS 9000*
- *Cisco MDS SAN-OS Release Compatibility Matrix for Storage Service Interface Images*

Regulatory Compliance and Safety Information

- *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*

Hardware Installation

- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9216 Switch Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9020 Fabric Switch Hardware Installation Guide*

Send documentation comments to mdsfeedback-doc@cisco.com.

Cisco Fabric Manager

- *Cisco MDS 9000 Family Fabric Manager Quick Configuration Guide*
- *Cisco MDS 9000 Family Fabric Manager Configuration Guide*
- *Cisco MDS 9000 Fabric Manager Online Help*
- *Cisco MDS 9000 Fabric Manager Web Services Online Help*

Command-Line Interface

- *Cisco MDS 9000 Family Software Upgrade and Downgrade Guide*
- *Cisco MDS 9000 Family CLI Quick Configuration Guide*
- *Cisco MDS 9000 Family CLI Configuration Guide*
- *Cisco MDS 9000 Family Command Reference*
- *Cisco MDS 9000 Family Quick Command Reference*
- *Cisco MDS 9020 Fabric Switch Configuration Guide and Command Reference*
- *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide*

Troubleshooting and Reference

- *Cisco MDS 9000 Family Troubleshooting Guide*
- *Cisco MDS 9000 Family MIB Quick Reference*
- *Cisco MDS 9020 Fabric Switch MIB Quick Reference*
- *Cisco MDS 9000 Family SMI-S Programming Reference*
- *Cisco MDS 9000 Family System Messages Reference*
- *Cisco MDS 9020 Fabric Switch System Messages Reference*

Installation and Configuration Note

- *Cisco MDS 9000 Family SSM Configuration Note*
- *Cisco MDS 9000 Family Port Analyzer Adapter Installation and Configuration Note*

Obtaining Documentation

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

Send documentation comments to mdsfeedback-doc@cisco.com.

Cisco.com

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

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

Ordering Documentation

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

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

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

Documentation Feedback

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

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

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

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

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

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

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

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

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- For Nonemergencies—psirt@cisco.com

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

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

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

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

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

http://www.cisco.com/techsupport

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

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

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

Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

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

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

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

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

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

  or view the digital edition at this URL:

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

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

CLI Overview

This chapter prepares you to configure switches from the CLI (command-line interface). It also lists the information you need to have before you begin, and it describes the CLI command modes.

This chapter includes the following sections:

About the Switch Prompt

If you are connected to the console port when the switch boots up, you see the output show in :

Note Refer to the *Cisco MDS 9200 Series Hardware Installation Guide* or the *Cisco MDS 9500 Series Hardware Installation Guide* for installation and connection instructions.

Once the switch is powered on successfully, you see the default switch prompt (`switch#`). You can perform embedded CLI operations, access command history, and use command parsing functions at this prompt. The switch gathers the command string upon detecting an **Enter** (CR) and accepts commands from a terminal.

Example 1-1 Output When a Switch Boots Up

```
Auto booting bootflash:/boot-279 bootflash:/system_image;...
Booting kickstart image:bootflash:/boot-279....
.........................................Image verification OK

Starting kernel...
INIT: version 2.78 booting
Checking all filesystems..... done.
Loading system software
Uncompressing system image: bootflash:/system_image
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
INIT: Entering runlevel: 3

<<<<<<SAN OS bootup log messages>>>>>>

         ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Use ctrl-c to abort configuration dialog at any prompt.

Basic management setup configures only enough connectivity for
management of the system.

Would you like to enter the basic configuration dialog (yes/no): yes

<<<<<<after configuration>>>>>>

switch login:
```

About the CLI Command Modes

Switches in the Cisco MDS 9000 Family have two main command modes—user EXEC mode and configuration mode. The commands available to you depend on the mode you are in. To obtain a list of available commands in either mode, type a question mark (?) at the system prompt.

Table 1-1 lists and describes the two commonly used modes, how to enter the modes, and the resulting system prompts. The system prompt helps you identify which mode you are in and hence, which commands are available to you.

Table 1-1 Frequently Used Switch Command Modes

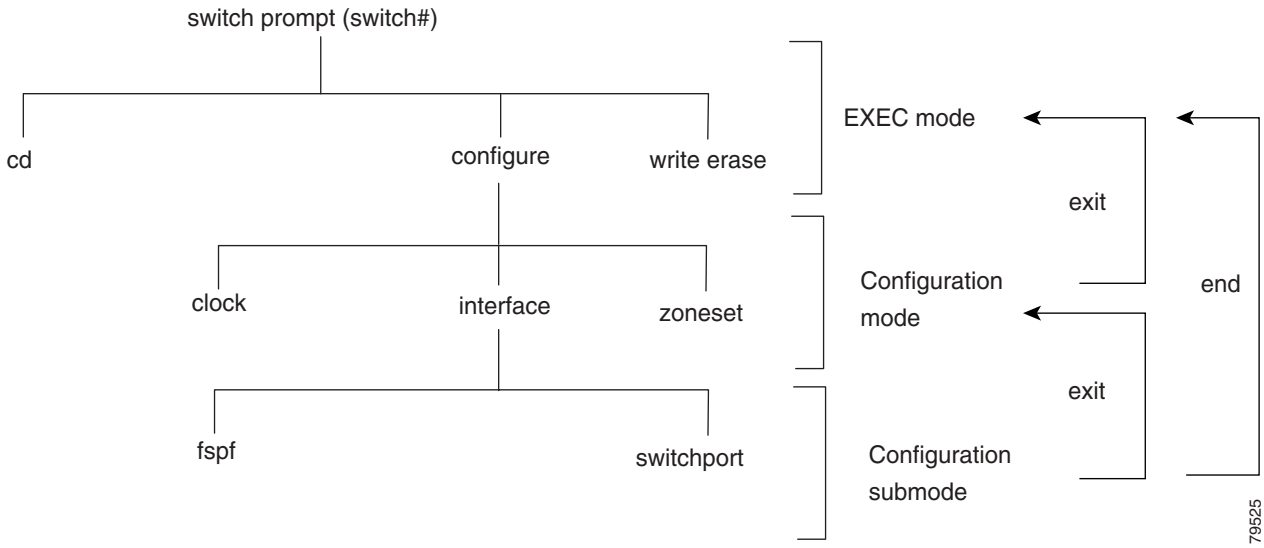
Mode	Description of Use	How to Access	Prompt
EXEC	Enables you to temporarily change terminal settings, perform basic tests, and display system information. **Note** Changes made in this mode are generally not saved across system resets.	At the switch prompt, enter the required EXEC mode command.	`switch#`
Configuration mode	Enables you to configure features that affect the system as a whole. **Note** Changes made in this mode are saved across system resets if you save your configuration. Refer to the Cisco *MDS 9000 Family CLI Configuration Guide* for further information.	From EXEC mode, enter the **config terminal** command.	`switch(config)#`

You can abbreviate commands and keywords by entering just enough characters to make the command unique from other commands. For example, you can abbreviate the **config terminal** command to **conf t**.

Understanding CLI Command Hierarchy

The CLI commands are organized hierarchically, with commands that perform similar functions grouped under the same level. For example, all commands that display information about the system, configuration, or hardware are grouped under the **show** command, and all commands that allow you to configure the switch are grouped under the **config terminal** command. Figure 1-1 illustrates a portion of the **config terminal** command hierarchy.

Figure 1-1 CLI Command Hierarchy Example



To execute a command, you enter the command by starting at the top level of the hierarchy. For example, to configure a Fibre Channel interface, use the **config terminal** command. Once you are in configuration mode, issue the **interface** command. When you are in the interface submode, you can query the available commands there.

The following example shows how to query the available commands in the interface submode:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface fc1/1
switch(config-if)# ?
Interface configuration commands:
  channel-group  Add to/remove from a port-channel
  exit           Exit from this submode
  fcdomain       Enter the interface submode
  fspf           To configure FSPF related parameters
  no             Negate a command or set its defaults
  shutdown       Enable/disable an interface
  switchport     Configure switchport parameters
```

EXEC Mode Options

When you start a session on the switch, you begin in EXEC mode. Based on the role or group to which you belong, you have access to limited commands or to all commands (see the "Role-Based CLI" section on page 1-33). From the EXEC mode, you can enter configuration mode. Most of the EXEC commands are one-time commands, such as **show** commands, which display the current configuration status. Here is a list of EXEC mode commands:

```
switch# ?
Exec commands:
  attach          Connect to a specific linecard
  callhome        Callhome commands
  cd              Change current directory
  clear           Reset functions
  cli             CLI commands
  clock           Manage the system clock
  cloud           Initiate Cloud Discovery
  config          Enter configuration mode
  copy            Copy from one file to another
  debug           Debugging functions
  delete          Delete a file
  dir             List files in a directory
  discover        Discover information
  exit            Exit from the EXEC
  fcping          Ping an N-Port
  fctrace         Trace the route for an N-Port.
  find            Find a file below the current directory
  format          Format disks
  gunzip          Uncompresses LZ77 coded files
  gzip            Compresses file using LZ77 coding
  install         Upgrade software
  ips             Various sibyte module related commands
  isns            Re-registers specified interface         with isns server
  mkdir           Create new directory
  modem           Modem commands
  move            Move files
  no              Disable debugging functions
  out-of-service  Make the current module out-of-service
  ping            Send echo messages
  port-channel    Port-Channel related commands
  purge           Deletes unused data
  pwd             View current directory
  reload          Reboot the entire box
  rmdir           Delete a directory
  run-script      Run shell scripts
  san-ext-tuner   Configure san_ext_tuner
  send            Send message to open sessions
  setup           Run the basic SETUP command facility
  show            Show running system information
  sleep           Sleep for the specified number of seconds
  ssh             SSH to another system
  system          System management commands
  tac-pac         Save tac information to a specific location
  tail            Display the last part of a file
  telnet          Telnet to another system
  terminal        Set terminal line parameters
  test            Test command
  traceroute      Trace route to destination
  undebug         Disable Debugging functions (See also debug)
  update          Update license
  write           Write current configuration
  zone            Execute Zone Server commands
```

```
  zoneset         Execute zoneset commands
```

Configuration Mode Options

Configuration mode allows you to make changes to the existing configuration. When you save the configuration, these commands are preserved across switch reboots. Once you are in configuration mode, you can enter interface configuration mode, zone configuration mode, and a variety of protocol-specific modes. Configuration mode is the starting point for all configuration commands. When you are in configuration mode, the switch expects configuration commands from the user.

The following example shows output from the **config terminal** command:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#
```

Configuration Mode Commands and Submodes

The following is a list of configuration mode commands:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ?
Configure commands:
  aaa                   Configure aaa functions
  arp                   [no] remove an entry from the ARP cache
  banner                Configure banner message
  boot                  Configure boot variables
  callhome              Enter the callhome configuration mode
  cdp                   CDP Configuration parameters
  cfs                   CFS configuration commands
  cimserver             Modify cimserver configuration
  cli                   CLI configuration commands
  clock                 Configure time-of-day clock
  cloud                 Configure Cloud Discovery
  cloud-discovery       Configure Cloud Discovery
  crypto                Set crypto settings
  device-alias          Device-alias configuration commands
  do                    EXEC command
  dpvm                  Configure Dynamic Port Vsan Membership
  end                   Exit from configure mode
  exit                  Exit from configure mode
  fabric-binding        Fabric Binding configuration
  fc-tunnel             Configure fc-tunnel
  fcalias               Fcalias configuration commands
  fcanalyzer            Configure cisco fabric analyzer
  fcc                   Configure FC Congestion Control
  fcdomain              Enter the fcdomain configuration mode
  fcdroplatency         Configure switch or network latency
  fcflow                Configure fcflow
  fcid-allocation       Add/remove company id(or OUIs) from auto area list
  fcinterop             Interop commands
  fcip                  Enable/Disable FCIP
  fcns                  Name server configuration
  fcroute               Configure FC routes
  fcrxbbcredit          Enable extended rx b2b credit configuration
  fcs                   Configure Fabric Config Server
  fcsp                  Config commands for FC-SP
  fctimer               Configure fibre channel timers
  fdmi                  Config commands for FDMI
```

```
ficon                 Configure ficon information
fspf                  Configure fspf
hw-module             Enable/Disable OBFL information
in-order-guarantee    Set in-order delivery guarantee
interface             Select an interface to configure
ip                    Configure IP features
ips                   Various sibyte module related commands
ipv6                  Configure IPv6 features
iscsi                 Enable/Disable iSCSI
islb                  ISCSI server load-balancing
isns                  Configure iSNS
isns-server           ISNS server
ivr                   Config commands for IVR
kernel                Kernel options
line                  Configure a terminal line
logging               Modify message logging facilities
mcast                 Configure multicast
no                    Negate a command or set its defaults
npiv                  Nx port Id Virtualization (NPIV) feature enable
ntp                   NTP Configuration
port-security         Configure Port Security
port-track            Configure Switch port track config
power                 Configure power supply
poweroff              Poweroff a module in the switch
qos                   QoS Configuration commands
radius                Configure RADIUS configuration
radius-server         Configure RADIUS related parameters
rib                   Configure RIB parameters
rmon                  Remote Monitoring
role                  Configure roles
rscn                  Config commands for RSCN
san-ext-tuner         Enable/Disable San Extension Tuner tool
scheduler             Config commands for scheduler
scsi-target           Scsi-target configuration
snmp-server           Configure snmp server
span                  Enter SPAN configuration mode
ssh                   Configure SSH parameters
switchname            Configure system's network name
system                System config command
tacacs+               Enable tacacs+
telnet                Enable telnet
tlport                Configure TL Port information
trunk                 Configure Switch wide trunk protocol
username              Configure user information.
vsan                  Enter the vsan configuration mode
wwn                   Set secondary base MAC addr and range for additional WWNs
zone                  Zone configuration commands
zone-attribute-group  Zone attribute group commands
zoneset               Zoneset configuration commands
```

Configuration mode, also known as terminal configuration mode, has several submodes. Each of these submodes places you deeper in the prompt hierarchy. When you type **exit**, the switch backs out one level and returns you to the previous level. When you type **end**, the switch backs out to the user EXEC level. You can also type **Ctrl-Z** in configuration mode as an alternative to typing **end**.

Note When in configuration mode, you can alternatively enter:

- **Ctrl-Z** instead of the **end** command
- **Ctrl-G** instead of the **exit** command

You can execute an EXEC mode command from a configuration mode or submode prompt. You can issue this command from any submode within the configuration mode. When in configuration mode (or in any submode), enter the **do** command along with the required EXEC mode command. The entered command is executed at the EXEC level and the prompt resumes its current mode level.

```
switch(config)# do terminal session-timeout 0
switch(config)#
```

In this example, **terminal session-timeout** is an EXEC mode command—you are issuing an EXEC mode command using the configuration mode **do** command.

The **do** command applies to all EXEC mode commands other than the **end** and **exit** commands. You can also use the help (?) and command completion (tab) features for EXEC commands when issuing a **do** command along with the EXEC command.

Table 1-2 lists some useful command keys that can be used in both EXEC and configuration modes:

Table 1-2 Useful Command Key Description

Command	Description
Ctrl-P	Up history
Ctrl-N	Down history
Ctrl-X-H	List history
Alt-P	History search backwards **Note** The difference between **Tab** completion and **Alt- P** or **Alt-N** is that TAB completes the current word while **Alt- P** and **Alt-N** completes a previously-entered command.
Alt-N	History search forwards
Ctrl-G	Exit
Ctrl-Z	End
Ctrl-L	Clear screen

Table 1-3 displays the commonly used configuration submodes.

Table 1-3 Submodes Within the Configuration Mode

Submode Name	From Configuration Mode Enter	Submode Prompt	Configured Information
Call Home	**callhome**	`switch(config-callhome)#`	Contact, destination, and e-mail
FCS Registration	**fcs register**	`switch(config-fcs-register)#`	FCS attribute registration
	From FCS registration submode: **platform name** *name* **vsan** *vsan-id*	`switch(config-fcs-register-attrib)#`	Platform name and VSAN ID association
Fibre Channel alias	**fcalias name** *name* **vsan** *vsan-id*	`switch(config-fcalias)#`	Alias member
FSPF	**fspf config vsan** *vsan-id*	`switch(config-(fspf-config))#`	Static SPF computation, hold time, and autonomous region
Interface configuration	**interface** *type slot/port*	`switch(config-if)#`	Channel groups, Fibre Channel domains, FSPF parameters, switch port trunk and beacon information, and IP address
	From the VSAN or mgmt0 (management) interface configuration submode: **vrrp** *number*	`switch(config-if-vrrp)#`	Virtual router (Refer to the *Cisco MDS 9000 Family CLI Configuration Guide* for further information.)
iSCSI target	**iscsi virtual-target name**	`switch(config-iscsi-tgt)`	iSCSI virtual target
iSLB initiator	**islb initiator**	`switch(config-islb-init)#`	iSCSI server load balancing (iSLB) initiator
iSLB target	**islb virtual-target name**	`switch(config-islb-tgt)`	iSCSI server load balancing (iSLB) virtual target
Line console	**line console**	`switch(config-console)#`	Primary terminal console
VTY	**line vty**	`switch(config-line)#`	Virtual terminal line
Role	**role name**	`switch(config-role)#`	Rule
SPAN	**span session** *number*	`switch(config-span)#`	SPAN source, destination, and suspend session information
VSAN database	**vsan database**	`switch(config-vsan-db)#`	VSAN database
Zone	**zone name** *string* **vsan** *vsan-id*	`switch(config-zone)#`	Zone member
Zone set	**zoneset name** *name* **vsan** *vsan-id*	`switch(config-zoneset)#`	Zone set member

Navigating Through CLI Commands

To redisplay a command you previously entered, press the **Up Arrow** key. You can continue to press the **Up Arrow** key to see more previously issued commands. Similarly, you can press the **Down Arrow**, **Right Arrow**, **Left Arrow**, and **Delete** keys to navigate through the command history and to modify an existing command string.

Getting Help

In any command mode, you can get a list of available commands by entering a question mark (?).

```
switch# ?
```

To obtain a list of commands that begin with a particular character sequence, type in those characters followed immediately by the question mark (?). Do not include a space.

```
switch# co?
configure copy
```

To list keywords or arguments, enter a question mark in place of a keyword or argument. Include a space before the question mark. This form of help is called command syntax help, because it reminds you which keywords or arguments are applicable based on the commands, keywords, and arguments you have already entered.

```
switch# config ?
 terminal Configure the system from the terminal
```

Tip If you are having trouble entering a command, check the system prompt and enter the question mark (?) for a list of available commands. You might be in the wrong command mode or using incorrect syntax.

Command Completion

In any command mode, you can begin a particular command sequence and immediately press the **Tab** key to complete the rest of the command.

```
switch (config)# ro<Tab>
switch (config)# role <Tab>
switch (config)# role name
```

This form of help is called command completion, because it completes a word for you. If several options are available for the typed letters, all options that match those letters are presented:

```
switch(config)# fc<Tab>
fcalias         fcdomain        fcs
fcanalyzer      fcdroplatency   fcns            fctimer
fcc             fcinterop       fcroute
switch(config)# fcd<Tab>
fcdomain        fcdroplatency
switch(config)# fcdo<Tab>
switch(config)# fcdomain
```

Using the no and Default Forms of Commands

You can issue the **no** form of any command to perform the following actions:

- Undo a wrongly issued command.

  If you issue the **zone member** command, you can undo the results:

```
switch(config)# zone name test vsan 1
switch(config-zone)# member pwwn 12:12:12:12:12:12:12:12
switch(config-zone)# no member pwwn 12:12:12:12:12:12:12:12
WARNING: Zone is empty. Deleting zone test. Exit the submode.
switch(config-zone)#
```

- Delete a created facility

  If you want to delete a zone that you created:

```
switch(config)# zone name test vsan 1
switch(config-zone)# exit
switch(config)# no zone name test vsan 1
switch(config)#
```

  You cannot delete a zone facility called test while residing in it. You must first exit the zone submode and return to configuration mode.

Entering CLI Commands

You can configure the software in one of two ways:

- You can create the configuration for the switch interactively by issuing commands at the CLI prompt.
- You can create an ASCII file containing a switch configuration and then load this file on the required system. You can then use the CLI to edit and activate the file. (Refer to the *Cisco MDS 9000 Family CLI Configuration Guide* for further information.)

Viewing Switch Configurations

You can view the ASCII form of the configuration file when required. To view the current configuration tree from the EXEC prompt, issue the **show running-config** command. If the running configuration is different from the startup configuration, issue the **show startup-config** command to view the ASCII version of the current startup configuration that was used to boot the switch.

You can also gather specific information on the entire switch configuration by issuing the relevant **show** commands. Configurations are displayed based a specified feature, interface, module, or VSAN. Available **show** commands for each feature are briefly described in this section and listed at the end of each chapter.

Examples 1-2 to 1-8 display a few **show** command examples.

Example 1-2 Displays Details on the Specified Interface

```
switch# show interface fc1/1
fc1/1 is up
    Hardware is Fibre Channel, 20:01:ac:16:5e:4a:00:00
    vsan is 1
    Port mode is E
```

```
    Speed is 1 Gbps
    Beacon is turned off
    FCID is 0x0b0100
      0 frames input, 0 bytes, 0 discards
      0 runts, 0 jabber, 0 too long, 0 too short
      0 input errors, 0 CRC, 0 invalid transmission words
      0 address id, 0 delimiter
      0 EOF abort, 0 fragmented, 0 unknown class
      0 frames output, 0 bytes, 0 discards
      Received 0 OLS, 0 LRR, 0 NOS, 0 loop inits
      Transmitted 0 OLS, 0 LRR, 0 NOS, 0 loop inits
```

Example 1-3 Displays the Software and Hardware Version

```
switch# show version
Cisco Storage Area Networking Operating System (SAN-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2003, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
Andiamo Systems, Inc. and/or other third parties and are used and
distributed under license. Some parts of this software are covered
under the GNU Public License. A copy of the license is available
at http://www.gnu.org/licenses/gpl.html.

Software
  BIOS:      version 1.0.8
  loader:    version 1.1(2)
  kickstart: version 2.0(1) [build 2.0(0.6)] [gdb]
  system:    version 2.0(1) [build 2.0(0.6)] [gdb]

  BIOS compile time:       08/07/03
  kickstart image file is: bootflash:///m9500-sf1ek9-kickstart-mzg.2.0.0.6.bin
  kickstart compile time:  10/25/2010 12:00:00
  system image file is:    bootflash:///m9500-sf1ek9-mzg.2.0.0.6.bin
  system compile time:     10/25/2020 12:00:00

Hardware
  RAM 1024584 kB

  bootflash: 1000944 blocks (block size 512b)
  slot0:           0 blocks (block size 512b)

  172.22.92.181 uptime is 0 days 2 hours 18 minute(s) 1 second(s)

  Last reset at 970069 usecs after Tue Sep 16 22:31:25 1980
    Reason: Reset Requested by CLI command reload
    System version: 2.0(0.6)
    Service:
```

Example 1-4 Displays the Running Configuration

```
switch# show running
Building Configuration ...
 interface fc1/1
 interface fc1/2
 interface fc1/3
 interface fc1/4
 interface mgmt0
ip address 172.22.95.112 255.255.255.0
no shutdown
vsan database
boot system bootflash:system-237; sup-1
```

```
boot kickstart bootflash:boot-237 sup-1
callhome
ip default-gateway 172.22.95.1
switchname switch
trunk protocol enable
username admin password 5 /AFDAMD4B2xK2  role network-admin
```

Example 1-5 Displays the Difference between the Running and Startup Configuration

```
switch# show running diff
Building Configuration ...
*** Startup-config
--- Running-config
****************** 1,16 ****
  fcip enable
  ip default-gateway 172.22.91.1
  iscsi authentication none
  iscsi enable
! iscsi import target fc
  iscsi virtual-target name vt
    pWWN 21:00:00:04:cf:4c:52:c1
  all-initiator-permit
--- 1,20 ----
  fcip enable
+ aaa accounting logsize 500
+
+
+
  ip default-gateway 172.22.91.1
  iscsi authentication none
  iscsi enable
! iscsi initiator name junk
  iscsi virtual-target name vt
    pWWN 21:00:00:04:cf:4c:52:c1
  all-initiator-permit
```

Example 1-6 Displays the Configuration for a Specified Interface

```
switch# show running interface fc2/9
interface fc2/9
switchport mode E
no shutdown
```

Note The **show running interface** command is different from the **show interface** command.

Example 1-7 Displays the Configuration for all Interfaces in a 16-Port Module

```
switch# show running interface fc2/10 - 12
interface fc2/10
switchport mode E
no shutdown

interface fc2/11
switchport mode E
no shutdown

interface fc2/12
switchport mode FL
no shutdown
```

Example 1-8 Displays the Configuration Per VSAN

```
switch# show runnning vsan 1
Building Configuration ...
zone name m vsan 1
  member pwwn 21:00:00:20:37:60:42:5c
  member pwwn 21:00:00:20:37:4b:00:a2
zoneset name m vsan 1
  member m
zoneset  activate name m vsan 1
```

Saving a Configuration

To save the configuration, enter the **copy running-config startup-config** command from the EXEC mode prompt to save the new configuration into nonvolatile storage. Once this command is issued, the running and the startup copies of the configuration are identical.

Refer to the *Cisco MDS 9000 Family CLI Configuration Guide* for further information.

Clearing a Configuration

To clear a startup configuration, enter the **write erase** command from the EXEC mode prompt. Once this command is issued, the switch's startup configuration reverts to factory defaults. The running configuration is not affected. The **write erase** command erases the entire startup configuration with the exception of any configuration that affects the loader functionality.

The **write erase boot** command only erases the configuration that affects the loader functionality. The loader functionality configuration includes the boot variables and the mgmt0 IP configuration information (IP address, netmask and default gateway).

```
switch# write erase boot
This command will erase the boot variables and the ip configuration of interface mgmt 0
```

Searching and Filtering CLI Output

The Cisco MDS SAN-OS CLI provides ways of searching through large amounts of command output and filtering output to exclude information you do not need. These features are enabled for the **show** command, which generally displays large amounts of data.

Note The **show** command is always entered in EXEC mode.

When output continues beyond what is displayed on your screen, the Cisco MDS SAN-OS CLI displays a --More-- prompt. Pressing **Return** displays the next line; pressing the **Spacebar** displays the next screen of output.

To search the **show** command output, use the following command in EXEC mode:

Command	Purpose
`switch# show` *any-command* `| begin` *pattern*	Begins unfiltered output of the **show** command with the first line that contains the pattern.

Note Cisco MDS SAN-OS documentation generally uses the vertical bar to indicate a choice of syntax. However, to search the output of the **show** command, you need to enter the pipe character (the vertical bar). In this section the pipe appears in bold (**|**) to indicate that you should enter this character.

To filter **show** command output, use one of the following commands in EXEC mode:

Command	Purpose
`switch# show any-command | exclude pattern`	Displays output lines that do not contain the pattern.
`switch# show any-command | include pattern`	Displays output lines that contain the pattern.
`switch# show any-command | include "pattern1|pattern2"`	Displays output lines that contain either pattern1 or pattern2. **Note** The alternation patterns, *"pattern1|pattern2"*, must appear within double quotes.
`switch# show any-command | include pattern [next number] [prev number]`	Displays output lines that contain the pattern. Optionally, using the **next** or **prev** parameter followed by a number also displays the designated number of lines.
`switch# show any-command | count number`	Displays the number lines of output in the display.

You can enter the **Ctrl-Z** key combination at any time to interrupt the output and return to EXEC mode. For example, you can enter the **show running-config | begin hostname** command to start the display of the running configuration file at the line containing the hostname setting, then use **Ctrl-Z** when you get to the end of the information you are interested in capturing. See the "Searching and Filtering CLI Output Examples" section on page 1-16.

Multiple Filter Commands

Cisco MDS SAN-OS Release 2.1(1a) supports using multiple filters in the same **show** command output. This means you can use a combination of the available filters to format the output of any **show** command.

Note The maximum number of commands allowed is four. For example, you can enter a maximum of three filter commands or two filter commands and a redirection.

Cisco MDS SAN-OS Release 2.1(1a) also supports both filters and redirection in the same command. Now you can apply the required filters to the output of any command, and save the output using the file redirection. See the next section, "Searching and Filtering CLI Output Examples" section on page 1-16.

Searching and Filtering CLI Output Examples

The following is partial sample output of the **show running-config | begin** EXEC command. It begins displaying unfiltered output with the first line that contain the pattern `vsan`.

```
switch# show running-config | begin vsan
fcdomain fcid persistent vsan 1
fcdomain fcid persistent vsan 2
fcdomain fcid persistent vsan 3
fcdomain fcid persistent vsan 101
fcdomain fcid persistent vsan 102
fcdomain fcid database
  vsan 1 wwn 29:00:00:05:30:00:06:ea fcid 0x680000 dynamic
  vsan 1 wwn 28:0f:00:05:30:00:06:ea fcid 0x680001 dynamic
  vsan 1 wwn 28:10:00:05:30:00:06:ea fcid 0x680002 dynamic
  vsan 1 wwn 28:11:00:05:30:00:06:ea fcid 0x680003 dynamic
  vsan 1 wwn 28:12:00:05:30:00:06:ea fcid 0x680004 dynamic
  vsan 1 wwn 28:13:00:05:30:00:06:ea fcid 0x680005 dynamic
  vsan 1 wwn 28:14:00:05:30:00:06:ea fcid 0x680006 dynamic
  vsan 1 wwn 28:1f:00:05:30:00:06:ea fcid 0x680007 dynamic
  vsan 1 wwn 28:20:00:05:30:00:06:ea fcid 0x680008 dynamic
  vsan 1 wwn 21:00:00:e0:8b:05:76:28 fcid 0x680100 area dynamic
  vsan 1 wwn 20:c5:00:05:30:00:06:de fcid 0x680200 area dynamic
  vsan 1 wwn 28:2b:00:05:30:00:06:ea fcid 0x680012 dynamic
  vsan 1 wwn 28:2d:00:05:30:00:06:ea fcid 0x680013 dynamic
  vsan 1 wwn 28:2e:00:05:30:00:06:ea fcid 0x680014 dynamic
  vsan 1 wwn 28:2f:00:05:30:00:06:ea fcid 0x680015 dynamic
  vsan 1 wwn 28:30:00:05:30:00:06:ea fcid 0x680016 dynamic
--More--
```

The following is partial sample output of the **show tech-support** EXEC command. It begins displaying unfiltered output with the first line that contain the string `show interface brief`.

```
switch# show tech-support | begin "show interface brief"
-------------------- show interface brief ------------------

--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          FCOT   Oper  Oper   Port
                  Mode   Trunk                         Mode  Speed  Channel
                         Mode                                (Gbps)
--------------------------------------------------------------------------------
fc4/1      1      FX     --      sfpAbsent        --     --           --
fc4/2      1      FX     --      sfpAbsent        --     --           --
fc4/3      1      FX     --      sfpAbsent        --     --           --
fc4/4      1      FX     --      sfpAbsent        --     --           --
fc4/5      1      FX     --      up               swl    F       1    --
fc4/6      1      FX     --      sfpAbsent        --     --           --
fc4/7      1      FX     --      sfpAbsent        --     --           --
fc4/8      1      FX     --      sfpAbsent        --     --           --
fc4/9      1      E      on      notConnected     swl    --           --
fc4/10     1      FX     --      sfpAbsent        --     --           --
fc4/11     1      FX     --      sfpAbsent        --     --           --
fc4/12     1      FX     --      sfpAbsent        --     --           --
fc4/13     1      FX     --      sfpAbsent        --     --           --
fc4/14     1      FX     --      sfpAbsent        --     --           --
fc4/15     1      FX     --      sfpAbsent        --     --           --
--More--
```

The following is partial sample output of the **show running-config | exclude** EXEC command. It excludes any output line that contain the pattern `vsan`.

```
switch# show running-config | exclude vsan
version 2.1(1a)
poweroff module 9
fcdomain fcid database
ssm enable feature nasb interface fc4/1-4
ssm enable feature santap module 4
ssm enable feature nasb interface fc9/1-4
ssm enable feature santap interface fc9/5-8
ssm enable feature santap interface fc9/21-28
switchname switch
boot kickstart bootflash:/b2193 sup-1
boot system bootflash:/r2193 sup-1
boot kickstart bootflash:/b2193 sup-2
boot system bootflash:/r2193 sup-2
boot ssi bootflash:/laslc1.bin module 1
boot ssi bootflash:/laslc1.bin module 2
boot ssi bootflash:/laslc1.bin module 3
boot ssi bootflash:/laslc1.bin module 4
boot ssi bootflash:/laslc1.bin module 7
boot ssi bootflash:/laslc1.bin module 8
boot ssi bootflash:/laslc1.bin module 9
line console
  speed 38400
--More--
```

The following is partial sample output of the **show interface** EXEC command. It includes all output with the pattern `vsan`.

```
switch# show interface | include vsan
    Port vsan is 1
    Port vsan is 1
    Port vsan is 1
    Port vsan is 1
    Port vsan is 1
    Port vsan is 1
[information deleted]
```

The following is partial sample output of the **show interface** EXEC command. It includes all output with the pattern `FX` plus the next and previous five lines of output.

```
switch# show interface | include FX next 5 prev 5
fc4/1 is down (SFP not present)
    Hardware is Fibre Channel
    Port WWN is 20:c1:00:05:30:00:06:de
    Admin port mode is FX
    Port vsan is 1
    Receive data field Size is 2112
    Beacon is turned off
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
--
      0 transmit B2B credit remaining
```

```
fc4/2 is down (SFP not present)
    Hardware is Fibre Channel
    Port WWN is 20:c2:00:05:30:00:06:de
    Admin port mode is FX
    Port vsan is 1
    Receive data field Size is 2112
    Beacon is turned off
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
--
--More--
```

The following output of the **show running-config** EXEC command. It displays the number lines, or count, of the output.

```
switch# show running-config | count
    214
switch#
```

The following output of the **show interface brief** EXEC command. It displays the interfaces where the administration mode is `FX`.

```
switch# show interface brief | include FX
fc4/1      1      FX     --      sfpAbsent        --     --           --
fc4/2      1      FX     --      sfpAbsent        --     --           --
fc4/3      1      FX     --      sfpAbsent        --     --           --
fc4/4      1      FX     --      sfpAbsent        --     --           --
fc4/5      1      FX     --      up               swl    F       1    --
fc4/6      1      FX     --      sfpAbsent        --     --           --
fc4/7      1      FX     --      sfpAbsent        --     --           --
fc4/8      1      FX     --      sfpAbsent        --     --           --
fc4/10     1      FX     --      sfpAbsent        --     --           --
fc4/11     1      FX     --      sfpAbsent        --     --           --
fc4/12     1      FX     --      sfpAbsent        --     --           --
fc4/13     1      FX     --      sfpAbsent        --     --           --
fc4/14     1      FX     --      sfpAbsent        --     --           --
fc4/15     1      FX     --      sfpAbsent        --     --           --
fc4/16     1      FX     --      sfpAbsent        --     --           --
fc4/17     1      FX     --      sfpAbsent        --     --           --
fc4/18     1      FX     --      sfpAbsent        --     --           --
fc4/19     1      FX     --      sfpAbsent        --     --           --
fc4/20     1      FX     --      sfpAbsent        --     --           --
fc4/21     1      FX     --      sfpAbsent        --     --           --
fc4/22     1      FX     --      sfpAbsent        --     --           --
fc4/23     1      FX     --      sfpAbsent        --     --           --
fc4/24     1      FX     --      sfpAbsent        --     --           --
fc4/25     1      FX     --      sfpAbsent        --     --           --
fc4/26     1      FX     --      sfpAbsent        --     --           --
fc4/27     1      FX     --      sfpAbsent        --     --           --
fc4/28     1      FX     --      down             swl    --           --
fc4/29     1      FX     --      sfpAbsent        --     --           --
fc4/30     1      FX     --      sfpAbsent        --     --           --
fc4/31     1      FX     --      sfpAbsent        --     --           --
fc4/32     1      FX     --      sfpAbsent        --     --           --
switch#
```

The following output of the **show interface brief** EXEC command uses multiple filter commands. It display the number of interfaces, or count, where the administration mode is `FX`.

```
switch# show interface brief | include FX | count
     31
switch#
```

The following **show interface brief** EXEC command uses multiple filter commands to redirect the output where the administration mode is `FX` to the file named `test.txt` in the directory `SavedData`.

```
switch# show interface brief | include FX > SavedData\test.txt
switch# cd SavedData
switch# dir
       2263     Jan 12 18:53:41 2005  SavedData\test.txt

Usage for volatile://
       8192 bytes used
   20963328 bytes free
   20971520 bytes total
switch#
```

Displaying Users

The **show users** command displays all users currently accessing the switch.

```
switch# show users
admin    pts/7        Jan 12 20:56 (10.77.202.149)
admin    pts/9        Jan 12 23:29 (modena.cisco.com)
admin    pts/11       Jan 13 01:53 (dhcp-171-71-49-49.cisco.com)
```

Sending Messages to Users

The **send** command sends a message to all active CLI users currently using the switch. This message is restricted to 80 alphanumeric characters with spaces.

This example sends a warning message to all active users about the switch being shut down.

```
switch# send Shutting down the system in 2 minutes. Please log off.

Broadcast Message from admin@excal-112
        (/dev/pts/3) at 16:50 ...
Shutting down the system in 2 minutes. Please log off.
```

Using the ping Command

The **ping** command verifies the connectivity of a remote host or server by sending echo messages.

The syntax for this command is **ping** <*host or ip address*>

```
switch# ping 171.71.181.19
PING 171.71.181.19 (171.71.181.19): 56 data bytes
64 bytes from 171.71.181.19: icmp_seq=0 ttl=121 time=0.8 ms
64 bytes from 171.71.181.19: icmp_seq=1 ttl=121 time=0.8 ms

--- 171.71.181.19 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.8/0.8/0.8 ms
```

To abnormally terminate a ping session, type the **Ctrl-C** escape sequence.

Using traceroute

The **traceroute** command prints the routes taken by a specified host or IP address.

The syntax for this command is **traceroute** <*host or ip address*>

```
switch# traceroute www.cisco.com
traceroute to www.cisco.com (171.71.181.19), 30 hops max, 38 byte packets
 1  kingfisher1-92.cisco.com (172.22.92.2)  0.598 ms  0.470 ms  0.484 ms
 2  nubulab-gw1-bldg6.cisco.com (171.71.20.130)  0.698 ms  0.452 ms  0.481 ms
 3  172.24.109.185 (172.24.109.185)  0.478 ms  0.459 ms  0.484 ms
 4  sjc12-lab4-gw2.cisco.com (172.24.111.213)  0.529 ms  0.577 ms  0.480 ms
 5  sjc5-sbb4-gw1.cisco.com (171.71.241.174)  0.521 ms  0.495 ms  0.604 ms
 6  sjc12-dc2-gw2.cisco.com (171.71.241.230)  0.521 ms  0.614 ms  0.479 ms
 7  sjc12-dc2-cec-css1.cisco.com (171.71.181.5)  2.612 ms  2.093 ms  2.118 ms
 8  www.cisco.com (171.71.181.19)  2.496 ms *  2.135 ms
```

To abnormally terminate a traceroute session, enter **Ctrl-C**.

Setting the Switch's Shell Timeout

Use the **exec-timeout** command in configuration mode to configure the lifetime of all terminal sessions on that switch. When the time limit configured by this command is exceeded, the shell exits and closes that session. The syntax for this command from is **exec-timeout** *minutes*

The default is 30 minutes. You can configure different timeout values for a console or a virtual terminal line (VTY) session. You can set the **exec-timeout** value to 0 to disable this feature so the session remains active until you exit the switch. This change is saved in the configuration file.

- From the console:

  ```
  switch(config)# line console
  switch(config-console)# exec-timeout 60
  ```

  Specifies the current console shell timeout to be 60 minutes.

- From a VTY session (Telnet or SSH):

  ```
  switch(config)# line vty
  switch(config-line)# exec-timeout 60
  ```

  Specifies the current console shell timeout to be 60 minutes.

Displaying VTY Sessions

Use the **show line** command to display all configured VTY sessions:

```
switch# show line
line Console:
    Speed:        9600 bauds
    Databits:     8 bits per byte
    Stopbits:     1 bit(s)
    Parity:       none
    Modem In: Disable
    Modem Init-String -
        default : ATE0Q1&D2&C1S0=1\015
    Statistics:  tx:5558511     rx:5033958     Register Bits:RTS|CTS|DTR|DSR|CD|RI
```

```
line Aux:
    Speed:        9600 bauds
    Databits:     8 bits per byte
    Stopbits:     1 bit(s)
    Parity:       none
    Modem In: Disable
    Modem Init-String -
        default : ATE0Q1&D2&C1S0=1\015
    Hardware Flowcontrol: ON
    Statistics:  tx:35     rx:0     Register Bits:RTS|DTR
```

Clearing VTY Sessions

Use the **clear line** command to close a specified VTY session:

```
switch# clear line Aux
```

Setting the Switch's Terminal Timeout

Use the **terminal session-timeout** command in EXEC mode to configure the automatic logout time for the current terminal session on that switch. When the time limit configured by this command is exceeded, the switch closes that session and exits.

The syntax for this command from is **terminal session-timeout** *minutes*

The default is 30 minutes. You can set the **terminal session-timeout** value to 0 to disable this feature so the terminal remains active until you choose to exit the switch. This change is not saved in the configuration file.

```
switch# terminal session-timeout 600
```

Specifies the terminal timeout to be 600 minutes for the current session.

Setting the Switch's Terminal Type

Use the **terminal terminal-type** command in EXEC mode to specify the terminal type for a switch:

The syntax for this command is **terminal terminal-type** *terminal-type*

```
switch# terminal terminal-type vt100
```

Specifies the terminal type. The *terminal-type* string is restricted to 80 characters and must be a valid type (for example vt100 or xterm). If a Telnet or SSH session specifies an unknown terminal type, the switch uses the vt100 terminal by default.

Setting the Switch's Terminal Length

To set the terminal screen length for the current session, use the **terminal length** command in EXEC mode. This command is specific to only the console port. Telnet and SSH sessions set the length automatically.

The syntax for this command is **terminal length** *lines*

```
switch# terminal length 20
```

Sets the screen length for the current session to 20 lines for the current terminal session. The default is 24 lines.

Setting the Switch's Terminal Width

To set the terminal screen width for the current session, use the **terminal width** command in EXEC mode. This command is specific to only the console port. Telnet and SSH sessions set the width automatically.

The syntax for this command is **terminal width** *columns*

```
switch# terminal width 86
```

Sets the screen length for the current session to 86 columns for the current terminal session. The default is 80 columns.

Displaying Terminal Settings

The show terminal command displays the terminal settings for the current session:

```
switch# show terminal
TTY: Type: "vt100"
Length: 24 lines, Width: 80 columns
Session Timeout: 525600 minutes
```

Using CLI Variables

The SAN-OS CLI parser supports definition and use of variables in CLI commands. CLI variables can be used as follows:

- Entered directly on the command line.
- Passed to the child script initiated using the **run-script** command. The variables defined in the parent shell are available for use in the child **run-script** command process.
- Passed as command line arguments to the **run-script** command.

CLI variables have the following characteristics:

- You cannot reference a variables through another variable using nested references.
- You can define persistent variables that are available across switch reloads.
- You can reference only one predefined system variable, the TIMESTAMP variable.

User-Defined CLI Session Variables

You can define CLI variables the persist only for the duration of your CLI session using the **cli var name** command in EXEC mode. These CLI variables are useful for scripts that you execute periodically.

The following example shows how to create a user-defined CLI session variable.

```
switch# cli var name testinterface fc 1/1
```

You can reference a variable using the syntax **$**(variable).

The following example shows how to reference a user-defined CLI session variable.

```
switch# show interface $(testinterface)
fc1/1 is up
    Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:01:00:0d:ec:0e:1d:00
    Admin port mode is auto, trunk mode is on
    snmp traps are enabled
    Port mode is F, FCID is 0x01000b
    Port vsan is 1
    Speed is 2 Gbps
    Transmit B2B Credit is 7
    Receive B2B Credit is 16
    Receive data field Size is 2112
    Beacon is turned off
    5 minutes input rate 256 bits/sec, 32 bytes/sec, 1 frames/sec
    5 minutes output rate 256 bits/sec, 32 bytes/sec, 1 frames/sec
      232692 frames input, 7447280 bytes
        0 discards, 0 errors
        0 CRC,  0 unknown class
        0 too long, 0 too short
      232691 frames output, 7448692 bytes
        0 discards, 0 errors
      0 input OLS, 0 LRR, 0 NOS, 0 loop inits
      1 output OLS, 1 LRR, 0 NOS, 1 loop inits
      16 receive B2B credit remaining
      7 transmit B2B credit remaining
```

Use the **show cli var** command to display user-defined CLI session variable.

The following example displays user-defined CLI session variables.

```
switch# show cli variables
VSH Variable List
-----------------
TIMESTAMP="2005-10-24-21.29.33"
testinterface="fc 1/1"
```

Use the **cli no var name** command to remove user-defined CLI session variables.

The following example removes a user-defined CLI session variable.

```
switch# cli no var name testinterface
```

User-Defined CLI Persistent Variables

You can define CLI variables the persist across CLI sessions and switch reloads using the **cli var name** command in configuration mode. These CLI variables are configured in the configuration mode and are saved in the running configuration file.

The following example shows how to create a user-defined CLI persistent variable.

```
switch# config t
switch(config)# cli var name mgmtport mgmt 0
switch(config)# exit
switch#
```

You can reference a variable using the syntax **$**(variable).

The following example shows how to reference a user-defined CLI persistent variable.

```
switch# show interface $(mgmtport)
mgmt0 is up
    Hardware is FastEthernet
    Address is 000e.38c6.2c6c
    Internet address is 10.10.10.1/24
    MTU 1500 bytes, BW 100 Mbps full Duplex
    288996 packets input, 97746406 bytes
      0 multicast frames, 0 compressed
      0 input errors, 0 frame, 0 overrun 0 fifo
    9089 packets output, 1234786 bytes, 0 underruns
      0 output errors, 0 collisions, 0 fifo
      0 carrier errors
```

Use the **show cli var** command to display user-defined CLI persistent variable.

The following example displays user-defined CLI persistent variables.

```
switch# show cli variables
VSH Variable List
-----------------
TIMESTAMP="2005-10-24-21.37.13"
mgmtport="mgmt 0"
```

Use the **no cli var name** command in configuration mode to remove user-defined CLI persistent variables.

The following example removes a user-defined CLI persistent variable.

```
switch# config t
switch(config)# no cli var name mgmtport
```

System Defined Variables

Cisco MDS SAN-OS supports one predefined variable: TIMESTAMP. This variable refers to the time of execution of the command in the format YYYY-MM-DD-HH.MM.SS.

Note The TIMESTAMP variable name is case sensitive. All letters must be uppercase.

The following example uses $(TIMESTAMP) when periodically gathering statistics into files using the command scheduler.

```
switch# config t 1
switch(config)# scheduler enable
switch(config)# scheduler logfile size 16
switch(config)# scheduler job name j1
switch(config-job)# show interface mgmt0 | include mgmt > file
switch(config-job)# copy volatile:file bootflash:file.$(TIMESTAMP)
switch(config-job)# end
switch(config)#
```

The following example uses $(TIMESTAMP) when redirecting **show** command output to a file.

```
switch# show running-config > rcfg.$(TIMESTAMP)
Preparing to copy....done
switch# dir volatile:
       7231     Oct 03 20:20:42 2005  rcfg.2005-10-03-20.20.42

Usage for volatile://sup-local
8192 bytes used
20963328 bytes free
20971520 bytes total
```

Using Command Aliases

Command alias support has the following characteristics:

- Command aliases are global for all user sessions.
- Command aliases are persist across reboots.
- Commands being aliased must be typed in full without abbreviation.
- Command alias translation always takes precedence over any keyword in any configuration mode or submode.
- Command alias support is only available on the supervisor module, not the switching modules.
- Command alias configuration takes effect for other user sessions immediately.
- You cannot override the default command alias **alias,** which aliases the **show cli alias**.
- Nesting of command aliases is permitted to a maximum depth of 1. One command alias can refer to another command alias that must refer to a valid command, not to another command alias.
- A command alias always replaces the first command keyword on the command line.
- You can define command aliases for commands in any configuration submode or the EXEC mode.

Defining Command Aliases

You can define command aliases using the **cli alias name** command in configuration mode.

This following example shows how to define command aliases.

```
switch# config t
switch(config)# cli alias name gigint interface gigabitethernet
switch(config)# cli alias name shintbr show interface brief
switch(config)# cli alias name shfcintup "shintbr| include up | include fc"
```

You can display the command aliases defined on the switch using the **alias** default command alias.

The following example shows how to display the command aliases defined on the switch.

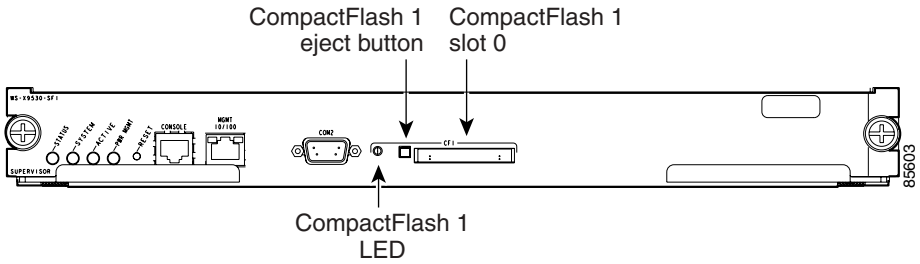
```
switch# alias
CLI alias commands
==================
alias      :show cli alias
gigint     :interface gigabitethernet
shintbr    :show interface brief
shfcintup  :shintbr | include up | include fc
```

About Flash Devices

Every switch in the Cisco MDS 9000 Family contains one internal bootflash (see Figure 1-2). The Cisco MDS 9500 Series additionally contains one external CompactFlash called slot0 (see Figure 1-2 and Figure 1-3).

Figure 1-2 Flash Devices in the Cisco MDS 9000 Supervisor Module

Figure 1-3 External CompactFlash in the Cisco MDS 9000 Supervisor Module



Internal bootflash:

All switches in the Cisco MDS 9000 Family have one internal bootflash: that resides in the supervisor or switching module.You have access to two directories within the internal bootflash: file system.

- The volatile: directory which provides temporary storage, and is also the default. Files in temporary storage (volatile:) are erased when the switch reboots.
- The bootflash (nonvolatile storage): directory which provides permanent storage. The files in bootflash are preserved through reboots and power outages.

External CompactFlash (Slot0)

Cisco MDS 9500 Series directors contain an additional external CompactFlash called slot0:

The external CompactFlash, an optional device for MDS 9500 Series directors, can be used for storing software images, logs, and core dumps.

Formatting Flash Disks and File Systems

By formatting a flash disk or a file system, you are essentially clearing out the contents of the disk or the file system and restoring it to its factory-shipped state (see the "About Flash Devices" section on page 1-26 and "Using the File System" section on page 1-28 for additional information).

Initializing bootflash:

When a switch is shipped, the **init system** command is already performed and you do not need to issue it again. Initializing the switch resets the entire internal disk and erases all data in the bootflash: partition. The internal disk is composed of several file systems with bootflash: being one of them. All files in bootflash: are erased and you must download the system and kickstart images again. After issuing an **init system** command, you don't have to format the bootflash: again since bootflash: is automatically formatted.

Note The **init system** command also installs a new loader from the existing (running) kickstart image. You can access this command from the `switch(boot)#` prompt.

If bootflash: is found corrupted during a boot sequence, you will see the following message:

```
ERROR:bootflash: has unrecoverable error; please do "format bootflash:"
```

Use the **format bootflash:** command to only format the bootflash: file system. You can issue the **format bootflash:** command from either the `switch#` or the `switch(boot)#` prompts.

If you issue the **format bootflash:** command, you must download the kickstart and system images again.

Formatting Slot0:

Be sure to format an external CompactFlash device before using it to save files or images.

You can verify if the external CompactFlash device is formatted by inserting it into slot0: and issuing the **dir slot0:** command.

- If the external CompactFlash device is already formatted, you can see file system usage information (along with any existing files).
- If the external CompactFlash device is unformatted (corrupted), you will see the following message:

  ```
  Device unavailable
  ```

  In this case, you need to format the CompactFlash device using the **format slot0:** command.

Note The slot0: file system cannot be accessed from the standby the `loader>` prompt or the `switch(boot)#` prompt, if the disk is inserted after booting the switch.

Caution The Cisco MDS SAN-OS software only supports Cisco-certified CompactFlash devices that are formatted using Cisco MDS switches. Using uncertified CompactFlash devices may result in unpredictable consequences; formatting CompactFlash devices using other platforms may result in errors.

Using the File System

The switch provides the following useful functions to help you manage software image files and configuration files:

Setting the Current Directory

The **cd** command changes the current directory level to a specified directory level. CLI defaults to the volatile: files system. This command expects a directory name input.

Tip Any file saved in the volatile: file system will be erased when the switch reboots.

The syntax for this command is **cd** *directory name*

This example changes the current directory to the mystorage directory that resides in the slot0 directory:

```
switch# cd slot0:mystorage
```

This example changes the current directory to the mystorage directory that is in the current directory.

```
switch# cd mystorage

If the current directory is slot0:mydir, this command changes the current directory to
slot0:mydir/mystorage.
```

Displaying the Current Directory

The **pwd** command displays the current directory location. This example changes the directory and displays the current directory.

```
switch# cd bootflash:
switch# pwd
bootflash:
```

Listing the Files in a Directory

The **dir** command displays the contents of the current directory or the specified directory. The syntax for this command is **dir** *directory or file name*

This example shows how to list the files on the default volatile: file system:

```
switch# dir
          Usage for volatile: filesystem
                        0 bytes total used
                 20971520 bytes free
                 20971520 bytes available
```

Creating a New Directory

The **mkdir** command creates a directory at the current directory level or at a specified directory level.

The syntax for this command is **mkdir** *directory name*

This example creates a directory called test in the slot0 directory.

```
switch# mkdir slot0:test
```

This example creates a directory called test at the current directory level.

```
switch# mkdir test
```

```
If the current directory is slot0:mydir, this command creates a directory called
slot0:mydir/test.
```

Deleting an Existing Directory

The **rmdir** command deletes an existing directory at the current directory level or at a specified directory level. The directory must be empty to be deleted.

The syntax for this command is **rmdir** *directory name*

This example deletes the directory called test in the slot0 directory.

```
switch# rmdir slot0:test
```

This example deletes the directory called test at the current directory level.

```
switch# rmdir test
```

```
If the current directory is slot0:mydir, this command deletes the slot0:mydir/test
directory.
```

Moving Files

The **move** command removes a file from the source directory and places it in the destination directory. If a file with the same name already exists in the destination directory, that file is overwritten by the moved file.

This example moves the file called samplefile from the slot0 directory to the mystorage directory.

```
switch# move slot0:samplefile slot0:mystorage/samplefile
```

```
This example moves a file from the current directory level.
```

```
switch# move samplefile mystorage/samplefile

If the current directory is slot0:mydir, this command moves slot0:mydir/samplefile to
slot0:mydir/mystorage/samplefile.
```

Copying Files

The **copy** command copies a file.

This example copies the file called samplefile from the external CompactFlash (slot0) directory to the mystorage directory.

```
switch# copy slot0:samplefile slot0:mystorage/samplefile

This example copies a file from the current directory level.

switch# copy samplefile mystorage/samplefile

If the current directory is slot0:mydir, this command copies slot0:mydir/samplefile to
slot0:mydir/mystorage/samplefile.
You can also use the copy command to upload and download files from the slot0: or
bootflash: file system to or from a FTP, TFTP, SFTP, or SCP server.
```

Refer to the *Cisco MDS 9000 Family CLI Configuration Guide* for further information.

Deleting Files

The **delete** command deletes a specified file or the specified directory and all its contents. Refer to the *Cisco MDS 9000 Family CLI Configuration Guide* for further information.

This example shows how to delete a file from the bootflash: directory (assuming you are already in the bootflash: directory):

```
switch# delete dns_config.cfg
```

This example shows how to delete a file from an external CompactFlash (slot0):

```
switch# delete slot0:dns_config.cfg
```

This example deletes the entire `my-dir` directory and all its contents:

```
switch# delete bootflash:my-dir
```

Caution If you specify a directory, the **delete** command deletes the entire directory and all its contents.

Displaying File Contents

The **show file** command displays the contents of a specified file in the file system.

The syntax for this command is **show file** *file_name*

This example displays the contents of the test file that resides in the slot0 directory.

```
switch# show file slot0:test
config t
Int fc1/1
no shut
```

```
end
show int
```

This example displays the contents of a file residing in the current directory.

```
switch# show file myfile
```

Saving Command Output to a File

You can force all screen output to go to a file by appending **>** *filename* to any command. For example, enter **show interface > samplefile** at the EXEC mode switch prompt to save the interface configuration to *samplefile*—a file created at the same directory level. At the EXEC mode switch prompt, issue a **dir** command to view all files in this directory, including the recently saved *samplefile*.

Refer to the *Cisco MDS 9000 Family CLI Configuration Guide* for further information.

Note Redirection is allowed only if the current directory is on the `volatile:` (default) or `slot0:` file systems. Redirection is not allowed if the current directory is on the `bootflash:` file system. The current directory can be viewed using the **pwd** command and changed using the **cd** command.

Directing show Command Output to a File

You can direct **show** command output to a file, either on the volatile file system, on slot0 CompactFlash memory, or on a remote server.

The following example shows how to direct the **show running-config** output to a file on the volatile file system.

```
switch1# show running-config > volatile:switch1-run.cfg
```

The following example shows how to direct the **show running-config** output to a file on slot0 CompactFlash memory.

```
switch2# show running-config > slot0:switch2-run.cfg
```

The following example shows how to direct the **show running-config** output to a file on a TFTP server.

```
switch3# show running-config > tftp://10.10.1.1/home/suser/switch3-run.cfg
Preparing to copy...done
```

Compressing and Uncompressing Files

The **gzip** command compresses (zips) the specified file using LZ77 coding.

This example directs the output of the show tech-support command to a file (Samplefile) and then zips the file and displays the difference in the space used up in the volatile: directory:

```
switch# show tech-support > Samplefile
Building Configuration ...
switch# dir
    1525859     Jul 04 00:51:03 2003 Samplefile
Usage for volatile://
    1527808 bytes used
   19443712 bytes free
   20971520 bytes total
```

```
switch# gzip volatile:Samplefile
switch# dir
     266069     Jul 04 00:51:03 2003 Samplefile.gz
Usage for volatile://
     266240 bytes used
   20705280 bytes free
   20971520 bytes total
```

The **gunzip** command uncompresses (unzips) LZ77 coded files.

This example unzips the file that was compressed in the previous example:

```
switch# gunzip samplefile
/volatile/samplefile.gz: No such file or directory
switch# gunzip Samplefile
switch# dir
    1525859     Jul 04 00:51:03 2003 Samplefile
Usage for volatile://
    1527808 bytes used
   19443712 bytes free
   20971520 bytes total
```

Displaying the Last Line in a File

The **tail** command displays the last lines (tail end) of a specified file.

The syntax for this command is **tail** <*file name*> *[<number of lines>]*

```
switch# tail mylog 10
```

You see the last 10 lines of the mylog file.

Executing Commands Specified in a Script

The **run-script** command executes the commands specified in a file. To use this command, be sure to create the file and specify commands in the required order.

Note You cannot create the script files at the switch prompt. You can create the script file on an external machine and copy it the bootflash: directory. This section assumes that the script file resides in the bootflash: directory.

The syntax for this command is **run-script** *file_name*

This example displays the CLI commands specified in the testfile that resides in the slot0 directory.

```
switch# show file slot0:testfile
conf t
interface fc 1/1
no shutdown
end
sh interface fc1/1
```

This file output is in response to the **run-script** command executing the contents in the testfile file:

```
switch# run-script slot0:testfile
'conf t'
Enter configuration commands, one per line. End with CNTL/Z.

'interface fc1/1'
```

```
'no shutdown'

'end'

'sh interface fc1/1'
fc1/1 is down (Fcot not present)
    Hardware is Fibre Channel
    Port WWN is 20:01:00:05:30:00:48:9e
    Admin port mode is auto, trunk mode is on
    vsan is 1
    Beacon is turned off
    Counter Values (current):
      0 frames input, 0 bytes, 0 discards
      0 runts, 0 jabber, 0 too long, 0 too short
      0 input errors, 0 CRC, 0 invalid transmission words
      0 address id, 0 delimiter
      0 EOF abort, 0 fragmented, 0 unknown class
      0 frames output, 0 bytes, 0 discards
      Received 0 OLS, 0 LRR, 0 NOS, 0 loop inits
      Transmitted 0 OLS, 0 LRR, 0 NOS, 0 loop inits
    Counter Values (5 minute averages):
      0 frames input, 0 bytes, 0 discards
      0 runts, 0 jabber, 0 too long, 0 too short
      0 input errors, 0 CRC, 0 invalid transmission words
      0 address id, 0 delimiter
      0 EOF abort, 0 fragmented, 0 unknown class
      0 frames output, 0 bytes, 0 discards
      Received 0 OLS, 0 LRR, 0 NOS, 0 loop inits
     Transmitted 0 OLS, 0 LRR, 0 NOS, 0 loop inits
```

Setting the Delay Time

The **sleep** command delays an action by a specified number of seconds.

The syntax for this command is **sleep** <*seconds*>

```
switch# sleep 30
```

You will see the switch prompt return after 30 seconds.

This command is useful within scripts. For example, if you create a script called test-script:

```
switch# show file slot0:test-script
discover scsi-target remote
sleep 10
show scsi-target disk

switch# run-script slot0:test-script
```

When you execute the slot0:test-script, the switch software executes the **discover scsi-target remote** command, and then waits for 10 seconds before executing the **show scsi-target disk command**.

Role-Based CLI

By default, two roles exist in all switches:

- Network operator—Has permission to view the configuration.

- Network administrator—Has permission to execute all commands and to set up to 64 permission levels based on user roles and groups.

When you execute a command, perform command completion, or obtain context sensitive help, the switch software allows the operation to progress if you have the correct permission as specified in the description of the command.

Using Valid Formats and Ranges

Note Do not enter ellipsis (...), vertical bar (|), less or great (< >), bracket ([ ]), or braces ({ }) in command lines. These characters have special meaning in Cisco MDS SAN-OS text strings.

Some commands require a MAC address, IP address, or IDs that must be designated in a standard format or given a range. See Table 1-4.

Table 1-4 Valid Formats and Ranges

Address	Description	Valid Format Example	Range
MAC address	6 bytes in hexadecimal format separated by colons (not case-sensitive)	00:00:0c:24:d2:Fe	—
IP address	32 bytes, written as 4 octets separated by periods (dotted decimal format) that are made up of a network section, an optional netmask section, and a host section.	126.2.54.1	—
VSAN	Integer that specifies the VSAN.	7	1 to 4093
VLAN	Integer that specifies the VLAN	11	1 to 4093
Port WWN (pWWN)	Eight hexadecimal numbers separated by colons (not case-sensitive).	12:34:56:78:9A:BC:dE:F1	—
Node WWN (nWWN)	Eight hexadecimal numbers separated by colons (not case-sensitive).	12:34:56:78:9A:BC:dE:F1	—
LUN	8 bytes in hexadecimal format separated by colons. A minimum of two hex characters are acceptable. The valid format is hhhh[:hhhh[:hhhh[:hhhh]]]	64 (100d = 64h)	—
FCID	Six character hexadecimal value prepended by 0x.	0xabc123	—
Domain ID	Integer that specifies the domain.	7	1 to 239
Timers	Integer that specifies timers in milliseconds for latency, FC time out values (TOV).	100	0 to 2147483647
Switching module	Slot in which the applicable switching module resides.	1	1 to 15
Switch priority	Integer specifying switch priority.	5	1 to 254
Channel group	Integer that specifies a PortChannel group addition.	1	1 to 100
Fabric Shortest Path First (FSPF)	Integer that specifies the hold time (in milliseconds) before making FSPF computations.	1000	0 to 65535
Fabric Analyzer	The allowed range for the frame size limit in bytes.	64	64 to 65536
Fabric Analyzer captures	An example of 10 frames, limits the number of frames captured to 10.	10	0 to 2147483647
FCIP profile	Integer that specifies the FCIP profile	101	1 to 255
TCP retransmit time	Integer that specifies the minimum retransmit time for the TCP connection in milliseconds	300	250 to 5000

Table 1-4 Valid Formats and Ranges (continued)

Address	Description	Valid Format Example	Range
Keepalive timeout	Integer that specifies the TCP connection's keepalive timeout in seconds.	60	1 to 7200
TCP retransmissions	Integer that specifies the maximum number of TCP transmissions.	6	1 to 8
PMTU	Integer that specifies the path MTU reset time in seconds	90	60 to 3600
TCP buffer size	Integer that specifies the advertised TCP buffer size in KB.	5000	0 to 8192
Traffic burst size	Integer that specifies the maximum burst size in KB.	30	10 to 100
Peer TCP port	Integer that specifies the TCP port number	3000	0 to 65535
Acceptable time difference	Integer that specifies the acceptable time difference in milliseconds for a packet being accepted.	4000	1 to 60,000
iSCSI pWWN allocation	Integer that specifies the number of pWWNs that must be allocated to an iSCSI initiator.	2	1 to 64
CDP refresh and hold time	Integer that specifies the refresh time interval and the hold time in seconds for the CDP protocol.	60	5 to 255

Using Debug Commands

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

All **debug** commands are entered in privileged EXEC mode, and most **debug** commands take no arguments. Use the **show debugging** command to display the state of each debugging option.

To list and see a brief description of all the debugging command options, enter the command **debug ?** at the command line in privileged EXEC mode. For example:

```
switch# debug ?
```

Not all debugging commands listed in the **debug ?** output are described in this document. Commands are included here based on their usefulness in assisting you to diagnose network problems. Commands not included are typically used internally by Cisco engineers during the development process and are not intended for use outside the Cisco environment.

To enable all system diagnostics, enter the **debug all** command at the command line in privileged EXEC mode. For example:

```
switch# debug all
```

To turn off all diagnostic output, enter the **no debug all** command at the command line in privileged EXEC mode. For example:

```
switch# no debug all
```

Using the **no debug all** command is a convenient way to ensure that you have not accidentally left any **debug** commands turned on.

Caution Because debugging output takes priority over other network traffic, and because the **debug all** command generates more output than any other **debug** command, it can severely diminish the performance of the router or even render it unusable. In virtually all cases, it is best to use more specific **debug** commands.

Generating debug Command Output

Enabling a **debug** command can result in output similar to the following example for the **debug modem** command:

```
Router# debug modem

15:25:51: TTY4: DSR came up
15:25:51: tty4: Modem: IDLE->READY
15:25:51: TTY4: Autoselect started
15:27:51: TTY4: Autoselect failed
15:27:51: TTY4: Line reset
15:27:51: TTY4: Modem: READY->HANGUP
15:27:52: TTY4: dropping DTR, hanging up
15:27:52: tty4: Modem: HANGUP->IDLE
15:27:57: TTY4: restoring DTR
15:27:58: TTY4: DSR came up
```

The router continues to generate such output until you enter the corresponding **no debug** command (in this case, the **no debug modem** command).

If you enable a **debug** command and no output is displayed, consider the following possibilities:

- The router may not be properly configured to generate the type of traffic you want to monitor. Use the **more system:running-config** EXEC command to check its configuration.
- Even if the router is properly configured, it may not generate the type of traffic you want to monitor during the particular period that debugging is turned on. Depending on the protocol you are debugging, you can use commands such as the TCP/IP **ping** EXEC command to generate network traffic.

Redirecting debug and Error Message Output

By default, the network server sends the output from **debug** commands and system error messages to the console. If you use this default, monitor debug output using a virtual terminal connection, rather than the console port.

To redirect debug output, use the **logging** command options within configuration mode as described in the following sections.

Possible destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. The syslog format is compatible with 4.3 Berkeley Standard Distribution (BSD) UNIX and its derivatives.

Note Be aware that the debugging destination you use affects system overhead. Logging to the console produces very high overhead, whereas logging to a virtual terminal produces less overhead. Logging to a syslog server produces even less, and logging to an internal buffer produces the least overhead of any method.

To configure message logging, you need to be in configuration command mode. To enter this mode, use the **configure terminal** command at the EXEC prompt.

Enabling Message Logging

To enable message logging to all supported destinations other than the console, enter the following command:

logging on

The default condition is **logging on**.

To direct logging to the console only and disable logging output to other destinations, enter the following command:

no logging on

Setting the Message Logging Levels

You can set the logging levels when logging messages to the following devices:

- Console
- Monitor
- Syslog server

Table 1-5 lists and briefly describes the logging levels and corresponding keywords you can use to set the logging levels for these types of messages. The highest level of message is level 0, emergencies. The lowest level is level 7, debugging, which also displays the greatest amount of messages. For information about limiting these messages, see sections later in this chapter.

Table 1-5 Message Logging Keywords and Levels

Level	Keyword	Description	Syslog Definition
0	**emergencies**	System is unusable.	LOG_EMERG
1	**alerts**	Immediate action is needed.	LOG_ALERT
2	**critical**	Critical conditions exist.	LOG_CRIT
3	**errors**	Error conditions exist.	LOG_ERR
4	**warnings**	Warning conditions exist.	LOG_WARNING
5	**notification**	Normal, but significant, conditions exist.	LOG_NOTICE
6	**informational**	Informational messages.	LOG_INFO
7	**debugging**	Debugging messages.	LOG_DEBUG

Limiting the Types of Logging Messages Sent to the Console

To limit the types of messages that are logged to the console, use the **logging console** router configuration command. The full syntax of this command follows:

logging console *level*

no logging console

The **logging console** command limits the logging messages displayed on the console to messages up to and including the specified severity level, which is specified by the *level* argument. Keywords are listed in order from the most severe level to the least severe.

The **no logging console** command disables logging to the console.

The following example sets console logging of messages at the **debugging** level, which is the least severe level and which displays all logging messages:

```
logging console debugging
```

Logging Messages to an Internal Buffer

The default logging device is the console; all messages are displayed on the console unless otherwise specified.

To log messages to an internal buffer, use the **logging buffered** router configuration command. The full syntax of this command follows:

logging buffered

no logging buffered

The **logging buffered** command copies logging messages to an internal buffer instead of writing them to the console. The buffer is circular in nature, so newer messages overwrite older messages. To display the messages that are logged in the buffer, use the **show logging** privileged EXEC command. The first message displayed is the oldest message in the buffer.

The **no logging buffered** command cancels the use of the buffer and writes messages to the console (the default).

Limiting the Types of Logging Messages Sent to Another Monitor

To limit the level of messages logged to the terminal lines (monitors), use the **logging monitor** router configuration command. The full syntax of this command follows:

logging monitor *level*

no logging monitor

The **logging monitor** command limits the logging messages displayed on terminal lines other than the console line to messages with a level up to and including the specified *level* argument. To display logging messages on a terminal (virtual console), use the **terminal monitor** privileged EXEC command.

The **no logging monitor** command disables logging to terminal lines other than the console line.

The following example sets the level of messages displayed on monitors other than the console to **notification**:

```
logging monitor notification
```

Logging Messages to a UNIX Syslog Server

To log messages to a syslog server host, use the **logging host** global configuration command. The full syntax of this command follows:

logging host {*ip-address* | *host-name*} [**xml**]

no logging host {*ip-address* | *host-name*} [**xml**]

The **logging host** command identifies a syslog server host that is to receive logging messages. The *ip-address* argument is the IP address of the host. By issuing this command more than once, you build a list of syslog servers that receive logging messages.

The **no logging host** command deletes the syslog server with the specified address from the list of syslogs.

Limiting Messages to a Syslog Server

To limit the number of messages sent to syslog servers, use the **logging trap** router configuration command. The full syntax of this command follows:

logging trap *level*

no logging trap

The **logging trap** command limits the logging messages sent to syslog servers to logging messages with a level up to and including the specified *level* argument.

To send logging messages to a syslog server, specify its host address with the **logging host** command.

The default trap level is **informational**.

The **no logging trap** command returns the trap level to the default.

The current software generates the following categories of syslog messages:

- Error messages at the **emergencies** level.
- Error messages at the **alerts** level.
- Error messages at the **critical** level.
- Error messages about software or hardware malfunctions, displayed at the **errors** level.
- Interface up/down transitions and system restart messages, displayed at the **notification** level.
- Reload requests and low-process stack messages, displayed at the **informational** level.
- Output from the **debug** commands, displayed at the **debugging** level.

The **show logging** privileged EXEC command displays the addresses and levels associated with the current logging setup. The command output also includes ancillary statistics.

Example of Setting Up a UNIX Syslog Daemon

To set up the syslog daemon on a 4.3 BSD UNIX system, include a line such as the following in the file /etc/syslog.conf:

```
local7.debugging /usr/adm/logs/tiplog
```

The **local7** keyword specifies the logging facility to be used.

The **debugging** keyword specifies the syslog level. See Table 1-5 for other keywords that can be listed.

The UNIX system sends messages at or above this level to the specified file, in this case /usr/adm/logs/tiplog. The file must already exist, and the syslog daemon must have permission to write to it.

For the System V UNIX systems, the line should read as follows:

```
local7.debug /usr/admin/logs/cisco.log
```

CHAPTER 2

A Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "Command Modes" section to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

aaa accounting logsize

To set the size of the local accounting log file, use the **aaa accounting logsize** command to set the size of the local accounting log file. To revert to the default logsize 250000 bytes, use the **no** form of the command.

aaa accounting logsize *integer*

no aaa accounting logsize

Syntax Description

aaa accounting	Configures accounting methods
logsize	Configures local accounting log file size (in bytes).
integer	Sets the size limit of the local accounting log file in bytes from 0 to 250000.

Defaults

25,0000

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
2.0	This command was deprecated.

Usage Guidelines

None.

Examples

The following example shows the log file size configured at 29000 bytes.

```
switch# config terminal
switch(config)# aaa accounting logsize 29000
```

Related Commands

Command	Description
show accounting logsize	Displays the configured log size.
show accounting log	Displays the entire log file.

aaa accounting default

To configure the default accounting method, use the **aaa accounting default** command. To revert to the default local accounting, use the **no** form of the command.

aaa accounting default {**group** *group-name* [**none**] | **none**} | **local** [**none**] | **none**}

no aaa accounting default {**group** *group-name* [**none**] | **none**} | **local** [**none**] | **none**}

Syntax Description

group *group-name*	Specifies the group authentication method. The group name is a maximum of 127 characters.
local	Specifies the local authentication method.
none	No authentication, everyone permitted.

Defaults

Local accounting.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Specify the currently configured command preceded by a **no** in order to revert to the factory default.

Examples

The following example enables accounting to be performed using remote TACACS+ servers which are member of the group called TacServer, followed by the local accounting method.

```
switch# config t
switch(config)# aaa accounting default group TacServer
```

The following example turns off accounting.

```
switch(config)# aaa accounting default none
```

The following example reverts to the local accounting (default).

```
switch(config)# no aaa accounting default group TacServer
```

Related Commands

Command	Description
show aaa accounting	Displays the configured accounting methods.

aaa authentication dhchap default

To configure DHCHAP authentication method, use the **aaa authentication dhchap default** command in configuration mode. To revert to factory defaults, use the **no** form of the command.

aaa authentication dhchap default {**group** *group-name* [**none**] | **none**} | **local** [**none**] | **none**}}

no aaa authentication dhchap default {**group** *group-name* [**none**] | **none**} | **local** [**none**] | **none**}

Syntax Description

group *group-name*	Specifies the group name authentication method. The group name is a maximum of 127 characters.
local	Specifies local user name authentication (default).
none	Specifies no authentication.

Defaults

local user name authentication.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The **local** option disables other authentication methods and configures local authentication to be used exclusively.

Specify the currently configured command preceded by a **no** in order to revert to the factory default.

Examples

The following example enables all DHCHAP authentication to be performed using remote TACACS+ servers which are member of the group called TacServers, followed by the local authentication.

```
switch# config terminal
switch(config)# aaa authentication dhchap default group TacServer
```

The following example reverts to the local authentication method (default).

```
switch(config)# no aaa authentication dhcahp default group TacServer
```

Related Commands

Command	Description
show aaa authentication	Displays the configured authentication methods.

aaa authentication iscsi default

To configure the iSCSI authentication method, use the **aaa authentication iscsi default** command in configuration mode. To negate the command or revert to factory defaults, use the **no** form of this command.

aaa authentication iscsi default {**group** *group-name* [**none**] | **none**} | **local** [**none**] | **none**}}

no aaa authentication iscsi default {**group** *group-name* [**none**] | **none**} | **local** [**none**] | **none**}}

Syntax Description

group *group-name*	Specifies the group name. The group name is a maximum of 127 characters.
local	Specifies local user name authentication (default).
none	Specifies no authentication.

Defaults

Local user name authentication.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The **local** option disables other authentication methods and configures local authentication to be used exclusively.

Specify the currently configured command preceded by a **no** in order to revert to the factory default.

Examples

The following example enables all iSCSI authentication to be performed using remote TACACS+ servers which are member of the group called TacServers, followed by the local authentication.

```
switch# config terminal
switch(config)# aaa authentication iscsi default group TacServer
```

The following example reverts to the local authentication method (default).

```
switch(config)# no aaa authentication iscsi default group TacServer
```

Related Commands

Command	Description
show aaa authentication	Displays the configured authentication methods.

aaa authentication login

To configure the authentication method for a login, use the **aaa authentication login** command in configuration mode. To revert to local authentication, use the **no** form of the command.

aaa authentication login {**default** {**group** *group-name* [**none**] | **none**} | **local** [**none**] | **none**} | **console** {*group-name* [**none**] | **none**} | **local** [**none**] | **none**}| **error-enable** | **mschap enable**}

no aaa authentication login {**default** {**group** *group-name* [**none**] | **none**} | **local** [**none**] | **none**} | **console** {*group-name* [**none**] | **none**} | **local** [**none**] | **none**}| **error-enable** | **mschap enable**}

Syntax Description

default	Configures the default method.
console	Configures the console authentication login method.
group *group-name*	Specifies the group name. The group name is a maximum of 127 characters.
local	Specifies the local authentication method.
none	Sets no authentication; everyone is permitted.
error-enable	Enables login error message display.
mschap enable	Enables MS-CHAP authentication for login.

Defaults

Local user name authentication.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Added the **mschap** option.

Usage Guidelines

Use the **console** option to override the console login method.

Specify the currently configured command preceded by a **no** to revert to the factory default.

Examples

The following example enables all login authentication to be performed using remote TACACS+ servers, which are members of the group called TacServer, followed by the local login method.

```
switch# config t
switch(config)# aaa authentication login default group TacServer
```

The following example enables console authentication to use the group called TacServer, followed by the local login method.

```
switch(config)# aaa authentication login console group TacServer
```

The following example turns off password validation.

```
switch(config)# aaa authentication login default none
```

The following example reverts to the local authentication method (default).

```
switch(config)# no aaa authentication login default group TacServer
```

The following example enables MS-CHAP authentication for login.

```
switch(config)# aaa authentication login mschap enable
```

The following example reverts to the default authentication method for login, which is the Password Authentication Protocol (PAP).

```
switch(config)# no aaa authentication login mschap enable
```

Related Commands

Command	Description
show aaa authentication	Displays the configured authentication methods.

aaa group server

To configure one or more independent server groups, use the **aaa group server** command in configuration mode. To remove the server group, use the **no** form of this command to remove the server group.

aaa group server {**radius** | **tacacs+**} *group-name*
server *server-name*
no server *server-name*

no aaa group server {**radius** | **tacacs+**} *group-name*

Syntax Description

radius	Specifies the RADIUS server group.
tacacs+	Specifies the TACACS+ server group.
group-name	Identifies the specified group of servers with a user-defined name. The name is limited to 64 alphanumeric characters.
server *server-name*	Specifies the server name to add or remove from the server group.

Defaults

None.

Command Modes

Configuration.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

You can configure these server groups at any time but they only take effect when you apply them to a AAA service using the **aaa authentication login** or the **aaa accounting** commands.

Examples

You can configure these server groups at any time but they only take effect when you apply them to a AAA service using the **aaa authentication** or the **aaa accounting** commands.

```
switch# config terminal
switch(config)# aaa group server tacacs+ TacacsServer1
switch(config-tacacs+)# server ServerA
switch(config-tacacs+)# exit
switch(config)# aaa group server radius RadiusServer19
switch(config-radius)# server ServerB
switch(config-radius)# no server ServerZ
```

Related Commands

Command	Description
show aaa groups	Displays all configured server groups.
show radius-server groups	Displays configured RADIUS server groups
show tacacs-server groups	Displays configured TACACS server groups

abort

To discard a Call Home configuration session in progress, use the **abort** command in Call Home configuration submode.

abort

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Call Home configuration submode

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to discard a Call Home configuration session in progress.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# abort
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

active equals saved

Enable the **active equals saved** command to automatically write any changes to the block, prohibit or port address name to the IPL file. To disable the configuration or to revert to factory defaults, use the **no** form of the command.

active equals saved

no active equals saved

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

FICON configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Enabling **active equals saved** ensures that you do not have to perform the **copy running-config startup-config** command to save the FICON configuration as well as the running configuration. If your switch or fabric consists of multiple FICON-enabled VSANs, and one of these VSANs has **active equals saved** enabled, changes made to the non-FICON configuration causes all FICON-enabled configurations to be saved to the IPL file.

Refer to the *Cisco MDS 9000 Family CLI Configuration Guide* for further information.

Examples

The following example enables the automatic save feature for a VSAN.

```
switch(config)# ficon vsan 2
switch(config-ficon)# active equals saved
```

The following example disables the automatic save feature for this VSAN.

```
switch(config-ficon)# no active equals saved
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration.
ficon vsan *vsan-id*	Enables FICON on the specified VSAN.
show ficon	Displays configured FICON details.

alert-group

To customize a Call Home alert group with user-defined **show** commands, use the **alert-group** command in Call Home configuration submode. To remove the customization, user the **no** form of the command.

alert-group *event-type* **user-def-cmd** *command*

no alert-group *event-type* **user-def-cmd** *command*

Syntax DescriptionT

event-type	Specifies event types by the following alert groups.
Avanti	Displays Avanti events.
Environmental	Displays power, fan, and temperature related events.
Inventory	Displays inventory status events.
License	Displays events related to licensing.
RMON	Displays events related to Remote Monitoring (RMON).
Supervisor-Hardware	Displays supervisor related events.
Syslog-group-port	Displays events relate to syslog messages filed by the the port manager.
System	Displays software related events.
test	Displays user-generated test events.
user-def-cmd *command*	Configures a CLI command for an alert-group. The maximum size is 512.

Defaults

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The **user-def-cmd** argument allows you to define a command whose outputs should be attached to the callhome message being sent. Only **show** commands can be specified and they must be associated with an alert group. Five commands can be specified per alert group. Invalid commands are rejected.

Note Make sure the destination profiles for the non-Cisco-TAC alert group, with a predefined **show** command, and the Cisco-TAC alert group are not the same.

Examples

The following example configures a user-defined command, called **show license usage**, for an alert group license.

```
switch(config-callhome)# alert-group license user-def-cmd "show license usage"
```

The following example removes a user-defined command, called **show license usage**, for an alert group license.

```
switch(config-callhome)# no alert-group license user-def-cmd "show license usage"
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

arp

To enable the Address Resolution Protocol (ARP) for the switch, use the **arp** command.To disable ARP for the switch, use the **no** form of the command.

arp *hostname*

no arp *hostname*

Syntax Description

hostname	Name of the host. Maximum length is 20 characters.

Defaults

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example disables the Address Resolution Protocol configured for the host with the IP address 10.1.1.1.

```
switch(config)# no arp 10.1.1.1
switch(config)#
```

Related Commands

Command	Description
show arp	Displays the ARP table.
clear arp	Deletes a specific entry or all entries from the ARP table.

attach module

To connect to a specific module, use the **attach module** command in EXEC mode.

attach module *slot-number*

Syntax Description

slot-number	Specifies slot number of the module to which to connect.

Command Modes

EXEC.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.0(2).

Usage Guidelines

You can use the **attach module** command to view the standby supervisor module information, but you cannot configure the standby supervisor module using this command.

You can also use the **attach module** command on the switching module portion of the Cisco MDS 9216 supervisor module, which resides in slot 1 of this two-slot switch.

To disconnect, use the **exit** command at the `module-number#` prompt, or type **$.** to forcibly abort the attach session.

Examples

The following example connects to the module in slot 2. Note that after you connect to the image on the module using the **attach module** command, the prompt changes to module-number#.

```
switch# attach module 1
Attaching to module 1 ...
To exit type 'exit', to abort type '$.'
module-1# exit
switch#
```

Related Commands

Command	Description
exit	Disconnects from the module.
show module	Displays the status of a module.

attribute qos

To configure a QOS attribute, use the **attribute qos** command in Inter-VSAN Routing (IVR) zone configuration submode. To disable this feature, use the **no** form of this command.

attribute qos {**high** | **low** | **medium**}

no attribute qos {**high** | **low** | **medium**}

Syntax Description

high	Configures frames matching zone to get high priority.
low	Configures frames matching zone to get low priority (Default).
medium	Configures frames matching zone to get medium priority.

Defaults

Disabled

Command Modes

IVR zone configuration submode

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure an IVR zone QOS attribute to low priority.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr zone name IvrZone
switch(config-ivr-zone)# attribute qos priority low
```

Related Commands

Command	Description
show ivr zone	Displays IVR zone configuration.

authentication

To configure the authentication method for an IKE protocol policy, use the **authentication** command in IKE policy configuration submode. To revert to the default authentication method, use the **no** form of the command.

authentication {**pre-share** | **rsa-sig**}

no authentication {**pre-share** | **rsa-sig**}

Syntax Description

pre-share	Configures the preshared key as the authentication method.
rsa-sig	Configures RSA signatures as the authentication method.

Defaults

Preshared key.

Command Modes

IKE policy configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

To use this command, enable the IKE protocol using the **crypto ike enable** command. In addition, you must configure the identity authentication mode using the fully qualified domain name (FQDN) before you can use RSA signatures for authentication. Use the **identity hostname** command for this purpose.

Examples

The following example shows how to configure the authentication method using the preshared key.

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# policy 1
switch(config-ike-ipsec-policy)# authentication pre-share
```

The following example shows how to configure the authentication method using the RSA signatures.

```
switch(config-ike-ipsec-policy)# authentication rsa-sig
```

The following example shows how to revert to the default authentication method (preshared key).

```
switch(config-ike-ipsec-policy)# no authentication rsa-sig
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.

Command	Description
identity hostname	Configures the identity for the IKE protocol.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

autonomous-fabric-id (IVR topology database configuration)

To configure an autonomous fabric ID (AFID) into the Inter-VSAN Routing (IVR) topology database, use the **autonomous-fabric-id** command. To remove the fabric ID, use the **no** form of the command.

autonomous-fabric-id *fabric-id* **switch-wwn** *swwn* **vsan-ranges** *vsan-id*

no autonomous-fabric-id *fabric-id* **switch-wwn** *swwn* **vsan-ranges** *vsan-id*

Syntax Description

fabric-id	Specifies the fabric ID for the IVR topology. **Note** For Cisco MDS SAN-OS images prior to release 2.1(1a), the *fabric-id* value is limited to 1. For Releases 2.1(1a) and later images, the *fabric-id* range is 1 to 64.
switch-wwn *swwn*	Configures the switch WWN in dotted hex format.
vsan-ranges *vsan-id*	Configures up to five ranges of VSANs to be added to the database. The range is 1 to 4093.

Defaults

None.

Command Modes

IVR topology database configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.1(1a)	Modified range for *fabric-id.*

Usage Guidelines

The following rules apply to configuring AFIDs to VSANs:

- The default AFID of a VSAN is 1.
- Each VSAN belongs to one and only one AFID.
- A switch can be a member of multiple AFIDs.
- AFIDs at a switch must not share any VSAN identifier (for example, a VSAN at a switch can belong to only one AFID).
- A VSAN identifier can be reused in different AFIDs, without merging the VSANs, as long as those AFIDs do not share a switch.

You can have up to 64 VSANs (or 128 VSANs for Cisco MDS SAN-OS Release 2.1(1a) or later) in an IVR topology. Specify the IVR topology using the following information:

- The switch WWNs of the IVR-enabled switches.
- A minimum of two VSANs to which the IVR-enabled switch belongs.

- The autonomous fabric ID (AFID), which distinguishes two VSANs that are logically and physically separate, but have the same VSAN number. Cisco MDS SAN-OS Release 1.3(1) and later supports only one default AFID (AFID 1) and thus does not support non-unique VSAN IDs in the network. As of Cisco MDS SAN-OS Release 2.1(1a), you can specify up to 64 AFIDs.

Note Two VSANs with the same VSAN number but different fabric IDs are counted as two VSANs out o f the 128 total VSANs allowed in the fabric.

The following command enters the configuration mode, enables the IVR feature, enters the VSAN topology database, and configures the pWWN-VSAN association for VSANs 2 and 2000:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr enable
switch(config)# ivr vsan-topology database
switch(config-ivr-topology-db)# autonomous-fabric-id 1 switch 20:00:00:00:30:00:3c:5e
vsan-ranges 2,2000
```

Related Commands

Command	Description
ivr enable	Enables the Inter-VSAN Routing (IVR) feature.
ivr vsan-topology database	Configures a VSAN topology database.
show autonomous-fabric-id database	Displays the contents of the AFID database.
show ivr	Displays IVR feature information.

autonomous-fabric-id (IVR service group configuration)

To configure an autonomous fabric ID (AFID) into an IVR service group, use the **autonomous-fabric-id** command in IVR service group configuration submode. To remove the autonomous fabric ID, use the **no** form of the command.

autonomous-fabric-id *afid* **vsan-ranges** *vsan-id*

no autonomous-fabric-id *afid* **vsan-ranges** *vsan-id*

Syntax Description

afid	Specifies the AFID to the local VSAN.
vsan-ranges *vsan-id*	Configures up to five ranges of VSANs to be added to the service group. The range is 1 to 4093.

Defaults

None.

Command Modes

IVR service group configuration submode.

Command History

Release	Modification
2.1	This command was introduced.

Usage Guidelines

Before configuring an IVR service group, you must enable the following:

- IVR using the **ivr Enable** command
- IVR distribution using the **ivr Distribute** command
- Automatic IVR topology discovery using the **ivr vsan-topology auto** command

To change to IVR service group configuration submode, use the **ivr service-group activate** command.

Examples

The following command enters the IVR service group configuration submode and configures AFID 10 to be in IVR service group serviceGroup1:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr enable
switch(config)# ivr distribute
switch(config)# ivr vsan-topology auto
switch(config)# ivr service-group name serviceGroup1
switch(config-ivr-sg)# autonomous-fabric-id 10 vsan 1-4
```

Related Commands

Command	Description
ivr enable	Enables the Inter-VSAN Routing (IVR) feature.
ivr service-group name	Configures an IVR service group and changes to IVR service group configuration submode.
show autonomous-fabric-id database	Displays the contents of the AFID database.
show ivr	Displays IVR feature information.

autonomous-fabric-id database

To configure an autonomous fabric ID (AFID) database, use the **autonomous-fabric-id database** command. To remove the fabric AFID database, use the **no** form of the command.

autonomous-fabric-id database

no autonomous-fabric-id database

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

You must configure the IVR VSAN topology to auto mode, using the **ivr vsan-topology auto** command, before you can use the **autonomous-fabric-id database** command to modify the database. The **autonomous-fabric-id database** command also enters AFID database configuration submode.

Note In user-configured VSAN topology mode, the AFIDs are specified in the IVR VSAN topology configuration itself and a separate AFID configuration is not needed.

Examples

The following example shows how to create an AFID database and enters AFID database configuration submode:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# autonomous-fabric-id database
switch(config-afid-db)#
```

Related Commands

Command	Description
ivr vsan-topology auto	Configures a VSAN topology for Inter-VSAN Routing (IVR) to auto configuration mode.
switch-wwn	Configures a switch WWN in the autonomous fabric ID (AFID) database
show autonomous-fabric-id database	Displays the contents of the AFID database.
show ivr	Displays IVR feature information.

CHAPTER 3

B Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "Command Modes" section to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

banner motd

To configure a message of the day (MOTD) banner, use the **banner motd** command in configuration mode.

banner motd [*delimiting-character message delimiting-character*]

no banner motd [*delimiting-character message delimiting-character*]

Syntax Description

delimiting-character	Identifies the delimiting character.
message	Specifies the banner message that is restricted to 40 lines with a maximum of 80 characters in each line.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

The configured MOTD banner is displayed before the login prompt on the terminal whenever a user logs in to a Cisco MDS 9000 Family switch.

Follow these guidelines when choosing your delimiting character:

- Do not use the *delimiting-character* in the *message* string.
- Do not use **"** and **%** as delimiters.

You can include tokens in the form $(token) in the message text. Tokens will be replaced with the corresponding configuration variable. For example:

- `$(hostname)` displays the host name for the switch
- `$(line)` displays the vty or tty line no or name
- The $(line-desc) and $(domain) tokens are not supported.

Examples

The following example configures a banner message with the following text “Testing the MOTD Feature.”

```
switch# config terminal
switch(config)# banner motd # Testing the MOTD Feature. #
```

The following example spans multiple lines and uses tokens to configure the banner message:

```
switch# config terminal
switch(config)# banner motd #
Enter TEXT message. End with the character '#'.
Welcome to switch $(hostname).
You tty line is $(line).
#
```

Related Commands

Command	Description
show banner motd	Displays the configured banner message.

boot

To perform operations on the system, use the **boot** command in configuration mode. To negate this feature or return to factory defaults, use the **no** form of the command.

boot {**asm-sfn** {**bootflash: | slot0: | tftp:**}[*image*] **[module** [*slot-number*]] **|**
auto-copy |
kickstart {**bootflash: | slot0: | tftp:**}[*image*] **[sup-1 [sup-2] | sup-2] |**
lasilc {**bootflash: | slot0: | tftp:**}[*image*] **[module** [*slot-number*]] **|**
ssi {**bootflash: | slot0:**} **|**
system {**bootflash: | slot0: | tftp:**}[*image*] **[sup-1 [sup-2] | sup-2]**}

no boot {**asm-sfn | auto-copy | kickstart | lasilc | system**}

Syntax Description

asm-sfn	Configures the virtualization image.
module *slot-number*	Specifies the slot number of the SSM.
auto-copy	Configures auto-copying of boot variable images.
kickstart	Configures the kickstart image.
lasilc	Configures the boot image.
ssi	Configures the SSI image.
system	Configures the system image.
bootflash:	Specifies system image URI for bootflash.
slot0:	Specifies system image URI for slot 0.
tftp:	Specifies system image URI for TFTP.
image	Specifies the image file name.
sup-1	The upper supervisor.
sup-2	The lower supervisor.

Defaults

Disabled.
The default state for **auto-copy** is enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.2(2)	This command was introduced
3.0(1)	Changed the default state for **auto-copy** to enabled.

Usage Guidelines

The **boot kickstart slot0:***image* command is currently not allowed. For kickstart, only bootflash: is allowed.

When the **boot auto-copy** command is issued, the system copies the boot variable images which are local (present) in the active supervisor module (but not in the standby supervisor module) to the standby supervisor module. For kickstart and system boot variables, only those images that are set for the standby supervisor module are copied. For modules (line card) images, all modules present in standby's corresponding locations (bootflash: or slot0:) will be copied.

Examples

The following example adds the new system image file to the SYSTEM environment variable.

```
switch(config)# boot system bootflash:system.img
```

The following example boots from the CompactFlash device (slot0:). The switch updates the SYSTEM environment variable to reflect the new image file in the specified Flash device.

```
switch(config)# boot system slot0:system.img
```

The following example overwrites the old Kickstart environment variable in the configuration file:

```
switch(config)# boot kickstart bootflash:kickstart.img
```

The following example specifies the SSM image to be used:

```
switch(config)# boot asm-sfn bootflash:m9000-ek9-asm-sfn-mz.1.2.2.bin
```

The following example enables automatic copying of boot variables from the active supervisor module to the standby supervisor module.

```
switch(config)# boot auto-copy
```

The following example disables the automatic copy feature (default).

```
switch(config)# no boot auto-copy
```

Related Commands

Command	Description
show boot	Displays the configured boot variable information.

bport

To configure a B port mode on a FCIP interface, use the **bport** option. To disable a B port mode on a FCIP interface, use the **no** form of the command.

bport

no bport

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Access this command from the `switch(config-if)#` submode.

Examples

The following example shows how to configure a B port mode on an FCIP interface.

```
switch# config terminal
switch(config)# interface fcip 1
switch(config-if)# bport
```

Related Commands

Command	Description
show interface fcip	Displays an interface configuration for a specified FCIP interface.
bport-keepalive	Configures B port keepalive responses.

bport-keepalive

To configure keepalive responses for B port FCIP interfaces, use the **bport-keepalive** option. To disable keepalive responses for B port FCIP interfaces, use the **no** form of the command.

bport-keepalive

no bport-keepalive

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Access this command from the `switch(config-if)#` submode.

Examples

The following example shows how to configure keepalive responses for B port FCIP interfaces.

```
switch# config terminal
switch(config)# interface fcip 1
switch(config-if)# bport-keepalives
```

Related Commands

Command	Description
show interface fcip	Displays an interface configuration for a specified FCIP interface.
bport	Configures a B port FCIP interface.

broadcast

To enable the broadcast frames attribute in a zone attribute group, use the **broadcast** command. To revert to the default, use the **no** form of the command.

broadcast

no broadcast

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Zone attribute configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

Broadcast frames are sent to all Nx ports.

If any NL port attached to an FL port shares a broadcast zone with the source of the broadcast frame, then the frames are broadcast to all devices in the loop.

This command only configures the broadcast attribute for enhanced zoning. To enable broadcast zoning for basic mode, use the **attribute broadcast** subcommand after entering zone configuration mode using the **zone name** command.

Examples

The following example shows how to set the broadcast attribute for a zone attribute group.

```
switch# config terminal
switch(config)# zone-attribute-group name admin-attributes vsan 10
switch(config-attribute-group)# broadcast
```

Related Commands

Command	Description
show zone-attribute-group	Displays zone attribute group information.
zone mode enhanced vsan	Enables enhanced zoning for a VSAN.
zone name	Configures zone attributes.
zone-attribute-group name	Configures zone attribute groups.

CHAPTER 4

C Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "About the CLI Command Modes" section on page 1-3 to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

callhome

To configure the Call Home function, use the **callhome** command.

callhome

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The Call Home configuration commands are available in the `(config-callhome)` submode.

A Call Home message is used to contact a support person or organization in case an urgent alarm is raised.

Once you have configured the contact information, you must enable the Call Home function. The **enable** command is required for the Call Home function to start operating. When you disable the Call Home function, all input events are ignored.

Note Even if Call Home is disabled, basic information for each Call Home event is sent to syslog.

The **user-def-cmd** command allows you to define a command whose outputs should be attached to the callhome message being sent. Only **show** commands can be specified and they must be associated with an alert group. Five commands can be specified per alert group. Invalid commands are rejected.

Note Customized **show** commands are only supported for full text and XML alert groups. Short text alert groups (short-txt-destination) do not support customized **show** commands because they only allow 128 bytes of text.

To assign **show** commands to be executed when an alert is sent, you must associate the commands with the alert group. When an alert is sent, Call Home associates the alert group with an alert type and attaches the output of the **show** commands to the alert message.

Note Make sure the destination profiles for the non-Cisco-TAC alert group, with a predefined **show** command, and the Cisco-TAC alert group are not the same.

The following example assigns contact information.

```
switch# config terminal
config terminal
switch# snmp-server contact personname@companyname.com
switch(config)# callhome
switch(config-callhome)# email-contact username@company.com
switch(config-callhome)# phone-contact +1-800-123-4567
switch(config-callhome)# streetaddress 1234 Picaboo Street, Any city, Any state, 12345
switch(config-callhome)# switch-priority 0
switch(config-callhome)# customer-id Customer1234
switch(config-callhome)# site-id Site1ManhattanNY
switch(config-callhome)# contract-id Company1234
```

The following example configures a user-defined **show** command for an alert-group license:

```
switch(config-callhome)# alert-group license user-def-cmd "show license usage"
```

Note The **show** command must be enclosed in double quotes.

The following example removes a user-defined **show** command for an alert-group license:

```
switch(config-callhome)# no alert-group license user-def-cmd "show license usage"
```

Related Commands

Command	Description
alert-group	Customizes a CallHome alert group with user-defined **show** commands.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

callhome test

To simulate a CallHome message generation, use the **callhome test** command.

callhome test [**inventory**]

Syntax Description

inventory	Sends a dummy CallHome inventory.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can simulate a message generation by issuing a **callhome test** command.

Examples

The following example sends a test message to the configured destination(s):

```
switch# callhome test
trying to send test callhome message
successfully sent test callhome message
```

The following example sends a test inventory message to the configured destination(s)

```
switch# callhome test inventory
trying to send test callhome message
successfully sent test callhome message
```

Related Commands

Command	Description
callhome	Configures Call Home functions.
show callhome	Displays configured Call Home information.

cd

To change the default directory or file system, use the **cd** command.

cd {*directory* | **bootflash:**[*directory*] | **slot0:**[*directory*] | **volatile:**[*directory*]}

Syntax Description

directory	Name of the directory on the file system.
bootflash:	URI or alias of the bootflash or file system.
slot0:	URI or alias of the slot0 file system.
volatile:	URI or alias of the volatile file system.

Defaults

The initial default file system is flash:. For platforms that do not have a physical device named flash:, the keyword flash: is aliased to the default Flash device.

If you do not specify a directory on a file system, the default is the root directory on that file system.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

For all EXEC commands that have an optional file system argument, the system uses the file system specified by the **cd** command when you omit the optional file system argument. For example, the **dir** command, which displays a list of files on a file system, contains an optional file system argument. When you omit this argument, the system lists the files on the file system specified by the **cd** command.

Examples

The following example sets the default file system to the Flash memory card inserted in slot 0:

```
switch# pwd
bootflash:/
switch# cd slot0:
switch# pwd
slot0:/
```

Related Commands

Command	Description
copy	Copies any file from a source to a destination.
delete	Deletes a file on a Flash memory device.
dir	Displays a list of files on a file system.
pwd	Displays the current setting of the cd command.
show file systems	Lists available file systems and their alias prefix names.
undelete	Recovers a file marked deleted on a Class A or Class B Flash file system.

cdp

Use the **cdp** command to globally configure the Cisco Discovery Protocol parameters. Use the **no** form of this command to revert to factory defaults.

cdp {**enable** | **advertise** {**v1** | **v2**} | **holdtime** *holdtime-seconds* | **timer** *timer-seconds*}

no cdp {**enable** | **advertise** | **holdtime** *holdtime-seconds* | **timer** *timer-seconds*}

Syntax Description

enable	Enables CDP globally on all interfaces on the switch.
advertise	Specifies the EXEC command to be executed.
v1	Specifies CDP version 1.
v2	Specifies CDP version 2.
holdtime	Sets the hold time advertised in CDP packets.
holdtime-seconds	Specifies the holdtime in seconds. The default is 180 seconds and the valid range is from 10 to 255 seconds.
timer	Sets the refresh time interval.
timer-seconds	Specifies the time interval in seconds. The default is 60 seconds and the valid range is from 5 to 255 seconds.

Defaults

CDP is enabled.

The hold time default interval is 180 seconds.

The refresh time interval is 60 seconds.

Command Modes

Configuration mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Use the **cdp enable** command to enable the Cisco Discovery Protocol (CDP) feature at the switch level or at the interface level. Use the **no** form of this command to disable this feature. When the interface link is established, CDP is enabled by default

CDP version 1 (v1) and version 2 (v2) are supported in Cisco MDS 9000 Family switches. CDP packets with any other version number are silently discarded when received.

Examples

The following example disables the CDP protocol on the switch. When CDP is disabled on an interface, one packet is sent to clear out the switch state with each of the receiving devices.

```
switch(config)# no cdp enable
Operation in progress. Please check global parameters
switch(config-console)#
```

The following example enables (default) the CDP protocol on the switch. When CDP is enabled on an interface, one packet is sent immediately. Subsequent packets are sent at the configured refresh time

```
switch(config)# cdp enable
Operation in progress. Please check global parameters
switch(config)#
```

The following example configures the Gigabit Ethernet interface 8/8 and disables the CDP protocol on this interface. When CDP is disabled on an interface, one packet is sent to clear out the switch state with each of the receiving devices.

```
switch(config)# interface gigbitethernet 8/8
switch(config-if)# no cdp enable
Operation in progress. Please check interface parameters
switch(config-console)#
```

The following example enables (default) the CDP protocol on the selected interface. When CDP is enabled on this interface, one packet is sent immediately. Subsequent packets are sent at the configured refresh time.

```
switch(config-if)# cdp enable
Operation in progress. Please check interface parameters
switch(config)#
```

The following example globally configures the refresh time interval for the CDP protocol in seconds. The default is 60 seconds and the valid range is from 5 to 255 seconds.

```
switch# config terminal
switch(config)# cdp timer 100
switch(config)#
```

The following example globally configures the hold time advertised in CDP packet in seconds. The default is 180 seconds and the valid range is from 10 to 255 seconds.

```
switch# config terminal
switch(config)# cdp holdtime 200
switch(config)#
```

The following example globally configures the CDP version. The default is version 2 (v2). The valid options are v1 and v2

```
switch# config terminal
switch(config)# cdp advertise v1
switch(config)#
```

Related Commands

Command	Description
clear cdp	Clears global or interface-specific CDP configurations.
show cdp	Displays configured CDP settings and parameters.

cfs distribute

To enable or disable Cisco Fabric Services (CFS) distribution on the switch, use the **cfs distribute** command in configuration mode. To disable this feature, use the **no** form of the command.

cfs distribute

no cfs distribute

Syntax Description

This command has no other arguments or keywords.

Defaults

CFS distribution is enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

By default CFS is in the distribute mode. In the distribute mode, fabric wide distribution is enabled. Applications can distribute data/configuration to all CFS-capable switches in the fabric where the application exists. This is the normal mode of operation.

If CFS distribution is disabled, using the **no cfs distribute** command causes the following to occurs:

- CFS and the applications using CFS on the switch are isolated from the rest of the fabric even though there is physical connectivity.
- All CFS operations are restricted to the isolated switch.
- All the CFS commands continue to work similar to the case of a physically isolated switch.
- Other CFS operations (for example, lock, commit, and abort) initiated at other switches do not have any effect at the isolated switch.
- CFS distribution is disabled over both Fibre Channel and IP.

Examples

The following example shows how to disable CFS distribution.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no cfs distribute
```

The following example shows how to reenable CFS distribution.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# cfs distribute
```

Related Commands

Command	Description
show cfs status	Displays whether CFS distribution is enabled or disabled.

cfs ipv4 distribute

To enable Cisco Fabric Services (CFS) distribution over IPv4 for applications that want to use this feature, use the **cfs ipv4** command in configuration mode. To disable this feature, use the **no** form of the command.

cfs ipv4 distribute

no cfs ipv4 distribute

Syntax Description

This command has no arguments or keywords.

Defaults

CFS distribution is enabled.
CFS over IP is disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

All CFS over IP enabled switches with similar multicast addresses form one CFS over IP fabric. CFS protocol specific distributions, such as the keep-alive mechanism for detecting network topology changes, use the IP multicast address to send and receive information.

Observe the following guidelines when using this command:

- If a switch is reachable over both IP and Fibre Channel, application data will be distributed over Fibre Channel.
- You can select either an IPv4 or IPv6 distribution when CFS is enabled over IP.
- Both IPv4 and IPv6 distribution cannot be enabled on the same switch.
- A switch that has IPv4 distribution enabled cannot detect a switch that IPv6 distribution enabled. The switches behave as if they are in two different fabrics even though they are connected to each other.

Examples

The following example shows how to disable CFS IPv4 distribution.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no cfs ipv4 distribute
This will prevent CFS from distributing over IPv4 network.
Are you sure? (y/n)  [n]
```

The following example shows how to reenable CFS IPv4 distribution.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
switch(config)# cfs ipv4 distribute
```

Related Commands

Command	Description
cfs ipv4 mcast-address	Configures an IPv4 multicast address for Cisco Fabric Services (CFS) distribution over IPv4.
show cfs status	Displays whether CFS distribution is enabled or disabled.

cfs ipv4 mcast-address

To configure an IPv4 multicast address for Cisco Fabric Services (CFS) distribution over IPv4, use the **cfs ipv4 mcast-address** command in configuration mode. To disable this feature, use the **no** form of the command.

cfs ipv4 mcast-address *ipv4-address*

no cfs ipv4 mcast-address *ipv4-address*

Syntax Description

ipv4-address	Specifies an IPv4 multicast address for CFS distribution over IPv4. The range of valid IPv4 addresses is 239.255.0.0 through 239.255.255.255, and 239.192.0.0 through 239.251.251.251.

Defaults

Multicast address: 239.255.70.83.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Before using this command, enable CFS distribution over IPv4 using the **cfs ipv4 distribute** command.

All CFS over IP enabled switches with similar multicast addresses form one CFS over IP fabric. CFS protocol specific distributions, such as the keep-alive mechanism for detecting network topology changes, use the IP multicast address to send and receive information.

Note CFS distributions for application data use directed unicast.

You can configure a value for a CFS over IP multicast address. The default IPv4 multicast address is 239.255.70.83.

Examples

The following example shows how to configure an IP multicast address for CFS over IPv4.

```
switch# config t
switch(config)# cfs ipv4 mcast-address 239.255.1.1
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?
Are you sure? (y/n) [n] y
```

The following example shows how to revert to the default IPv4 multicast address for CFS distribution over IPv4. The default IPv4 multicast address for CFS is 239.255.70.83.

```
switch(config)# no cfs ipv4 mcast-address 10.1.10.100
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?

Are you sure? (y/n) [n] y
```

Related Commands

Command	Description
cfs ipv4 distribute	Enables or disables Cisco Fabric Services (CFS) distribution over IPv4.
show cfs status	Displays whether CFS distribution is enabled or disabled.

cfs ipv6 distribute

To enable Cisco Fabric Services (CFS) distribution over IPv6 for applications that want to use this feature, use the **cfs ipv6 distribute** command in configuration mode. To disable this feature, use the **no** form of the command.

cfs ipv6 distribute

no cfs ipv6 distribute

Syntax Description

This command has no arguments or keywords.

Defaults

CFS distribution is enabled.
CFS over IP is disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

All CFS over IP enabled switches with similar multicast addresses form one CFS over IP fabric. CFS protocol specific distributions, such as the keep-alive mechanism for detecting network topology changes, use the IP multicast address to send and receive information.

Observe the following guidelines when using this command:

- If a switch is reachable over both IP and Fibre Channel, application data will be distributed over Fibre Channel.
- You can select either an IPv4 or IPv6 distribution when CFS is enabled over IP.
- Both IPv4 and IPv6 distribution cannot be enabled on the same switch.
- A switch that has IPv4 distribution enabled cannot detect a switch that IPv6 distribution enabled. The switches behave as if they are in two different fabrics even though they are connected to each other.

Examples

The following example shows how to disable CFS IPv6 distribution.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no cfs ipv6 distribute
This will prevent CFS from distributing over IPv6 network.
Are you sure? (y/n)  [n]
```

The following example shows how to reenable CFS IPv6 distribution.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
switch(config)# cfs ipv6 distribute
```

Related Commands

Command	Description
cfs ipv6 mcast-address	Configures an IPv6 multicast address for Cisco Fabric Services (CFS) distribution over IPv6.
show cfs status	Displays whether CFS distribution is enabled or disabled.

cfs ipv6 mcast-address

To configure an IPv6 multicast address for Cisco Fabric Services (CFS) distribution over IPv6, use the **cfs ipv6 mcast-address** command in configuration mode. To disable this feature, use the **no** form of the command.

cfs ipv6 mcast-address *ipv6-address*

no cfs ipv6 mcast-address *ipv6-address*

Syntax Description

ipv6-address	Specifies an IPv6 multicast address or CFS distribution over IPv6. The IPv6 Admin scope range is [ff15::/16, ff18::/16].

Defaults

Multicast address: ff15::efff:4653.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Before using this command, enable CFS distribution over IPv6 using the **cfs ipv6 distribute** command.

All CFS over IP enabled switches with similar multicast addresses form one CFS over IP fabric. CFS protocol specific distributions, such as the keep-alive mechanism for detecting network topology changes, use the IP multicast address to send and receive information.

Note CFS distributions for application data use directed unicast.

You can configure a CFS over IP multicast address value for IPv6. The default IPv6 multicast address is ff15::efff:4653. Examples of the IPv6 Admin scope range are ff15::0000:0000 to ff15::ffff:ffff and ff18::0000:0000 to ff18::ffff:ffff.

Examples

The following example shows how to configure an IP multicast address for CFS over IPv6.

```
switch# config t
switch(config)# cfs ipv6 mcast-address ff13::e244:4754
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?
Are you sure? (y/n) [n] y
```

The following example shows how to revert to the default IPv6 multicast address for CFS distribution over IPv6. The default IPv6 multicast address for CFS is ff13:7743:4653.

```
switch(config)# no cfs ipv6 ff13::e244:4754
Distribution over this IP type will be affected
```

```
Change multicast address for CFS-IP ?
Are you sure? (y/n) [n) y
```

Related Commands

Command	Description
cfs ipv6 distribute	Enables or disables Cisco Fabric Services (CFS) distribution over IPv6.
show cfs status	Displays whether CFS distribution is enabled or disabled.

channel mode active

To enable channel mode on a PortChannel interface, use the **channel mode active** command. To disable this feature, use the **no** form of the command.

channel mode active

no channel mode

Syntax Description

This command has no other arguments or keywords.

Defaults

Enabled.

Command Modes

Interface configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

This command determines the protocol behavior for all the member ports in the channel group associated with the port channel interface.

Examples

The following example shows how to disable channel mode on a PortChannel interface.

```
switch# config terminal
switch(config)# interface port-channel 10
switch(config-if)# no channel mode active
```

Related Commands

Command	Description
show interface port-channel	Displays PortChannel interface information.

channel-group

To add a port to a PortChannel group, use the **channel-group** command. To remove a port, use the **no** form of the command.

channel-group {*port-channel-number* **force | auto**}

no channel-group {*port-channel-number* **force | auto**}

Syntax Description

port-channel-number	Specifies the PortChannel number. The range is 1 to 256.
force	Specifies using the force option to add a port.
auto	Enables auto creation of a PortChannel.

Defaults

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable auto creation of a PortChannel.

```
switch# config terminal
switch(config)# interface fc3/9
switch(config-if)# channel-group auto
```

Related Commands

Command	Description
show interface port-channel	Displays PortChannel interface information.

cimserver

Use the **cimserver** command to configure the Common Information Models (CIM) parameters. Use the **no** form of this command to revert to factory defaults.

cimserver
{**certificate** {**bootflash:***filename* | **slot0:***filename* | **volatile:***filename*} |
clearcertificate *filename* |
enable |
enablehttp |
enablehttps}

no cimserver
{**certificate** {**bootflash:***filename* | **slot0:***filename* | **volatile:***filename*} |
clearcertificate *filename*
enable
enablehttp
enablehttps}

Syntax Description

certificate	Installs the Secure Socket Layer (SSL) certificate
bootflash:	Specifies the location for internal bootflash memory.
slot0:	Specifies the location for the CompactFlash memory or PCMCIA card.
volatile:	Specifies the location for the volatile file system.
filename	The name of the license file with a .pem extension.
clearcertificate	Clears a previously-installed SSL certificate.
enable	Enables and starts the CIM server.
enablehttp	Enables the HTTP (non-secure) protocol for the CIM server—(default).
enablehttps	Enables the HTTPS (secure) protocol for the CIM server.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

A CIM client is required to access the CIM server. The client can be any client that supports CIM.

Examples

The following example installs a Secure Socket Layer (SSL) certificate specified in the file named with a .pem extension.

```
switch# config terminal
switch(config)# cimserver certificateName bootflash:simserver.pem
```

The following example clears the specified SSL certificate.

```
switch(config)# cimserver clearCertificateName bootflash:simserver.pem
```

The following example enables HTTPS (secure protocol).

```
switch(config)# cimserver enablehttps
```

The following example disables HTTPS (default).

```
switch(config)# no cimserver enablehttps
```

The following example

```
switch(config)# cimserver enable
```

The following example disables the CIM server (default).

```
switch(config)# no cimserver enable
```

The following example enables HTTP and reverts to the switch default.

```
switch(config)# cimserver enablehttp
```

The following example disables HTTP and reverts to the switch default.

```
switch(config)# no cimserver enablehttp
```

Related Commands

Command	Description
show csimserver	Displays configured CIM settings and parameters.

class

To select a QoS policy map class for configuration, use the **class** command in QoS policy map configuration submode. To disable this feature, use the **no** form of the command.

class *class-map-name*

no class *class-map-name*

Syntax Description

class-map-name	Selects the QoS policy class map to configure.

Defaults

Disabled

Command Modes

QoS policy map configuration submode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Before you can configure a QoS policy map class you must complete the following:

- Enable the QoS data traffic feature using the **qos enable** command.
- Configure a QoS class map using the **qos class-map** command.
- Configure a QoS policy map using the **qos policy-map** command.

After you configure the QoS policy map class, you can configure the Differentiated Services Code Point (DSCP) and priority for frames matching this class map.

Examples

The following example shows how to select a QoS policy map class to configure.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# qos enable
switch(config)# qos class-map class-map1
switch(config)# qos policy-map policyMap1
switch(config-pmap)# class class-map1
switch(config-pmap-c)#
```

Related Commands

Command	Description
qos enable	Enables the QoS data traffic feature on the switch.
qos class-map	Configures a QoS class map.
qos policy-map	Configures a QoS policy map.
dscp	Configures the DSCP in the QoS policy map class.

Command	Description
priority	Configures the priority in the QoS policy map class.
show qos	Displays the current QoS settings.

clear accounting log

To clear the accounting log, use the **clear accounting log** command.

clear accounting log

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example clears the accounting log.

```
switch# clear accounting session
```

Related Commands

Command	Description
show accounting log	Displays the accounting log contents.

clear arp-cache

To clear the ARP cache table entries, use the **clear arp-cache** command in EXEC mode.

clear arp-cache

Syntax Description

This command has no arguments or keywords.

Defaults

The ARP table is empty by default.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Examples

The following example shows how to clear the arp-cache table entries.

```
switch# clear arp-cache
```

Related Commands

Command	Description
show arp	Displays Address Resolution Protocol (ARP) entries.

clear callhome session

To clear Call Home Cisco Fabric Services (CFS) session configuration and locks, use the **clear callhome session** command.

clear callhome session

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to clear the Call Home session configuration and locks.

```
switch# clear callhome session
```

Related Commands

Command	Description
show callhome	Displays Call Home information.

clear cdp

Use the **clear cdp** command to delete global or interface-specific CDP configurations.

clear cdp {**counters** | **table**} **[interface** {**gigabitethernet** *slot*/*port* | **mgmt 0**}**]**

Syntax Description

counters	Enables CDP on globally or on a per-interfaces basis.
table	Specifies the EXEC command to be executed.
interface	Displays CDP parameters for an interface.
gigabitethernet	Specifies the Gigabit Ethernet interface.
slot/*port*	Specifies the slot number and port number separated by a slash (/).
mgmt 0	Specifies the Ethernet management interface.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

You can issue this command for a specified interface or for all interfaces (management and Gigabit Ethernet interfaces)

Examples

The following example clears CDP traffic counters for all interfaces.

```
switch# clear cdp counters
switch#
```

The following example clears CDP entries for the specified Gigabit Ethernet interface.

```
switch# clear cdp table interface gigabitethernet 4/1
switch#
```

Related Commands

Command	Description
cdp	Configures global or interface-specific CDP settings and parameters.
show cdp	Displays configured CDP settings and parameters.

clear cores

To clear all core dumps for the switch, use the **clear cores** command in EXEC mode.

clear cores

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The system software keeps the last few cores per service and per slot and clears all other cores present on the active supervisor module.

Examples

The following example shows how to clear all core dumps for the switch.

```
switch# clear cores
```

Related Commands

Command	Description
show cores	Displays core dumps that have been made.

clear counters (EXEC mode)

To clear the interface counters, use the **clear counters** command in EXEC mode.

clear counters {all | interface {fc | mgmt | port-channel | sup-fc | vsan} *number***}**

Syntax Description

all	Clears all interface counters.
interface	Clears interface counters for the specified interface.
type	Specifies the interface type. See the Keywords table in the "Usage Guidelines" section.
number	Specifies the number of the slot or interface being cleared.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The following table lists the keywords and number ranges for the **clear counters** interface types:

Keyword	Interface Type	Number
fc	Fibre Channel	1- 2 or 1 - 9 (slot)
gigabitethernet	Gigabit Ethernet	1- 2 or 1 - 9 (slot)
mgmt	Management	0-0 (management interface)
port-channel	PortChannel	1-128 (PortChannel)
sup-fc	Inband	0-0 (Inband interface)
vsan	VSAN	1- 4093 (VSAN ID)

This command clears counter displayed in the **show interface** command output.

Examples

The following example shows how to clear counters for a VSAN interface.

```
switch# clear counters interface vsan 13
```

Related Commands

Command	Description
show interface	Displays interface information.

clear counters (SAN extension N port configuration mode)

To clear SAN extension tuner N port counters, use the **clear counters** command.

clear counters

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

SAN extension N port configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to clear SAN extension tuner N port counters.

```
switch# san-ext-tuner
switch(san-ext)# nWWN 10:00:00:00:00:00:00:00
switch(san-ext)# nport pwwn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2
switch(san-ext-nport)# clear counters
```

Related Commands

Command	Description
show san-ext-tuner	Displays SAN extension tuner information.

clear crypto ike domain ipsec sa

To clear the IKE tunnels for IPsec, use the **clear crypto ike domain ipsec sa** command.

clear crypto ike domain ipsec sa [*tunnel-id*]

Syntax Description

tunnel-id	Specifies a tunnel ID. The range is 1 to 2147483647.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

If the tunnel ID is not specified, all IKE tunnels are cleared.

Examples

The following example shows how to clear all IKE tunnels.

```
switch# clear crypto ike domain ipsec sa
```

Related Commands

Command	Description
crypto ike domain ipsec	Configures IKE information.
crypto ike enable	Enables the IKE protocol.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

clear crypto sa domain ipsec

To clear the security associations for IPsec, use the **clear crypto sa domain ipsec** command.

clear crypto sa domain ipsec interface gigabitethernet *slot/port* {**inbound** | **outbound**} **sa** *sa-index*

Syntax Description

interface gigabitethernet *slot/port*	Specifies the Gigabit Ethernet interface.
inbound	Specifies clearing inbound associations.
outbound	Specifies clearing output associations.
sa *sa-index*	Specifies the security association index. The range is 1 to 2147483647.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To clear security associations, IPsec must be enabled using the **crypto ipsec enable** command.

Examples

The following example shows how to clear a security association for an interface.

```
switch# clear crypto sa domain ipsec interface gigabitethernet 1/2 inbound sa 1
```

Related Commands

Command	Description
show crypto sad domain ipsec	Displays IPsec security association database information.

clear debug-logfile

To delete the debug logfile, use the **clear debug-logfile** command in EXEC mode.

clear debug-logfile *filename*

Syntax Description

filename	The name (restricted to 80 characters) of the log file to be cleared. The maximum size of the log file is 1024 bytes.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Examples

The following example shows how to clear the debug logfile.

```
switch# clear debug-logfile debuglog
```

Related Commands

Command	Description
show debug logfilw	Displays the logfile contents.

clear device-alias

To clear device alias information, use the **clear device-alias** command.

clear device-alias {**session** | **statistics**}

Syntax Description

session	Clears session information.
statistics	Clears device alias statistics.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to clear the device alias session.

```
switch# clear device-alias session
```

Related Commands

Command	Description
show device-alias	Displays device alias database information.

clear dpvm

To clear Dynamic Port VSAN Membership (DPVM) information, use the **clear dpvm** command.

clear dpvm {**auto-learn** [**pwwn** *pwwn-id*] | **session**}

Syntax Description

auto-learn	Clears automatically learned (autolearn) DPVM entries.
pwwn *pwwn-id*	Specifies the pWWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
session	Clears the DPVM session and locks.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, DVPM must be enabled using the **dpvm enable** command.

Examples

The following example shows how to clear a single autolearned entry.

```
switch# clear dpvm auto-learn pwwn 21:00:00:20:37:9c:48:e5
```

The following example shows how to clear all autolearn entries.

```
switch# clear dpvm auto-learn
```

The following example shows how to clear a session.

```
switch# clear dpvm session
```

Related Commands

Command	Description
dpvm enable	Enables DPVM.
show dpvm	Displays DPVM database information.

clear fabric-binding statistics

To clear fabric binding statistics in a FICON enabled VSAN, use the **clear fabric-binding statistics** command in EXEC mode.

clear fabric-binding statistics vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the FICON-enabled VSAN. The ID of the VSAN is from 1 to 4093.

Defaults

None

Command Modes

EXEC mode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example clears existing fabric binding statistics in VSAN 1.

```
switch# clear fabric-binding statistics vsan 1
```

Related Commands

Command	Description
show fabric-binding efmd statistics	Displays existing fabric binding statistics information.

clear fcanalyzer

To clear the entire list of configured hosts for remote capture, use the **clear fcanalyzer** command in EXEC mode.

clear fcanalyzer

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command clears only the list of configured hosts. Existing connections are not terminated.

Examples

The following example shows how to clear the entire list of configured hosts for remote capture.

```
switch# clear fcanalyzer
```

Related Commands

Command	Description
show fcanalyzer	Displays the list of hosts configured for a remote capture.

clear fcflow stats

To clear Fibre Channel flow statistics, use the **clear fcflow stats** command in EXEC mode.

clear fcflow stats [**aggregated**] **module** *module-number* **index** *flow-number*

Syntax Description

aggregated	Clears the Fibre Channel flow aggregated statistics.
module	Clears the statistics for a specified module.
module-number	Specifies the module number.
index	Clears the Fibre Channel flow counters for a specified flow index.
flow-number	Specifies the flow index number.

Defaults

None.

Command Modes

EXEC.

Command History

Release	Modification
1.0(2)	This command was introduced.

Examples

The following example shows how to clear aggregated Fibre Channel flow statistics for flow index 1 of module 2.

```
switch(config)# # clear fcflow stats aggregated module 2 index 1
```

Related Commands

Command	Description
show fcflow	Displays the fcflow statistics.

clear fcns statistics

To clear the name server statistics, use the **clear fcns statistics** command in EXEC mode.

clear fcns statistics vsan *vsan-id*

Syntax Description

vsan *vsan-id*	FCS statistics are to be cleared for a specified VSAN ranging from 1 to 4093.

Defaults

None.

Command Modes

EXEC.

Command History

Release	Modification
1.0(3)	This command was introduced.

Examples

The following example shows how to clear the name server statistics.

```
switch# show fcns statistics

Name server statistics for vsan 1
=================================
registration requests received = 0
deregistration requests received = 0
queries received = 23
queries sent = 27
reject responses sent = 23
RSCNs received = 0
RSCNs sent = 0

switch# clear fcns statistics vsan 1

switch# show fcns statistics

Name server statistics for vsan 1
=================================
registration requests received = 0
deregistration requests received = 0
queries received = 0
queries sent = 0
reject responses sent = 0
RSCNs received = 0
RSCNs sent = 0
switch#
```

Related Commands

Command	Description
show fcns statistics	Displays the name server statistics.

clear fcs statistics

To clear the fabric configuration server statistics, use the **clear fcs statistics** command in EXEC mode.

clear fcs statistics vsan *vsan-id*

Syntax Description

vsan *vsan-id*	FCS statistics are to be cleared for a specified VSAN ranging from 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Examples

The following example shows how to clear the fabric configuration server statistics for VSAN 10.

```
switch# clear fcs statistics vsan 10
```

Related Commands

Command	Description
show fcs statistics	Displays the fabric configuration server statistics information.

clear fctimer session

To clear fctimer Cisco Fabric Services (CFS) session configuration and locks, use the **clear fctimer session** command.

clear fctimer session

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to clear fctimer session.

```
switch# clear fctimer session
```

Related Commands

Command	Description
show fctimer	Displays fctimer information.

clear ficon

Use the **clear ficon** command in EXEC mode to clear the FICON information for the specified VSAN.

clear ficon vsan *vsan-id* [**allegiance** | **timestamp**]

Syntax Description

vsan *vsan-id*	Specifies the FICON-enabled VSAN. The ID of the VSAN is from 1 to 4093.
allegiance	Clears FICON device allegiance.
timestamp	Clears FICON VSAN specific timestamp.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The **clear ficon vsan** *vsan-id* **allegiance** command aborts the currently-executing session.

Examples

The following example clears the current device allegiance for VSAN 1.

```
switch# clear ficon vsan 1 allegiance
```

The following example clears the VSAN clock for VSAN 20.

```
switch# clear ficon vsan 20 timestamp
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.

clear fspf counters

To clear the Fabric Shortest Path First statistics, use the **clear fspf counters** command in EXEC mode.

clear fspf counters vsan *vsan-id* [**interface** *type*]

Syntax Description

vsan	Indicates that the counters are to be cleared for a VSAN.
vsan-id	The ID of the VSAN is from 1 to 4093.
interface *type*	(Optional). The counters are to be cleared for an interface. The interface types are fc for Fibre Channel, and port-channel for PortChannel.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

If the interface is not specified, then all of the counters of a VSAN are cleared. If the interface is specified, then the counters of the specific interface are cleared.

Examples

The following example clears the FSPF t statistics on VSAN 1.

```
switch# clear fspf counters vsan 1
```

The following example clears FSPF statistics specific to the Fibre Channel interface in VSAN 1, Slot 9 Port 32.

```
switch#  clear fspf counters vsan 1 interface fc 9/32
```

Related Commands

Command	Description
show fspf	Displays global FSPF information for a specific VSAN.

clear ip access-list counters

To clear IP access list counters, use the **clear ip access-list counters** command in EXEC mode.

clear ip access-list counters *list-name*

Syntax Description

list-name	Specifies the IP access list name (maximum 64 characters).

Defaults

None.

Command Modes

EXEC.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

The following example clears the counters for an IP access list.

```
switch# clear ip access-list counters adminlist
```

Related Commands

Command	Description
show ip access-list	Displays IP access list information.

clear ips arp

To clear ARP caches, use the **clear ips arp** command in EXEC mode.

clear ips arp {address *ip-address*| **interface gigabitethernet** *module-number*}

Syntax Description

address	Clears fcflow aggregated statistics.
ip-address	Enters the peer IP address.
interface gigabitethernet	Specifies the Gigabit Ethernet interface.
module-number	Specifies slot and port of the Gigabit Ethernet interface.

Defaults

None.

Command Modes

EXEC.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

The ARP cache can be cleared in two ways: clearing just one entry or clearing all entries in the ARP cache.

The following example clears one ARP cache entry:

```
switch# clear ips arp address 10.2.2.2 interface gigabitethernet 8/7
arp clear successful
```

The following example clears all ARP cache entries

```
switch# clear ips arp interface gigabitethernet 8/7
arp clear successful
```

clear ips stats

To clear IP storage statistics, use the **clear ips stats** command in EXEC mode.

clear ips stats {all [interface gigabitethernet *slot/port*] |
buffer interface gigabitethernet *slot/port* |
dma-bridge interface gigabitethernet *slot/port* |
icmp interface gigabitethernet *slot/port* |
ip interface gigabitethernet *slot/port* |
ipv6 traffic interface gigabitethernet *slot/port* |
mac interface gigabitethernet *slot/port* |
tcp interface gigabitethernet *slot/port*}

Syntax Description

all	Clears all IPS statistics.
interface gigabitethernet	Clears the Gigabit Ethernet interface.
slot/port	Specifies the slot and port numbers.
buffer	Clears IP storage buffer information.
dma-bridge	Clears direct memory access (DMA) statistics.
icmp	Clears ICMP statistics.
ip	Clears IP statistics.
ipv6	Clears IPv6 statistics.
mac	Clears Ethernet MAC statistics.
tcp	Clears TCP statistics.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Examples

The following example clears all IPS statistics on the specified interface.

```
switch# clear ips all interface gigabitethernet 8/7
switch#
```

clear ipv6 access-list

To clear IPv6 access control list statistics, use the **clear ipv6 access-list** command.

clear ipv6 access-list [*list-name*]

Syntax Description

access-list	Displays a summary of access control lists (ACLs).
list-name	Specifies the name of the ACL. The maximum size is 64.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(0)	This command was introduced.

Usage Guidelines

You can use the **clear ipv6 access-list** command to clear IPv6-ACL statistics.

Examples

The following example displays information about an IPv6-ACL.

```
switch# clear ipv6 access-list testlist
switch#
```

Related Commands

Command	Description
ipv6 access-list	Configures an IPv6-ACL.
show ipv6	Displays IPv6 configuration information.

clear ipv6 neighbors

To clear the IPv6 neighbor cache table, use the **clear ipv6 neighbors** command.

clear ipv6 neighbors

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(0)	This command was introduced.

Usage Guidelines

None.

Examples

The following example flushes the IPv6 neighbor cache table.

```
switch# clear ipv6 neighbors
switch#
```

Related Commands

Command	Description
ipv6 nd	Configures IPv6 neighbor discovery commands.
show ipv6 neighbors	Displays IPv6 neighbors configuration information.

clear islb session

To clear a pending iSLB configuration, use the **clear islb session** command.

clear islb session

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can use the **clear islb session** command to clear a pending iSLB configuration. This command can be executed from any switch by a user with admin privileges.

Examples

The following example clears a pending iSLB configuration.

```
switch# clear islb session
```

Related Commands

Command	Description
islb abort	Discards a pending iSLB configuration.
show islb cfs-session status	Displays iSLB session details.
show islb pending	Displays an iSLB pending configuration.
show islb pending-diff	Displays iSLB pending configuration differences.
show islb session	Displays iSLB session information.
show islb status	Displays iSLB CFS status.
show islb vrrp	Displays iSBL VRRP load balancing information.

clear ivr fcdomain database

To clear the IVR fcdomain database, use the **clear ivr fcdomain database** command in EXEC mode.

clear ivr fcdomain database

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.1(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example clears all IVR fcdomain database information.

```
switch# clear ivr fcdomain database
```

Related Commands

Command	Description
show ivr fcdomain database	Displays IVR fcdomain database entry information.

clear ivr service-group database

To clear an inter-VSAN routing (IVR) service group database, use the **clear ivr service-group database** command.

clear ivr service-group database

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example clears the ivr service-group database.

```
switch# clear ivr service-group database
```

Related Commands

Command	Description
show ivr service-group database	Displays an IVR service group database.

clear ivr zone database

To clear the Inter-VSAN Routing (IVR) zone database, use the **clear ivr zone database** command in EXEC mode.

clear ivr zone database

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC.

Command History

Release	Modification
1.3(1)	This command was introduced.

Examples

The following example clears all configured IVZ information.

```
switch# clear ivr zone database
```

clear license

To uninstall a license, use the **clear license** command in EXEC mode.

clear license *filename*

Syntax Description

filename	Specifies the license file to be uninstalled.

Defaults

None.

Command Modes

EXEC.

Command History

Release	Modification
1.3(2)	This command was introduced.

Examples

The following example clears a specific license.

```
switch# clear license Ficon.lic
Clearing license Ficon.lic:
SERVER this_host ANY
VENDOR cisco
# An example fcports license
INCREMENT SAN_EXTN_OVER_IP cisco 1.000 permanent 1 HOSTID=VDH=ABCD \
        NOTICE=<LicFileID>san_extn2.lic</LicFileID><LicLineID>1</LicLineID> \
        SIGN=67CB2A8CCAC2

Do you want to continue? (y/n) y
Clearing license ..done
switch#
```

Related Commands

Command	Description
show license	Displays license information.

clear line

To clear VTY sessions, use the **clear line** command in EXEC mode.

clear line *vty-name*

Syntax Description

vty-name	Specifies the VTY name (maximum 64 characters).

Defaults

None.

Command Modes

EXEC.

Command History

Release	Modification
1.2(1)	This command was introduced.

Examples

The following example clears one ARP cache entry:

```
switch# clear line Aux
arp clear successful
```

Related Commands

Command	Description
show line	Displays line information.

clear logging

To delete the syslog information, use the **clear logging** command in EXEC mode.

clear logging {**logfile** | **nvram** | **onboard** *information* [**module** *slot*] | **session**}

Syntax Description

logfile	Clears log file messages.
nvram	Clears NVRAM logs.
onboard *information*	Clears onboard failure logging (OBFL) information. The types of information include **boot-uptime**, **cpu-hog**, **device-version**, **endtime**, **environmental-history**, **error-stats**, **exception-log**, **interrupt-stats**, **mem-leak**, **miscellaneous-error**, **module**, **obfl-history**, **obfl-log**, **register-log**, **stack-trace**, **starttime**, **status**, and **system-health**.
module *slot*	Clears OBFL information for a specified module.
session	Clears a logging session.

Defaults

None.

Command Modes

EXEC.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the **onboard**, **module** and **session,** options.

Examples

The following example shows how to clear the debug log file.

```
switch# clear logging logfile
```

The following example shows how to clear the onboard system health log file.

```
switch# clear logging onboard system-health
!!!WARNING! This will clear the selected logging buffer!!
Do you want to continue? (y/n)  [n]
```

Related Commands

Command	Description
show logging	Displays logging information.

clear ntp

To clear Network Time Protocol (NTP) information, use the **clear ntp** command in EXEC mode.

clear ntp {**session** | **statistics** {**all-peers** | **io** | **local** | **memory**}}

Syntax Description

session	Clears NTP CFS session configuration and locks.
statistics	Clears NTP statistics.
all-peers	Clears I/O statistics for all peers.
io	Clears I/O statistics for I/O devices.
local	Clears I/O statistics for local devices.
memory	Clears I/O statistics for memory.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None mode.

Examples

The following example shows how to clear NTP statistics for all peers.

```
switch# clear ntp statistics all-peers
```

The following example shows how to clear NTP statistics for I/O devices.

```
switch# clear ntp statistics io
```

The following example shows how to clear NTP statistics for local devices.

```
switch# clear ntp statistics local
```

The following example shows how to clear NTP statistics for memory.

```
switch# clear ntp statistics memory
```

Related Commands

Command	Description
show ntp	Displays the configured server and peer associations.

clear port-security

To clear the port security information on the switch, use the **clear port-security** command in EXEC mode.

clear port-security {**database auto-learn** {**interface fc** *slot*/*port* | **port-channel** *port*} | **session** | **statistics**} **vsan** *vsan-id*

Syntax Description

database	Clears the port security active configuration database.
session	Clears the port security CFS configuration session and locks.
statistics	Clears the port security counters.
auto-learn	Clears the auto-learnt entries for a specified interface or VSAN.
interface fc *slot*/*port*	Clears entries for a specified interface.
port-channel *port*	Clears entries for a specified PortChannel. The range is 1 to 128.
vsan *vsan-id*	Clears entries for a specified VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.
2.0(1b)	Added the **session** option.

Usage Guidelines

The active database is read-only and **clear port-security database** command can be used when resolving conflicts.

Examples

The following example clears all existing statistics from the port security database for a specified VSAN.

```
switch# clear port-security statistics vsan 1
```

The following example clears learnt entries in the active database for a specified interface within a VSAN.

```
switch# clear port-security database auto-learn interface fc1/1 vsan 1
```

The following example clears learnt entries in the active database up to for the entire VSAN.

```
switch# clear port-security database auto-learn vsan 1
```

Related Commands

Command	Description
show port-security	Displays the configured port security information.

clear processes log

To clear the log files on the switch, use the **clear processes log** command in EXEC mode.

clear processes log {all | pid *pid-number*}

Syntax Description

all	Deletes all of the log files.
pid	Deletes the log files of a specific process.
pid-number	Specifies the process ID, which must be from 0 to 2147483647.

Defaults

None.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following examples show how to clear all of the log files on the switch.

```
switch# clear processes log all
```

Related Commands

Command	Description
show processes	Displays the detailed running or log information of processes or high availability applications.

clear qos statistics

To clear the quality of services statistics counters, use the **clear qos statistics** command in EXEC mode.

clear qos statistics

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following examples shows how to clear the quality of service counters.

```
switch# clear qos statistics
```

Related Commands

Command	Description
show qos statistics	Displays the current QoS settings, along with a number of frames marked high priority.

clear radius session

To clear RADIUS Cisco Fabric Services (CFS) session configuration and locks, use the **clear radius session** command.

clear radius session

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to clear RADIUS session.

```
switch# clear radius session
```

Related Commands

Command	Description
show radius	Displays RADIUS CFS distribution status and other details.

clear rlir

To clear the Registered Link Incident Report (RLIR), use the **clear rlir** command in EXEC mode.

clear rlir {**history** | **recent** {**interface fc** *slot*/*port* | **portnumber** *port-number*} | **statistics vsan** *vsan-id*}

Syntax Description

history	Clears RLIR link incident history.
recent	Clears recent link incidents.
interface fc *slot*/*port*	Clears entries for a specified interface.
portnumber *port-number*	Displays the port number for the link incidents.
statistics	Clears RLIR statistics.
vsan *vsan-id*	Specifies the VSNA ID for which the RLIR statistics are to be cleared.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example clears all existing statistics for a specified VSAN.

```
switch# clear rlir statistics vsan 1
```

The following example clears the link incident history.

```
switch# clear rlir history
```

The following example clears recent RLIR information for a specified interface.

```
switch# clear rlir recent interface fc 1/2
```

The following example clears recent RLIR information for a specified port number.

```
switch# clear rlir recent portnumber 16
```

Related Commands

Command	Description
show rscn	Displays RSCN information.

clear role session

To clear authentication role Cisco Fabric Services (CFS) session configuration and locks, use the **clear role session** command.

clear role session

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to clear authentication role CFS session.

```
switch# clear role session
```

Related Commands

Command	Description
show role	Displays role configuration information.

clear rscn session vsan

To clear a Registered State Change Notification (RSCN) session for a specified VSAN, use the **clear rscn session vsan** command.

clear rscn session vsan *vsan-id*

Syntax Description

vsan-id	Specifies a VSAN where the RSCN session should be cleared. The ID of the VSAN is from 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example clears an RSCN session on VSAN 1.

```
switch# clear rscn session vsan 1
```

Related Commands

Command	Description
rscn	Configures an RSCN.
show rscn	Displays RSCN information.

clear rscn statistics

To clear the registered state change notification statistics for a specified VSAN, use the **clear rscn statistics** command in EXEC mode.

clear rscn statistics vsan *vsan-id*

Syntax Description

vsan	The RSCN statistics are to be cleared for a VSAN.
vsan-id	The ID for the VSAN for which you want to clear RSCN statistics.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to clear rcsn statistics for VSAN 1.

```
switch# clear rscn statistics 1
```

Related Commands

Command	Description
show rscn	Displays RSCN information.

clear santap module

To clear SANTap information, use the **clear santap module** command.

clear santap module *slot-number* {**avt** *avt-pwwn* [**lun** *avt-lun*] |
itl *target-pwwn host-pwwn* |
session *session-id*}

Syntax Description

slot-number	Specifies the Storage Services Module (SSM) module number. The range is 1 through 13.
avt *avt-pwwn*	Removes the appliance virtual target (AVT) pWWN. The format is *hh:hh:hh:hh:hh:hh:hh:hh*.
lun *avt-lun*	Removes the appliance virtual target (AVT) LUN. The format is *0xhhhh*[*:hhhh*[*:hhhh*[*:hhhh*]]].
itl *target-pwwn host-pwwn*	Removes the SANTap Initiator Target LUN (ITL) triplet. The format of the *target-pwwn* and the *host-pwwn* is *hh:hh:hh:hh:hh:hh:hh:hh*.
session *session-id*	Removes a session. The range for session ID is 0 through 2147483647

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to remove a SANTap session.

```
switch# clear santap module 13 session 2020
```

Related Commands

Command	Description
santap module	Configures the mapping between the Storage Services Module (SSM) and the VSAN where the appliance is configured.
show santap module	Displays the configuration and statistics of the SANTap feature.

clear scheduler logfile

To clear the command scheduler logfile, use the **clear scheduler logfile** command.

clear scheduler logfile

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to clear the command scheduler logfile.

```
switch# clear scheduler logfile
```

Related Commands

Command	Description
show scheduler	Displays command scheduler information.

clear screen

To clear the terminal screen, use the **clear screen** command in EXEC mode.

clear screen

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to clear the terminal screen.

```
switch# clear screen
```

clear scsi-flow statistics

To clear the SCSI flow statistics counters, use the **clear scsi-flow statistics** command.

clear scsi-flow statistics flow-id *flow-id*

Syntax Description

flow-id *flow-id*	Configures the SCSI flow identification number.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to clear the SCSI flow statistics counters for SCSI flow ID 3.

```
switch# clear scsi-flow statistics flow-id 3
```

Related Commands

Command	Description
scsi-flow flow-id	Configures the SCSI flow services.
show scsi-flow	Displays SCSI flow configuration and status.

clear ssh hosts

To clear trusted SSH hosts, use the **clear ssh hosts** command in EXEC mode.

clear ssh hosts

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to clear reset-reason information from NVRAM and volatile storage.

```
switch# clear ssh hosts
```

Related Commands

Command	Description
show ssh hosts	Displays SSH host information.

clear system reset-reason

To clear the reset-reason information stored in NVRAM and volatile persistent storage, use the **clear system reset-reason** command in EXEC mode.

clear system reset-reason

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(2a)	This command was introduced.

Usage Guidelines

Use this command as listed below:

- In a Cisco MDS 9500 Series switch, this command clears the reset-reason information stored in NVRAM and volatile persistent storage in the active and standby supervisor modules.
- In a Cisco MDS 9200 Series switch, this command clears the reset-reason information stored in NVRAM and volatile persistent storage in the active supervisor module.

Examples

The following example shows how to clear trusted SSH hosts.

```
switch# clear system reset-reason
```

Related Commands

Command	Description
show system reset-reason	Displays system reset-reason information.

clear tacacs+ session

To clear TACACS+ Cisco Fabric Services (CFS) session configuration and locks, use the **clear tacacs+ session** command.

clear tacacs+ session

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, TACACS+ must be enabled using the **tacacs+ enable** command.

Examples

The following example shows how to clear the TACACS+ session.

```
switch# clear tacacs+ session
```

Related Commands

Command	Description
show tacacs+	Displays TACACS+ CFS distribution status and other details.
tacacs+ enable	Enables TACACS+.

clear tlport alpa-cache

To clear the entire contents of the alpa-cache, use the **clear tlport alpa-cache** command in EXEC mode.

clear tlport alpa-cache

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(5)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to clear a TL port ALPA cache.

```
switch# clear tlport alpa-cache
```

Related Commands

Command	Description
show tlport alpa-cache	Displays TL port alpa-cache information.

clear user

To clear trusted SSH hosts, use the **clear user** command in EXEC mode.

clear user *username*

Syntax Description

username	Specifies the user name to clear.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to log out a specified user.

```
switch# clear user vsam
```

Related Commands

Command	Description
show users	Displays user information.

clear vrrp

To clear all the software counters for the specified virtual router, use the **clear vrrp** command in EXEC mode.

clear vrrp {**statistics** [**ipv4** | **ipv6**] **vr** *number* **interface** {**gigabitethernet** *slot/port* | **mgmt 0** | **port-channel** *portchannel-id* | **vsan** *vsan-id*}}

Syntax Description

statistics	Clears global VRRP statistics.
ipv4	Clears IPv4 virtual router statistics.
ipv6	Clears IPv6 virtual router statistics.
vr *number*	Clears specific virtual router statistics and specifies a VR number from 1 to 255.
interface	Clears an interface.
gigabitethernet *slot/port*	Clears a specified Gigabit Ethernet interface.
mgmt 0	Specifies the management interface.
port-channel *port-channel-number*	Clears a specified PortChannel interface.The ID of the PortChannel interface is from 1 to 128.
vsan *vsan-id*	Clears a specified VSAN. The ID of the VSAN is from 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the **ipv4** and **ipv6** arguments.

Usage Guidelines

None.

Examples

The following example shows how to clear all the software counters for virtual router 7 on VSAN 2.

```
switch# clear vrrp vr 7 interface vsan2
```

Related Commands

Command	Description
show vrrp	Displays VRRP configuration information.
vrrp	Enables VRRP.

clear zone

To clear all configured information in the zone server for a specified VSAN, use the **clear zone** command in EXEC mode.

clear zone {database | lock | statistics {lun-zoning | read-only-zoning}} vsan *vsan-id*

Syntax Description

database	Clears zone server database information.
lock	Clears a zone server database lock.
statistics	Clears zone server statistics.
lun-zoning	Clears LUN-zoning related statistics.
read-only-zoning	Clears read-only zoning related statistics.
vsan	Clears zone information for a VSAN.
vsan-id	The ID of the VSAN is from 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the **lock** option.

Usage Guidelines

After issuing a **clear zone database** command, you need to explicitly issue the **copy running-config startup-config** to ensure that the running configuration is used when you next start the switch.

When you issue the **clear zone lock** command from a remote switch, only the lock on that remote switch is cleared. When you issue the **clear zone lock** command from the switch where the lock originated, all locks in the VSAN are cleared.

Note The recommended method to clear a session lock on a switch where the lock originated is by issuing the **no zone commit vsan** command.

Examples

The following examples shows how to clear all configured information in the zone server for VSAN 1.

```
switch# clear zone database vsan 1
```

Related Commands

Command	Description
show zone	Displays zone information for any configured interface.

cli alias name

To define a command alias name, use the **cli alias name** command in configuration submode. To remove the user-defined command alias, use the **no** form of the command.

cli alias name *command definition*

no cli alias name *command*

Syntax Description

command	Specifies an alias command name. The maximum size is 30 characters.
definition	Specifies the alias command definition. The maximum size is 80 characters.

Defaults

alias command.

Command Modes

Configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Follow these guidelines when defining a command alias:

- Command aliases are global for all user sessions.
- Command aliases persist across reboots.
- Commands being aliased must be typed in full without abbreviation.
- Command alias translation always takes precedence over any keyword in any configuration mode or submode.
- Command alias support is only available on the supervisor module, not the switching modules.
- Command alias configuration takes effect for other user sessions immediately.
- You cannot override the default command alias **alias,** which is an alias for **show cli alias**.
- Nesting of command aliases is permitted to a maximum depth of 1. One command alias can refer to another command alias that refers to a valid command, not to another command alias.
- A command alias always replaces the first command keyword on the command line.
- You can define command aliases in either EXEC mode or configuration submode.

Examples

The following example shows how to define command aliases in configuration submode.

```
switch# config t
switch(config)# cli alias name gigint interface gigabitethernet
switch(config)# cli alias name shintbr show interface brief
switch(config)# cli alias name shfcintup "shintbr| include up | include fc"
```

You can display the command aliases defined on the switch using the **alias** default command alias.

The following example shows how to display the command aliases defined on the switch.

```
switch# alias
CLI alias commands
==================
alias :show cli alias
gigint :interface gigabitethernet
shintbr :show interface brief
shfcintup :shintbr | include up | include fc
```

Related Commands

Command	Description
alias	Displays the default alias command for **show cli alias**.
show cli alias	Displays all configured aliases.

cli var name (EXEC)

To define a CLI session variable that persists only for the duration of a CLI session, use the **cli var name** command in either EXEC mode or configuration submode.

cli var name *name value*

To remove a user-defined session CLI variable, use the **no** form of the command as follows:

cli no var name *name*

Syntax Description

name	Specifies a variable name. The maximum size is 31 characters.
value	Specifies a variable value. The maximum size is 80.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

CLI session variables can be used as follows:

- Entered directly on the command line.
- Passed to the child script and initiated using the **run-script** command. The variables defined in the parent shell are available for use in the child **run-script** command process.
- Passed as command-line arguments to the **run-script** command.
- Referenced using the syntax $(variable).

CLI variables have the following limitation:

- You cannot reference a variable through another variable using nested references.

Examples

The following example creates a user-defined CLI variable for a session.

```
switch# cli var name testinterface 3/4
```

The following example removes a user-defined CLI variable for a session.

```
switch# cli no var name testinterface 3/4
```

Related Commands

Command	Description
cli no var name	Removes a user-defined session CLI variable.
show cli variables	Displays all CLI variables (persistent, session and system).

cli var name (configuration)

To define a CLI variable that persists across CLI sessions and switch reloads, use the **cli var name** command in configuration submode. To remove the user-defined persistent CLI variable, use the **no** form of the command.

cli var name *name value*

no cli var name *name*

Syntax Description

name	Specifies a variable name. The maximum size is 31 characters.
value	Specifies a variable value. The maximum size is 80.

Defaults

None.

Command Modes

Configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

CLI variables can be used as follows:

- Entered directly on the command line.
- Passed to the child script and initiated using the **run-script** command. The variables defined in the parent shell are available for use in the child **run-script** command process.
- Passed as command-line arguments to the **run-script** command.
- Referenced using the syntax $(variable).

CLI variables have the following limitations:

- You cannot reference a variable through another variable using nested references.

Examples

The following example creates a persistent user-defined CLI variable.

```
switch# config t
switch(config)# cli var name mgmtport mgmt 0
```

Related Commands

Command	Description
show cli variables	Displays all CLI variables (persistent, session and system).

clock

To configure the time zone and the summer time of day, use the **clock** command in configuration mode. To disable the daylight saving time adjustment, use the **no** form of the command.

clock {summer-time | time-zone *daylight-timezone-name start-week start-day start-month start-time end-week end-day end-month end-time daylight-offset-to-be-added-in-minutes***}**

no clock {summer-time | time-zone *daylight-timezone-name start-week start-day start-month start-time end-week end-day end-month end-time daylight-offset-to-be-added-in-minutes***}**

Syntax Description

summer-time	Adjusts the daylight savings time for the Pacific time zone by 60 minutes starting the first sunday in April at 2 a.m. and ending the last Sunday in October at 2 a.m.
time-zone	Sets the time zone for a specified time zone name.
daylight-timezone-name	The 8-character name of the time zone
start-week *end-week*	The week ranging from 1 through 5
start-day *end-day*	The day ranging from Sunday through Saturday
start-month *end-month*	The month ranging from January through December
start-time *end-time*	The time ranging from
daylight-offset-to-be-added-in-minutes	The daylight offset ranges from1 through 1440 minutes that will be added to the start time and deleted from the end time

Defaults

Coordinated Universal Time (UTC), which is the same as Greenwich Mean Time (GMT).

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use this command if you need to change the UTC or GMT time or time zone.

Examples

The following example shows how to configure the time zone and summer time of day.

```
switch# config terminal
switch(config)# clock timezone <daylight timezone name> <start week> <start day> <start
month> <start time> <end week> <end day> <end month> <end time> <daylight offset to be
added in minutes>
switch(config)# clock summer-time Pacific 1 Sun Apr 02:00 5 Sun Oct 02:00 60
switch(config)# no clock summer-time
switch(config)# exit
switch#
```

Related Commands

Command	Description
clock set	Changes the default time on the switch.
show clock	Displays the current date and time.
show run	Displays changes made to the time zone configuration along with other configuration information.

clock set

To change the system time on a Cisco MDS 9000 Family switch, use the **clock set** command in EXEC mode.

clock set *HH*:*MM*:*SS DD Month YYYY*

Syntax Description

HH	The two-digit time in hours in military format (15 for 3 p.m.).
MM	The two-digit time in minutes (58).
SS	The two-digit time in seconds(15).
DD	The two-digit date (12).
Month	The month in words (August).
YYYY	The four-digit year (2002).

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Generally, if the system is synchronized by a valid outside timing mechanism, such as an NTP clock source, or if you have a switch with calendar capability, you do not need to set the system clock. Use this command if no other time sources are available. The time specified in this command is relative to the configured time zone.

The **clock set** command changes are saved across system resets.

Examples

The following example displays the **clock set** command:

```
switch# clock set 15:58:15 12 August 2002
Mon Aug 12 15:58:00 PDT 2002
```

cloud discover

To initiate manual, on-demand cloud discovery, use the **cloud discover** command.

cloud discover [interface {gigabitethernet *slot/port* **| port-channel** *port-channel-number*}]

Syntax Description

interface	Specifies an interface for cloud discovery.
gigabitethernet *slot/port*	Specifies a Gigabit Ethernet interface.
port-channel *port-channel-number*	Specifies a PortChannel interface. The range for the PortChannel number is 1 to 256.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example initiates manual, on-demand cloud discovery.

```
switch# cloud discover
```

The following example initiates manual, on-demand cloud discovery on Gigabit Ethernet interface 2/2.

```
switch# cloud discover interface gigabitethernet 2/2
```

Related Commands

Command	Description
cloud discovery	Configures cloud discovery.
cloud-discovery enable	Enables discovery of cloud memberships.
show cloud discovery	Displays discovery information about the cloud.
show cloud membership	Displays information about members of the cloud.

cloud discovery

To configure cloud discovery, use the **cloud discovery** command in configuration mode. To remove the configuration, use the **no** form of the command.

cloud discovery {auto | fabric distribute | message icmp}

no cloud discovery {auto | fabric distribute | message icmp)

Syntax Description

auto	Enables auto fabric discovery.
fabric distribute	Enables cloud discovery fabric distribution.
message icmp	Configures Internet Control Message Protocol (ICMP) as the method for sending a discovery message.

Defaults

Auto.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The iSNS server distributes cloud and membership information across all of the switches using CFS. Therefore, the cloud view is the same on all of the switches in the fabric.

Note If auto discovery is disabled, interface changes result in new members becoming part of an undiscovered cloud. No new clouds are formed.

Examples

The following example enables auto cloud discovery.

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# cloud disovery auto
```

The following example enables auto cloud discovery fabric distribution.

```
switch(config)# cloud disovery fabric distribute
```

The following example disables auto cloud discovery fabric distribution.

```
switch(config)# no cloud disovery fabric distribute
```

Related Commands

Command	Description
cloud discover	Initiates manual, on-demand cloud discovery.
cloud-discovery enable	Enables discovery of cloud memberships.
show cloud discovery	Displays cloud discovery information.
show cloud membership	Displays information about members of the cloud.

cloud-discovery enable

To enable discovery of cloud memberships, use the **cloud-discovery** command in configuration mode. To disable discovery of cloud memberships, use the **no** form of the command.

cloud-discovery enable

no cloud-discovery enable

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example enables discovery of cloud memberships.

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# cloud-discovery enable
```

The following example disables discovery of cloud memberships.

```
switch(config)# no cloud-discovery enable
```

Related Commands

Command	Description
cloud discover	Initiates manual, on-demand cloud discovery.
cloud discovery	Configures cloud discovery.
show cloud	Displays cloud discovery and membership information.

code-page

Use the **code-page** command to configure the EBCDIC format. To disable the configuration or to revert to factory defaults, use the **no** form of the command.

code-page brazil |france | france | international-5 | italy | japan | spain-latinamerica | uk | us-canada

Syntax Description

code-page	Configures code page on a FICON-enabled VSAN
brazil	Configures the **brazil** EBCDIC format.
france	Configures the **france** EBCDIC format.
international-5	Configures the **international-5** EBCDIC format.
italy	Configures the **italy** EBCDIC format.
japan	Configures the **japan** EBCDIC format.
spain-latinamerica	Configures the **spain-latinamerica** *EBCDIC format.*
uk	Configures the **uk** EBCDIC format.
us-canada	Configures the **us-canada** EBCDIC format.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

This is an optional configuration. If you are not sure of the EBCDIC format to be used, we recommend retaining the **us-canada** (default) option.

Examples

The following example configures the **italy** EBCDIC format.

```
switch(config)# ficon vsan 2
switch(config-ficon)# code-page italy
```

The following example reverts to the factory default of using the **us-canada** EBCDIC format.

```
switch(config-ficon)# no code-page
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.
ficon vsan *vsan-id*	Enables FICON on the specified VSAN.

code-page

Use the **code-page** command to configure the EBCDIC format. To disable the configuration or to revert to factory defaults, use the **no** form of the command.

code-page {**brazil** | **france** | **france** | **international-5** | **italy** | **japan** | **spain-latinamerica** | **uk** | **us-canada**}

Syntax Description

brazil	Specifies **brazil** EBCDIC format.
france	Specifies **france** EBCDIC format.
international-5	Specifies **international-5** EBCDIC format.
italy	Specifies **italy** EBCDIC format.
japan	Specifies **japan** EBCDIC format.
spain-latinamerica	Specifies **spain-latinamerica** EBCDIC format.
uk	Specifies **uk** EBCDIC format.
us-canada	Specifies **us-canada** EBCDIC format.

Defaults

us-canada

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

This is an optional configuration. If you are not sure of the EBCDIC format to be used, we recommend retaining the **us-canada** (default) option.

Examples

The following example configures the **italy** EBCDIC format.

```
switch(config)# ficon vsan 2
switch(config-ficon)# code-page italy
```

The following example reverts to the factory default of using the **us-canada** EBCDIC format.

```
switch(config-ficon)# no code-page
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.
ficon vsan *vsan-id*	Enables FICON on the specified VSAN.

commit

To apply the pending configuration pertaining to the Call Home configuration session in progress, use the **commit** command in Call Home configuration submode.

commit

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

CFS distribution must be enabled before you can commit the Call Home configuration.

Examples

The following example shows how to commit the Call Home configuration commands.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# commit
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

contract-id

To configure the service contract ID of the customer with the Call Home function, use the **contract-id** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

contract-id *customer-id*

no contract-id *customer-id*

Syntax Description

contract-id	(Optional) Configures the service contract ID of the customer. Allows up to 64 characters for the contract number.

Defaults

None.

Command Modes

Call Home configuration submode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the contract ID in the Call Home configuration.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# contract-id Customer1234
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

configure terminal

To enter the configuration mode, use the **configure terminal** command in EXEC mode.

configure terminal

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example enters the configuration mode:

```
switch# configure terminal
switch(config)#
```

The following example enters the configuration mode using an abbreviated format of the command:

```
switch# config terminal
switch(config)#
```

copy

To save a backup of the system software, use the **copy** command in EXEC mode.

copy *source-URL destination-URL*

Syntax Description

source-URL	The location URL or alias of the source file or directory to be copied.
destination-URL	The destination URL or alias of the copied file or directory.

The following table lists the aliases for source and destination URLs.

running-config	Specifies the configuration currently running on the switch. The **system:running-config** keyword represents the current running configuration file.
startup-config	Specifies the configuration used during initialization (startup). You can copy the startup configuration from NVRAM. The **nvram:startup-config** keyword represents the configuration file used during initialization.
bootflash:	Specifies the location for internal bootflash memory.
log:	Specifies the location for the log file system.
slot0:	Specifies the location for the CompactFlash memory or PCMCIA card.
volatile:	Specifies the location for the volatile file system.
system:	Specifies the location for system memory, which includes the running configuration.
fabric	Specifies a fabric wide startup configuration update using Cisco Fabric Services (CFS) where all the remote switches in the fabric copy their running configuration (source) file into their startup configuration (destination) file. The syntax for this command is **copy running-config startup-config fabric**.
tftp:	Specifies the location for a Trivial File Transfer Protocol (TFTP) network server. The syntax for this alias is **tftp:**[[**//***location*]**/***directory*]**/***filename*.
ftp:	Specifies the location for a File Transfer Protocol (FTP) network server. The syntax for this alias is **ftp:**[[**//***location*]**/***directory*]**/***filename*.
scp:	Specifies the location for a secure copy (scp) network server. The syntax for this alias is **scp:**[[**//***location*]**/***directory*]**/***filename*.
sftp:	Specifies the location for a Secure Trivial File Transfer Protocol (SFTP) network server. The syntax for this alias is **sftp:**[[**//***location*]**/***directory*]**/***filename*.
log:	Specifies the location for log files stored in the same directory.
debug:	Specifies the location for the debug files stored in the debug partition
nvram:	Specifies the switch NVRAM.
core:	Specifies the location of the cores from any switching or supervisor module to an external flash (slot 0) or a TFTP server.
filename	The name of the Flash file.
sup-1 **sup-2**	The number of the supervisor module, where sup-1 is the slot 5 supervisor (active) and sup-2 is the slot 6 supervisor (standby).

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	Command modified.
2.1(1a)	Added the **fabric** keyword and functionality.

Usage Guidelines

This command makes the running and the backup copy of the software identical.

A file can only be copied from an active supervisor to a standby supervisor, not from standby to active.

This command does not allow 127.x.x.x IP addresses.

The copy function will not be completed if the required space is not available in the directory. First change to the required directory (for example, **cd bootflash:**) and verify the available space (for example, **dir bootflash:**).

The entire copying process may take several minutes.

Do not copy a file from an external source directly to the standby supervisor. You must copy from the external source to the active supervisor, and then copy the saved file to the standby supervisor.

You can save cores (from the active supervisor module, the standby supervisor module, or any switching module) to an external flash (slot 0) or to a TFTP server in one of two ways:

- On demand—to copy a single file based on the provided process ID.
- Periodically—to copy core files periodically as configured by the user.

You copy the logfile to a different location using the **copy log:messages** command.

The debug partition contains debugging files created by the software for troubleshooting purposes.

The **running-config startup-config fabric** parameters allow you to use CFS to force every switch in the Fibre Channel fabric to copy their running configuration (source) to their startup configuration (destination).

Note If any remote switch fails to complete the **copy running-config startup-config fabric** process, the initiator switch also does not complete saving its startup-configuration. This means, both the remote switch and the initiator switch have failed to save their startup-configuration (the old startup-configuration reverts back). All the other switches in the network would have succeeded.

Examples

The following example saves your configuration to the startup configuration.

```
switch# copy system:running-config nvram:startup-config
```

The following example copies the file called samplefile from the slot0 directory to the mystorage directory.

```
switch# copy slot0:samplefile slot0:mystorage/samplefile
```

The following example copies a file from the current directory level.

```
switch# copy samplefile mystorage/samplefile
```

If the current directory is slot0:mydir, this command copies slot0:mydir/samplefile to slot0:mydir/mystorage/samplefile.

The following example downloads a configuration file from an external CompactFlash to the running configuration.

```
switch copy slot0:dns-config.cfg system:running-config
```

The following example saves a running configuration file to an external CompactFlash.

```
switch# copy system:running-config slot0:dns-config.cfg
```

The following example saves a startup configuration file to an external CompactFlash.

```
switch# copy system:startup-config slot0:dns-config.cfg
```

The following example uses CFS to cause all switches in the fabric to copy their running configuration (source) file to their startup configuration (destination) file.

```
switch# copy running-config startup-config fabric
[########################################] 100%
switch#
```

Note If any remote switch fails to complete the **copy running-config startup-config fabric** process, the initiator switch also does not complete saving its startup-configuration. This means, both the remote switch and the initiator switch have failed to save their startup-configuration (the old startup-configuration reverts back). All the other switches in the network would have succeeded.

The following example creates a backup copy of the binary configuration.

```
switch# copy nvram:startup-config nvram:snapshot-config
```

The following example copies an image in bootflash on the active supervisor to the bootflash on the standby supervisor.

```
switch# copy bootflash:myimage bootflash://sup-2/myimage
```

The following example creates a running configuration copy in bootflash.

```
switch# copy system:running-config bootflash:my-config
```

The following examples creates a startup configuration copy in bootflash.

```
switch# copy nvram:startup-config bootflash:my-config
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
dir	Displays a list of files on a file system.
reload	Reloads the operating system.
show version	Displays the version of the running configuration file.

copy licenses

To save a backup of the installed license files, use the **copy licenses** command in EXEC mode.

copy licenses *source-URL destination-URL*

Syntax Description

source-URL	The location URL or alias of the source file or directory to be copied.
destination-URL	The destination URL or alias of the copied file or directory.

The following table lists the aliases for source and destination URLs.

bootflash:	Specifies the location for internal bootflash memory.
slot0:	Specifies the location for the CompactFlash memory or PCMCIA card.
volatile:	Specifies the location for the volatile file system.
filename	Specifies the name of the license file with a.tar extension.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

The copy function will not be completed if the required space is not available in the directory. First change to the required directory (for example, **cd bootflash:**) and verify the available space (for example, **dir bootflash:**).

We recommend backing-up your license files immediately after installing them and just before issuing a **write erase** command.

Examples

The following example saves a file called Enterprise.tar to the bootflash: directory.

```
switch# copy licenses bootflash:/Enterprise.tar
Backing up license done
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
dir	Displays a list of files on a file system.
install license	Installs a license file.

copy ssm-nvram standby-sup

To copy the contents of the Storage Services Module (SSM) NVRAM to the standby Supervisor 2 module when migrating from a Supervisor 1 to Supervisor 2 module, use the **copy ssm-nvram standby-sup** command in EXEC mode.

copy ssm-nvram standby-sup

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

This command should only be used for migrating from a Supervisor 1 to a Supervisor 2 module. When both modules in the switch are the same, you should not use this command; use the **copy** command instead.

Examples

The following example copies the contents of the SSM NVRAM to the standby Supervisor 2 module.

```
switch# copy ssm-nvram standby-sup
```

Related Commands

Command	Description
copy	Saves a backup of the system software.

crypto ca authenticate

To associate and authenticate a certificate of the certificate authority (CA) and configure its CA certificate (or certificate chain), use the **crypto ca authenticate** command in configuration mode. The CA certificate or certificate chain is assumed to already be available in Privacy Enhanced Mail (PEM) (base-64) encoded format.

crypto ca authenticate *trustpoint-label*

Syntax Description

trustpoint-label	Specifies the name of the trust point. The maximum size is 64 characters.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

This command authenticates the CA to the switch by obtaining the self-signed certificate of the CA that contains the public key of the CA. Because the CA signs its own certificate, you should manually authenticate the public key of the CA by contacting the CA administrator when you execute this command.

This command is required when you initially configure certificate authority support for the switch. Before you attempt CA authentication, first create the trust point using the **crypto ca trustpoint** command. The CA certificate fingerprint (the MD5 or SHA hash of the certificate) is generally published by the CA. When authenticating the CA, the certificate fingerprint is displayed. The administrator needs to compare it with the one published by the CA and accept the CA certificate only if it matches.

If the CA being authenticated is a subordinate CA (meaning that is is not self-signed), then it is certified by another CA which in turn my be certified by yet another CA and so on until there is a self-signed CA. In this case, the subordinate CA in question is said to have a CA certificate chain certifying it. The entire chain must be input during CA authentication. The maximum length that the CA certificate chain supports is ten.

The trust point CA is the certificate authority configured on the switch as the trusted CA. Any peer certificate obtained will be accepted if it is signed by a locally trusted CA or its subordinates.

Note The trust point configuration (created by the **crypto ca trustpoint** command) is persistent only if saved explicitly using the **copy running-config startup-config** command. The certificates and CRL associated to a trust point are automatically made persistent if the trust point in question was already saved in the startup configuration. Conversely, if the trust point was not saved in the startup configuration, the certificates and CRL associated to it are not made persistent automatically because they do not exist without the corresponding trust point after the switch reboots.

To ensure the that the configured certificates, CRLs and key pairs are made persistent, always save the running configuration to the startup configuration

Examples

The following example authenticates a CA certificate called admin-ca.

```
switch# config terminal
switch(config)# crypto ca authenticate myCA
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO
MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD
QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Vs6mXp1//w==
-----END CERTIFICATE-----
 END OF INPUT
Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12


Do you accept this certificate? [yes/no]:y
```

Related Commands

Command	Description
crypto ca trustpoint	Configures the trust point.
show crypto ca certificates	Displays configured trust point certificates.
show crypto ca trustpoints	Displays trust point configurations.

crypto ca crl request

To configure a new certificate revocation list (CRL) downloaded from the certificate authority (CA), use the **crypto ca crl request** command in configuration mode.

crypto ca crl request *trustpoint-label source-file*

Syntax Description

trustpoint-label	Specifies the name of the trust point. The maximum size is 64 characters.
source-file	Specifies the location of the CRL in the form **bootflash**:*filename*. The maximum size is 512.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Cisco MDS SAN-OS allows you to pre-download CRLs for the trust points and cache the CRLs in the cert store using the **crypto ca crl request** command. During the verification of a peer certificate by IPsec/IKE or SSH, the issuer CA's CRL will be consulted only if it had already been configured locally, and revocation checking is configured to use CRL. Otherwise, CRL checking is not done and a certificate is considered to be not revoked if no other revocation checking methods are configured. This mode of CRL checking is called CRL optional.

The other modes of revocation checking are called CRL best-effort and CRL mandatory. In these modes, if the CRL is not found locally, there is an attempt to fetch it automatically from the CA. These modes are not supported in MDS SAN-OS release 3.0(1).

The CRL file specified should contain the latest CRL in either Privacy Enhanced Mail (PEM) format or Distinguished Encoding Rules (DER) format.

Note The trust point configuration (created by the **crypto ca trustpoint** command) is persistent only if saved explicitly using the **copy running-config startup-config** command. The certificates and CRL associated to a trust point are automatically made persistent if the trust point in question was already saved in the startup configuration. Conversely, if the trust point was not saved in the startup configuration, the certificates and CRL associated to it are not made persistent automatically because they do not exist without the corresponding trust point after the switch reboots.

To ensure the that the configured certificates, CRLs and key pairs are made persistent, always save the running configuration to the startup configuration.

Examples

The following example configures a CRL for the trust point or replaces the current CRL.

```
switch# config t
switch(config)# crypto ca crl request admin-ca bootflash:admin-ca.crl
```

Related Commands

Command	Description
revocation-check	Configures trust point revocation check methods.
show crypto ca crl	Displays configured certificate revocation lists (CRL).

crypto ca enroll

To request a certificate for the switch's RSA key pair created for this trust point CA, use the **crypto ca enroll** command in configuration mode.

crypto ca enroll *trustpoint-label*

Syntax Description

trustpoint-label	Specifies the name of the trust point. The maximum size is 64 characters.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

An MDS switch can enroll with the trust point CA to get an identity in the form of a certificate. You can enroll your switch with multiple trust points, thereby getting a separate identity certificate from each.

When enrolling with a trust point, you must specify an RSA key pair to be certified. This key pair must be generated and associated to the trust point before generating the enrollment request. The association between the trust point, key pair, and identity certificate is valid until it is explicitly removed by deleting the identity certificate first, followed by disassociating the key pair, and deleting the CA certificates (in any order), and finally deleting the trust point itself, in that order only.

Use the **crypto ca enroll** command to generate a request to obtain an identity certificate from each of your trust points corresponding to authenticated CAs. The certificate signing request (CSR) generated is per Public-Key Cryptography Standards (PKCS) #10 standard, and is displayed in PEM format. Cut and paste it and submit it to the corresponding CA through e-mail or the CA website. The CA administrator issues the certificate and makes it available to you either through the website or by sending it in e-mail. You need to import the obtained identity certificate to the corresponding trust point using the **crypto ca import** *trustpoint-label* **certificate** command.

The challenge password is not saved with the configuration. This password is required in the event that your certificate needs to be revoked, so you must remember this password.

Examples

The following example generates a certificate request for an authenticated CA.

```
switch# config t
switch(config)# crypto ca enroll myCA
 Create the certificate request ..
 Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.
  Password:nbv123
```

```
 The subject name in the certificate will be: Vegas-1.cisco.com
 Include the switch serial number in the subject name? [yes/no]:no
 Include an IP address in the subject name [yes/no]:yes
ip address:172.22.31.162
 The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ
DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ
KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----
```

Related Commands

Command	Description
crypto ca import *trustpoint-label* **certificate**	Imports the identity certificate obtained fromthe CA to the trust point.
crypto key generate rsa	Generates an RSA key pair.
rsakeypair	Configures and associates the RSA key pair details to a trust point.
show crypto key mypubkey rsa	Displays all RSA public key configurations.

crypto ca export

To export the RSA key pair and the associated certificates (identity and CA) of a trust point within a Public-Key Cryptography Standards (PKCS) #12 format file to a specified location, use the **crypto ca export** command in configuration mode.

crypto ca export *trustpoint-label* **pkcs12** *destination-file-url pkcs12-password*

Syntax Description

trustpoint-label	Specifies the name of the trust point. The maximum size is 64 characters.
pkcs12 *destination-file-url*	Specifies a destination file in **bootflash**:*filename* format. The maximum size is 512 characters.
pkcs12-password	Specifies the password to be used to protect the RSA private key inthe exported file. The maximum size is 64 characters.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can export the identity certificate along with the associated RSA key pair and CA certificate (or certificate chain) to a PKCS #12 format file for backup purposes. You can later import the certificate and RSA key pair to recover from a system crash on your switch.

Examples

The following example shows how to export a certificate and key pair in PKCS #12 format.

```
switch# config terminal
switch(config)# crypto ca export admin-ca pkcs12 bootflash:adminid.p12 nbv123
```

Related Commands

Command	Description
crypto ca import *trustpoint-label* **certificate**	Imports the identity certificate obtained from the CA to the trust point.
crypto ca import *trustpoint-label* **pkcs12**	Imports the identity certificate and associated RSA key pair and CA certificate (chain) to a trust point.
crypto key generate rsa	Generates an RSA key pair.

Command	Description
rsakeypair	Configures and associates the RSA key pair details to a trust point.
show crypto key mypubkey rsa	Displays any RSA public key configurations.

crypto ca import

To import the identity certificate alone in PEM format or the identity certificate and associated RSA key pair and CA certificate (or certificate chain) in Public-Key Cryptography Standards (PKCS) #12 form, use the **crypto ca import** command in configuration mode.

crypto ca import *trustpoint-label* {**certificate** | **pkcs12** *source-file-url pkcs12-password*}

Syntax Description

trustpoint-label	Specifies the name of the trust point. The maximum size is 64 characters.
pkcs12 *source-file-url*	Specifies a source file in **bootflash**:*filename* format. The maximum size is 512 characters.
pkcs12-password	Specifies the password that was used to protect the RSA private key in the imported PKCS#12 file. The maximum size is 64 characters.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The first form of the command, **crypto ca import** *trustpoint-label* **certificate,** is used to import (by cut and paste means) the identity certificate obtained from the CA, corresponding to the enrollment request generated earlier in the trust point and submitted to the CA. The administrator is prompted to cut and paste the certificate.

The second form of the command, **crypto ca import** *trustpoint-label* **pkcs12** *source-file-url pkcs12-password*, is used to import the complete identity information (that is, the identity certficate and associated RSA key pair and CA certificate or certficate chain) into an empty trust point. This command is useful for restoring the configuration after a system goes down.

Note The trust point configuration (created by the **crypto ca trustpoint** command) is persistent only if saved explicitly using the **copy running-config startup-config** command. The certificates and CRL associated to a trust point are automatically made persistent if the trust point in question was already saved in the startup configuration. Conversely, if the trust point was not saved in the startup configuration, the certificates and CRL associated to it are not made persistent automatically because they do not exist without the corresponding trust point after the switch reboots.

To ensure the that the configured certificates, CRLs and key pairs are made persistent, always save the running configuration to the startup configuration

Examples

The following example installs an identity certificate obtained from a CA corresponding to an enrollment request made and submitted earlier.

```
switch# config t
switch(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD
VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz
Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w
NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu
Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE
BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh
cm5hIENBghAFYNKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6
Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRFbnJvbGwvc3Nl
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4
XENlcnRFbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw
E36cIZu4WsExREqxbTk8ycx7V5o=
-----END CERTIFICATE-----
```

The following example shows how to import a certificate and key pair in a Public-Key Cryptography Standards (PKCS) #12 format file.

```
switch# config t
witch(config)# crypto ca import admin-ca pkcs12 bootflash:adminid.p12 nbv123
```

Related Commands

Command	Description
crypto ca export *trustpoint-label* **pkcs12**	Exports the RSA key pair and associated certificates of a trust point.
crypto ca enroll	Generates a certificate signing request for a trust point.
crypto key generate rsa	Generates the RSA key pair.
rsakeypair	Configures trust point RSA key pair details.
show crypto ca certificates	Displays the identity and CA certificate details.
show crypto key mypubkey rsa	Displays any RSA public key configurations.

crypto ca test verify

To verify a certificate file, use the **crypto ca test verify** command in configuration mode.

crypto ca test verify *certificate-file*

Syntax Description

certificate-file	Specifies the certificate filename in the form **bootflash**:*filename*. The maximum size is 512 characters.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The **crypto ca test verify** command is only a test command. It verifies the specified certificate in PEM format by using the trusted CAs configured and by consulting the CRL or OCSP if needed, as per the revocation checking configuration.

Examples

The following example shows how to verify a certificate file. Verify status code 0 means the verification is successful.

```
switch(config)# crypto ca test verify bootflash:id1.pem
verify status oode:0
verify error msg:
```

Related Commands

Command	Description
show crypto ca certificates	Displays configured trust point certificates.

crypto ca trustpoint

To create a trust point certificate authority (CA) that the switch should trust, and enter trust point configuration submode (config-trustpoint), use the **crypto ca trustpoint** command in configuration mode. To remove the trust point, use the **no** form of the command.

crypto ca trustpoint *trustpoint-label*

no crypto ca trustpoint *trustpoint-label*

Syntax Description

trustpoint-label	Specifies the name of the trust point. The maximum size is 64 characters.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Trust points have the following characteristics:

- A trust point corresponds to a single CA, which an MDS switch trusts for peer certificate verification for any application.
- A CA must be explicitly associated to a trust point using the CA authentication process using the **crypto ca authenticate** command.
- An MDS switch can have many trust points and all applications on the switch can trust a peer certificate issued by any of the trust point CAs.
- A trust point is not restricted to a specific application.
- The MDS switch can optionally enroll with a trust point CA to get an indemnity certificate for itself.

You do not need to designate one or more trust points to an application. Any application should be able to use any certificate issued by any trust point as long as the certificate purpose satisfies application requirement.

You do not need more than one identity certificate from a trust point or more than one key pair to be associated to a trust point. A CA certifies a given identity (name) only once and does not issue multiple certificates with the same subject name. If you need more than one identity certificate for a CA, define another trust point for the same CA, associate another key pair to it, and have it certified, provided CA allows multiple certificates with same subject name.

Note Before using the **no crypto ca trustpoint** command to remove the trust point, first delete the identity certificate and CA certificate (or certificate chain) and then disassociated the RSA key pair from the trust point. The switch enforces this behavior to prevent the accidental removal of the trust point along with the certificates.

Examples

The following example declares a trust point CA that the switch should trust and enters trust point configuration submode.

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)#
```

The following example removes the trust point CA.

```
switch# config terminal
switch(config)# no crypto ca trustpoint admin-ca
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the certificate of the certificate authority.
crypto ca enroll	Generates a certificate signing request for a trust point.
show crypto ca certificates	Displays the identity and CA certificate details.
show crypto ca trustpoints	Displays trust point configurations.

crypto global domain ipsec security-association lifetime

To configure global parameters for IPsec, use the **crypto global domain ipsec security-association lifetime** command. To revert to the default, use the **no** form of the command.

crypto global domain ipsec security-association lifetime {**gigabytes** *number* | **kilobytes** *number* | **megabytes** *number* | **seconds** *number*}

no crypto global domain ipsec security-association lifetime {**gigabytes** | **kilobytes** | **megabytes** | **seconds**}

Syntax Description

gigabytes *number*	Specifies a volume-based key duration in gigabytes. The range is 1 to 4095.
kilobytes *number*	Specifies a volume-based key duration in kilobytes. The range is 2560 to 2147483647.
megabytes *number*	Specifies a volume-based key duration in megabytes. The range is 3 to 4193280.
seconds *number*	Specifies a time-based key duration in seconds. The range is 120 to 86400.

Defaults

450 gigabytes and 3600 seconds

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, IPsec must be enabled using the **crypto ipsec enable** command.

The global security association lifetime value can be overridden for individual IPsec crypto maps using the **set** command in IPsec crypto map configuration submode.

Examples

The following example shows how to configure the system default before the IPsec.

```
switch# config terminal
switch(config)# crypto global domain ipsec security-association lifetime gigabytes 500
```

Related Commands

Command	Description
crypto ipsec enable	Enables IPsec.
set (IPsec crypto map configuration submode)	Configures IPsec crypto map entry parameters.
show crypto global domain ipsec	Displays the global attributes for IPsec.

crypto ike domain ipsec

To enter IKE configuration submode, use the **crypto ike domain ipsec** command.

crypto ike domain ipsec

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To configure IKE protocol attributes, IKE must be enabled using the **crypto ike enable** command.

Examples

The following example shows how enter IKE configuration mode.

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)#
```

Related Commands

Command	Description
crypto ike enable	Enables the IKE protocol.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

crypto ike domain ipsec rekey sa

To rekey an IKE crypto security association (SA) in the IPsec domain, use the **crypto ike domain ipsec rekey sa** command.

crypto ike domain ipsec rekey sa *sa-index*

Syntax Description

sa-index	Specifies the SA index. The range is 1 to 2147483647.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, IKE must be enabled using the **crypto ike enable** command.

Examples

The following example rekeys an IKE crypto SA.

```
switch# crypto ike domain ipsec rekey sa 100
```

Related Commands

Command	Description
crypto ike enable	Enables the IKE protocol.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

crypto ike enable

To enable IKE, use the **crypto ike enable** command. To disable IKE, use the **no** form of the command.

crypto ike enable

no crypto ike enable

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

The IKE protocol cannot be disabled unless IPsec is disabled.

The configuration and verification commands for the IKE protocol are only available when the IKE protocol is enabled on the switch. When you disable this feature, all related configurations are automatically discarded.

Examples

The following example shows how to enable the IKE protocol.

```
switch# config terminal
switch(config)# crypto ike enable
```

Related Commands

Command	Description
clear crypto ike domain ipsec sa	Clears IKE protocol information clear IKE SAs.
crypto ipsec enable	Enables IPsec.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

crypto ipsec enable

To enable IPsec, use the **crypto ipsec enable** command. To disable IPsec, use the **no** form of the command.

crypto ipsec enable

no crypto ipsec enable

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To enable the IPsec, the IKE protocol must be enabled using the **crypto ike enable** command.

The configuration and verification commands for IPsec are only available when IPsec is enabled on the switch. When you disable this feature, all related configurations are automatically discarded.

Examples

The following example shows how to enable IPsec.

```
switch# config terminal
switch(config)# crypto ipsec enable
```

Related Commands

Command	Description
show crypto global domain ipsec	Displays IPsec crypto global information.
show crypto map domain ipsec	Displays IPsec crypto map information.
show crypto transform-set domain ipsec	Displays IPsec crypto transform set information.

crypto key generate rsa

To generate an RSA key pair, use the **crypto key generate rsa** command in configuration mode.

crypto key generate rsa [label *key-pair-label*] **[exportable] [modulus** *key-pair-size*]

Syntax Description

label *key-pair-label*	Specifies the name of the key pair. The maximum size is 64 characters.
exportable	Configures the key pair to be exportable.
modulus *key-pair-size*	Specifies the size of the key pair. The size ranges from 512 to 2048.

Defaults

By default, the **key** is not exportable.
The default **label** is switch FQDN.
The default **modulus** is 512.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can generate one or more RSA key pairs and associate each RSA key pair with a distinct trust point CA, where the MDS switch enrolls to obtain identity certificates. The MDS switch needs only one identity per CA, which consists of one key pair and one identity certificate.

Cisco MDS SAN-OS allows you to generate RSA key pairs with a configurable key size (or modulus). The default key size is 512. Valid modulus values are 512, 768, 1024, 1536, and 2048.

You can also configure an RSA key pair label. The default key pair label is FQDN.

Examples

The following example shows how to configure an RSA key pair called newkeypair.

```
switch# config terminal
switch(config)# crypto key generate rsa label newkeypair
```

The following example shows how to configure an RSA key pair called testkey, of size 768, that is exportable.

```
switch# config terminal
switch(config)# crypto key generate rsa label testkey exportable modulus 768
```

The following example shows how to generate an exportable RSA key with the switch name as the default label and 512 as the default modulus.

```
switch# config terminal
switch(config)# crypto key generate rsa exportable
```

Related Commands

Command	Description
crypto key zeroize rsa	Deletes RSA key pair configurations.
rsakeypair	Configures trust point RSA key pair details.
show crypto key mypubkey rsa	Displays information about configured RSA key pairs.

crypto key zeroize rsa

To delete an RSA key pair from the switch, use the **crypto key zeroize rsa** command in configuration mode.

crypto key zeroize rsa *key-pair-label*

Syntax Description

key-pair-label	Specifies the RSA key pair to delete. The maximum size is 64 characters.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

If you believe the RSA key pair on your switch was compromised in some way and should no longer be used, you should delete it.

After you delete the RSA key pair on the switch, ask the CA administrator to revoke your switch's certificates at the CA. You must supply the challenge password you created when you originally requested the switch's certificates.

Before deleting a key pair, you should delete the identity certificates corresponding to it in various trust points if the identity certificates exist, and then disassociate the key pair from those trust points. The purpose of this is to prevent accidental deletion of a key pair for which there exists an identity certificate in a trust point.

Note The trust point configuration, certificates, and key pair configurations are made persistent only after saving to the startup configuration. To be consistent with this configuration behavior, the delete behavior is also the same. That is, the deletions are made persistent only after saving to the startup configuration.

Use the **copy running-config startup-config** command to make the certificate and key pair deletions persistent.

Examples

The following example shows how to delete an RSA key pair called testkey.

```
switch# config terminal
switch(config)# crypto key zeroize rsa testkey
```

Related Commands

Command	Description
crypto key generate rsa	Configures an RSA key pair.
rsakeypair	Configures trust point RSA key pair details.
show crypto key mypubkey rsa	Displays information about configured RSA key pairs.

crypto map domain ipsec (configuration mode)

To specify an IPsec crypto map and enter IPsec crypto map configuration mode, use the **crypto map domain ipsec** command. To delete an IPsec crypto map or a specific entry in an IPsec crypto map, use the **no** form of the command.

crypto map domain ipsec *map-name seq-number*

no crypto map domain ipsec *map-name* [*seq-number*]

Syntax Description

map-name	Specifies the map name. Maximum length is 63 characters.
seq-number	Specifies the sequence number for the map entry. The range is 1 to 65535.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, IPsec must be enabled using the **crypto ipsec enable** command.

The sequence number determines the order in which IPsec crypto map entries are applied.

Examples

The following example specifies entry 1 for IPsec crypto map IPsecMap and enters IPsec crypto map configuration mode.

```
switch# config terminal
switch(config)# crypto map domain ipsec IPsecMap 1
switch(config-crypto-map-ip)#
```

The following example deletes an IPsec crypto map entry.

```
switch# config terminal
switch(config)# no crypto map domain ipsec IPsecMap 1
```

The following example deletes the entire IPsec crypto map.

```
switch# config terminal
switch(config)# no crypto map domain ipsec IPsecMap
```

Related Commands

Command	Description
crypto ipsec enable	Enables IPsec.
crypto transform-set domain ipsec	Configures the transform set for an IPsec crypto map.
set (IPsec crypto map configuration submode)	Configures IPsec crypto map entry parameters.
show crypto map domain ipsec	Displays IPsec crypto map information.

crypto map domain ipsec (interface configuration submode)

To configure an IPsec crypto map on a Gigabit Ethernet interface, use the **crypto map domain ipsec** command in interface configuration submode. To remove the IPsec crypto map, use the **no** form of the command.

crypto map domain ipsec *map-name*

no crypto map domain ipsec

Syntax Description

map-name	Specifies the map name. Maximum length is 63 characters.

Defaults

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, IPsec must be enabled using the **crypto ipsec enable** command.

The sequence number determines the order in which crypto maps are applied.

Examples

The following example shows how to specify an IPsec crypto map for a Gigabit Ethernet interface.

```
switch# config terminal
switch(config)# interface gigabitethernet 1/2
switch(config-if)# crypto map domain ipsec IPsecMap
```

Related Commands

Command	Description
crypto ipsec enable	Enables IPsec.
show crypto map domain ipsec	Displays IPsec crypto map information.
show interface	Displays interface information.

crypto transform-set domain ipsec

To create and configure IPsec transform sets, use the **crypto transform-set domain ipsec** command. To delete an IPsec transform set, use the **no** form of the command.

crypto transform-set domain ipsec *set-name* {**esp-3des** | **esp-des**} [**esp-aes-xcbc-mac** | **esp-md5-hmac** | **esp-sha1-hmac**]

crypto transform-set domain ipsec *set-name* **esp-aes** {**128** | **256**} [**ctr** {**esp-aes-xcbc-mac** | **esp-md5-hmac** | **esp-sha1-hmac**} | **esp-aes-xcbc-mac** | **esp-md5-hmac** | **esp-sha1-hmac**]

crypto transform-set domain ipsec *set-name* **[**{**esp-3des** | **esp-des**} [**esp-aes-xcbc-mac** | **esp-md5-hmac** | **esp-sha1-hmac**]]

crypto transform-set domain ipsec *set-name* **esp-aes [**{**128** | **256**} [**ctr** {**esp-aes-xcbc-mac** | **esp-md5-hmac** | **esp-sha1-hmac**} | **esp-aes-xcbc-mac** | **esp-md5-hmac** | **esp-sha1-hmac**]]

Syntax Description

set-name	Specifies the transform set name. Maximum length is 63 characters.
esp-3des	Specifies ESP transform using the 3DES cipher (128 bits).
esp-des	Specifies ESP transform using the DES cipher (56 bits).
esp-aes-xcbc-mac	Specifies ESP transform using AES-XCBC-MAC authentication.
esp-md5-hmac	Specifies ESP transform using MD5-HMAC authentication.
esp-sha1-hmac	Specifies ESP transform using SHA1-HMAC authentication
esp-aes	Specifies ESP transform using the AES cipher (128 or 256 bits).
128	Specifies ESP transform using AES 128-bit cipher.
256	Specifies ESP transform using AES 256-bit cipher.
ctr	Specifies AES in counter mode.

Defaults

None.

The default mode of AES is CBC (Cyber Block Chaining).

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, IPsec must be enabled using the **crypto ipsec enable** command.

You can use this command to modify existing IPsec transform sets. If you change a transform set definition, the change is only applied to crypto map entries that reference the transform set. The change is not applied to existing security associations, but used in subsequent negotiations to establish new security associations. If you want the new settings to take effect sooner, you can clear all or part of the security association database using the **clear crypto sa domain ipsec** command.

Examples

The following example shows how to configure an IPsec transform set.

```
switch# config terminal
switch(config)# crypto transform-set domain ipsec Set1 esp-aes 128
```

Related Commands

Command	Description
clear crypto sa domain ipsec	Clears security associations.
crypto ipsec enable	Enables IPsec.
show crypto transform-set domain ipsec	Displays IPsec crypto transform set information.

customer-id

To configure the customer ID with the Call Home function, use the **customer-id** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

customer-id *customer-id*

no customer *customer-id*

Syntax Description

customer-id	(Optional) Specifies the customer ID. The maximum length is 64 alphanumeric characters in free format.

Defaults

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the customer ID in the Call Home configuration submode.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# customer-id Customer1234
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

CHAPTER 5

D Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "Command Modes" section to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

data-pattern-file

To configure data pattern file for a SAN tuner extension N port, use the **data-pattern-file** command in interface configuration submode. To remove data pattern file, use the **no** form of the command.

data-pattern-file *filename*

no data-pattern-file

Syntax Description

filename	Specifies the data pattern file name.

Defaults

All zero pattern.

Command Modes

SAN extension N port configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

By default, an all-zero pattern is used as the pattern for data generated by the virtual N ports. You can optionally specify a file as the data pattern to be generated by selecting a data pattern file from one of three locations: the bootflash: directory, the volatile: directory, or the slot0: directory. This option is especially useful when testing compression over FCIP links. You can also use Canterbury corpus or artificial corpus files for benchmarking purposes.

Examples

The following example configures the data pattern file for an N port.

```
switch# san-ext-tuner
switch(san-ext)# nWWN 10:00:00:00:00:00:00:00
switch(san-ext)# nport pwwn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2
switch(san-ext-nport)# data-pattern-file bootflash://DataPatternFile
```

Related Commands

Command	Description
nport pwwn	Configures SAN extension tuner N port pWWNs.
san-ext-tuner	Enters SAN extension tuner configuration mode.
show san-ext-tuner	Displays SAN extension tuner information.

deadtime (radius group configuration)

To configure a periodic time interval where a nonreachable (nonresponsive) RADIUS server is monitored for responsiveness, use the **deadtime** command in RADIUS group configuration submode. To disable the monitoring of the nonresponsive server, use the **no** form of the command.

deadtime *time*

no deadtime *time*

Syntax Description

time	Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.

Defaults

Zero.

Command Modes

RADIUS group configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

If the dead time interval for an individual RADIUS server is greater than zero (0), that value takes precedence over the value set for the server group.

When the dead time interval is 0 minutes, RADIUS server monitoring is not performed unless the RADIUS server is part of a server group and the dead time interval for the group is greater than 0 minutes.

Examples

The following example shows the **deadtime** command in RADIUS group configuration submode.

```
switch# config terminal
switch(config)# aaa group server radius testgroup
switch(config-radius)# deadtime 10
```

Related Commands

Command	Description
radius-server deadtime	Sets a time interval for monitoring a nonresponsive RADIUS server.
show radius-server	Displays RADIUS server information.

deadtime (tacacs+ group configuration)

To configure a periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness, use the **deadtime** command in TACACS+ group configuration submode. To disable the monitoring of the nonresponsive server, use the **no** form of the command.

deadtime *time*

no deadtime *time*

Syntax Description

time	Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.

Defaults

Zero.

Command Modes

TACACS+ group configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

If the dead time interval for an individual TACACS+ server is greater than zero (0), that value takes precedence over the value set for the server group.

When the dead time interval is 0 minutes, TACACS+ server monitoring is not performed unless the TACACS+ server is part of a server group and the dead time interval for the group is greater than 0 minutes.

Examples

The following example shows the **deadtime** command in TACACS+ group configuration submode.

```
switch# config terminal
switch(config)# aaa group server tacacs mygroup
switch(config-tacacs)# deadtime 5
```

Related Commands

Command	Description
tacacs-server deadtime	Sets a time interval for monitoring a nonresponsive TACACS+ server.
show tacacs-server	Displays TACACS+ server information.

delete

To delete a specified file or directory on a Flash memory device, use the **delete** command in EXEC mode.

delete {**bootflash:***filename* | **debug:***filename* | **log:***filename* | **modflash:***filename* | **slot0:***filename* | **volatile:***filename*}

Syntax Description

bootflash:	Flash image that resides on the supervisor module.
debug:	Contains the debug files.
log:	Contains the two default logfiles. The file dmesg contains the kernel log-messages and the file messages contains the system application log-messages.
modflash:	Flash image that resides on a module.
slot0:	Flash image that resides on another module.
volatile:	Flash image that resides on the volatile file system.
filename	The name of the file to be deleted.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2	This command was introduced.
2.1(1a)	Added **debug**, **log**, and **modflash** keywords.

Usage Guidelines

When you delete a file, the software erases the file.

If you attempt to delete the configuration file or image specified by the CONFIG_FILE or BOOTLDR environment variable, the system prompts you to confirm the deletion. Also, if you attempt to delete the last valid system image specified in the BOOT environment variable, the system prompts you to confirm the deletion.

Caution If you specify a directory, the **delete** command deletes the entire directory and all its contents.

Examples

The following example deletes the file named test from the Flash card inserted in slot 0.

```
switch# delete slot0:test
Delete slot0:test? [confirm]
```

The following example deletes a file from a directory.

```
switch# delete dns_config.cfg
```

The following example deletes a file from an external CompactFlash (slot0).

```
switch# delete slot0:dns_config.cfg
```

The following example deletes the entire `my-dir` directory and all its contents:

```
switch# delete bootflash:my-dir
```

The following example deletes the entire user created `dk` log file on the active supervisor:

```
switch# delete log://sup-active/
log://sup-active/dk        log://sup-active/dmesg     log://sup-active/messages
switch# delete log://sup-active/dk
switch# dir log:
         31     Feb 04 18:22:03 2005  dmesg
      14223     Feb 04 18:25:30 2005  messages

Usage for log://sup-local
   35393536 bytes used
  174321664 bytes free
  209715200 bytes total
switch#
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
dir	Displays a list of files on a file system.
show boot	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.

delete ca-certificate

To delete certificate authority certificates, use the **delete ca-certificate** command in trust point configuration submode.

delete ca-certificate

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Trust point configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

This command deletes the CA certificate or certificate chain corresponding to the trust point CA. As a result, the trust point CA is no longer trusted. If there is an identity certificate form the CA, you should delete it before attempting to delete the CA certificate. Doing so prevents the accidental deletion of a CA certificate when you have not yet deleted the identity certificate from that CA. This action may be necessary when you do not want to trust the CA any more for a reason such as the CA is compromised or the CA certificate is already expired, with the latter being a very rare event.

Note The trust point configuration, certificates, and key pair configurations are made persistent only after saving to the startup configuration. To be consistent with this configuration behavior, the delete behavior is also the same. That is, the deletions are made persistent only after saving to the startup configuration.

Use the **copy running-config startup-config** command to make the certificate and key pair deletions persistent.

Examples

The following example shows how to delete a certificate authority certificate.

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete ca-certificate
```

Related Commands

Command	Description
delete certificate	Deletes the identity certificate.
delete crl	Deletes the crl from the trustpoint.

delete certificate

To delete the identity certificate, use the **delete certificate** command in trust point configuration submode.

delete certificate [force]

Syntax Description

force	Forces the deletion of the identity certificate.

Defaults

None.

Command Modes

Trust point configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Use this command to delete the identity certificate from the trust point CA. This action may be necessary when the identity certificate expires or the corresponding key pair is compromised. Applications will be left without any identity certificate to use after the deletion of the last or the only identity certificate present. Accordingly, an error message is generated if the certificate being deleted is the last or only identity certificate present. If needed, the deletion can still be accomplished by forcing it using the force option.

Note The trust point configuration, certificates, and key pair configurations are made persistent only after saving to the startup configuration. To be consistent with this configuration behavior, the delete behavior is also the same. That is, the deletions are made persistent only after saving to the startup configuration.

Use the **copy running-config startup-config** command to make the certificate and key pair deletions persistent.

Examples

The following example shows how to delete the identity certificate.

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete certificate
```

The following example shows how to force the deletion of the identity certificate.

```
switch(config-trustpoint)# delete certificate force
```

Related Commands

Command	Description
delete ca-certificate	Deletes the certificate authority certificate.
delete crl	Deletes the crl from the trustpoint.

delete crl

To delete the crl from the trustpoint, use the **delete crl** command in trust point configuration submode.

delete crl

Syntax Description

This command has no argument or keywords.

Defaults

None.

Command Modes

Trust point configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to delete the crl from the trustpoint.

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete crl
```

Related Commands

Command	Description
delete ca-certificate	Deletes the certificate authority certificate.
delete certificate	Deletes the identity certificate.

deny (IPv6-ACL configuration)

To configure deny conditions for an IPv6 access control list (ACL), use the **deny** command in IPv6-ACL configuration submode. To remove the conditions, use the **no** form of the command.

deny {*ipv6-protocol-number* | **ipv6**}
{*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*}
{*dest-ipv6-prefix/prefix-length* | **any** | **host** *dest-ipv6-address*}
[log-deny]

deny icmp
{*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*}
{*dest-ipv6-prefix/prefix-length* | **any** | **host** *dest-ipv6-address*}
[*icmp-type* [*icmp-code*]]
[log-deny]

deny tcp
{*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*}
[*source-port-operator source-port-number* |
range *source-port-number source-port-number*]
{*dest-ipv6-prefix/prefix-length* | **any** | **host** *dest-ipv6-address*}
[*dest-port-operator dest-port-number* |
range *dest-port-number dest-port-number*]
[established] [log-deny]

deny udp
{*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*}
[*source-port-operator source-port-number* |
range *source-port-number source-port-number*]
{*dest-ipv6-prefix/prefix-length* | **any** | **host** *dest-ipv6-address*}
[*dest-port-operator dest-port-number* |
range *dest-port-number dest-port-number*]
[log-deny]

no deny {*ipv6-protocol-number* | **ipv6** | **icmp** | **tcp** | **udp**}

Syntax Description

ipv6-protocol-number	Specifies an IPv6 protocol number. The range is 0 to 255.
ipv6	Applies the ACL to any IPv6 packet.
source-ipv6-prefix/ prefix-length	Specifies a source IPv6 network or class of networks. The format is *X:X:X::X/n*.
any	Applies the ACL to any source or destination prefix.
host *source-ipv6-address*	Applies the ACL to the specified source IPv6 host address. The format is *X:X:X::X*.
dest-ipv6-prefix/prefix-length	Specifies a destination IPv6 network or class of networks. The format is *X:X:X::X/n*.
host *dest-ipv6-address*	Applies the ACL to the specified destination IPv6 host address. The format is *X:X:X::X*.
log-deny	For packets that are dropped, creates an informational log message about the packet that matches the entry. The message includes the input interface.

icmp	Applies the ACL to any Internet Control Message Protocol (ICMP) packet.
icmp-type	Specifies an ICMP message type. The range is 0 to 255.
icmp-code	Specifies an ICMP message code. The range is 0 255.
tcp	Applies the ACL to any TCP packet.
source-port-operator	Specifies an operand that compares the source ports of the specified protocol. The operands are **lt** (less than), **gt** (greater than), and **eq** (equals).
source-port-number	Specifies the port number of a TCP or UDP port. The number can be from 0 to 65535. A range requires two port numbers.
udp	Applies the ACL to any UDP packet.
dest-port-operator	Specifies an operand that compares the destination ports of the specified protocol. The operands are **lt** (less than), **gt** (greater than), and **eq** (equals).
dest-port-operator	Specifies the port number of a TCP or UDP port. The number can be from 0 to 65535. A range requires two port numbers.
range	Specifies a range of ports to compare for the specified protocol.
established	Indicates an established connection, which is defined as a packet whole SYN flag is not set.

Defaults

None.

Command Modes

IPv6-ACL configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The following guidelines can assist you in configuring an IPv6-ACL. For complete information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

- You can apply IPv6-ACLs to VSAN interfaces, the management interface, Gigabit Ethernet interfaces on IPS modules and MPS-14/2 modules, and Ethernet PortChannel interfaces. However, if IPv6-ACLs are already configured in a Gigabit Ethernet interface, you cannot add this interface to a Ethernet PortChannel group.

Caution Do not apply IPv6-ACLs to just one member of a PortChannel group. Apply IPv6-ACLs to the entire channel group.

- Use only the TCP or ICMP options when configuring IPv6-ACLs on Gigabit Ethernet interfaces.
- Configure the order of conditions accurately. Because the IPv6-ACL filters are applied sequentially to the IP flows, the first match determines the action taken. Subsequent matches are not considered. Be sure to configure the most important condition first. If no conditions match, the software drops the packet.

Examples

The following example configures an IPv6-ACL called List1, enters IPv6-ACL submode, and adds an entry to deny TCP traffic from any source address to any destination address.

```
switch# config terminal
switch(config)# ipv6 access-list List1
switch(config-ipv6-acl)# deny tcp any any
```

The following example removes a deny condition set for any destination prefix on a specified UDP host.

```
switch# config terminal
switch(config)# ipv6 access-list List1
switch(config-ipv6-acl)# no deny udp host 2001:db8:200d::4000 any
```

The following example removes the IPv6-ACL called List1 and all its entries.

```
switch# config terminal
switch(config)# no ipv6 access-list List1
```

Related Commands

Command	Description
ipv6 access-list	Configures an IPv6 ACL and enters IPv6-ACL configuration submode.
permit	Configures permit conditions for an IPv6 ACL.

destination interface

To configure a switched port analyzer (SPAN) destination interface, use the **destination interface** command in SPAN session configuration submode. To disable this feature, use the **no** form of the command.

destination interface {**fc** *slot*/*port* | **fc-tunnel** *tunnel-id*}

no destination interface {**fc** *slot*/*port* | **fc-tunnel** *tunnel-id*}

Syntax Description

fc *slot*/*port*	Specifies the Fibre Channel interface ID at a slot and port.
fc-tunnel *tunnel-id*	Specifies the Fibre Channel tunnel interface ID.

Defaults

Disabled.

Command Modes

SPAN session configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.
1.2(1)	Added the **fc-tunnel** parameter.

Usage Guidelines

The SPAN destination interface must be configured as SPAN destination port (SD port) mode using the **switchport** command before the interface can be associated with SPAN session as a destination interface.

Examples

The following example shows how to configure an interface as a SPAN destination port (SD port), create a SPAN session, and then configure the interface fc3/13 as the SPAN destination interface.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# interface fc3/13
switch(config-if)# switchport mode sd
switch(config)# span session 1
switch(config-span)# destination interface fc3/13
switch(config-span)# do show span session 1
switch(config-span)# show span session 1
Session 1 (inactive as destination is down)
   Destination is fc3/13
   No session filters configured
   No ingress (rx) sources
   No egress (tx) sources

switch(config-span)#
```

Related Commands

Command	Description
switchport	Configures the switchport mode on the Fibre Channel interface.
span session	Selects or configures the SPAN session and changes to SPAN configuration submode.
source	Configures a SPAN source.
suspend	Suspends a SPAN session.
show span session	Displays specific information about a SPAN session

destination-profile

To configure the customer ID with the Call Home function, use the **destination-profile** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

destination-profile {*profile-name* | **full-txt-destination** | **short-txt-destination** | **xml-destination**} {**alert-group** {**all** | **avanti** | **cisco-tac** | **environmental** | **inventory** | **license** | **linecard-hardware** | **rmon** | **supervisor-hardware** | **syslog-group-port** | **system** | **test**}

no destination-profile {*profile-name* | **full-txt-destination** | **short-txt-destination** | **xml-destination**} {**alert-group** {**all** | **avanti** | **cisco-tac** | **environmental** | **inventory** | **license** | **linecard-hardware** | **rmon** | **supervisor-hardware** | **syslog-group-port** | **system** | **test**}

Syntax Description

profile-name	Specifies a user-defined user profile with a maximum of 32 alphanumeric characters.
full-txt-destination	Configures destination profile for plain text message.
short-txt-destination	(Optional) Configures a destination for a short text message.
xml-destination	(Optional) Configures destination profile for XML message.
alert-group	Specifies one or more of the alert groups
all	Specifies an alert group consisting of all Call Home messages.
avanti	Specifies an alert group consisting of events that are meant only for Avanti.
cisco-tac	Specifies an alert group consisting of events that are meant only for Cisco TAC.
environmental	Specifies an alert group consisting of power, fan, temperature-related events.
inventory	Specifies an alert group consisting of inventory status events.
license	Specifies an alert group consisting of license status events.
linecard-hardware	Specifies an alert group consisting of module-related events.
rmon	Specifies an alert group consisting of RMON status events.
supervisor-hardware	Specifies an alert group consisting of supervisor related events.
syslog-port-group	Specifies an alert group consisting of syslog port group status events.
system	Specifies an alert group consisting of software related events.
test	Specifies an alert group consisting of user-generated test events.

Defaults

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures full-text destination profiles.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# destination-profile full-txt-destination email-addr person@place.com
switch(config-callhome)# destination-profile full-txt-destination message-size 1000000
```

The following example configures short-text destination profiles.

```
switch(config-callhome)# destination-profile short-txt-destination email-addr person@place.com
switch(config-callhome)# destination-profile short-txt-destination message-size 100000
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

device-alias (IVR fcdomain database configuration submode)

To map a device alias to a persistent FC ID for IVR, use the **device-alias** command in IVR fcdomain database configuration submode. To remove the mapping for the device alias, use the **no** form of the command.

device-alias *device-name fc-id*

no device-alias *device-name*

Syntax Description

device-name	Specifies the device name. Maximum length is 64 characters.
fc-id	Specifies the FC ID for the device.

Defaults

None.

Command Modes

IVR fcdomain database configuration submode.

Command History

Release	Modification
2.1(2)	This command was introduced.

Usage Guidelines

Only one FC ID can be mapped to a device alias.

Examples

The following example shows how to map the device alias to the persistent FC ID.

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config-fcdomain)# native-autonomous-fabric-num 20 native-vsan 30 domain 15
switch(config-fcdomain-fcid)# device-alias SampleName 0x123456
```

The following example shows how to remove the mapping between the device alias and the FC ID.

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config-fcdomain)# native-autonomous-fabric-num 20 native-vsan 30 domain 15
switch(config-fcdomain-fcid)# no device-alias SampleName
```

Related Commands

Command	Description
ivr fcdomain database autonomous-fabric-num	Creates IVR persistent FC IDs.
native-autonomous-fabric-num	Creates an IVR persistent FC ID database entry.
show ivr fcdomain database	Displays IVR fcdomain database entry information.

device-alias abort

To discard a Distributed Device Alias Services (device alias) Cisco Fabric Services (CFS) distribution session in progress, use the **device-alias abort** command in configuration mode.

device-alias abort

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to discard a device alias CFS distribution session in progress.

```
switch# config terminal
switch(config)# device-alias abort
```

Related Commands

Command	Description
device-alias database	Configures and activates the device alias database.
device-alias distribute	Enables CFS distribution for device aliases.
show device-alias	Displays device alias information.

device-alias commit

To apply the pending configuration pertaining to the Distributed Device Alias Services (device alias) Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **device-alias commit** command in configuration mode.

device-alias commit

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to commit pending changes to the active DPVM database.

```
switch# config terminal
switch(config)# device-alias commit
```

Related Commands

Command	Description
device-alias database	Configures and activates the device alias database.
device-alias distribute	Enables CFS distribution for device aliases.
show device-alias	Displays device alias information.

device-alias database

To initiate a Distributed Device Alias Services (device alias) session and configure device alias database, use the **device-alias database** command. To deactivate the device alias database, use the **no** form of the command.

device-alias database

no device-alias database

Syntax Description

This command has no other arguments or keywords.

Defaults

Deactivated.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

The **device-alias database** command starts a device alias session that locks all the databases on all the switches in this fabrics. When you exit device alias database configuration submode, the device alias session ends and the locks are released.

You can only perform all modifications in the temporary device alias database. To make the changes permanent, use the **device-alias commit** command.

Examples

The following example shows how to activate a device alias session and enter device alias database configuration submode;.

```
switch# config terminal
switch(config)# device-alias database
switch(config-device-alias-db)#
```

Related Commands

Command	Description
device-alias commit	Commits changes to the temporary device alias database to the active device alias database.
show device-alias	Displays device alias database information.

device-alias distribute

To enable Cisco Fabric Services (CFS) distribution for Distributed Device Alias Services (device alias), use the **device-alias distribute** command. To disable this feature, use the **no** form of the command.

device-alias distribute

no device-alias distribute

Syntax Description

This command has no other arguments or keywords.

Defaults

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

Use the **device-alias commit** command to apply pending changes to the CFS distribution session.

Examples

The following example shows how to enable distribution for device alias information.

```
switch# config terminal
switch(config)# device-alias distribute
```

Related Commands

Command	Description
device-alias commit	Commits changes to the active device alias database.
device-alias database	Configures and activates the device alias database.
show device-alias	Displays device alias information.

device-alias import fcalias

To import device alias database information from another VSAN, use the **device-alias import fcalias** command. To revert to the default configuration or factory defaults, use the **no** form of the command.

device-alias import fcalias vsan *vsan-id*

no device-alias import fcalias vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

You can import legacy device name configurations using this feature without losing data, if they satisfy the following restrictions:

- Each fcalias has only one member.
- The member type is supported by the device name implementation.

If any name conflict exists, the fcaliases are not imported. The device name database is completely independent from the VSAN dependent fcalias database.

When the import operation is complete, the modified global fcalias table can distributed to all other switches in the physical fabric using the **device-alias distribute** command so that new definitions are available everywhere.

Examples

The following example shows how to import device alias information.

```
switch# config terminal
switch(config)# device-alias import fcalias vsan 10
```

Related Commands

Command	Description
device-alias database	Configures and activates the device alias database.
device-alias distribute	Distributes fcalias database changes to the fabric.
show device-alias	Displays device alias database information.

device-alias name

To configure device names in the device alias database, use the **device-alias name** command. To remove device names from the device alias database, use the **no** form of the command.

device-alias name *device-name* **pwwn** *pwwn-id*

no device-alias name *device-name*

Syntax Description

device-name	Specifies the device name. Maximum length is 64 characters.
pwwn *pwwn-id*	Specifies the pWWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.

Defaults

None.

Command Modes

Device alias database configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure a device name alias entry in the device name database.

```
switch# config terminal
switch(config)# device-alias database
switch(config-device-alias-db)# device-alias name Device1 pwwn 21:00:00:20:37:6f:db:bb
```

Related Commands

Command	Description
device-alias database	Enters device alias database configuration submode.
show device-alias	Displays device alias database information.

dir

To display the contents of the current directory or the specified directory, use the **dir** command in EXEC mode.

dir [**bootflash:***module* | *directory-or-filename* | **debug:***directory-or-filename* | **log:***module* | *directory-or-filename* | **modflash:***module* | *directory-or-filename* | **slot0:***directory-or-filename* | **volatile:***module* | *directory-or-filename*]

Syntax Description

bootflash:	(Optional) Flash image that resides on the supervisor module.
debug:	(Optional) Provides information about the debug capture directory.
log:	(Optional) Provides information about the two default logfiles. The file dmesg contains the kernel log-messages and the file messages contains the system application log-messages.
modflash:	(Optional) Provides information about the flash image that resides in a module flash file directory.
slot0:	(Optional) Flash image that resides on another module.
module	(Optional) Module name and number.
filename-or-directory	(Optional) Name of the file or directory to display on a specified device. The files can be of any type. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.
volatile:	Flash image on the volatile file system.

Defaults

The default file system is specified by the **cd** command.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.
2.1(1a)	Added **debug**, **log**, and **modflash** keywords.

Usage Guidelines

None.

Examples

The following example shows how to list the files on the bootflash directory.

```
switch# dir bootflash:
40295206     Aug 05 15:23:51 1980  i1c1.bin
12456448     Jul 30 23:05:28 1980  kickstart-image1
12288       Jun 23 14:58:44 1980  lost+found/
27602159     Jul 30 23:05:16 1980  system-image1
12447232     Aug 05 15:08:30 1980  kickstart-image2
28364853     Aug 05 15:11:57 1980  system-image2

Usage for bootflash://sup-local
  135404544 bytes used
   49155072 bytes free
  184559616 bytes total
```

The following example shows how to list the files in the debug directory.

```
switch# dir debug:
Usage for debug://sup-local
          0 bytes used
    2097152 bytes free
    2097152 bytes total
switch#
```

The following example shows how to list the files in the log file directory.

```
switch# dir log:
         31     Feb 05 05:00:57 2005  dmesg
       8445     Feb 06 10:34:35 2005  messages

Usage for log://sup-local
   35196928 bytes used
  174518272 bytes free
  209715200 bytes total
switch#
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
delete	Deletes a file on a Flash memory device.

disable

To disable the Call Home function, use the **disable** command in Call Home configuration submode.

disable

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

To enable the Call Home function, use the **enable** command.

Examples

The following example shows how to disable the Call Home function.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# disable
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

discover custom-list

To selectively initiate discovery for specified domain IDs in a VSAN, use the **discover custom-list** command in EXEC mode.

discover custom-list {**add** | **delete**} **vsan** *vsan-id* **fcid** *fc-id*

Syntax Description

add	Add a targets to the customized list.
delete	Deletes a target from the customized list.
vsan *vsan-id*	Discovers SCSI targets for the specified VSAN ID. The range is 1 to 4093.
fcip *fc-id*	Discovers SCSI targets for the specified FCID. The format is *0xhhhhhhh*, where *h* is a hexadecimal digit.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example selectively initiates discovery for the specified VSAN and FCID.

```
switch# discover custom-list add vsan 1 fcid 0X123456
```

The following example deletes the specified VSAN and FCID from the customized list.

```
switch# discover custom-list delete vsan 1 fcid 0X123456
```

discover scsi-target

To discover SCSI targets on local storage to the switch or remote storage across the fabric, use the **discover scsi-target** command in EXEC mode.

discover scsi-target {**custom-list** | **local** | **remote** | **vsan** *vsan-id* **fcid** *fc-id*} **os** {**aix** | **all** | **hpux** | **linux** | **solaris** | **windows**} [**lun** | **target**]

Syntax Description

custom-list	Discovers SCSI targets from the customized list.
local	Discovers local SCSI targets.
remote	Discovers remote SCSI targets.
vsan *vsan-id*	Discovers SCSI targets for the specified VSAN ID. The range is 1 to 4093.
fcip *fc-id*	Discovers SCSI targets for the specified FCID. The format is *0xhhhhhhh*, where *h* is a hexadecimal digit.
os	Discovers the specified operating system.
aix	Discovers the AIX operating system
all	Discovers all operating systems
hpux	Discovers the HPUX operating system
linux	Discovers the Linux operating system
solaris	Discovers the Solaris operating system
windows	Discovers the Windows operating system
lun	Discovers SCSI targets and LUNs.
target	Discovers SCSI targets.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(2a)	This command was introduced.

Usage Guidelines

On-demand discovery only discovers Nx ports present in the name server database that have registered a FC4 Type = SCSI_FCP.

Examples

The following example shows how to discover local targets assigned to all OSs.

```
switch# discover scsi-target local os all
discovery started
```

The following example shows how to discover remote targets assigned to the Windows OS.

```
switch# discover scsi-target remote os windows
discovery started
```

The following example shows how to discover SCSI targets for the specified VSAN (1) and FCID (0x9c03d6).

```
switch# discover scsi-target vsan 1 fcid 0x9c03d6
discover scsi-target vsan 1 fcid 0x9c03d6
VSAN:    1 FCID: 0x9c03d6 PWWN: 00:00:00:00:00:00:00:00
  PRLI RSP: 0x01 SPARM: 0x0012...
```

The following example begins discovering targets from a customized list assigned to the Linux operating system.

```
switch# discover scsi-target custom-list os linux
discovery started
```

distribute

To enable distribution of the Call Home function using CFS, use the **distribute** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

distribute

no distribute

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable distribution of the Call Home function using CFS.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# distribute
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

do

Use the **do** command to execute an EXEC-level command from any configuration mode or submode.

do *command*

Syntax Description

command	Specifies the EXEC command to be executed.

Defaults

None.

Command Modes

All configuration modes.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Use this command to execute EXEC commands while configuring your switch. After the EXEC command is executed, the system returns to the mode from which you issued the do command.

Examples

The following example disables the **terminal session-timeout** command using the **do** command in configuration mode.

```
switch(config)# do terminal session-timeout 0
switch(config)#
```

The following example create, enables, and displays the interface from configuration mode.

```
switch(config)# int fc 3/1
switch(config-if)# no shut
switch(config-if)# do show interface fc 3/1
fc3/1 is trunking
    Hardware is Fibre Channel
    Port WWN is 20:81:00:05:32:00:4a:9e
    Peer port WWN is 20:43:00:0c:88:00:4a:e2
    Admin port mode is auto, trunk mode is on
    Port mode is TE
    Port vsan is 1
    Speed is 2 Gbps
    Transmit B2B Credit is 0
    Receive B2B Credit is 255
    Receive data field Size is 2112
    Beacon is turned off
    Trunk vsans (admin allowed and active) (1-10)
    Trunk vsans (up)                       (1-10)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             ()
    5 minutes input rate 504 bits/sec, 63 bytes/sec, 0 frames/sec
    5 minutes output rate 344 bits/sec, 43 bytes/sec, 0 frames/sec
      69390 frames input, 4458680 bytes
        0 discards, 0 errors
        0 CRC,  0 unknown class
        0 too long, 0 too short
      69458 frames output, 3086812 bytes
        0 discards, 0 errors
      2 input OLS, 1 LRR, 0 NOS, 2 loop inits
      1 output OLS, 1 LRR, 1 NOS, 1 loop inits
```

dpvm abort

To discard a dynamic port VSAN membership (DPVM) Cisco Fabric Services (CFS) distribution session in progress, use the **dpvm abort** command in configuration mode.

dpvm abort

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

Examples

The following example shows how to discard a DPVM CFS distribution session in progress.

```
switch# config terminal
switch(config)# dpvm abort
```

Related Commands

Command	Description
dpvm database	Configures the DPVM database.
dpvm distribute	Enables CFS distribution for DPVM.
dpvm enable	Enables DPVM.
show dpvm	Displays DPVM information.

dpvm activate

To activate the dynamic port VSAN membership (DPVM) configuration database, use the **dpvm activate** command. To deactivate the DPVM configuration database, use the **no** form of the command.

dpvm activate [**force**]

no dpvm activate [**force**]

Syntax Description

force	Forces the activation or deactivation if conflicts exist between the configured DPVM database and the active DPVM database.

Defaults

Deactivated.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

Activation might fail if conflicting entries are found between the configured DPVM database and the currently activated DPVM database. You can ignore the conflicts using the **force** option.

Examples

The following example shows how to activate the DPVM database.

```
switch# config terminal
switch(config)# dpvm activate
```

The following example shows how to deactivate the DPVM database.

```
switch# config terminal
switch(config)# no dpvm activate
```

Related Commands

Command	Description
dpvm database	Configures the DPVM database.
dpvm enable	Enables DPVM.
show dpvm	Displays DPVM database information.

dpvm auto-learn

To enable the automatic learning feature (autolearn) for the active dynamic port VSAN membership (DPVM) database, use the **dpvm auto-learn** command. To disable this feature, use the **no** form of the command.

dpvm auto-learn

no dpvm auto-learn

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

When autolearn is enabled, the system automatically creates the DPVM database by learning about devices currently logged or newly logged devices with a VSAN. This is a quick way to create the DPVM database, which can later be edited. Autolearn features include the following:

- An autolearned entry is created by adding the device PWWN and VSAN to the active DPVM database.
- The active DPVM database must be present when autolearning is enabled.
- Autolearned entries can be deleted from the active DPVM database by the user until autolearning is disabled. Autolearned entries are not permanent in the active DPVM database until autolearning is disabled.
- If a device logs out when autolearning is enabled, the device entry is deleted from the active DPVM database.
- If a particular device logs into the switch multiple times through different ports, then only the VSAN corresponding to last login is associated with the device.
- Autolearn entries do not override previously configured activate entries.

Examples

The following example shows how to enable autolearning for the DPVM database.

```
switch# config terminal
switch(config)# dpvm auto-learn
```

The following example shows how to disable autolearning for the DPVM database.

```
switch# config terminal
switch(config)# no dpvm auto-learn
```

Related Commands

Command	Description
dpvm enable	Enables DPVM.
show dpvm	Displays DPVM database information.

dpvm commit

To apply the pending configuration pertaining to the dynamic port VSAN membership (DPVM) Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **dpvm commit** command.

dpvm commit

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

Examples

The following example shows how to commit changes to the DPVM database.

```
switch# config terminal
switch(config)# dpvm commit
```

Related Commands

Command	Description
dpvm distribute	Enables CFS distribution for DPVM.
dpvm enable	Enables DPVM.
show dpvm	Displays DPVM information.

dpvm database

To activate and configure the dynamic port VSAN membership (DPVM) database, use the **dpvm database** command. To deactivate the database, use the **no** form of the command.

dpvm database

no dpvm database

Syntax Description

This command has no other arguments or keywords.

Defaults

Deactivated.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

The DPVM database consists of a series of device mapping entries. Each entry consists of device pWWN or nWWN along with the dynamic VSAN to be assigned. Use the **nwwn** command or **pwwn** command to add the entries to the DPVM database. This database is global to the whole switch (and fabric) and is not maintained for each VSAN.

Examples

The following example shows how to activate the DPVM database and enter DPVM database configuration submode.

```
switch# config terminal
switch(config)# dpvm database
switch(config-dpvm-db)#
```

Related Commands

Command	Description
dpvm enable	Enables DPVM.
nwwn (DPVM database configuration submode)	Adds entries to the DPVM database using the nWWN.
pwwn (DPVM database configuration submode)	Adds entries to the DPVM database using the pWWN.
show dpvm	Displays DPVM database information.

dpvm database copy active

To copy the active dynamic port VSAN membership (DPVM) database to the config DPVM database, use the **dpvm database copy active** command.

dpvm database copy active

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

The following circumstances may require the active database to be copied to the config database:

- When the autolearned entries are only added to the active database.
- When the config database or entries in the config database are accidently deleted.

Note If you want to copy the DPVM database and fabric distribution is enabled, you must first commit the changes.

Examples

The following example shows how to copy the active DPVM database to the config DPVM database.

```
switch# dpvm database copy active
```

Related Commands

Command	Description
dpvm enable	Enables DPVM.
show dpvm	Displays DPVM database information.

dpvm database diff

To display the active dynamic port VSAN membership (DPVM) database, use the **dpvm database diff** command.

dpvm database diff {**active** | **config**}

Syntax Description

active	Displays differences in the DPVM active database compared to the DPVM config database.
config	Displays differences in the DPVM config database compared to the DPVM active database.

Defaults

Deactivated.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

Examples

The following example displays the differences in the DPVM active database when compared with the DPVM config database.

```
switch# dpvm database diff active
Legend: "+" New Entry, "-" Missing Entry, "*" Possible Conflict Entry
--------------------------------------------------------------------
- pwwn 44:22:33:44:55:66:77:88 vsan 44
* pwwn 11:22:33:44:55:66:77:88 vsan 11
```

The following example displays the differences in the DPVM config database when compared with the DPVM active database.

```
switch# dpvm database diff config
Legend: "+" New Entry, "-" Missing Entry, "*" Possible Conflict Entry
--------------------------------------------------------------------
- pwwn 44:22:33:44:55:66:77:88 vsan 44
* pwwn 11:22:33:44:55:66:77:88 vsan 11
```

Related Commands

Command	Description
dpvm enable	Enables DPVM.
show dpvm	Displays DPVM database information.

dpvm distribute

To enable Cisco Fabric Services (CFS) distribution for dynamic port VSAN membership (DPVM), use the **dpvm distribute** command. To disable this feature, use the **no** form of the command.

dpvm distribute

no dpvm distribute

Syntax Description

This command has no other arguments or keywords.

Defaults

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

Temporary changes to the DPVM database must be committed to the active DPVM database using the **dpvm commit** command before being distributed to the fabric.

Examples

The following example shows how to disable distribution for the DPVM database.

```
switch# config terminal
switch(config)# no dpvm distribute
```

The following example shows how to enable distribution for the DPVM database.

```
switch# config terminal
switch(config)# dpvm distribute
```

Related Commands

Command	Description
dpvm enable	Enables DPVM.
show dpvm	Displays DPVM information.

dpvm enable

To enable dynamic port VSAN membership (DPVM), use to **dpvm enable** command. To disable DPVM, use the **no** form of the command.

dpvm enable

no dpvm enable

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

The configuration and verification commands for DPVM are only available when DPVM is enabled on the switch. When you disable this feature, all related configurations are automatically discarded.

Examples

The following example shows how to enable DPVM.

```
switch# config terminal
switch(config)# dpvm enable
```

Related Commands

Command	Description
dpvm activate	Activates the DPVM database.
dpvm database	Configures the DPVM database.
show dpvm	Displays DPVM database information.

dscp

To configure a differentiated services code point (DSCP) in a QoS policy map class, use the **dscp** command in EXEC mode. To disable this feature, use the **no** form of the command.

dscp *value*

no dscp *value*

Syntax Description

value	Configures the DSCP value. The range is 0 to 63. DSCP value 46 is reserved.

Defaults

The default DSCP value is 0.

Command Modes

QoS policy map class configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Before you can configure a QoS policy map class you must complete the following:

- Enable the QoS data traffic feature using the **qos Enable** command.
- Configure a QoS class map using the **qos Class-map** command.
- Configure a QoS policy map using the **qos Policy-map** command.
- Configure a QoS policy map class using the **class** command.

Examples

The following example configures a DSCP value of 56 in QoS policy classMap1.

```
switch(config-pmap)# class classMap1
switch(config-pmap-c)# dscp 56
switch(config-pmap-c)#
```

Related Commands

Command	Description
qos enable	Enables the QoS data traffic feature on the switch.
qos class-map	Configures a QoS class map.
qos policy-map	Configure a QoS policy map.
class	Configure a QoS policy map class.
show qos	Displays the current QoS settings.

duplicate-message throttle

To enable throttling of duplicate Call Home alert messages, use the **duplicate-message throttle** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

duplicate-message throttle

no duplicate-message throttle

Syntax Description

This command has no other arguments or keywords.

Defaults

Enabled.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

The rate of throttling is a maximum of thirty messages in 2 hours.

Examples

The following example shows how to enable throttling of duplicate Call Home alert messages.

```
switch# config terminal
switch(config)# callhome
switch(config-callhome)# duplicate-message throttle
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

CHAPTER 6

Debug Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All debug commands are issued in EXEC mode and are shown here in alphabetical order. For more information, refer to the *Cisco MDS 9000 Family Troubleshooting Guide* and the *Cisco MDS 9000 Family System Messages Guide*.

Using the CLI, you can enable debugging modes for each switch feature and view a real-time updated activity log of the control protocol exchanges. Each log entry is time-stamped and listed in chronological order. Access to the debug feature can be limited through the CLI roles mechanism and can be partitioned on a per-role basis.

debug aaa

To enable debugging for boot variables, use the **debug aaa** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug aaa {**all** | **conf-events** | **errors** | **events** | **mts**}

no debug aaa {**all** | **conf-events** | **errors** | **events** | **mts**}

Syntax Description

all	Enables all AAA debug options.
conf-events	Enables AAA configuration events debugging.
errors	Enables debugging for AAA errors.
events	Enables debugging for AAA events.
mts	Enables AAA transmit and receive MTS packets debugging.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modifications
1.3(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug aaa conf-events** command is issued:

```
switch# debug aaa conf-events
Nov 20 06:29:52 aaa: aaa_cleanup_session
Nov 20 06:29:52 aaa: mts_drop of request msg
Nov 20 06:29:52 aaa: Configured method local Succeeded
Nov 20 06:29:58 aaa: Src: 0x00000101/10886  Dst: 0x00000101/0  ID: 0x003
ize: 197 [REQ] Opc: 8402 (MTS_OPC_AAA_REQ) RR: 0x003A48F7  HA_SEQNO: 0x0
 TS: 0x9FC1C1234E7C  REJ:0  SYNC:0
Nov 20 06:29:58 aaa: 01 01 0C 00 00 00 00 00 00 00 00 00 00 00 02 01
Nov 20 06:29:58 aaa: 00 00 00 00 00 00 00 06 08 00 03 05 00 00 00 00
Nov 20 06:29:58 aaa: 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Nov 20 06:29:58 aaa: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Nov 20 06:29:58 aaa: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Nov 20 06:29:58 aaa: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Nov 20 06:29:58 aaa: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Nov 20 06:29:58 aaa: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Nov 20 06:29:58 aaa: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Nov 20 06:29:58 aaa: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Related Commands

Command	Description
aaa authentication login	Configures the authentication mode for a login.
no debug all	Disables all debugging.
show aaa authentication	Displays the configured authentication methods.

debug all

To enable debugging for all features on the switch, use the **debug all** command in EXEC mode. To disable this command and turn off all debugging, use the **no** form of the command.

debug all

no debug all

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The **no debug all** command turns off all diagnostic output. Using the **no debug all** command is a convenient way to ensure that you have not accidentally left any debug commands turned on.

Caution Because debugging output takes priority over other network traffic, and because the **debug all** command generates more output than any other **debug** command, it can severely diminish the performance of the switch or even render it unusable. In virtually all cases, it is best to use more specific **debug** commands.

Examples

The following example displays the system output when the **debug all** command is issued:

```
switch# debug all
```

Related Commands

Command	Description
show debug	Displays the debug commands configured on the switch.

debug biosd

To configure bios_daemon debugging, use the **debug biosd** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug biosd all

no debug biosd all

Syntax Description

all	Enables all bios_daemon debug options.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
2.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug biosd** command is issued:

```
switch# debug biosd
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug bootvar

To enable debugging for boot variables, use the **debug bootvar** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug bootvar {**all** | **errors** | **events** | **info** | **pss**}

no debug bootvar {**all** | **errors** | **events** | **info** | **pss**}

Syntax Description

all	Enables all boot variable debug options.
errors	Enables debugging for boot variable errors.
events	Enables debugging for boot variable events.
info	Enables debugging for boot variable information.
pss	Enables debugging for boot variable PSS operations.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug bootvar all** command is issued:

```
switch# debug bootvar all
```

Related Commands

Command	Description
debug all	Enables debugging for all features on the switch.
show boot	Displays the boot variables or modules.

debug callhome

To enable debugging for the Call Home function, use the **debug callhome** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug callhome {**all** | **events** | **mts**}

no debug callhome {**all** | **events** | **mts**}

Syntax Description

all	Enables debugging for all Call Home features.
events	Enables debugging for all Call Home events.
mts	Enables debugging for all Call Home tx/rx packets of MTS

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The **debug callhome** command, when used with the **all** parameter, displays the troubleshooting information for both Call Home event traces and a dump of the messaging and transaction service (MTS) messages that the Call Home function receives.

Note The debug Call Home function displays event traces for both successful and unsuccessful Call Home e-mail transmissions.

Examples

The following example displays the system output when the **debug callhome events** command is issued:

```
switch# debug callhome events
2005-03-09T05:37:21 2005 Mar  9 05:37:21 callhome: filling in name field with Test
2005 Mar  9 05:37:21 callhome: filling in the header list
2005 Mar  9 05:37:21 callhome: filling up the chassis list
2005 Mar  9 05:37:21 callhome: filling up the main body list
2005 Mar  9 05:37:21 callhome: filling up the fru list 2005 Mar  9 05:37:21 callhome:
Entering function do_event_correlation
2005 Mar  9 05:37:21 callhome: getting dest profiles for alert group test
2005 Mar  9 05:37:21 callhome: getting dest profiles for alert group cisco-tac
2005 Mar  9 05:37:21 callhome: Applying the event rule for destination profile full_txt
2005 Mar  9 05:37:21 callhome: Applying the event rule for destination profile short_txt
2005 Mar  9 05:37:21 callhome: Applying the event rule for destination profile xml 2005
Mar  9 05:37:21 callhome: Applying the event rule for destination profile basu
2005 Mar  9 05:37:21 callhome: Exiting function do_event_correlation
2005 Mar  9 05:37:21 callhome: running cli commands for alert name : Test, message id :
1540383426
2005 Mar  9 05:37:21 callhome: process scheduled for running cli commands for alert Test,
message id 1540383426, destination profile basu
2005 Mar  9 05:37:21 callhome: process scheduled for running cli commands for alert Test,
message id 1540383426, destination profile xml
2005 Mar  9 05:37:21 callhome: process scheduled for running cli commands for alert Test,
message id 1540383426, destination profile short_txt
.
.
.
```

The following example displays the system output when the **debug callhome mts** command is issued:

```
switch# debug callhome mts
Apr  8 13:09:42 callhome: Src: 0x00000501/4067  Dst: 0x00000501/66  ID: 0x0004FA
0D  Size: 252 [REQ] Opc: 182 (MTS_OPC_DEBUG_WRAP_MSG) RR: 0x0004FA0D  HA_SEQNO:
0x00000000  TS: 0x86708AFE37B  REJ:0
Apr  8 13:09:42 callhome: 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00
Apr  8 13:09:42 callhome: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr  8 13:09:42 callhome: 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF
...
Apr  8 13:09:42 callhome: Src: 0x00000501/4067  Dst: 0x00000501/66  ID: 0x0004FA
10  Size: 252 [REQ] Opc: 182 (MTS_OPC_DEBUG_WRAP_MSG) RR: 0x0004FA10  HA_SEQNO:
0x00000000  TS: 0x86708D6A974  REJ:0
Apr  8 13:09:42 callhome: 00 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00
Apr  8 13:09:42 callhome: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr  8 13:09:42 callhome: 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF
...
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show callhome	Displays Call Home information configured on a switch.

debug cert-enroll

To enable debugging for the certificate enroll daemon, use the **debug cert-enroll** command in EXEC mode. To disable a **debug** command use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug cert-enroll {all | config | config-lowlevel | request | request-lowlevel}

no debug cert-enroll {all | config | config-lowlevel | request | request-lowlevel}

Syntax Description

all	Enables all debugging flags.
config	Enables debugging for the certificate enroll configuration.
config-lowlevel	Enables low-level debugging for the certificate enroll configuration
request	Enables debugging for the certification enroll request.
request-lowlevel	Enables low-level debugging for the certification enroll request.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug cert-enroll all** command is issued:

```
switch# debug cert-enroll all
2006 Jan 21 00:44:52.875125 cert_enroll: cert_en_debug_conf_open: entering...
2006 Jan 21 00:44:52.875602 cert_enroll: cert_en_debug_conf_open: exiting
2006 Jan 21 00:44:52.876284 cert_enroll: cert_en_conf_close: entering...
2006 Jan 21 00:44:52.876349 cert_enroll: cert_en_conf_close: returning 0
2006 Jan 21 00:44:52.876400 cert_enroll: cert_en_enable_info_config: entering for
Cert-enroll Daemon debug
2006 Jan 21 00:44:52.876428 cert_enroll: cert_en_debug_conf_open: entering...
2006 Jan 21 00:44:52.876679 cert_enroll: cert_en_debug_conf_open: exiting
sw-46-180# 2006 Jan 21 00:44:52.876712 cert_enroll: cert_en_enable_info_config:
SET_REQ for Cert-enroll Daemon debug with 1
2006 Jan 21 00:44:52.876857 cert_enroll: cert_en_enable_info_config: SET_REQ done for
Cert-enroll Daemon debug with 1
2006 Jan 21 00:44:52.876896 cert_enroll: cert_en_enable_info_config: got back the return
value of configuration operation:success
2006 Jan 21 00:44:52.876922 cert_enroll: cert_en_debug_conf_close: entering...
2006 Jan 21 00:44:52.876965 cert_enroll: cert_en_debug_conf_close: returning 0
2006 Jan 21 00:44:52.876991 cert_enroll: cert_en_enable_info_config: exiting for
 Cert-enroll Daemon debug...
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show crypto ca certificates	Displays configured trust point certificates.

debug cdp

To enable debugging for the Cisco Discovery Protocol (CDP) function, use the **debug cdp** command in EXEC mode. To disable a **debug** command use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug cdp {**all** | **errors** | **events** {**mts** | **packets** | **pss**}}
[**interface** {**gigabitethernet** *slot*/*port* | **mgmt 0**}]

no debug cdp {**all** | **errors** | **events** {**mts** | **packets** | **pss**}}
[**interface** {**gigabitethernet** *slot*/*port* | **mgmt 0**}]

Syntax Description

all	Enables debugging for all CDP features.
errors	Enables debugging for CDP error conditions.
events	Enables debugging for CDP events.
mts	Enables debugging for CDP tx/rx MTS packets.
packets	Enables debugging for CDP tx/rx CDP packets.
pss	Enables debugging for all PSS related CDP events.
interface	Specifies debugging for the specified interface.
gigbitethernet *slot*/*port*	Specifies the Gigabit Ethernet interface slot and port.
mgmt 0	Specifies the management interface.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug cdp events packets** command is issued:

```
switch# debug cdp events packets
Apr  8 21:22:34 cdp: Sent CDP packet, interface 0x2380000
Apr  8 21:22:34 cdp: Sent CDP packet, interface 0x2381000
Apr  8 21:22:35 cdp: Sent CDP packet, interface 0x2382000
Apr  8 21:22:35 cdp: Sent CDP packet, interface 0x2383000
Apr  8 21:22:51 cdp: Received CDP packet, interface 0x5000000
Apr  8 21:23:01 cdp: Sent CDP packet, interface 0x5000000
Apr  8 21:23:34 cdp: Sent CDP packet, interface 0x2380000
Apr  8 21:23:34 cdp: Sent CDP packet, interface 0x2381000
Apr  8 21:23:35 cdp: Sent CDP packet, interface 0x2382000
...
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show cdp	Displays CDP parameters configured globally or for a specific interface.

debug cfs

To enable debugging for Cisco Fabric Services (CFS), use the **debug cfs** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug cfs {**all** | **errors** | **events** {**db** [**vsan** *vsan-id*] | **fc2** [**vsan** *vsan-id*] | **fsm-action** [**vsan** *vsan-id*] | **fsm-trans** [**sap** *sap-id*] | **mts** [**vsan** *vsan-id*] | **pss** [**vsan** *vsan-id*]} | **fsm** {**ha** | **trans**} | **merge**}

no debug cfs {**all** | **errors** | **events** {**db** [**vsan** *vsan-id*] | **fc2** [**vsan** *vsan-id*] | **fsm-action** [**vsan** *vsan-id*] | **fsm-trans** [**sap** *sap-id*] | **mts** [**vsan** *vsan-id*] | **pss** [**vsan** *vsan-id*]} | **fsm** {**ha** | **trans**} | **merge**}

Syntax Description

all	Enables all CFS debugging.
errors	Enables debugging for CFS error conditions.
events	Enables debugging for CFS events.
db	Enables debugging for CFS database events.
vsan *vsan-id*	Restricts debugging to the specified VSAN ID. The range is 1 to 4093.
fc2	Enables debugging for CFS FC2 events.
fsm-action	Enables debugging for CFS FSM action events.
fsm-trans	Enables debugging for CFS FSM transition events.
sap *sap-id*	Restricts debugging to the specified SAP ID. The range is 0 to 2147483647
mts	Enables debugging for CFS MTS events.
pss	Enables debugging for CFS PSS events.
fsm	Enables debugging for CFS FSM events.
ha	Enables debugging for CFS FSM high availability events.
trans	Enables debugging for CFS FSM transition events.
merge	Enables debugging for CFS merge events.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug cfs all** command is issued.

```
switch# debug cfs all
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show cfs	Displays CFS information.

debug cimserver

To enable debugging for the Common Information Model (CIM) management applications function, use the **debug cimserver** command in EXEC mode. To disable a debug command use the no form of the command or use the no debug all command to turn off all debugging.turn off all debugging).

debug cimserver {**all** | **errors** | **events** | **mts** | **trace**}

no debug cimserver {**all** | **errors** | **events** | **mts** | **trace**}

Syntax Description

all	Enables debugging for all CIM features.
errors	Enables debugging for CIM error conditions.
events	Enables debugging for CIM events.
mts	Enables debugging for CIM tx/rx MTS packets.
trace	Enables debugging for CIM traces.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug cimserver all** command is issued:

```
switch# debug cimserver all
2004 Mar 29 20:05:22 cimsrvprov: cim_mts_dispatch(): Opcode is 182
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show cimserver	Displays the CIM configurations and settings.

debug cloud

To enable debugging of cloud discovery, use the **debug cloud** command in EXEC mode.To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug cloud {all | bypass ficon_mgr | cloud | conditional | demux vsan *vsan-id* **| deque | discovery | error | event vsan** *vsan-id* **| ha vsan** *vsan-id* **| init | member | memory | messages | remotesync | trace [detail vsan** *vsan-id* **| vsan** *vsan-id*] **| warning [***vsan-id*] **| xipc | xipc}**

no debug cloud {all | bypass ficon_mgr | cloud | conditional | demux vsan *vsan-id* **| deque | discovery | error | event vsan** *vsan-id* **| ha vsan** *vsan-id* **| init | member | memory | messages | remotesync | trace [detail vsan** *vsan-id* **| vsan** *vsan-id*] **| warning [***vsan-id*] **| xipc | xipc}**

Syntax Description

all	Enables debugging of all features of the cloud.
bypass	Enables some components in cloud execution to be bypassed during debugging.
ficon_mgr	Enables the FICON manager to be bypassed during debugging.
cloud	Enables debugging of all cloud commands.
conditional	Enables debugging of the cloud discovery conditional service.
demux	Enables debugging of the cloud message demux.
vsan *vsan-id*	Restricts debugging to the specified VSAN ID. The range is 1 to 4094.
deque	Enables debugging of the cloud message dequeue.
discovery	Enables debugging of the discovery process.
error	Enables debugging of the cloud errors.
event	Enables debugging of the cloud finite state machine (FSM) and events.
ha	Enables debugging of cloud high availability (HA).
init	Enables debugging of cloud discovery initialization.
member	Enables debugging of cloud member changes.
memory	Enables debugging of cloud memory allocation.
messages	Enables debugging of cloud discovery messaging and transaction service (MTS) messages.
remotesync	Enables debugging of discovery remote sync.
trace	Enables debugging of the cloud trace.
detail	Enables debugging of the cloud detailed trace.
warning	Enables debugging of cloud warnings.
xipc	Enables debugging of XIPC messages.
xipc	Enables debugging of cloud data serialization.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays system output from the **debug cloud all** command.

```
switch# debug cloud all
1980 Feb 15 22:03:41.650721 cloud: fu_fsm_execute_all: match_msg_id(0), log_alre
ady_open(0)
1980 Feb 15 22:03:41.650874 cloud: fu_fsm_execute_all: null fsm_event_list
1980 Feb 15 22:03:41.650956 cloud: fu_fsm_engine_post_event_processing: mts msg
MTS_OPC_DEBUG_WRAP_MSG(msg_id 1302150) dropped
1980 Feb 15 22:03:41.651000 cloud: cloud_deque
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show cloud discovery	Displays cloud discovery information.
show cloud membership	Displays information about members of the cloud.

debug core

To enable core daemon debugging, use the **debug core** command in EXEC mode. To disable a debug command use the no form of the command or use the **no debug all** command to turn off all debugging.

debug core {**error** | **flow**}

no debug core {**error** | **flow**}

Syntax Description

error	Enables debugging for core demon error conditions.
flow	Enables debugging for the core demon flow.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug core flow** command is issued:

```
switch# debug core flow
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show cores	Displays all the cores presently available for upload from active sup.

debug device-alias

To enable debugging for device aliases, use the **debug device-alias** command in EXEC mode. To disable a **debug** command use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug device-alias {**all** | **database** {**detail** | **errors** | **events**} | **fsm** | **ha** | **import** {**errors** | **events**} | **merge** {**errors** | **events** | **packets**} | **pss** {**errors** | **events**} | **session** {**errors** | **events** | **packets**} | **trace**}

no debug device-alias {**all** | **database** {**detail** | **errors** | **events**} | **fsm** | **ha** | **import** {**errors** | **events**} | **merge** {**errors** | **events** | **packets**} | **pss** {**errors** | **events**} | **session** {**errors** | **events** | **packets**} | **trace**}

Syntax Description

all	Enables all device alias debugging.
database	Enables debugging for device alias database events.
detail	Enables detailed debugging for device alias database events.
errors	Enables debugging for device alias error conditions.
events	Enables debugging for device alias events.
fsm	Enables debugging for device alias FSM events.
ha	Enables debugging for device alias HA events.
import	Enables debugging for device alias imports.
merge	Enables debugging for device alias merges.
packets	Enables debugging for device alias packets.
pss	Enables debugging for device alias PSS.
session	Enables debugging for device alias sessions.
trace	Enables debugging for device alias traces.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug device-alias all** command is issued.

```
switch# debug device-alias all
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show device-alias	Displays device alias information.

debug dpvm

To enable debugging for dynamic port VSAN membership (DPVM), use the **debug dpvm** command in EXEC mode. To disable a **debug** command use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug dpvm {**all** | **cfs-events** | **change-events** | **db-events** | **errors** | **ftrace** | **merge-event** | **mts-events** | **pss-events** | **session-events** | **snmp-events** | **sys-events**}

no debug dpvm {**all** | **cfs-events** | **change-events** | **db-events** | **errors** | **ftrace** | **merge-event** | **mts-events** | **pss-events** | **session-events** | **snmp-events** | **sys-events**}

Syntax Description

all	Enables debugging for all DPVM.
cfs-events	Enables debugging for Cisco Fabric Services (CFS).
change-events	Enables debugging for change events.
db-events	Enables debugging for database events.
errors	Enables debugging for error.
ftrace	Enables debugging for function trace.
merge-event	Enables debugging for merge events.
mts-events	Enables debugging for MTS events.
pss-events	Enables debugging for PSS events.
session-events	Enables debugging for session events.
snmp-events	Enables debugging for SNMP events.
sys-events	Enables debugging for system events.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

Examples

The following example displays the system output when the **debug dpvm all** command is issued.

```
switch# debug dpvm all
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show dpvm	Displays DPVM database information.

debug dstats

To enable delta statistics debugging, use the **debug dstats** command in EXEC mode. To disable a **debug** command use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug dstats {**error** | **flow**}

no debug dstats {**error** | **flow**}

Syntax Description

error	Enables debugging for delta statistics error conditions.
flow	Enables debugging for the delta statistics flow.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug dstats flow** command is issued:

```
switch# debug dstats flow
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug ethport

To enable Ethernet port debugging, use the **debug ethport** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug ethport {all | error |
event [**interface gigabitethernet** *slot*/*port* | **module** *slot*] |
ha [**interface gigibetethernet** *slot*/*port* | **module** *slot*] |
trace [**interface gigibetethernet** *slot*/*port* | **module** *slot*]**}**

no debug ethport {all | error |
event [**interface gigabitethernet** *slot*/*port* | **module** *slot*] |
ha [**interface gigibetethernet** *slot*/*port* | **module** *slot*] |
trace [**interface gigibetethernet** *slot*/*port* | **module** *slot*]**}**

Syntax Description

all	Enables debugging for all Ethernet port features.
error	Enables debugging for Ethernet port error conditions.
event	Enables debugging for Ethernet port events.
ha	Enables debugging for port high availability.
trace	Enables debugging for Ethernet port traces.
interface gigibetethernet *slot*/*port*	Specifies the slot and port of the Gigabit Ethernet interface.
module *slot*	Specifies the slot number of the module being debugged.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug ethport all** command is issued:

```
switch# debug ethport all
1981 May  5 07:28:59 ethport: fu_fsm_execute_all: match_msg_id(0), log_already_open(0)
1981 May  5 07:28:59 ethport: fu_fsm_execute_all: null fsm_event_list
1981 May  5 07:28:59 ethport: fu_fsm_engine_post_event_processing: mts msg
MTS_OPC_DEBUG_WRAP_MSG(msg_id 52343) dropped
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug exceptionlog

To enable the exception log debugging feature, use the **debug exceptionlog** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug exceptionlog {**demux** | **deque** | **error** | **flow** | **info**}

no debug exceptionlog {**demux** | **deque** | **error** | **flow** | **info**}

Syntax Description

demux	Enables debugging for the exception logger demux functions.
deque	Enables debugging for the exception logger deque function.
error	Enables debugging for exception logger errors.
flow	Enables debugging for the exception logger flow.
info	Enables debugging for exception logger information.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug exceptionlog** command is issued:

```
switch# debug exceptionlog
7), credit(3), empty
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug fabric-binding

To enable debugging for the fabric binding feature, use the **debug fabric-binding** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug fabric-binding {**all** | **efmd** {**db-events** | **errors** | **merge** {**errors** | **events** | **packets**}} | **mts-events** | **pss-events**} | **errors** [**vsan** *vsan-id*] | **events** [**vsan** *vsan-id*] | **mts-events** | **pss-events** | **snmp-events** | **trace** [**vsan** *vsan-id*]}

no debug fabric-binding {**all** | **efmd** {**db-events** | **errors** | **merge** {**errors** | **events** | **packets**}} | **mts-events** | **pss-events**} | **errors** [**vsan** *vsan-id*] | **events** [**vsan** *vsan-id*] | **mts-events** | **pss-events** | **snmp-events** | **trace** [**vsan** *vsan-id*]}

Syntax Description

all	Enables debugging for all fabric binding features.
efmd	Enables debugging for Exchange Fabric Membership Data (EFMD) protocol.
db-events	Enables debugging for EFMD protocol database events.
merge	Enables debugging for EFMD protocol merges.
packets	Enables debugging for EFMD protocol packets.
errors	Enables debugging for fabric binding errors.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
events	Enables debugging for fabric binding events.
mts-events	Enables debugging for fabric binding MTS events.
pss-events	Enables debugging for fabric binding PSS events.
snmp-events	Enables debugging for fabric binding SNMP events
trace	Enables debugging for fabric binding traces.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug fabric-binding all** command is issued:

```
switch# debug fabric-binding all
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show fabric-binding	Displays configured fabric binding information.

debug fc-tunnel

To enable debugging for the Fibre Channel tunnel feature, use the **debug fc-tunnel** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug fc-tunnel {**all** | **errors** | **external-events** | **ha** | **label-update** | **mts** {**pkt** | **pkthdr**} {**both** | **rx** | **tx**} | **pss** | **route-update** [**vsan** *vsan-id*] | **rsvp-messages** [**tunnel** *tunnel-id* | **vsan** *vsan-id*] | **state-machine**}

no debug fc-tunnel {**all** | **errors** | **external-events** | **ha** | **label-update** | **mts** {**pkt** | **pkthdr**} {**both** | **rx** | **tx**} | **pss** | **route-update** [**vsan** *vsan-id*] | **rsvp-messages** [**tunnel** *tunnel-id* | **vsan** *vsan-id*] | **state-machine**}

Syntax Description

all	Enables debugging for all FC tunnel features.
errors	Enables debugging for FC tunnel errors.
external-events	Enables debugging for external FC tunnel events.
ha	Enables debugging for FC tunnel high availability (HA) events.
label-update	Enables debugging for FC tunnel label updates.
mts	Enables debugging for FC tunnel MTS events.
pkt	Specifies debugging of packets.
pkthdr	Specifies debugging of headers.
both	Specifies debugging in both the transmit and receive directions.
tx	Specifies debugging in the transmit direction.
rx	Specifies debugging in the receive direction.
pss	Enables debugging for FC tunnel PSS events.
route-update	Enables debugging for FC tunnel route updates.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
rsvp-messages	Enables debugging for FC tunnel SNMP events
tunnel *tunnel-id*	Specifies the tunnel ID. The range is 1 to 255.
state-machine	Enables debugging for FC tunnel traces.
node	Specifies the node for the packets in the receive direction.
opcode	Specifies the opcode for the packets in the receive direction.
sap	Specifies the sap for the packets in the receive direction.
range	Specifies the integer range from 1 to 4096.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug fc-tunnel all** command is issued:

```
switch# debug fc-tunnel all
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show fc-tunnel	Display configured FC tunnel information.

debug fc2

To enable debugging for the FC2 feature, use the **debug fc2** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug fc2 {**credit** |
error [**fcid** *fcid* [**interface** {**fc** *slot/port* | **fcip** *port*} | **vsan** *vsan-id* [**interface** {**fc** *slot/port* | **fcip** *port*}]] | **interface** {**fc** *slot/port* | **fcip** *port*} | **vsan** *vsan-id* [**interface** {**fc** *slot/port* | **fcip** *port*}]]
flag |
flow [**fcid** *fcid* [**interface** {**fc** *slot/port* | **fcip** *port*} | **vsan** *vsan-id* [**interface** {**fc** *slot/port* | **fcip** *port*}]] | **interface** {**fc** *slot/port* | **fcip** *port*} | **vsan** *vsan-id* [**interface** {**fc** *slot/port* | **fcip** *port*}]] | (**interface fc** *type number* | **vsan** *vsan-id*) |
frame |
loopback |
pkt {**both** | **tx** | **rx**} [**bytes** *bytes* | **fcid** *fcid* [**bytes** *bytes* | **interface** {**fc** *slot/port* | **fcip** *port*} [**bytes** *bytes* | **pkts** *pkts* [**bytes** *bytes*]] | **pkts** *pkts* [**bytes** *bytes*] | **vsan** *vsan-id* [**bytes** *bytes* | **interface** {**fc** *slot/port* | **fcip** *port*} [**bytes** *bytes* | **pkts** *pkts* [**bytes** *bytes*]]] |
pkthdr {**both** | **tx** | **rx**} [**bytes** *bytes* | **fcid** *fcid* [**bytes** *bytes* | **interface** {**fc** *slot/port* | **fcip** *port*} [**bytes** *bytes* | **pkts** *pkts* [**bytes** *bytes*]] | **pkts** *pkts* [**bytes** *bytes*] | **vsan** *vsan-id* [**bytes** *bytes* | **interface** {**fc** *slot/port* | **fcip** *port*} [**bytes** *bytes* | **pkts** *pkts* [**bytes** *bytes*]]] |
rdl |
rxhdrhistory [**fcid** *fcid* [**interface** {**fc** *slot/port* | **fcip** *port*} | **vsan** *vsan-id* [**interface** {**fc** *slot/port* | **fcip** *port*}]] | **interface** {**fc** *slot/port* | **fcip** *port*} | **vsan** *vsan-id* [**interface** {**fc** *slot/port* | **fcip** *port*}]]
txhdrhistory [**fcid** *fcid* [**interface** {**fc** *slot/port* | **fcip** *port*} | **vsan** *vsan-id* [**interface** {**fc** *slot/port* | **fcip** *port*}]] | **interface** {**fc** *slot/port* | **fcip** *port*} | **vsan** *vsan-id* [**interface** {**fc** *slot/port* | **fcip** *port*}]]}

no debug fc2 {**credit** |
error [**fcid** *fcid* [**interface** {**fc** *slot/port* | **fcip** *port*} | **vsan** *vsan-id* [**interface** {**fc** *slot/port* | **fcip** *port*}]] | **interface** {**fc** *slot/port* | **fcip** *port*} | **vsan** *vsan-id* [**interface** {**fc** *slot/port* | **fcip** *port*}]]
flag |
flow [**fcid** *fcid* [**interface** {**fc** *slot/port* | **fcip** *port*} | **vsan** *vsan-id* [**interface** {**fc** *slot/port* | **fcip** *port*}]] | **interface** {**fc** *slot/port* | **fcip** *port*} | **vsan** *vsan-id* [**interface** {**fc** *slot/port* | **fcip** *port*}]] | (**interface fc** *type number* | **vsan** *vsan-id*) |
frame |
loopback |
pkt {**both** | **tx** | **rx**} [**bytes** *bytes* | **fcid** *fcid* [**bytes** *bytes* | **interface** {**fc** *slot/port* | **fcip** *port*} [**bytes** *bytes* | **pkts** *pkts* [**bytes** *bytes*]] | **pkts** *pkts* [**bytes** *bytes*] | **vsan** *vsan-id* [**bytes** *bytes* | **interface** {**fc** *slot/port* | **fcip** *port*} [**bytes** *bytes* | **pkts** *pkts* [**bytes** *bytes*]]] |
pkthdr {**both** | **tx** | **rx**} [**bytes** *bytes* | **fcid** *fcid* [**bytes** *bytes* | **interface** {**fc** *slot/port* | **fcip** *port*} [**bytes** *bytes* | **pkts** *pkts* [**bytes** *bytes*]] | **pkts** *pkts* [**bytes** *bytes*] | **vsan** *vsan-id* [**bytes** *bytes* | **interface** {**fc** *slot/port* | **fcip** *port*} [**bytes** *bytes* | **pkts** *pkts* [**bytes** *bytes*]]] |
rdl |
rxhdrhistory [**fcid** *fcid* [**interface** {**fc** *slot/port* | **fcip** *port*} | **vsan** *vsan-id* [**interface** {**fc** *slot/port* | **fcip** *port*}]] | **interface** {**fc** *slot/port* | **fcip** *port*} | **vsan** *vsan-id* [**interface** {**fc** *slot/port* | **fcip** *port*}]]
txhdrhistory [**fcid** *fcid* [**interface** {**fc** *slot/port* | **fcip** *port*} | **vsan** *vsan-id* [**interface** {**fc** *slot/port* | **fcip** *port*}]] | **interface** {**fc** *slot/port* | **fcip** *port*} | **vsan** *vsan-id* [**interface** {**fc** *slot/port* | **fcip** *port*}]]}

Syntax Description

credit	Enables FC2 credit debugging.
error	Enables FC2 error debugging.
fcid *fcid*	Restricts debugging to the specified FCID.
interface	Restricts debugging to the specified interface.
fc *slot/port*	Restricts debugging to the specified interface.
fcip *port*	Restricts debugging to the specified interface.
vsan *vsan-id*	Restricts debugging to the specified VSAN.
flag	Enables FC2 flags debugging.
flow	Enables FC2 flow debugging.
frame	Enables FC2 frame debugging.
loopback	Enables FC2 loopback debugging.
pkt	Enables FC packet debugging.
both	Enables debugging in both the transmit and receive directions.
tx	Enables debugging in the transmit direction,
rx	Enables debugging in the receive direction.
bytes *bytes*	Specifies the number of bytes to display.
pkts *pkts*	Specifies the number of packets to display.
pkthdr	Enables FC header debugging.
rdl	Enables FC2 RDL debugging.
rxhdrhistory	Enables FC2 received header history debugging.
txhdrhistory	Enables FC2 transmitted header history debugging.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

If FSPF receives a bad FC2 packet analyze the output of the **debug fc2 pkt** command.

Examples

The following example displays the system output when the **debug fc2 error vsan 1** command is issued:

```
switch1# debug fc2 error vsan 1
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show fc2	Displays FC2 information.

debug fc2d

To enable debugging for the FC2 feature, use the **debug fc2** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug fc2 {**all** | **bypass ficon_mgr** | **demux [vsan** *vsan-id*] | **deque** | **error** | **event [vsan** *vsan-id*] | **ha [vsan** *vsan-id*] | **trace [detail] [vsan** *vsan-id*] | **warning [vsan** *vsan-id*]}

no debug fc2 {**all** | **bypass ficon_mgr** | **demux [vsan** *vsan-id*] | **deque** | **error** | **event [vsan** *vsan-id*] | **ha [vsan** *vsan-id*] | **trace [detail] [vsan** *vsan-id*] | **warning [vsan** *vsan-id*]}

Syntax Description

all	Enables all FC2D debug flags.
bypass	Enables bypassing some components in fc2d execution.
ficon_mgr	Enables bypassing FICON Manager in fc2d execution.
demux	Enables debugging of FC2D message demux.
vsan *vsan-id*	Restricts debugging to the specified VSAN.
deque	Enables debugging of FC2D message dequeue.
error	Enables debugging of FC2D error.
event	Enables debugging of FC2D FSM and Events.
ha	Enables debugging of FC2D HA.
trace	Enables debugging of FC2D trace.
detail	Enables detailed debugging of FC2D trace.
warning	Enables debugging of FC2D warning.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug fc2d all** command is issued:

```
switch1# debug fc2d all
2004 Mar 29 22:57:25 fc2d: fu_fsm_execute_all: match_msg_id(0), log_already_open (0)
2004 Mar 29 22:57:25 fc2d: fu_fsm_execute_all: null fsm_event_list
2004 Mar 29 22:57:25 fc2d: fu_fsm_engine_post_event_processing: mts msg MTS_OPC_
DEBUG_WRAP_MSG(msg_id 6894921) dropped
```

Related Commands

Command	Description
debug all	Enables debugging for the FC2 feature.
no debug all	Disables all debugging.
show fc2	Displays FC2 information.

debug fcc

To enable debugging for the Fibre Channel Congestion (FCC) function, use the **debug fcc** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug fcc {**all** | **error** [**module** *slot*] | **event** [**module** *slot*] |
mts [pkt {**both** | **rx** [**node** *range* | **opcode** *range* | **sap** *range*] | **tx**} | **pkthdr** {**both** | **tx** | **rx** [**numpkt** *range*]}**]** | **trace** [**module** *slot*]}

no debug fcc {**all** | **error** [**module** *slot*] | **event** [**module** *slot*] |
mts {pkt {**both** | **rx** [**node** *range* | **opcode** *range* | **sap** *range*] | **tx**} | **pkthdr** {**both** | **tx** | **rx** [**numpkt** *range*]}**}** | **trace** [**module** *slot*]}

Syntax Description

all	Enables debugging for all FCC features.
errors	Enables debugging for FCC error conditions.
events	Enables debugging for FCC events.
mts	Enables debugging for FCC tx/rx MTS packets.
trace	Enables debugging for FCC traces.
module *slot*	Specifies the slot number of the module being debugged.
pkt	Enables debugging for FCC tx/rx FCC packets.
pkthdr	Enables debugging for FCC tx/rx FCC headers.
numpkt	Specifies the number of required packets
both	Specifies debugging in both the transmit and receive directions.
tx	Specifies debugging in the transmit direction,
rx	Specifies debugging in the receive direction.
node	Specifies the node for the packets in the receive direction.
opcode	Specifies the opcode for the packets in the receive direction.
sap	Specifies the sap for the packets in the receive direction.
range	Specifies the integer range from 1 to 4096.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug fcc all** command is issued:

```
switch# debug fcc all
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show fcc	Displays FCC settings.

debug fcdomain

To enable debugging for the fcdomain feature, use the **debug fcdomain** command in EXEC mode.To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug fcdomain {**all** | **critical** | **error** |
fc {**pkt** | **pkthdr**} {**both** | **rx** | **tx**} [**interface** *type number* [**vsan** *vsan-id*] | **vsan** *vsan-id*] |
ipc {**pkt** | **pkthdr**} {**both** | **rx** [**node** *range* | **opcode** *range* | **sap** *range*] | **tx**} |
memory | **notify** | **phase**}

no debug fcdomain {**all** | **critical** | **error** |
fc {**pkt** | **pkthdr**} {**both** | **rx** | **tx**} [**interface** *type number* [**vsan** *vsan-id*] | **vsan** *vsan-id*] |
ipc {**pkt** | **pkthdr**} {**both** | **rx** [**node** *range* | **opcode** *range* | **sap** *range*] | **tx**} |
memory | **notify** | **phase**}

Syntax Description

all	Enables debugging of all fcdomain parameters.
critical	Enables debugging of critical operations.
error	Enables debugging of error operation.
fc	Enables debugging of Fibre Channel packets and headers.
fcip	Enables debugging of Fibre Channel IP packets and headers.
port-channel	Enables debugging of PortChannel packets and headers.
pkt	Enables debugging of packets.
pkthdr	Enables debugging of headers.
both	Enables debugging in both the transmit and receive directions.
rx	Enables debugging in the receive direction.
interface *type number*	Specifies the interface to be debugged.
vsan *vsan-id*	Restricts debugging to the specified VSAN.
tx	Enables debugging in the transmit direction,
memory	Enables debugging of memory operations.
notify	Enables debugging of notifications
phase	Enables debugging of global phases

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug fcdomain critical** command is issued:

```
switch# debug fcdomain critical
Jan 27 07:04:31 fcdomain: Src: 0x00000501/6243  Dst: 0x00000501/14  ID: 0x0005BF
41  Size: 252 [REQ] Opc: 182 (MTS_OPC_DEBUG_WRAP_MSG) RR: 0x0005BF41  HA_SEQNO:
0x00000000  TS: 0x183C4D027F4A3
Jan 27 07:04:31 fcdomain: 00 00 00 00 68 00 00 00 00 00 00 00 00 00 00 00
Jan 27 07:04:31 fcdomain: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Jan 27 07:04:31 fcdomain: 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF
Jan 27 07:04:31 fcdomain: 2F 64 65 76 2F 70 74 73 2F 30 00 00 00 00 00 00
Jan 27 07:04:31 fcdomain: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
...
```

The following example displays the system output when the **debug fcdomain error** command is issued:

```
switch# debug fcdomain error
Jan 27 07:05:29 fcdomain: Src: 0x00000501/6245  Dst: 0x00000501/14  ID: 0x0005BF
7E  Size: 252 [REQ] Opc: 182 (MTS_OPC_DEBUG_WRAP_MSG) RR: 0x0005BF7E  HA_SEQNO:
0x00000000  TS: 0x183D5E63C081A
Jan 27 07:05:29 fcdomain: 00 00 00 00 64 00 00 00 00 00 00 00 00 00 00 00
Jan 27 07:05:29 fcdomain: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Jan 27 07:05:29 fcdomain: 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF
Jan 27 07:05:29 fcdomain: 2F 64 65 76 2F 70 74 73 2F 30 00 00 00 00 00 00
...
```

The following example displays the system output when the **debug fcdomain ipc pkthdr both** command is issued:

```
vegas2# debug fcdomain ipc pkthdr both
Apr  8 20:44:38 fcdomain: Src: 0x00000501/3883  Dst: 0x00000501/14  ID: 0x00038E
1D  Size: 252 [REQ] Opc: 182 (MTS_OPC_DEBUG_WRAP_MSG) RR: 0x00038E1D  HA_SEQNO:
0x00000000  TS: 0x5DD9B14EA3AA  REJ:0
Apr  8 20:44:38 fcdomain: 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00
Apr  8 20:44:38 fcdomain: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr  8 20:44:38 fcdomain: 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF
Apr  8 20:44:38 fcdomain: 2F 64 65 76 2F 70 74 73 2F 30 00 00 00 00 00 00
Apr  8 20:44:38 fcdomain: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr  8 20:44:38 fcdomain: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
...
Apr  8 20:44:38 fcdomain: Src: 0x00000501/3883  Dst: 0x00000501/14  ID: 0x00038E
20  Size: 252 [REQ] Opc: 182 (MTS_OPC_DEBUG_WRAP_MSG) RR: 0x00038E20  HA_SEQNO:
0x00000000  TS: 0x5DD9B186CCEB  REJ:0
Apr  8 20:44:38 fcdomain: 00 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00
Apr  8 20:44:38 fcdomain: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr  8 20:44:38 fcdomain: 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF
Apr  8 20:44:38 fcdomain: 2F 64 65 76 2F 70 74 73 2F 30 00 00 00 00 00 00
Apr  8 20:44:38 fcdomain: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr  8 20:44:38 fcdomain: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
...
```

Related Commands

Command	Description
show fcdomain domain-list	Displays current domains in the fabric.
fcdomain	Enables fcdomain features.

debug fcfwd

To enable debugging for the Fibre Channel forwarding feature, use the **debug fcfwd** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug fcfwd {**flogimap** | **idxmap** | **pcmap** | **sfib** | **spanmap**} {**error** | **event** | **trace**} [**module** *slot* | **vsan** *vsan-id* [**module** *slot*]]

no debug fcfwd {**flogimap** | **idxmap** | **pcmap** | **sfib** | **spanmap**} {**error** | **event** | **trace**} [**module** *slot* | **vsan** *vsan-id* [**module** *slot*]]

Syntax Description

flogimap	Enables flogimap debugging.
idxmap	Enables idxmap debugging.
pcmap	Enables pcmap debugging.
sfib	Enables sfib debugging.
spanmap	Enables spanmap debugging.
error	Enables debugging for FCC error conditions.
event	Enables debugging for FCC events.
trace	Enables debugging for FCC traces.
module *slot*	Specifies the slot number of the module being debugged.
vsan *vsan-id*	Restricts debugging to the specified VSAN.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug fcfwd error** command is issued:

```
switch# debug fcfwd error
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show fcfwd	Displays the configured fcfwd tables and statistics.

debug fcns

To enable debugging for name server registration, use the **debug fcns** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug fcns {**all** | **errors** | **events** {**mts** | **query** | **register**}} [**vsan** *vsan-id*]

no debug fcns {**all** | **errors** | **events** {**mts** | **query** | **register**}} [**vsan** *vsan-id*]

Syntax Description

all	Enables debugging for all name server features.
errors	Enables debugging for name server error conditions.
events	Enables debugging for name server events.
mts	Enables debugging for name server tx/rx MTS packets.
query	Enables debugging for name server tx/rx CDP packets.
register	Enables debugging for name server PSS related events.
vsan *vsan-id*	Restricts debugging to the specified VSAN.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug fcns events register vsan 99** command is issued:

```
switch# debug fcns events register vsan 99
Feb 17 04:42:54 fcns: vsan 99: Got Entry for port-id 27800
Feb 17 04:42:54 fcns: vsan 99: Registered port-name 36a4078be0000021 for port-id 780200
Feb 17 04:42:54 fcns: vsan 99: Registered node-name 36a4078be0000020 for port-id 780200
...
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show fcns database	Displays the results of the discovery or the name server database for a specified VSAN or for all VSANs.
show fcns statistics	Displays the statistical information for a specified VSAN or for all VSANs.

debug fcs

To enable debugging for the fabric configuration server, use the **debug fcs** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug fcs {**all** | **discovery events** | **errors** [**vsan** *vsan-id*] | **ess-events** [**vsan** *vsan-id*] | **mts events** {**brief** | **detail**} | **pss events** | **queries events** [**vsan** *vsan-id*] | **registrations events** [**vsan** *vsan-id*] | **rscn events** [**vsan** *vsan-id*] | **snmp events**}

no debug fcs {**all** | **discovery events** | **errors** [**vsan** *vsan-id*] | **ess-events** [**vsan** *vsan-id*] | **mts events** {**brief** | **detail**} | **pss events** | **queries events** [**vsan** *vsan-id*] | **registrations events** [**vsan** *vsan-id*] | **rscn events** [**vsan** *vsan-id*] | **snmp events**}

Syntax Description

all	Enables debugging for all FCS features.
discovery events	Enables debugging for FCS discovery events.
errors	Enables debugging for FCS error conditions.
mts events	Enables debugging for FCS tx/rx MTS events.
pss events	Enables debugging for FCS
brief	Provides brief information for each event.
detail	Provides detailed information for each event.
queries events	Enables debugging for FCS tx/rx events.
registration events	Enables debugging for FCS PSS related events.
rscn events	Enables debugging for FCS RSCN events.
snmp events	Enables debugging for FCS SNMP events.
vsan *vsan-id*	Restricts debugging to the specified VSAN.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug fcs all** command is issued:

```
switch# debug fcs all
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show fcs	Displays the status of the fabric configuration.

debug fcsp-mgr

To enable debugging for the Fibre Channel Security Protocol (FC-SP) manager, use the **debug fcsp-mgr** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug fcsp-mgr {**all** | **critical** | **datastructure** | **dhchap** | **error** | **event-gen** | **fc2** | **fsm** | **general** | **ha** | **init** | **level1** | **level2** | **level3** | **level4** | **level5** | **message** | **mts** | **notify** | **trace**}

no debug fcsp-mgr {**all** | **critical** | **datastructure** | **dhchap** | **error** | **event-gen** | **fc2** | **fsm** | **general** | **ha** | **init** | **level1** | **level2** | **level3** | **level4** | **level5** | **message** | **mts** | **notify** | **trace**}

Syntax Description

all	Enables debugging for all FC-SP features.
critical	Enables debugging of FC-SP critical errors.
datastructure	Enables debugging of FC-SP data structures.
dhchap	Enables debugging of DHCHAP.
error	Enables debugging of FC-SP error.
event-gen	Enables debugging of FC-SP event generation.
fc2	Enables debugging of FC-SP FC2 messages.
fsm	Enables debugging of FC-SP events.
general	Enables general debugging of FC-SP.
ha	Enables debugging of FC-SP High Availability
init	Enables debugging of FC-SP Initialization.
level1	Sets debugging level of FC-SP Mgr to 1.
level2	Sets debugging level of FC-SP Mgr to 2.
level3	Sets debugging level of FC-SP Mgr to 3.
level4	Sets debugging level of FC-SP Mgr to 4.
level5	Set debugging level of FC-SP Mgr to 5.
message	Enables debugging of FC-SP messages.
mts	Enables debugging of FC-SP MTS messages.
notify	Sets debug level to notify.
trace	Enables debugging of FC-SP function enter/exit.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug fcsp-mgr all** command is issued:

```
switch# debug fcsp-mgr all
2004 Mar 29 23:33:56 fcsp-mgr: fu_fsm_execute_all: match_msg_id(0), log_already_open(0)
2004 Mar 29 23:33:56 fcsp-mgr: fu_fsm_execute_all: null fsm_event_list
2004 Mar 29 23:33:56 fcsp-mgr: fu_fsm_engine_post_event_processing: mts msg MTS_
OPC_DEBUG_WRAP_MSG(msg_id 7061762) dropped
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show fcsp	Displays the status of the FC-SP configuration

debug fdmi

To enable debugging for the Fabric-Device Management Interface (FDMI) feature, use the **debug fdmi** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug fdmi {**all** | **errors** | **fdmi-messages** [**vsan** *vsan-id*] | **ha** | **mts** {**pkt** {**both** | **rx** [**node** *range* | **opcode** *range* | **sap** *range*] | **tx**} | **pkthdr** {**both** | **tx** | **rx** [**numpkt** *range*]}} | **pss** | **trace**}

no debug fdmi {**all** | **errors** | **fdmi-messages** [**vsan** *vsan-id*] | **ha** | **mts** {**pkt** {**both** | **rx** [**node** *range* | **opcode** *range* | **sap** *range*] | **tx**} | **pkthdr** {**both** | **tx** | **rx** [**numpkt** *range*]}} | **pss** | **trace**}

Syntax Description

all	Enables debugging for all FDMI features.
errors	Enables debugging for FDMI error conditions.
fdmi-messages	Enables the dump of FDMI PDUs.
ha	Enables the dump of HA synchronization messages.
mts	Enables debugging for FDMI tx/rx MTS events.
pkt	Enables debugging for FCC tx/rx FCC packets.
both	Specifies debugging in both the transmit and receive directions.
tx	Specifies debugging in the transmit direction,
rx	Specifies debugging in the receive direction.
node	Specifies the node for the packets in the receive direction.
range	Specifies the integer range from 1 to 4096.
opcode	Specifies the opcode for the packets in the receive direction.
sap	Specifies the sap for the packets in the receive direction.
pkthdr	Enables debugging for FCC tx/rx FCC headers.
numpkt	Specifies the number of required packets
pss	Enables debugging for FDMI PSSs.
trace	Restricts debugging for FDMI traces.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug fdmi all** command is issued:

```
switch# debug fdmi all
2005 Mar 10 02:37:28 fdmi: 00 00 00 02 00 00 00 1C 04 19 65 08 00 82 39 08
2005 Mar 10 02:37:28 fdmi: C4 16 65 08 44 19 65 08 E4 87 39 08 04 17 65 08
2005 Mar 10 02:37:28 fdmi: 84 19 65 08 4C 8D 39 08 44 17 65 08 C4 19 65 08
2005 Mar 10 02:37:28 fdmi: B4 92 39 08 00 17 65 08 04 1A 65 08 1C 98 39 08
2005 Mar 10 02:37:28 fdmi: C4 17 65 08 44 1A 65 08 84 9D 39 08 04 18 65 08
2005 Mar 10 02:37:28 fdmi: 84 1A 65 08 EC A2 39 08 44 18 65 08 C4 1A 65 08
2005 Mar 10 02:37:28 fdmi: 54 A8 39 08 84 18 65 08 04 1B 65 08 BC AD 39 08
2005 Mar 10 02:37:28 fdmi: 00 00 00 02 00 00 0B B8 00 00 00 00 00 00 00 00
2005 Mar 10 02:37:28 fdmi: 00 00 00 00 00 00 00 00 00 00 00 00
2005 Mar 10 02:37:28 fdmi: Src: 0x00000601/27  Dst: 0x00000601/105  ID: 0x0069E217  Size:
140 [REQ] Opc: 7804 (MTS_OPC_FDMI_SNMP) RR: 0x0069E217  HA_SEQNO: 0x00000000  TS:
0x25218CC5A40E3  REJ:0  SYNC:0
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show fdmi	Displays the FDMI database information.

debug ficon

To enable debugging for the FI-bre CON-nection (FICON) interface capabilities, use the **debug ficon** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug ficon {**all** | **bypass** {**acl** | **esa** | **file** | **pm** | **postcheck** | **precheck**} |
control-device {**all** | **bypass ficon_mgr** | **demux** [**vsan** *vsan-id*] | **deque** | **error** | **event** [**vsan** *vsan-id*] | **ficon_mgr** | **ha** [**vsan** *vsan-id*] | **demux** [**vsan** *vsan-id*] | **sb3** {**error** | **flow**} **trace** **[detail]** [**vsan** *vsan-id*] | **warning** [**vsan** *vsan-id*]} |
error | **event** | **file-trace** | **ha** | **max-port-number** *ports* | **pss-trace** |
stat {**all** | **demux** [**vsan** *vsan-id*] | **deque** | **error** | **event** [**vsan** *vsan-id*] | **ha** [**vsan** *vsan-id*] | **trace** [**detail**] [**vsan** *vsan-id*] | **warning** [**vsan** *vsan-id*]} |
timer | **trace**}

no debug ficon {**all** | **bypass** {**acl** | **esa** | **file** | **pm** | **postcheck** | **precheck**} |
control-device {**all** | **bypass ficon_mgr** | **demux** [**vsan** *vsan-id*] | **deque** | **error** | **event** [**vsan** *vsan-id*] | **ficon_mgr** | **ha** [**vsan** *vsan-id*] | **demux** [**vsan** *vsan-id*] | **sb3** {**error** | **flow**} **trace** **[detail]** [**vsan** *vsan-id*] | **warning** [**vsan** *vsan-id*]} |
error | **event** | **file-trace** | **ha** | **max-port-number** *port* | **pss-trace** |
stat {**all** | **demux** [**vsan** *vsan-id*] | **deque** | **error** | **event** [**vsan** *vsan-id*] | **ha** [**vsan** *vsan-id*] | **trace** [**detail**] [**vsan** *vsan-id*] | **warning** [**vsan** *vsan-id*]} |
timer | **trace**}

Syntax Description

all	Enables debugging for all FICON features.
bypass	Enables bypass flags for FICON error conditions.
acl	Bypass ACL manager execution.
esa	Bypass ESA execution.
file	Bypass file operations execution.
pm	Bypass port manager execution.
postcheck	Bypass post check execution for VSAN enable.
precheck	Bypass precheck execution for VSAN enable.
control-device	Enables the dump of FICON control devices.
all	Specifies all debug flags of FICON control device.
bypass ficon_mgr	Bypass FICON Manager.
demux	Configure debugging of FICON control device message demux.
deque	Configure debugging of FICON control device message deque.
error	Configure debugging of FICON control device error.
event	Configure debugging of FICON control device FSM and Events.
ficon_mgr	Configure debugging of FICON manager control device.
ha	Configure debugging of FICON control device HA.
sb3	Configure debugging of SB3 library.
trace	Configure debugging of FICON control device trace.
warning	Configure debugging of FICON control device warning.
error	Enables debugging for FICON errors.

event	Enables debugging for FICON events.
file-trace	Enables debugging of FICON file flow
ha	Enables the debugging of HA synchronization messages.
max-port-number *ports*	Specifies maximum number of ports.
pss-trace	Enables debugging of FICON PSS flow.
stat	Enables debugging of FICON statistics.
all	Specifies all debug flags of FICON statistics.
demux	Specifies FICON statistics message demux.
deque	Specifies FICON statistics message deque.
error	Specifies FICON statistics errors.
event	Specifies FICON statistics FSM and events.
ha	Specifies FICON statistics HA.
trace	Specifies FICON statistics trace.
warning	Specifies FICON statistics warnings
timer	Enables debugging of FICON timer messages.
trace	Enables debugging of FICON flow.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(2)	This command was introduced.

Usage Guidelines

FICON must be enabled on the switch to use this command.

Examples

The following example displays the system output when the **debug ficon all** command is issued:

```
switch# debug ficon all
2005 Mar 10 02:38:58 ficon: fu_fsm_execute_all: match_msg_id(0), log_already_open(0)
2005 Mar 10 02:38:58 ficon: fu_fsm_execute_all: null fsm_event_list
2005 Mar 10 02:38:58 ficon: fu_fsm_engine_post_event_processing: mts msg
MTS_OPC_DEBUG_WRAP_MSG(msg_id 6943776) dropped
switch# undebug all
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show ficon	Displays configured FICON information.

debug flogi

To enable debugging for the fabric login (FLOGI) feature, use the **debug flogi** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug flogi {**action** [**interface** *type number* | **vsan** *vsan-id*] |
all |
bypass {**acl** | **dm** | **dpvm** | **fcsp** | **lcp** | **npiv** | **ns** | **pl** | **pm** | **pmvc** | **rib**| **vsan_mgr** | **zs**} |
demux [**interface** *type number* | **vsan** *vsan-id*] |
error |
event [**interface** *type number* | **vsan** *vsan-id*] |
ha [**interface** *type number* | **vsan** *vsan-id*] |
init [**interface** *type number* | **vsan** *vsan-id*] |
timers [**interface** *type number* | **vsan** *vsan-id*] |
trace [**interface** *type number* | **vsan** *vsan-id*] |
warning}

Syntax Description

action	Enables all FLOGI debug features.
all	Enables all FLOGI debug options.
bypass	Bypass some components in FLOGI execution.
acl	Bypass ACL execution.
dm	Bypass domain manager execution.
dpvm	Bypass DPVM execution.
fcsp	Bypass FCSP execution.
lcp	Bypass LCP execution.
npiv	Bypass NPIV execution.
ns	Bypass name server execution.
pl	Bypass port lock execution.
pm	Bypass port manager execution.
pmvc	Bypass PM VSAN change execution.
rib	Bypass RIB execution.
vsan_mgr	Bypass VSAN manager execution.
zs	Bypass zone server execution.
demux	Enables FLOGI demux
error	Enables debugging for FLOGI error conditions.
event	Enables debugging for FLOGI FSMs and events.
ha	Enables debugging for FLOGI high availability.
init	Enables debugging of FLOGI addition, deletion, and initialization.
timer	Enables debugging for FLOGI message timers
trace	Enables debugging for FLOGI traces.
warning	Enables debugging for FLOGI warnings.
interface *type number*	Restricts debugging to the specified interface.
vsan *vsan-id*	Restricts debugging to the specified VSAN.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug flogi all** command is issued:

```
switch# debug flogi all
Apr  9 22:44:08 flogi: fs_demux: msg consumed by sdwrap_process msg
Apr  9 22:44:08 flogi: fu_fsm_execute_all: match_msg_id(0), log_already_open(0)
Apr  9 22:44:08 flogi: fu_fsm_execute_all: null fsm_event_list
Apr  9 22:44:08 flogi: fu_fsm_engine: mts msg MTS_OPC_DEBUG_WRAP_MSG(msg_id 67690) dropped
```

The following example displays the system output when the **debug flogi event** command is issued:

```
switch# debug flogi event
Apr 10 00:07:16 flogi: fu_fsm_execute_all: match_msg_id(0), log_already_open(0)
Apr 10 00:07:16 flogi: fu_fsm_execute_all: null fsm_event_list
Apr 10 00:07:16 flogi: fu_fsm_engine: mts msg MTS_OPC_DEBUG_WRAP_MSG(msg_id 71314) dropped
```

The following example displays the system output when the **debug flogi trace** command is issued:

```
switch# debug flogi trace
Apr 10 00:42:36 flogi: fs_genport_vsan_hash_fn: key: 0x1 index: 0x1
Apr 10 00:42:36 flogi: fs_mts_hdlr_fs_flogo: FLOGI HOLD(0x8122144) refcnt:3
Apr 10 00:42:36 flogi: fs_clear_all_outstanding_responses_for_flogi: FLOGI FREE(
a07e00300500252b) refcnt:3
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show flogi database	Displays all the FLOGI sessions through all interfaces across all VSANs.

debug fm

To enable feature manager debugging, use the **debug fm** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug fm {**error** | **flow**}

no debug fm {**error** | **flow**}

Syntax Description

error	Enables debugging for feature manager error conditions.
flow	Enables debugging for the feature manager flow.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug fm flow** command is issued:

```
switch# debug fm flow
switch# 2005 Mar 10 02:40:19 feature-mgr: fm_event_loop: ----------- EVENT START
2005 Mar 10 02:40:19 feature-mgr: fm_event_loop: received MTS message:
2005 Mar 10 02:40:19 feature-mgr: fm_event_loop: Src: 0x00000601/27  Dst: 0x00000601/121
ID: 0x006A0FC4  Size: 160 [REQ] Opc: 8922 (MTS_OPC_FM_CMI_GET_FEATURE_OP) RR: 0x006A0FC4
HA_SEQNO: 0x00000000  TS: 0x2524B48D52B53  REJ:0  SYNC:0
2005 Mar 10 02:40:19 feature-mgr: fm_handle_cmi_get_feature_op: Get feature (1) op request
2005 Mar 10 02:40:19 feature-mgr: fm_handle_cmi_get_feature_op: Reply to get feature ivr
op request: op 2, op_state 0, result 0x0 (success)
2005 Mar 10 02:40:19 feature-mgr: fm_event_loop: ----------- EVENT START
2005 Mar 10 02:40:19 feature-mgr: fm_event_loop: received MTS message:
2005 Mar 10 02:40:19 feature-mgr: fm_event_loop: Src: 0x00000601/27  Dst: 0x00000601/121
ID: 0x006A0FC6  Size: 160 [REQ] Opc: 8922 (MTS_OPC_FM_CMI_GET_FEATURE_OP) RR: 0x006A0FC6
HA_SEQNO: 0x00000000  TS: 0x2524B48EBF55D  REJ:0  SYNC:0
2005 Mar 10 02:40:19 feature-mgr: fm_handle_cmi_get_feature_op: Get feature (1) op request
2005 Mar 10 02:40:19 feature-mgr: fm_handle_cmi_get_feature_op: Reply to get feature ivr
op request: op 2, op_state 0, result 0x0 (success)
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug fspf

To enable debugging for the FSPF feature, use the **debug fspf** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug fspf {**all** [**interface** *type number*] [**vsan** *vsan-id*] |
database [**interface** *type number*] [**vsan** *vsan-id* |
error |
event [**interface** *type number*] [**vsan** *vsan-id*] |
fc {**pkt** | **pkthdr**} {**both** | **tx** | **rx**} [**interface** *type number*] [**vsan** *vsan-id*] |
flood [**interface** *type number*] [**vsan** *vsan-id*] |
ha [**interface** *type number*] [**vsan** *vsan-id*] |
mts {pkt {**both** | **rx** [**node** *range* | **opcode** *range* | **sap** *range*] | **tx**} | **pkthdr** {**both** | **rx** [**numpkt** *range*] | **tx**}**}** |
retrans [**interface** *type number*] [**vsan** *vsan-id*] |
route |
timer}

no debug fspf {**all** [**interface** *type number*] [**vsan** *vsan-id*] |
database [**interface** *type number*] [**vsan** *vsan-id* |
error |
event [**interface** *type number*] [**vsan** *vsan-id*] |
fc {**pkt** | **pkthdr**} {**both** | **tx** | **rx**} [**interface** *type number*] [**vsan** *vsan-id*] |
flood [**interface** *type number*] [**vsan** *vsan-id*] |
ha [**interface** *type number*] [**vsan** *vsan-id*] |
mts {pkt {**both** | **rx** [**node** *range* | **opcode** *range* | **sap** *range*] | **tx**} | **pkthdr** {**both** | **rx** [**numpkt** *range*] | **tx**}**}** |
retrans [**interface** *type number*] [**vsan** *vsan-id*] |
route |
timer}

Syntax Description

all	Enables debugging for all FSPF features.
database	Enables debugging for the FSPF database.
error	Enables debugging for FSPF error conditions.
events	Enables debugging for FSPF events.
fc	Enables debugging of Fibre Channel packets and headers.
fc-tunnel	Enables debugging of Fibre Channel tunnel interface.
fcip	Enables debugging of Fibre Channel IP packets and headers.
fv	Enables debugging of Fibre Channel Virtualization interface.
gigbitethernet *slot/port*	Specifies the Gigabit Ethernet interface slot and port.
ipc	Enables debugging of IPC packets and headers.
mgmt 0	Specifies the management interface.
port-channel	Enables debugging of PortChannel packets and headers.
sup-fc	Enables debugging of inband Interface.
pkt	Enables debugging for FCC tx/rx FCC packets.
both	Specifies debugging in both the transmit and receive directions.

tx	Specifies debugging in the transmit direction,
rx	Specifies debugging in the receive direction.
node	Specifies the node for the packets in the receive direction.
range	Specifies the integer range from 1 to 4096.
opcode	Specifies the opcode for the packets in the receive direction.
sap	Specifies the sap for the packets in the receive direction.
pkthdr	Enables debugging for FCC tx/rx FCC headers.
numpkt	Specifies the number of required packets
flood	Enables debugging for FSPF flooding events.
ha	Enables debugging for FSPF high availability.
mts	Enables debugging for FSPF tx/rx MTS events.
retrans	Enables debugging for FSPF retransmits.
route	Enables debugging for FSPF route computation.
timer	Enables debugging for FSPF timers.
interface *type number*	Restricts debugging to the specified interface.
vsan *vsan-id*	Restricts debugging to the specified VSAN.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

If you receive bad packets on an interface, use the **debug fc pkt** command.

If you receive an error in processing a packet on an interface in VSAN, turn on **debug fspf error** to get more information. Make sure there is no misconfiguration of FSPF parameters on the two ends of the interface. Also issue the **debug fspf fc pkt** command for the specific interface.

If you receive an error in flooding the local LSR in a VSAN issue the **debug fspf flood** and **debug fspf error** commands. If error is reported in transmitting packet check if interface is up and turn on **debug fc2 error**.

If you receive an error in processing a timer event for the interface in a VSAN, issue the **debug fspf error** command.

If you receive an error in processing due to a wrong MTS message, use the **debug fspf mts pkt** and **debug fspf error** commands.

If you receive an error when interacting with RIB, use the **debug fspf route** command along with the RIB debug traces.

If you receive an error in computing routes for VSANs, issue the **debug fspf error** and the **debug fspf route** commands.

If you receive an error due to the interface being stuck in a state other than FULL, use the **debug fspf event** and **debug fspf fc pkt** commands on the interfaces involved.

Examples

The following example displays the system output when the **debug fspf all** command is issued:

```
switch1# debug fspf all
Apr 5 11:50:01 fspf: Wrong hello interval for packet on interface 100f000 in VSAN 1
Apr 5 11:50:04 fspf: Error in processing hello packet , error code = 4
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show fspf	Displays global FSPF information.

debug hardware arbiter

To configures debugging for the hardware arbiter driver, use the **debug hardware arbiter** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug hardware arbiter {**error** | **flow**} [**group** *number*]}

no debug hardware arbiter {**error** | **flow**} [**group** *number*]}

Syntax Description

error	Enables debugging for hardware arbiter kernel errors.
flow	Enables debugging for hardware arbiter kernel flow.
group *number*	Restricts debugging to the specified group. The range is 0 to 17.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug hardware arbiter error group** command is issued:

```
switch# debug hardware arbiter error group 1
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show hardware	Displays switch hardware inventory details.

debug idehsd

To enable IDE hot swap handler debugging, use the **debug idehsd** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug idehsd {**cmd dbglevel** [*debug-level*] | **error** | **flow**}

no debug idehsd {**cmd dbglevel** [*debug-level*] | **error** | **flow**}

Syntax Description

cmd dbglevel	Enables debugging for the IDE hot swap handler.
debug-level	Specifies the debug level (0 to 8).
error	Enables debugging for IDE hot swap handler error conditions.
flow	Enables debugging for IDE hot swap handler flow.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug idehsd cmd dbglevel** command is issued:

```
switch# debug idehsd cmd dbglevel 5
set debug level to 5 succeeded
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug ike

To enable debugging for the IKE protocol, use the **debug ike** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug ike {**all** | **error** | **event** | **message** | **mts** | **protocol** | **verbose** | **warning**}

no debug ike {**all** | **error** | **event** | **message** | **mts** | **protocol** | **verbose** | **warning**}

Syntax Description

all	Enables all of the debugging flags for IKE.
error	Enables debugging for IKE errors.
event	Enables debugging for IKE event generation.
message	Enables debugging for IKE messages.
mts	Enables debugging for MTS-related IKE activity.
protocol	Enables debugging for IKE protocol-related handling.
verbose	Enables verbose debugging for IKE protocol-related handling.
warning	Enables debugging for IKE warnings.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, IKE must be enabled using the **crypto ike enable** command.

Examples

The following example displays the system output when the **debug ike all** command is issued.

```
switch# debug ike all
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show crypto ike domain ipsec	Displays IKE protocol information.

debug ilc_helper

To enable ILC helper debugging, use the **debug ilc_helper** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug ilc_helper {**all** | **errors** | **events** | **info**}

no debug ilc_helper {**all** | **errors** | **events** | **info**}

Syntax Description

all	Enables debugging for all ILC helper features.
errors	Enables debugging for ILC helper error conditions.
events	Enables debugging for the ILC helper events.
info	Enables debugging for ILC helper information.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug ilc_helper all** command is issued:

```
switch# debug ilc_helper all
For Application :125, sdwrap:mts_send : Broken pipe
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug ipacl

To enable IP access control list (ACL) debugging, use the **debug ipacl** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug ipacl {**all** | **error** | **event** | **trace**}

no debug ipacl {**all** | **error** | **event** | **trace**}

Syntax Description

all	Enables debugging for all IP ACL features.
error	Enables debugging for IP ACL error conditions.
event	Enables debugging for the IP ACL events.
trace	Enables debugging for IP ACL trace.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug ipacl all** command is issued:

```
switch# debug ipacl all
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show ip access-list	Displays the IP access control lists that are currently active.

debug ipconf

To enable IP configuration debugging, use the **debug ipconf** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug ipconf {**all** | **errors** | **events** | **info** | **pss**}

no debug ipconf {**all** | **errors** | **events** | **info** | **pss**}

Syntax Description

all	Enables debugging for all IP configuration features.
errors	Enables debugging for IP configuration error conditions.
events	Enables debugging for IP configuration tx/rx MTS events.
info	Enables debugging for IP configuration information.
pss	Enables debugging for IP configuration PSS operations.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug ipconf all** command is issued:

```
switch# debug ipconf all
switch# 2005 Mar 10 02:45:30 ipconf: Received MTS message
2005 Mar 10 02:45:30 ipconf: MTS message received opcode 862 source 0x00000601/27
2005 Mar 10 02:45:30 ipconf: Getting ip addresses on interface 5000000
2005 Mar 10 02:45:30 ipconf: Received MTS message
2005 Mar 10 02:45:30 ipconf: MTS message received opcode 862 source 0x00000601/27
2005 Mar 10 02:45:30 ipconf: Getting ip addresses on interface 5000000
2005 Mar 10 02:45:30 ipconf: Received MTS message
2005 Mar 10 02:45:30 ipconf: MTS message received opcode 862 source 0x00000601/27
2005 Mar 10 02:45:30 ipconf: Getting ip addresses on interface 5000000
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug ipfc

To enable IP over Fibre Channel (IPFC) debugging, use the **debug ipfc** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug ipfc {**all** | **errors** | **events** | **info** | **kernel** {**errors** | **events**}}

Syntax Description

all	Enables debugging for all IPFC features.
errors	Enables debugging for IPFC error conditions.
events	Enables debugging for IPFC tx/rx MTS events.
info	Enables debugging for IPFC information.
kernel	Enables debugging for IPFC kernel operations.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug ipfc kernel errors** command is issued:

```
switch# debug ipfc kernel errors
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug ips

To enable debugging for the IP Storage Services (IPS) module, use the **debug ips** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug ips {**acl** {**flow** | **flow-detail**} | **all** | **demux** | **error** | **flow** {**ethernet** | **fcip**} | **fsm** | **ha** | **init** | **iscsi** {**config** | **config-detail** | **flow** | **flow-detail** | **msgs**} | **islb** {**cfs** {**config** | **config-detail** | **error** | **flow** | **flow-detail**} | **config** | **config-detail** | **flow** | **flow-detail** | **vrrp** {**error** | **flow** | **flow-detail**}} | **isns** {**config** | **config-detail** | **error** | **flow** | **flow-detail** | **msgs** | **packet**} | **show_all** | **upgrade**}

no debug ips {**acl** {**flow** | **flow-detail**} | **all** | **demux** | **error** | **flow** {**ethernet** | **fcip**} | **fsm** | **ha** | **init** | **iscsi** {**config** | **config-detail** | **flow** | **flow-detail** | **msgs**} | **islb** {**cfs** {**config** | **config-detail** | **error** | **flow** | **flow-detail**} | **config** | **config-detail** | **flow** | **flow-detail** | **vrrp** {**error** | **flow** | **flow-detail**}} | **isns** {**config** | **config-detail** | **error** | **flow** | **flow-detail** | **msgs** | **packet**} | **show_all** | **upgrade**}

Syntax Description

acl	Enables debugging for ACLs.
flow	Enables debugging for the IPS flow.
flow-detail	Enables detailed debugging for the IPS flow.
all	Enables all IPS debug options.
demux	Enables debugging for IPS demux
error	Enables debugging for IPS error conditions.
ethernet	Restricts debugging to the Ethernet flow
fcip	Restricts debugging to the FCIP flow
fsm	Enables debugging for IPS FSM and events.
ha	Enables debugging for IPS high availability.
init	Enables debugging of IPS addition, deletion, and initialization.
iscsi	Enables debugging of iSCSI.
config	Enables debugging of the iSCSI configuration.
config-detail	Enables detailed debugging of the iSCSI configuration.
msgs	Enables debugging of the iSCSI messages received and responded.
islb	Enables debugging of iSLB.
cfs	Enables debugging of iSLB CFS.
config	Enables debugging of the iSLB CFS configuration.
config-detail	Enables detailed debugging of the iSLB CFS configuration.
error	Enables debugging of iSLB CFS error conditions.
flow	Enables debugging for the iSLB CFS flow.
flow-detail	Enables detailed debugging for the iSLB CFS flow.
config	Enables debugging of the iSLB configuration.
config-detail	Enables detailed debugging of the iSLB configuration.
flow	Enables debugging for the iSLB flow.
flow-detail	Enables detailed debugging for the iSLB flow.

vrrp	Enables debugging of iSLB VRRP.
config	Enables debugging of the iSNS configuration.
config-detail	Enables detailed debugging of the iSNS configuration.
error	Enables debugging of iSNS error conditions.
flow	Enables debugging for the iSNS flow.
flow-detail	Enables detailed debugging for the iSNS flow.
msgs	Enables debugging of the iSNS messages received and responded.
packet	Enables debugging of an iSNS packet.
show_all	Enables all debugging IPS manager flags.
upgrade	Enables debugging for upgrade.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.
3.0(1)	Added the **iSLB** and **iSNS** options.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug ips show_all** command is issued:

```
switch# debug ips show_all
IPS Manager:
iSCSI Trace Detail debugging is on
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show ips stats	Displays IP storage statistics.
show ips status	Displays the IP storage status.

debug ipsec

To enable debugging for IPsec, use the **debug ipsec** command in EXEC mode.To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug ipsec {**all** | **bypass ficon_mgr** | **config** | **config-detail** | **demux** | **deque** | **error** | **event** | **flow** | **flow-detail** | **ha** | **trace** [**detail**] | **warning**}

no debug ipsec {**all** | **bypass ficon_mgr** | **config** | **config-detail** | **demux** | **deque** | **error** | **event** | **flow** | **flow-detail** | **ha** | **trace** [**detail**] | **warning**}

Syntax Description

all	Enables all IPsec debugging.
bypass ficon_mgr	Bypasses the FICON manager.
config	Enables debugging for IPsec configuration.
config-detail	Enables debugging for detailed IPsec configuration.
demux	Enables debugging for IPsec message demux.
deque	Enables debugging for IPsec message dequeue.
error	Enables debugging for IPsec errors.
event	Enables debugging for IPsec FSM and events.
flow	Enables debugging for IPsec flow.
flow-detail	Enables debugging for detailed IPsec flow.
ha	Enables debugging for IPsec high availability.
trace	Enables debugging for IPsec trace.
detail	Specifies detailed trace.
warning	Enables debugging for IPsec warning.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, IPsec must be enabled using the **crypto ipsec enable** command.

Examples

The following example displays the system output when the **debug ipsec config** command is issued.

```
switch# debug ipsec config
```

Related Commands

Command	Description
crypto ipsec enable	Enables IPsec.
no debug all	Disables all debugging.

debug isns

To enable debugging for Internet storage name services (iSNS), use the **debug isns** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug isns {**all** | **bypass ficon_mgr** | **cloud** | **db** | **deque** | **error** | **event** [**vsan** *vsan-id*] | **fabric distribute** | **ha** [**vsan** *vsan-id*] | **prot** | **trace** [**detail**] | **warning** [**vsan** *vsan-id*]}

no debug isns {**all** | **bypass ficon_mgr** | **cloud** | **db** | **deque** | **error** | **event** [**vsan** *vsan-id*] | **fabric distribute** | **ha** [**vsan** *vsan-id*] | **prot** | **trace** [**detail**] | **warning** [**vsan** *vsan-id*]}

Syntax Description

all	Enables all iSNS debugging.
bypass ficon_mgr	Enables bypassing FICON manager execution.
cloud	Enables debugging for iSNS cloud discovery.
db	Enables debugging for iSNS database.
deque	Enables debugging for iSNS message dequeue.
error	Enables debugging for iSNS error.
event	Enables debugging for iSNS event.
vsan *vsan-id*	Restricts debugging to the specified VSAN ID. The range is 1 to 4093.
fabric distribute	Enables debugging for iSNS fabric distribution.
ha	Enables debugging for iSNS high availability.
prot	Enables debugging for iSNS protocol.
trace	Enables debugging for iSNS trace.
detail	Enables detailed iSNS trace.
warning	Enables debugging for iSNS warning.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, iSNS must be enabled using the **isns-server enable** command.

Examples

The following example displays the system output when the **debug isns error** command is issued.

```
switch# debug isns error
```

Related Commands

Command	Description
isns-server enable	Enables the iSNS server.
no debug all	Disables all debugging.
show isns	Displays iSNS information.

debug ivr

To enable debugging for inter-VSAN routing (IVR), use the **debug ivr** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug {**all** | **demux** | **dep** | **dep-detail** | **dequeue** | **drav-fsm** | **drav-fsm-detail** | **errors** | **fcid-rewrite** | **fcid-rewrite-detail** | **ficon** | **ficon-detail** | **ha** | **pnat** | **pv** | **pv-detail** | **state-machine** [**vsan** *vsan-id*] | **test** | **trace** | **trace-detail** | **tu-fsm** | **tu-fsm-detail** | **zone-distrib-errors** | **zone-distrib-events** | **zone-fsm** | **zone-fsm-detail**}

no debug {**all** | **demux** | **dep** | **dep-detail** | **dequeue** | **drav-fsm** | **drav-fsm-detail** | **errors** | **fcid-rewrite** | **fcid-rewrite-detail** | **ficon** | **ficon-detail** | **ha** | **pnat** | **pv** | **pv-detail** | **state-machine** [**vsan** *vsan-id*] | **test** | **trace** | **trace-detail** | **tu-fsm** | **tu-fsm-detail** | **zone-distrib-errors** | **zone-distrib-events** | **zone-fsm** | **zone-fsm-detail**}

Syntax Description

all	Enables all filters for IVR debugging.
demux	Enables debugging of IVR event demultiplexing.
dep	Enables debugging of IVR DEP.
dep-detail	Enables debugging of IVR DEP detail.
dequeue	Enables debugging of IVR event dequeue.
drav-fsm	Enables debugging of IVR DRAV finite state machine (FSM).
drav-fsm-detail	Enables debugging of IVR DRAV FSM detail.
errors	Enables debugging for IVR errors.
fcid-rewrite	Enables debugging of IVR FC ID rewrite.
fcid-rewrite-detail	Enables debugging of IVR FC ID rewrite detail.
ficon	Enables debugging of IVR FICON.
ficon-detail	Enables debugging of IVR FICON detail.
ha	Enables debugging of IVR high-availability.
pfcid	Enables debugging of the IVR persistent FCID module.
pfcid-detail	Enables detailed debugging of the IVR persistent FCID module.
pnat	Enables debugging of IVR payload Network Address Translation (NAT).
pv	Enables debugging of IVR PV state machine.
pv-detail	Enables debugging of IVR PV state machine detail.
state-machine	Enables debugging of FSM.
vsan *vsan-id*	Restricts debugging to the specified VSAN.
test	Enables debugging of IVR test features.
trace	Enables debugging of IVR trace.
trace-detail	Enables debugging of IVR detail trace.
tu-fsm	Enables debugging of IVR TU FSM.
tu-fsm-detail	Enables debugging of IVR TU FSM detail.
zone-distrib-errors	Enables debugging of IVR zone distribution errors.
zone-distrib-events	Enables debugging of IVR zone distribution events.

zone-fsm	Enables debugging of IVR zone FSM.
zone-fsm-detail	Enables debugging of IVR zone FSM detail.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
2.1(1)	This command was introduced.
3.0(1)	• Added the **ficon** and **ficon-detail** options. • Added the **pfcid** and **pfcid-detail** options.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug ivr all** command is issued:

```
switch# debug ivr all
2005 Mar 10 01:27:27 ivr: fu_fsm_execute_all: match_msg_id(0), log_already_open(0)
2005 Mar 10 01:27:27 ivr: fu_fsm_execute_all: null fsm_event_list
2005 Mar 10 01:27:27 ivr: fu_fsm_engine_post_event_processing: mts msg
MTS_OPC_DEBUG_WRAP_MSG(msg_id 6774251) dropped
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show ivr	Displays IVR configurations.

debug klm

To enable kernel loadable module parameter debugging, use the **debug klm** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug klm {**fc2** {**cpuhog** *seconds* | **flag** *flags*} | **scsi-target** {**driver** | **error** [**vsan** *vsan-id*] [**fcid** *fc-id*] | **flag** *flags* | **flow** [**vsan** *vsan-id*] [**fcid** *fc-id*] | **snmp** | **syscall**} | **sdip** {**all** | **error** | **flow** | **warning**}}

no debug klm {**fc2** {**cpuhog** *seconds* | **flag** *flags*} | **scsi-target** {**driver** | **error** [**vsan** *vsan-id*] [**fcid** *fc-id*] | **flag** *flags* | **flow** [**vsan** *vsan-id*] [**fcid** *fc-id*] | **snmp** | **syscall**} | **sdip** {**all** | **error** | **flow** | **warning**}}

Syntax Description

fc2	Enables debugging for FC2 driver debug parameters.
cpuhog *seconds*	Specify the FC2 CPU hog value. The ranges is 0 to 10000 seconds.
flag *flags*	Specify the flag values. The ranges is 0x0 to 0xffffffff.
scsi-target	Enables debugging for the SCSI target driver.
driver	Enables debugging for SCSI target driver flags.
error	Enables debugging for driver error conditions.
vsan *vsan-id*	Restricts debugging to the specified VSAN.
fcid *fc-id*	Restricts debugging to the specified FCID interface.
flow	Enables debugging for SCSI target flow.
snmp	Enables debugging for SCSI target SNMP requests.
syscall	Enables debugging for SCSI target system call request.
sdip	Enables debugging for the SDIP driver.
all	Enables debugging for the SCSI target driver.
flow	Enables debugging for driver flow.
warning	Enables debugging for driver warnings.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug klm scsi-target driver** command is issued:

```
switch# debug klm scsi-target driver
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug license

To enable licensing debugging, use the **debug license** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug license {**all** | **errors** | **event s** | **mts**}

no debug license {**all** | **errors** | **events** | **mts**}

Syntax Description

all	Enables debugging for all licensing features.
errors	Enables debugging for licensing error conditions.
events	Enables debugging for the licensing events.
mts	Enables debugging for Tx/Rx packets of MTS.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug license all** command is issued:

```
switch# debug license all
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show license	Displays license information.

debug logfile

To direct the output of the debug commands to a specified file, use the **debug logfile** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug logfile *filename* [**size** *bytes*]

Syntax Description

filename	Assigns the name of the log file. Maximum length is 80 characters.
size *bytes*	Specifies the logfile size in bytes. The range is 4096 to 4194304.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use this command to log debug messages to a special log file. This file is more secure and easier to process than sending the debug output to the console.

When you use the **debug logfile** command to create a log file, the file is automatically created in the log: directory on the supervisor module unless you specify a different path.

For example, using the **debug logfile** command to created a log file named captureDebug, you must enter the **dir log://sup-local/?** command to find the log file you created. Following example shows you how to find the log file created.

```
switch# debug logfile captureDebug
switch#  dir log://sup-local/?
  log:                        Enter URL "log:[//<module-number>]/<filename>"
  log://sup-local/dmesg
  log://sup-local/messages
➔ log://sup-local/captureDebug

switch#  dir log://sup-local/
```

Examples

The following example redirects the output of the debug commands to the file named *sample*.

```
switch# debug logfile sample
```

The following example assigns the log file size for the file named *sample*.

```
switch# debug logfile sample size 410000
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show logging	Displays the current message logging configuration.

debug mcast

To enable debugging for multicast definitions, use the **debug mcast** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug mcast {all | error [**vsan** *vsan-id*] [**interface fc** *slot*/*port*] **| event** [**vsan** *vsan-id*] [**interface fc** *slot*/*port*] **| mts {pkt** {**both | rx** [**node** *range* **| opcode** *range* **| sap** *range*] **| tx**} **| pkthdr** {**both | rx** [**numpkt** *range*] **| tx**}**} | trace** [**vsan** *vsan-id*] [**interface fc** *slot*/*port*]**]**

no debug mcast {all | error [**vsan** *vsan-id*] [**interface fc** *slot*/*port*] **| event** [**vsan** *vsan-id*] [**interface fc** *slot*/*port*] **| mts {pkt** {**both | rx** [**node** *range* **| opcode** *range* **| sap** *range*] **| tx**} **| pkthdr** {**both | rx** [**numpkt** *range*] **| tx**}**} | trace** [**vsan** *vsan-id*] [**interface fc** *slot*/*port*]**]**

Syntax Description

all	Enables debugging for all multicast definitions.
error	Enables debugging for multicast errors.
event	Enables debugging for multicast events.
mts	Enables debugging for multicast tx/rx MTS events.
trace	Enables debugging for multicast traces.
vsan *vsan-id*	Restricts debugging to the specified VSAN.
interface fc *slot*/*port*	Restricts debugging to the specified interface.
pkt	Specifies debugging of packets.
pkthdr	Specifies debugging of headers.
numpkt	Specifies the number of required packets
both	Specifies debugging in both the transmit and receive directions.
tx	Specifies debugging in the transmit direction,
rx	Specifies debugging in the receive direction.
node	Specifies the node for the packets in the receive direction.
opcode	Specifies the opcode for the packets in the receive direction.
sap	Specifies the sap for the packets in the receive direction.
range	Specifies the integer range from 1 to 4096.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug mcast all** command is issued:

```
switch# debug mcast all
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show mcast	Displays multicast information.

debug mip

To enable debugging for multiple IP (MIP) kernel drivers, use the **debug mip** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug mip {**errors** | **events**}

no debug mip {**errors** | **events**}

Syntax Description

errors	Enables debugging for MIP error conditions.
events	Enables debugging for MIP events.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug mip errors** command is issued:

```
switch# debug mip errors
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug module

To enable debugging for switching or service modules, use the **debug module** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug module {**all** | **error** [**module** *slot*] | **event** | **ha** | **no-powerdown** | **trace** [**module** *slot*]}

no debug module {**all** | **error** [**module** *slot*] | **event** | **ha** | **no-powerdown** | **trace** [**module** *slot*]}

Syntax Description

all	Enables debugging for all module features.
error	Enables debugging for module error conditions.
event	Enables debugging for module events.
ha	Enables debugging for a module's high availability features.
no-powerdown	Disables the power cycle feature for the module.
trace	Enables debugging for a module's trace flows.
module *slot*	Restricts debugging to the specified module.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug module all** command is issued:

```
switch# debug module all
2005 Mar 10 02:51:01 module: fu_fsm_execute_all: match_msg_id(0), log_already_open(0)
2005 Mar 10 02:51:01 module: fu_fsm_execute_all: null fsm_event_list
2005 Mar 10 02:51:01 module: fu_fsm_engine_post_event_processing: mts msg
MTS_OPC_DEBUG_WRAP_MSG(msg_id 6986564) dropped
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show module	Displays the status of a module.

debug ntp

To enable debugging for the Network Time Protocol (NTP) module, use the **debug ntp** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug ntp {**errors** | **info**}

no debug ntp {**errors** | **info**}

Syntax Description

errors	Enables debugging for NTP error conditions.
info	Enables debugging for NTP information and events.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug ntp info** command is issued:

```
switch# debug ntp info
2005 Mar 10 03:00:42 ntp: Dropping msg_ref with rr_token [7002722]
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show ntp	Displays the configured NTP server and peer associations.

debug obfl

To enable debugging for Onboard Failure Logging (OBFL), use the **debug obfl** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug obfl {**error** | **trace**}

no debug obfl {**error** | **trace**}

Syntax Description

error	Enables debugging for OBFL error conditions.
info	Enables debugging for OBFL events.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug obfl error** command is issued:

```
switch# debug obfl error
2006 Jan 23 21:30:59.573503 obfl: obfl_process_mts_msgs(): OBFL received mts mes
sage: opc:182
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show logging onboard	Displays OBFL information.

debug platform

To enable debugging for the platform manager, use the **debug platform** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug platform {**all** [**fc_id** *fc-id*] | **error** [**module** *slot*] | **flow** [**module** *slot*] | **fsm** | **ha** | **hitless** | **mts** {**pkt** | **pkthdr**} {**tx** | **rx**} | **nopowerdown** | **supervisor-reset**}

no debug platform {**all** [**fc_id** *fc-id*] | **error** [**module** *slot*] | **flow** [**module** *slot*] | **fsm** | **ha** | **hitless** | **mts** {**pkt** | **pkthdr**} {**tx** | **rx**} | **nopowerdown** | **supervisor-reset**}

Syntax Description

all	Enables debugging for all platform features.
error	Enables debugging for platform-related error conditions.
flow	Enables debugging for platform-related flows.
fsm	Enables debugging for platform-related FSMs.
ha	Enables debugging for platform-related high availability.
hitless	Enables the platform loading feature while the switch is in hitless mode.
mts	Enables debugging for platform-related tx/rx MTS events.
nopowerdown	Enables powering down modules
supervisor-reset	Resets the local supervisor.
fcid *f c-id*	Restricts debugging to the specified FC ID module number. The range is 0 to 2147483647.
pkt	Enables debugging of packets.
pkthdr	Enables debugging of headers.
tx	Enables debugging in the transmit direction,
rx	Enables debugging in the receive direction.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug platform all** command is issued:

```
switch# debug platform all
2005 Mar 10 03:01:56 platform: fu_fsm_execute_all: match_msg_id(0), log_already_open(0)
2005 Mar 10 03:01:56 platform: fu_fsm_execute_all: null fsm_event_list
2005 Mar 10 03:01:56 platform: fu_fsm_engine_post_event_processing: mts msg
MTS_OPC_DEBUG_WRAP_MSG(msg_id 7004045) dropped
v-185# 2005 Mar 10 03:01:56 platform: env_chg_none: ps 0 old 1 new 1
2005 Mar 10 03:01:57 platform: env_chg_none: ps 0 old 1 new 1
2005 Mar 10 03:01:58 platform: env_chg_none: ps 0 old 1 new 1
v-185# debug platform all
2005 Mar 10 03:01:59 platform: fu_priority_select:  - setting fd[7] for select call
2005 Mar 10 03:01:59 platform: fu_priority_select_select_queue: round credit(5)
2005 Mar 10 03:01:59 platform:     curr_q - FU_PSEL_Q_CAT_CQ, usr_q_info(0), priority(1),
credit(0), empty
2005 Mar 10 03:01:59 platform: fu_priority_select: returning FU_PSEL_Q_CAT_FD queue,
fd(7), usr_q_info(1)
2005 Mar 10 03:01:59 platform: fu_fsm_engine: line[2139]
.
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug plog

To enable debugging of persistent logging (PLOG), use the **debug plog** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug plog {error | trace}

no debug plog {error | trace}

Syntax Description

error	Enables debugging of PLOG error conditions.
trace	Enables debugging of PLOG events.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug plog** command is issued:

```
switch# debug plog
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug port

To enable debugging for ports, use the **debug port** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug port {**all** | **bypass** {**acl_manager** | **domain_manager** | **fcsp** | **ficon** | **fport_server** | **lcp** | **loopback_diag** | **port_channel_mgr** | **port_lock** | **qos_mgr** | **span** | **switch_wwn** | **vsan_mgr** | **wwn_mgr** |**xbar_mgr** | **zone_server**} | **error** | **event** [**interface** *type number* | **module** *slot*] | **ha** [**interface** *type number* | **module** *slot*] | **trace** [**interface** *type number* | **module** *slot*]}

no debug port {**all** | **bypass** {**acl_manager** | **domain_manager** | **fcsp** | **ficon** | **fport_server** | **lcp** | **loopback_diag** | **port_channel_mgr** | **port_lock** | **qos_mgr** | **span** | **switch_wwn** | **vsan_mgr** | **wwn_mgr** | **xbar_mgr** | **zone_server**} | **error** | **event** [**interface** *type number* | **module** *slot*] | **ha** [**interface** *type number* | **module** *slot*] | **trace** [**interface** *type number* | **module** *slot*]}

Syntax Description

all	Enables all port debug options.
bypass	Bypasses some components in port execution.
error	Enables debugging for port error conditions.
event	Enables debugging for port FSMs and events.
ha	Enables debugging for port high availability.
trace	Enables debugging for port traces.
acl_manager	Bypasses ACL manager execution.
domain_manager	Bypasses domain manager execution.
fcsp	Bypasses FCSP execution.
ficon	Bypasses FICON execution.
fport_server	Bypasses FPort server execution.
lcp	Bypasses LCP execution.
loopback_diag	Bypasses loopback diagnostics execution.
port_channel_mgr	Bypasses PortChannel manager execution.
port_lock	Bypasses port lock execution.
qos_mgr	Bypasses QOS manager execution.
span	Bypasses SPAN execution.
switch_wwn	Bypasses using switch WWN and uses VSAN WWN in ELP.
vsan_mgr	Bypasses VSAN manager execution.
wwn_mgr	Bypasses WWN manager execution.
xbar_mgr	Bypasses XBAR manager execution.
zone_mgr	Bypasses zone manager execution.
interface *type number*	Restricts debugging to the specified interface.
module *slot*	Restricts debugging to the specified module.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug port all** command is issued:

```
switch# debug port all
Apr 10 00:49:38 port: fu_fsm_execute_all: match_msg_id(0), log_already_open(0)
Apr 10 00:49:38 port: fu_fsm_execute_all: null fsm_event_list
Apr 10 00:49:38 port: fu_fsm_engine: mts msg MTS_OPC_DEBUG_WRAP_MSG(msg_id 40239) dropped
```

The following example displays the system output when the **debug port event** command is issued:

```
switch# debug port event
Apr 10 15:30:35 port: fu_fsm_execute_all: match_msg_id(0), log_already_open(0)
Apr 10 15:30:35 port: fu_fsm_execute_all: null fsm_event_list
Apr 10 15:30:35 port: fu_fsm_engine: mts msg MTS_OPC_DEBUG_WRAP_MSG(msg_id 7002)
 dropped
switch# Apr 10 15:30:35 port: fu_priority_select:  - setting fd[3] for select call  -
setting fd[5] for select call  - setting fd[6] for select call
Apr 10 15:30:35 port: fu_priority_select_select_queue: round credit(16)
Apr 10 15:30:35 port:     curr_q - FU_PSEL_Q_CAT_FD, usr_q_info(32), fd(5), priority(3),
credit(2), empty
Apr 10 15:30:35 port: fu_priority_select: returning FU_PSEL_Q_CAT_MTS queue, fd(3),
usr_q_info(8)
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug port-channel

To enable debugging for PortChannels, use the **debug port-channel** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug port-channel {**all** | **error** | **event** | **ha** | **trace** | **warning**}

no debug port-channel {**all** | **error** | **event** | **ha** | **trace** | **warning**}

Syntax Description

all	Enables all PortChannel debug options.
demux	Enables debugging of PortChannel messages.
deque	Enables debugging of PortChannel message dequeues.
error	Enables debugging for PortChannel error conditions.
event	Enables debugging for PortChannel FSMs and events.
ha	Enables debugging for PortChannel high availability.
trace	Enables debugging for PortChannel traces.
warning	Enables debugging for PortChannel warning.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug port-channel all** command is issued:

```
switch# debug port-channel all
2005 Mar 10 03:03:26 port_channel: fu_fsm_execute_all: match_msg_id(0),
log_already_open(0)
2005 Mar 10 03:03:26 port_channel: fu_fsm_execute_all: null fsm_event_list
2005 Mar 10 03:03:26 port_channel: fu_fsm_engine_post_event_processing: mts msg
MTS_OPC_DEBUG_WRAP_MSG(msg_id 7005958) dropped
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show port-channel	Displays information about existing PortChannel configurations.

debug port-resources

To enable debugging for a port resources module, use the **debug port-resources** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug port-channel {**all** | **demux** | **deque** | **error** | **event** | **ha** | **mts** | **trace** | **warning**}

no debug port-channel {**all** | **demux** | **deque** | **error** | **event** | **ha** | **mts** | **trace** | **warning**}

Syntax Description

all	Enables all port resources debug options.
demux	Enables debugging of port resources messages.
deque	Enables debugging of port resources message dequeues.
error	Enables debugging for port resources error conditions.
event	Enables debugging for port resources FSMs and events.
ha	Enables debugging for port resources high availability.
mts	Enables debugging for port resources message MTS events.
trace	Enables debugging for port resources traces.
warning	Enables debugging for port resources warning.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug port-resources demux** command is issued:

```
switch# debug port-resources demux vsan 2
2006 Jan 19 22:10:59.244892 port-resources: fu_priority_select:  - setting fd[5]
 for select call
2006 Jan 19 22:10:59.244985 port-resources: fu_priority_select_select_queue: rou
nd credit(12)
2006 Jan 19 22:10:59.245018 port-resources:     curr_q - FU_PSEL_Q_CAT_CQ, usr_q
_info(2), priority(7), credit(6), empty
2006 Jan 19 22:10:59.245051 port-resources: fu_priority_select: returning FU_PSE
L_Q_CAT_MTS queue, fd(5), usr_q_info(1)
2006 Jan 19 22:10:59.245168 port-resources: prm_get_data_from_queue(664): dequeued mts msg
(128136), MTS_OPC_DEBUG_WRAP_MSG
```

```
2006 Jan 19 22:10:59.245205 port-resources: fu_fsm_engine: line[2205]
2006 Jan 19 22:10:59.245248 port-resources: prm_demux: ev[0]
ips-hac2# 2006 Jan 19 22:10:59.246440 port-resources: fu_fsm_execute_all: match_
msg_id(0), log_already_open(0)
2006 Jan 19 22:10:59.246507 port-resources: fu_fsm_execute_all: null fsm_event_list
2006 Jan 19 22:10:59.246578 port-resources: fu_fsm_engine_post_event_processing:
 mts msg MTS_OPC_DEBUG_WRAP_MSG(msg_id 128136) dropped
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show port-resources module	Displays information about port resources in a Generation 2 module.

debug qos

To enable debugging for quality of service (QoS), use the **debug qos** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug qos {**all** [**interface fc** *slot*/*port*] | **detail** | **errors supervisor** | **flow** | **trace**}

no debug qos {**all** [**interface fc** *slot*/*port*] | **detail** | **errors supervisor** | **flow** | **trace**}

Syntax Description

all	Enables all QoS debug options.
interface fc *slot*/*port*	Restricts debugging to the specified interface.
detail	Enables all QoS debug output.
errors supervisor	Enables debugging for supervisor QoS error conditions.
flow	Enables flow-level QoS debug options.
trace	Enables debugging for QoS traces.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug qos all** command is issued:

```
switch# debug qos all
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show qos	Displays the current QoS settings along with a the number of frames marked high priority.

debug radius

To enable debugging for boot variables, use the **debug radius** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug radius {**aaa-request** | **aaa-request-lowlevel** | **all** | **config** | **config-lowlevel** | **server-monitor** | **server-monitor-errors**}

no debug radius {**aaa-request** | **aaa-request-lowlevel** | **all** | **config** | **config-lowlevel** | **server-monitor** | **server-monitor-errors**}

Syntax Description

aaa-request	Enables RADIUS AAA request debug.
aaa-request-lowlevel	Enables RADIUS AAA request low-level debugging.
all	Enables Enable all the debug flags.
config	Enables RADIUS configuration debugging.
config-lowlevel	Enables RADIUS configuring low-level debugging.
server-monitor	Enables RADIUS server monitoring.
server-monitor-errors	Enables RADIUS server monitor errors.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Added the **server-monitor** and **server-monitor-errors** options.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug radius config-lowlevel** command is issued:

```
switch# debug radius config-lowlevel
Nov 20 06:36:42 radius: radius_new_debug_conf_open: entering...
Nov 20 06:36:42 radius: radius_new_conf_close: entering...
Nov 20 06:36:42 radius: radius_new_conf_close: returning 0
Nov 20 06:36:42 radius: radius_new_enable_info_config: entering for Radius Daemon debug
Nov 20 06:36:42 radius: radius_new_debug_conf_open: entering...
Nov 20 06:36:42 radius: radius_new_debug_conf_open: exiting
Nov 20 06:36:42 radius: radius_new_enable_info_config: SET_REQ for Radius Daemon debug
with 1
Nov 20 06:36:42 radius: radius_new_enable_info_config: SET_REQ done for Radius Daemon
debug with 1
```

```
Nov 20 06:36:42 radius: radius_new_enable_info_config: got back the return value of
configuration operation:success
Nov 20 06:36:42 radius: radius_new_debug_conf_close: entering...
Nov 20 06:36:42 radius: radius_new_debug_conf_close: returning 0
Nov 20 06:36:42 radius: radius_new_enable_info_config: exiting for Radius Daemon debug
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show radius	Displays the RADIUS Cisco Fabric Services (CFS) distribution status and other details.

debug rd-reg

To enable debugging for the list of devices using the read-register feature, use the **debug rd-reg** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug rd-reg [*device-name* | *register address*]

Syntax Description

device-name	Specifies the device name for the required device.
register address	Specifies the register address for the required device.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug rd-reg abc** command is issued:

```
switch# debug rd-reg abc
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug rdl errors

To enable debugging for RDL errors, use the **debug rdl errors** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug rdl errors

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug rdl errors** command is issued:

```
switch# debug rdl errors
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug rib

To enable debugging for the routing information base (RIB) feature, use the **debug rib** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug rib {**all** | **detail** | **error** | **event** | **liod_error** | **liod_event** | **liod_trace** | **trace**}

Syntax Description

all	Enables debugging for all RIB features.
detail	Enables detailed debugging for all RIB features.
error	Enables debugging for RIB errors.
event	Enables debugging for RIB events.
liod_error	Enables debugging for lossless in-order delivery (LIOD) errors.
liod_event	Enables debugging for LIOD errors.
liod_trace	Enables debugging for LIOD trace events.
trace	Enables debugging for trace events.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the **liod_error**, **liod_event**, and **liod_trace** options.

Usage Guidelines

If a RIB operation is ignored or not supported, then issue the **debug rib all** command to find out more details.

Examples

The following example shows the **debug rib error** command.

```
switch# debug rib error
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug rlir

To enable Registered Link Incident Report (RLIR) debugging, use the **debug rlir** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug rlir {**all** | **errors** | **events** | **mts-errors** | **mts-events**}

no debug rlir {**all** | **errors** | **events** | **mts-errors** | **mts-events**}

Syntax Description

all	Enables debugging for all RLIR features.
errors	Enables debugging for RLIR error conditions.
events	Enables debugging for the RLIR events.
mts-errors	Enables debugging for MTS error conditions.
mts-events	Enables debugging for MTS events.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug rlir all** command is issued:

```
switch# debug rlir all
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show rlir	Displays information about RLIR, Link Incident Record Registration (LIRR), and Distribute Registered Link Incident Record (DRLIR) frames.

debug rscn

To enable debugging for the registered state change notification (RSCN) feature, use the **debug rscn** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug rscn {**all** | **errors** | **events** | **mts-errors** | **mts-events**} [**vsan** *vsan-id*]

no debug rscn {**all** | **errors** | **events** | **mts-errors** | **mts-events**} [**vsan** *vsan-id*]

Syntax Description

all	Enables debugging for all RSCN features.
errors	Enables debugging for RSCN errors.
events	Enables debugging for RSCN events.
mts-errors	Enables debugging for RSCN MTS errors.
mts-events	Enables debugging for RSCN MTS events.
vsan *vsan-id*	Restricts debugging to the specified VSAN.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug rscn errors** command is issued:

```
switch# debug rscn errors
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show rscn	Displays RSCN information.

debug san-ext-tuner

To enable debugging for SAN extension tuner, use the **debug san-ext-tuner** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug isns {**all** | **demux** | **deque** | **error** | **event** | **ha** | **trace** [**detail**] | **warning**}

no debug isns {**all** | **bypass ficon_mgr** | **demux** | **deque** | **error** | **event** | **ha** | **trace** [**detail**] | **warning**}

Syntax Description

all	Enables all SAN extension tuner debugging.
demux	Enables debugging for SAN extension tuner message demux.
deque	Enables debugging for SAN extension tuner message dequeue.
error	Enables debugging for SAN extension tuner error conditions.
event	Enables debugging for SAN extension tuner events.
ha	Enables debugging for SAN extension tuner high availability.
trace	Enables debugging for SAN extension tuner trace.
detail	Enables detailed debugging for SAN extension tuner trace.
warning	Enables debugging for SAN extension tuner warnings.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug san-ext-tuner error** command is issued.

```
switch# debug san-ext-tuner error
```

Related Commands

Command	Description
isns-server enable	Enables the iSNS server.
no debug all	Disables all debugging.
show isns	Displays iSNS information.
show san-ext-tuner	Displays SAN extension tuner information.

debug scsi-flow

To enable debugging of a SCSI flow, use the **debug scsi-flow** command. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug scsi-flow {**all** | **demux vsan** *vsan-id* | **deque** | **error** | **event vsan** *vsan-id* | **ha** | **trace** {**detail vsan** *vsan-id* | **vsan** *vsan-id*} | **warning vsan** *vsan-id*}

no debug scsi-flow {**all** | **demux vsan** *vsan-id* | **deque** | **error** | **event vsan** *vsan-id* | **ha** | **trace** {**detail vsan** *vsan-id* | **vsan** *vsan-id*} | **warning vsan** *vsan-id*}

Syntax Description

all	Enables all debug flags for all SCSI flows.
demux	Enables debugging for SCSI flow demux functions.
deque	Enables debugging for SCSI flow deque events.
error	Enables debugging for SCSI flow errors.
event	Enables debugging for SCSI flow events.
ha	Enables debugging for SCSI flow high availability events.
trace	Enables debugging for SCSI flow traces.
detail	Enables debugging of SCSI flow detail trace.
warning	Enables debugging for SCSI flow warning messages.
vsan *vsan-id*	Restricts debugging to the specified VSAN. The range is 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example enables all debug flags for all SCSI flows.

```
switch# debug scsi-flow all
2004 Nov 29 17:24:49 sfm: fu_fsm_execute_all: match_msg_id(0), log_already_open(0)
2004 Nov 29 17:24:49 sfm: fu_fsm_execute_all: null fsm_event_list
2004 Nov 29 17:24:49 sfm: fu_fsm_engine_post_event_processing: mts msg
MTS_OPC_DEBUG_WRAP_MSG(msg_id 536440) dropped
switch#
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show scsi-flow	Displays SCSI flow information.

debug scsi-target

To enable debugging for SCSI targets, use the **debug scsi-target** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug scsi-target {**error** | **flow**}

no debug scsi-target {**error** | **flow**}

Syntax Description

error	Enables debugging for SCSI target daemon error conditions.
flow	Enables debugging for the SCSI target flow.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug scsi-target flow** command is issued:

```
switch# debug scsi-target flow
Apr 28 21:11:52 vhbad: vhba_mts_handler: sdwrap_dispatch: retval:0
Apr 28 21:11:54 vhbad: vhbad_handle_timeout: timer:1 context:(nil)
Apr 28 21:12:06 vhbad: vhba_mts_handler: sysmgr_dispatch: retval:-1
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show scsi-target	Displays information about existing SCSI target configurations.

debug security

To enable debugging for the security and accounting features, use the **debug security** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug security {**all** | **events** | **mts** | **radius**}

no debug security {**all** | **events** | **mts** | **radius**}

Syntax Description

all	Enables debugging for all security features.
events	Enables debugging for security events.
mts	Enables debugging for security MTS packets.
radius	Enables debugging for RADIUS events.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug security radius** command is issued:

```
switch# debug security radius
Mar  5 00:51:13 securityd: RADIUS is enabled, hence it will be tried first for CHAP
authentication
Mar  5 00:51:13 securityd: reading RADIUS configuration
Mar  5 00:51:13 securityd: opening radius configuration for group:default
Mar  5 00:51:13 securityd: opened the configuration successfully
Mar  5 00:51:13 securityd: GET request for RADIUS global config
Mar  5 00:51:13 securityd: got back the return value of global radius configuration
operation:success
Mar  5 00:51:13 securityd: closing RADIUS pss configuration
Mar  5 00:51:13 securityd: opening radius configuration for group:default
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug sensor

To enable debugging for the sensor manager, use the **debug sensor** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug sensor {**demux** | **deque** | **error** | **info** | **init**}

no debug sensor {**demux** | **deque** | **error** | **info** | **init**}

Syntax Description

demux	Enables debugging for sensor demux functions.
deque	Enables debugging for sensor deque events.
error	Enables debugging for sensor errors.
info	Enables debugging for sensor information.
init	Enables debugging for sensor initialization.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use this command to debug sensor manager events and information.

Examples

The following example displays the system output when the **debug sensor info** command is issued:

```
switch# debug sensor info
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show environment temperature	Displays current temperature threshold settings and state.

debug snmp

To enable debugging for the SNMP manager, use the **debug snmp** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug snmp {
all |
errors |
mts {pkt {**both** | **rx** [**node** *range* | **opcode** *range* | **sap** *range*] | **tx**} |
pkthdr {**both** | **rx** [**numpkt** *range*] | **tx**}} |
pkt-dump | **trace** {**trace-entryexit** | **trace-stub**}}

no debug snmp {
all |
errors |
mts {pkt {**both** | **rx** [**node** *range* | **opcode** *range* | **sap** *range*] | **tx**} |
pkthdr {**both** | **rx** [**numpkt** *range*] | **tx**}} |
pkt-dump | **trace** {**trace-entryexit** | **trace-stub**}}

Syntax Description

all	Enables debugging for all SNMP output.
errors	Enables debugging for SNMP error output.
mts	Enables debugging for SNMP packets and headers.
pkt-dump	Enables a packet dump of debug output.
trace	Enables trace level debug output.
pkt	Specifies debugging of packets.
pkthdr	Specifies debugging of headers.
both	Specifies debugging in both the transmit and receive directions.
tx	Specifies debugging in the transmit direction.
rx	Specifies debugging in the receive direction.
node	Specifies the node for the packets in the receive direction.
opcode	Specifies the opcode for the packets in the receive direction.
sap	Specifies the sap for the packets in the receive direction.
numpkt	Specifies the number of required packets
range	Specifies the integer range from 1 to 4095.
trace-entryexit	Specifies trace-level entry or exit debug output.
trace-stub	Specifies trace-level stub debug output.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug snmp trace** command is issued:

```
switch# debug snmp trace
Apr 29 16:03:34 snmpd[1177]: SDWRAP message Successfully processed
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show snmp	Displays SNMP status and setting information.
snmp-server	Configures the SNMP server information, switch location, and switch name.
snmp-server enable traps	Enables SNMP server notifications (informs and traps).

debug span

To enable SPAN debugging, use the **debug span** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug span {**all** | **buffer-size** *bytes* | **error** | **event** | **trace** | **warning**}

no debug span {**all** | **error** | **event** | **trace** | **warning**}

Syntax Description

all	Enables debugging for all SPAN features.
buffer-size *bytes*	Configures event logs buffer size for SPAN. The range is 4096 to 131072.
error	Enables debugging for SPAN errors.
event	Enables debugging for SPAN events.
ha	Enables debugging for SPAN HA.
lib	Enables debugging for SPAN library.
trace	Enables debugging for SPAN traces.
warning	Enables debugging for SPAN warning messages.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug span all** command is issued:

```
switch# debug span all
Apr 29 16:06:44 span: span_demux: msg consumed by sdwrap_process msg
Apr 29 16:06:44 span: fu_fsm_execute_all: match_msg_id(0), log_already_open(0)
Apr 29 16:06:44 span: fu_fsm_execute_all: null fsm_event_list
Apr 29 16:06:44 span: fu_fsm_engine: mts msg MTS_OPC_DEBUG_WRAP_MSG(msg_id 2548887)
dropped
Apr 29 16:06:48 span: fu_priority_select:  - setting fd[3] for select call
Apr 29 16:06:48 span: fu_priority_select_select_queue: round credit(12)
Apr 29 16:06:48 span:     curr_q - FU_PSEL_Q_CAT_CQ, usr_q_info(4), priority(7),
credit(6), empty
Apr 29 16:06:48 span: fu_priority_select: returning FU_PSEL_Q_CAT_MTS queue, fd(3),
usr_q_info(2)
Apr 29 16:06:48 span: span_get_data_from_mts_q dequeued mts msg (26e525),
MTS_OPC_DEBUG_WRAP_MSG
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show span session	Displays specific information about a Switched Port Analyzer (SPAN) session.

debug system health

To enable system health monitoring debugging, use the **debug system health** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug system health {**all** | **asic-counters** | **battery-charger** | **cache-disk** | **eobc** | **error** | **event** | **external-loopback** | **failure-analysis** | **fc2** | **free-disk** | **ha** | **inband** | **loopback** | **mgmt** | **misc** | **mts** | **nvram** | **plog** | **pss** | **serdes** | **special** | **trace** | **xipc**}

no debug system health {**all** | **asic-counters** | **battery-charger** | **cache-disk** | **eobc** | **error** | **event** | **external-loopback** | **failure-analysis** | **fc2** | **free-disk** | **ha** | **inband** | **loopback** | **mgmt** | **misc** | **mts** | **nvram** | **plog** | **pss** | **serdes** | **special** | **trace** | **xipc**}

Syntax Description

all	Enables debugging of all online health flags.
asic-counters	Enables debugging of system health ASIC statistics.
battery-charger	Enables debugging of system health battery charger tests.
cache-disk	Enables debugging of system health cache-disk tests.
eobc	Enables debugging of system health EOBC tests.
error	Enables debugging of system health error conditions.
event	Enables debugging of system health events.
external-loopback	Enables debugging of system health external loopback tests.
failure-analysis	Enables debugging of system health failure analysis.
fc2	Enables debugging of system health FC2 frames.
free-disk	Enables debugging of system health free disk.
ha	Enables debugging of health monitoring HA flags.
inband	Enables debugging of system health inband tests.
loopback	Enables debugging of system health loopback tests.
mgmt	Enables debugging of system health management-port port tests.
misc	Enables debugging of system health misc.
mts	Enables debugging of system health MTS.
nvram	Enables debugging of system health nvram.
plog	Enables debugging of system health persistent logging.
pss	Enables debugging of system health pss.
serdes	Enables debugging of system health SerDes tests.
special	Enables debugging of system health special.
trace	Enables debugging of health monitoring trace flags.
xipc	Enables debugging of system health XIPC.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the **free-disk**, **nvram**, and **plog** options.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug system health** command is issued:

```
switch# debug system health all
2005 Mar 10 01:49:28 SystemHealth: ohms_snake_fd_activity: Module 1 Snake Frame came.
2005 Mar 10 01:49:28 SystemHealth: ohms_snake_fd_activity: Module 8 waiting for Snake
Frame to come.
2005 Mar 10 01:49:28 SystemHealth: ohms_dequeue: select timeout 0 998000
2005 Mar 10 01:49:28 SystemHealth: fu_priority_select:  - setting fd[4] for select call  -
setting fd[20] for select call  - setting fd[22] for select call  - setting fd[28] for
select call  - setting fd[29] for select call  - setting fd[30] for select call
2005 Mar 10 01:49:28 SystemHealth: fu_priority_select_select_queue: round credit(14)
2005 Mar 10 01:49:28 SystemHealth:     curr_q - FU_PSEL_Q_CAT_FD, usr_q_info(466240),
fd(29), priority(6), credit(3), empty
2005 Mar 10 01:49:28 SystemHealth: fu_priority_select: returning FU_PSEL_Q_CAT_CQ queue,
usr_q_info(1)
2005 Mar 10 01:49:28 SystemHealth: ohms_dequeue: Select woken up
2005 Mar 10 01:49:28 SystemHealth: ohms_dequeue: Process event type 0x1
2005 Mar 10 01:49:28 SystemHealth: ohms_dequeue: Processing timer type
2005 Mar 10 01:49:28 SystemHealth: fu_fsm_engine: line[2139]
2005 Mar 10 01:49:28 SystemHealth: fu_fsm_handle_sysmgr_msg: Not mts event
2005 Mar 10 01:49:28 SystemHealth: ohms_timer_event_handler: called.
2005 Mar 10 01:49:28 SystemHealth: fu_fsm_execute_all: match_msg_id(0),
log_already_open(0)
.
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show system health	Displays configured Online System Health Management (OSHM) information.

debug tacacs+

To enable debugging for boot variables, use the **debug tacacs+** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug tacacs+ {**aaa-request** | **aaa-request-lowlevel** | **all** | **config** | **config-lowlevel** | **server-monitor** | **server-monitor-errors**}

no debug tacacs+ {**aaa-request** | **aaa-request-lowlevel** | **all** | **config** | **config-lowlevel** | **server-monitor** | **server-monitor-errors**}

Syntax Description

aaa-request	Enables TACACS+ AAA request debug.
aaa-request-lowlevel	Enables TACACS+ AAA request low-level debugging.
all	Enables Enable all the debug flags.
config	Enables TACACS+ configuration debugging.
config-lowlevel	Enables TACACS+ configuring low-level debugging.
server-monitor	Enables TACACS+ server monitoring.
server-monitor-errors	Enables TACACS+ server monitor errors.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Added the **server-monitor** and **server-monitor-errors** options.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug tacacs+ config-lowlevel** command is issued:

```
switch# debug tacacs+ config-lowlevel
Nov 20 06:39:44 tacacs: tacacs_debug_conf_open: entering...
172.22.94.252# Nov 20 06:39:44 tacacs: tacacs_debug_conf_open: exiting
Nov 20 06:39:44 tacacs: tacacs_conf_close: entering...
Nov 20 06:39:44 tacacs: tacacs_conf_close: returning 0
Nov 20 06:39:44 tacacs: tacacs_enable_info_config: entering for TACACS+ Daemon debug
Nov 20 06:39:44 tacacs: tacacs_debug_conf_open: entering...
Nov 20 06:39:44 tacacs: tacacs_debug_conf_open: exiting
Nov 20 06:39:44 tacacs: tacacs_enable_info_config: SET_REQ for TACACS+ Daemon debug with 1
Nov 20 06:39:44 tacacs: tacacs_enable_info_config: SET_REQ done for TACACS+ Daemon debug
with 1
```

```
Nov 20 06:39:44 tacacs: tacacs_enable_info_config: got back the return value of
configuration operation:success
Nov 20 06:39:44 tacacs: tacacs_debug_conf_close: entering...
Nov 20 06:39:44 tacacs: tacacs_debug_conf_close: returning 0
Nov 20 06:39:44 tacacs: tacacs_enable_info_config: exiting for TACACS+ Daemon debug
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show tacacs+	Displays the TACACS+ Cisco Fabric Services (CFS) distribution status and other details.

debug tcap

To enable debugging the exception logger, use the **debug tcap** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug tcap {**demux** | **deque** | **error** | **info** | **init**}

no debug tcap {**demux** | **deque** | **error** | **info** | **init**}

Syntax Description

demux	Enables debugging for terminal capture demux functions.
deque	Enables debugging for terminal capture deque events.
error	Enables debugging for terminal capture errors.
info	Enables debugging for terminal capture information.
init	Enables debugging for terminal capture initialization.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use this command to debug terminal capture utility events and information.

Examples

The following example displays the system output when the **debug tcap demux** command is issued:

```
switch# debug tcap demux
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug tlport

To enable debugging for TL port interfaces, use the **debug tlport** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug tlport {**all** | **errors** | **events** {**fc2** {**terminal** | **transit**} | **mts** | **pss**}} [**interface fc** *slot*/*port*]

no debug tlport {**all** | **errors** | **events** {**fc2** {**terminal** | **transit**} | **mts** | **pss**}} [**interface fc** *slot*/*port*]

Syntax Description

all	Enables debugging for all TL port features.
errors	Enables debugging for TL port error conditions.
events	Enables debugging for TL port monitoring events.
fc2	Enables debugging for TL port monitoring FC 2 events.
terminal	Specifies TL port monitoring FC 2 terminating events.
transit	Specifies TL port monitoring FC 2 transit events.
mts	Enables debugging for TL port monitoring MTS packets.
pss	Enables debugging for TL port monitoring PSS packets.
interface fc *slot*/*port*	Restricts debugging to the specified interface.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug tlport events pss** command is issued:

```
switch# debug tlport events pss
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show tlport	Displays configured TL port information.

debug ttyd

To enable TTYD debugging, use the **debug ttyd** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug ttyd {**all** | **errors** | **events**}

no debug ttyd {**all** | **errors** | **events**}

Syntax Description

all	Enables debugging for all TTYD features.
errors	Enables debugging for TTYD error conditions.
events	Enables debugging for TTYD events.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug ttyd events** command is issued:

```
switch# debug ttyd events
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug vni

To enable debugging for a virtual network interface (VNI), use the **debug vni** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug vni {**all** | **errors** | **events** | **info** | **pss**}

no debug vni {**all** | **errors** | **events** | **info** | **pss**}

Syntax Description

all	Enables debugging for all VNI features.
errors	Enables debugging for VNI error conditions.
events	Enables debugging for VNI events.
info	Enables debugging for VNI events.
pss	Enables debugging for VNI PSS packets.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug vni all** command is issued:

```
switch# debug vni all
Apr 29 17:00:59 vni: Received MTS message
Apr 29 17:00:59 vni: message not processed by system mgr library , so process it normal
way
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug vrrp

To enable debugging for a Virtual Router Redundancy Protocol (VRRP), use the **debug vrrp** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug vrrp {**configuration** | **engine**} {**all** | **error** | **event** | **info**}

no debug vrrp {**configuration** | **engine**} {**all** | **error** | **event** | **info**}

Syntax Description

configuration	Enables VRRP configuration debugging.
engine	Enables VRRP engine debugging.
all	Enables debugging for all VRRP features.
error	Enables debugging for VRRP error conditions.
event	Enables debugging for VRRP events.
info	Enables debugging for VRRP events.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug vrrp engine all** command is issued:

```
switch# debug vrrp engine all
Apr 29 17:35:58 vrrp_eng: fu_priority_select:  - setting fd[7] for select call - setting
fd[11] for select call  - setting fd[12] for select call  - setting fd [13] for select
call  - setting fd[15] for select call
Apr 29 17:35:58 vrrp_eng: fu_priority_select_select_queue: round credit(6)
Apr 29 17:35:58 vrrp_eng:     curr_q - FU_PSEL_Q_CAT_FD, usr_q_info(6), fd(15),
priority(2), credit(1), empty
Apr 29 17:35:58 vrrp_eng: fu_priority_select: returning FU_PSEL_Q_CAT_FD queue, fd(7),
usr_q_info(3)
Apr 29 17:35:58 vrrp_eng: heartbeat sent
Apr 29 17:35:58 vrrp_eng: message not processed by system mgr library , so process it
normal way
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show vrrp	Displays VRRP configuration information.

debug vsan

To enable debugging for VSANs, use the **debug vsan** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug vsan {**all** | **global** | **ha** | **info** | **membership** | **mts**}

no debug vsan {**all** | **global** | **ha** | **info** | **membership** | **mts**}

Syntax Description

all	Enables all debugging flags for the VSAN feature.
global	Enables debugging of events for the VSAN global parameter database
ha	Enables debugging of VSAN's HA-related events.
info	Enables debugging of events for VSAN information database.
membership	Enables debugging of events for VSAN membership database.
mts	Enables debugging of Tx/Rx packets of MTS.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug vsan all** command is issued:

```
switch# debug vsan all
2005 Mar 10 01:44:35 vsan: Calling handling function
2005 Mar 10 01:44:35 vsan: querying trunking membership(readonly) for interface:16859136
2005 Mar 10 01:44:35 vsan: Replying to trunking membership query for interface:fc1/21 with
VSAN bitmap:1-4093
2005 Mar 10 01:44:35 vsan: got back reply_code:0
2005 Mar 10 01:44:35 vsan: Returned from handling function
2005 Mar 10 01:44:35 vsan: Freeing notifications
2005 Mar 10 01:44:35 vsan: Src: 0x00000601/15  Dst: 0x00000601/27  ID: 0x0067CEA1  Size:
520 [RSP] Opc: 116 (MTS_OPC_VSAN_GET_PORT_TRUNKING_MEMBERSHIP) RR: 0x0067CEA0  HA_SEQNO:
0x00000000  TS: 0x24E717EAC7CE2  REJ:0  SYNC:1
2005 Mar 10 01:44:35 vsan: 00 00 00 00 00 00 02 00 7F FF FF FF FF FF FF FF
2005 Mar 10 01:44:35 vsan: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
2005 Mar 10 01:44:35 vsan: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
2005 Mar 10 01:44:35 vsan: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
2005 Mar 10 01:44:35 vsan: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
.
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show vsan	Displays information about configured VSANs.

debug wr-reg

To enable debugging for the list of devices using the write-register feature, use the **debug wr-reg** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug wr-reg [*device-name* | *register-address*]

no debug wr-reg [*device-name* | *register-address*]

Syntax Description

device-name	Specifies the device name for the required device.
register-address	Specifies the register address for the required device.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug wr-reg** command is issued:

```
switch# debug wr-reg
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug wwn

To enable debugging for the world wide name (WWN) manager, use the **debug wwn** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug wwn {**all** | **detail** | **errors** | **flow** | **trace**}

no debug wwn {**all** | **detail** | **errors** | **flow** | **trace**}

Syntax Description

all	Enables all WWN debug options.
detail	Enables all WWN output
error	Enables debugging for WWN error conditions.
flow	Enables flow-level WWN debug options.
trace	Enables debugging for WWN traces.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug wwn all** command is issued:

```
switch# debug wwn all
Apr 29 19:24:17 wwn: 53601-wwnm_sdwrap_dispatch:77|SDWRAP massage Successfully processed
Apr 29 19:24:17 wwn: Src: 0x00000601/5206  Dst: 0x00000601/46  ID: 0x002C7DE4  Size: 252
[REQ] Opc: 182 (MTS_OPC_DEBUG_WRAP_MSG) RR: 0x002C7DE4  HA_SEQNO: 0x00000000  TS:
0x55D49A130243  REJ:0
Apr 29 19:24:17 wwn: 2F 64 65 76 2F 70 74 73 2F 30 00 00 00 00 00 00
Apr 29 19:24:17 wwn: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr 29 19:24:17 wwn: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr 29 19:24:17 wwn: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr 29 19:24:17 wwn: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr 29 19:24:17 wwn: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr 29 19:24:17 wwn: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr 29 19:24:17 wwn: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr 29 19:24:17 wwn: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr 29 19:24:17 wwn: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr 29 19:24:17 wwn: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr 29 19:24:17 wwn: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr 29 19:24:17 wwn: 00 00 00 00 00 00 00 00 2E 00 00 00
```

```
Apr 29 19:24:17 wwn: 53601-wwnm_unmask_sigalrm:1261|TRACE:
FILE=_manager/wwnm/wwnm_utilities.c
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show wwn	Displays the status of the WWN configuration.

debug xbar

To enable crossbar debugging (XBAR), use the **debug xbar** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug xbar {**all** | **demux** | **deque** | **error** [**module** *slot*] | **fsm** [**module** *slot*] | **ha** [**module** *slot*] | **init** | **main**}

Syntax Description

all	Enables all XBAR debug options.
demux	Enables debugging for XBAR demux functions.
deque	Enables debugging for XBAR deque events.
error	Enables debugging for XBAR errors.
fsm	Enables debugging for XBAR FSMs.
ha	Enables debugging for XBAR high availability information.
init	Enables debugging for XBAR initialization.
main	Enables XBAR debugging for main functions.
module *slot*	Specifies the slot number of the module being debugged.

Defaults

Enabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug xbar all** command is issued:

```
switch# debug xbar all
Apr 29 19:48:34 xbar:  its a sdwrap msg, fsm utils dropping the mts msg
Apr 29 19:48:34 xbar: fu_fsm_engine: (Error) SYSERR_FU_xx: 0x10, err_num (16) in demux
Apr 29 19:48:34 xbar: fu_fsm_execute_all: match_msg_id(0), log_already_open(0)
Apr 29 19:48:34 xbar: fu_fsm_execute_all: null fsm_event_list
...
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug xbar_driver

To enable debugging of the crossbar driver (XBAR driver), use the **debug xbar_driver** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug xbar {**error** | **flow** | **trace**}

Syntax Description

error	Enables debugging of XBAR driver errors.
flow	Enables debugging of the XBAR driver flow.
trace	Enables debugging of the XBAR driver trace.

Defaults

Enabled.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug xbar_driver** command is issued:

```
switch# debug xbar_driver error
switch# 2006 Jan 23 22:02:41.770329 xbar_driver:  sc_stats_timer_hdlr  called
2006 Jan 23 22:03:41.780356 xbar_driver:  sc_stats_timer_hdlr  called
2006 Jan 23 22:04:41.780356 xbar_driver:  sc_stats_timer_hdlr  called
2006 Jan 23 22:05:41.780357 xbar_driver:  sc_stats_timer_hdlr  called
2006 Jan 23 22:06:41.780356 xbar_driver:  sc_stats_timer_hdlr  called
2006 Jan 23 22:07:41.780359 xbar_driver:  sc_stats_timer_hdlr  called
2006 Jan 23 22:08:41.790341 xbar_driver:  sc_stats_timer_hdlr  called...
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug xbc

To enable crossbar client debugging (XBC), use the **debug xbc** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug xbc {**demux** | **deque** | **init** | **main**}

no debug xbc {**demux** | **deque** | **init** | **main**}

Syntax Description

demux	Enables debugging for crossbar demux functions.
deque	Enables debugging for crossbar deque events.
init	Enables debugging for crossbar initialization.
main	Enables debugging for crossbar main functions.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use this command to debug crossbar client events and information.

Examples

The following example displays the system output when the **debug xbc init** command is issued:

```
switch# debug xbc init
```

Related Commands

Command	Description
no debug all	Disables all debugging.

debug zone

To enable debugging for zones, use the **debug zone** command in EXEC mode. To disable a **debug** command, use the **no** form of the command or use the **no debug all** command to turn off all debugging.

debug zone {**all** |
change {**errors** | **events** | **packets**} |
database {**detail** | **errors** | **events**} |
gs errors {**errors** | **events** | **packets**} |
lun-zoning {**errors** | **events** | **packets**} |
merge {**errors** | **events** | **packets**} |
mts notifications |
pss {**errors** | **events**} ||
read-only-zoning {**errors** | **events** | **packets**} |
tcam errors {**errors** | **events** | **packets**} |
transit {**errors** | **events**}} [**vsan** *vsan-id*]

no debug zone {**all** |
change {**errors** | **events** | **packets**} |
database {**detail** | **errors** | **events**} |
gs errors {**errors** | **events** | **packets**} |
lun-zoning {**errors** | **events** | **packets**} |
merge {**errors** | **events** | **packets**} |
mts notifications |
pss {**errors** | **events**} ||
read-only-zoning {**errors** | **events** | **packets**} |
tcam errors {**errors** | **events** | **packets**} |
transit {**errors** | **events**}} [**vsan** *vsan-id*]

Syntax Description

all	Enables all zone server debug options.
vsan *vsan-id*	Restricts debugging to the specified VSAN.
change	Enables debugging for change protocol messages.
database	Enables debugging for the zone database messages.
errors	Enables debugging for zone errors.
events	Enables debugging for zone events.
packets	Enables debugging for zone packets.
database	Enables debugging for database messages.
gs	Enables debugging for GS protocol messages.
lun-zoning	Enables debugging for LUN zoning messages.
merge	Enables debugging for merge protocol messages.
mts notification	Enables debugging for MTS notification messages.
pss	Enables debugging for PSS debug messages
read-only-zoning	Enables debugging for read-only Zoning messages.
tcam	Enables debugging for TCAM messages.
transit	Enables debugging for transit frame messages.

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system output when the **debug zone all** command is issued:

```
switch# debug zone all
2005 Mar 10 01:46:36 zone: Src: 0x00000601/18  Dst: 0x00000601/94  ID: 0x0067D5CD  Size:
276 [REQ] Opc: 182 (MTS_OPC_DEBUG_WRAP_MSG) RR: 0x0067D5CD  HA_SEQNO: 0x00000000  TS:
0x24E95060E0EF4  REJ:0  SYNC:0
2005 Mar 10 01:46:36 zone: 01 00 00 00 E8 03 00 00 00 00 00 00 00 00 00 00
2005 Mar 10 01:46:36 zone: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2005 Mar 10 01:46:36 zone: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2005 Mar 10 01:46:36 zone: FF FF FF FF 2F 64 65 76 2F 70 74 73 2F 30 00 00
2005 Mar 10 01:46:36 zone: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2005 Mar 10 01:46:36 zone: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.
```

Related Commands

Command	Description
no debug all	Disables all debugging.
show zone	Displays zone information.

CHAPTER 7

E Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "Command Modes" section to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

email-contact

To configure an e-mail contact with the Call Home function, use the **email-addr** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

email-addr *email-address*

no email-addr *email-address*

Syntax Description

email-address	Configures an e-mail address. Uses a standard e-mail address that does not have any text size restrictions.

Defaults

None.

Command Modes

Call Home configuration submode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure e-mail contact in the Call Home configuration.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# email-contact username@company.com
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

enable

To enable the Call Home function, use the **enable** command in Call Home configuration submode. To disable this feature, use the **disable** command.

enable

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

To disable the Call Home function, use the **disable** command.

Examples

The following example shows how to enable the Call Home function.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# enable
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

encryption

To configure an encryption algorithm for an IKE protocol policy, use the **encryption** command. To revert to the default, use the **no** form of the command.

encryption {**3des** | **aes** | **des**}

no encryption

Syntax Description

3des	168-bit DES (3DES)
aes	128-bit AES-CBC
des	56-bit DES-CBS

Defaults

3des

Command Modes

IKE policy configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Examples

The following example shows how to configure the encryption algorithm for the IKE protocol.

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# policy 1
switch(config-ike-ipsec-policy)# encryption 3des
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
policy	Configures IKE policy parameters.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

end

To exit any of the configuration modes and return to EXEC mode, use the **end** command in configuration mode.

end

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can also press **Ctrl-Z** to exit configuration mode.

Examples

The following example changes the name to george. Entering the **end** command causes the system to exit configuration mode and return to EXEC mode.

```
switch(config)# hostname george
george(config)# end
switch#
```

Related Commands

Command	Description
exit	Exits configuration mode, or any of the configuration modes.

enrollment terminal

To enable manual cut-and-paste certificate enrollment through the switch console, use the **enrollment terminal** command in trust point configuration submode. To revert to the default certificate enrollment process, use the **no** form of the command.

enrollment terminal

no enrollment terminal

Syntax Description

This command has no arguments or keywords.

Defaults

The default enrollment method is manual cut-and-paste, which is the only enrollment method that the MDS switch currently supports.

Command Modes

Trust point configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure trust point enrollment through the switch console.

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# enrollment terminal
```

The following example shows how to discard a trust point enrollment through the switch console.

```
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# no enrollment terminal
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the certificate of the certificate authority.

exit

To exit any configuration mode or close an active terminal session and terminate the EXEC, use the exit command at the system prompt.

exit

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC and Configuration modes.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use the **exit** command at the EXEC levels to exit the EXEC mode. Use the **exit** command at the configuration level to return to privileged EXEC mode. Use the **exit** command in interface configuration mode to return to configuration mode. You also can press **Ctrl-Z**, or use the **end** command, from any configuration mode to return to EXEC mode.

Note The **exit** command is associated with privilege level 0. If you configure AAA authorization for a privilege level greater than 0, this command will not be included in the command set for that privilege level.

Examples

The following example displays an exit from the interface configuration mode for VRRP to return to the interface configuration mode.

```
switch(config-if-vrrp)# exit
switch(config-if)#
```

The following example displays an exit from the interface configuration mode to return to the configuration mode.

```
switch(config-if)# exit
switch(config)#
```

The following example shows how to exit an active session (log-out).

```
switch# exit
```

Related Commands

Command	Description
end	Returns you to EXEC mode.

CHAPTER 8

F Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "Command Modes" section to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

fabric-binding activate

To activate fabric binding in a VSAN, use the **fabric-binding activate** command in configuration mode. To disable this feature, use the **no** form of the command.

fabric-binding activate vsan *vsan-id* [**force**]

no fabric-binding activate vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN. The ID of the VSAN is from 1 to 4093.
force	Forces fabric binding activation.

Defaults

Disabled

Command Modes

Configuration mode

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Extended support for fabric binding to Fibre Channel VSANs.

Usage Guidelines

Fabric binding is configured on a per-VSAN basis and can be implemented in both FICON VSANs and Fibre Channel VSANs.

Examples

The following example activates the fabric binding database for the specified VSAN.

```
switch# config terminal
switch(config)# fabric-binding activate vsan 1
```

The following example deactivates the fabric binding database for the specified VSAN.

```
switch(config)# no fabric-binding activate vsan 10
```

The following example activates the fabric binding database for the specified VSAN forcefully—even if the configuration is not acceptable.

```
switch(config)# fabric-binding activate vsan 3 force
```

The following example reverts to the previously-configured state or to the factory default (if no state is configured)

```
switch(config)# no fabric-binding activate vsan 1 force
```

Related Commands

Command	Description
fabric-binding database	Configures a fabric-binding database.
fabric-binding enable	Enables fabric-binding.

fabric-binding database copy

To copy from the active fabric binding database to the configuration fabric binding database, use the **fabric-binding database copy** command in EXEC mode.

fabric-binding database copy vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN. The ID of the VSAN is from 1 to 4093.

Defaults

None

Command Modes

EXEC mode

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Extended support for fabric binding to Fibre Channel VSANs.

Usage Guidelines

Fabric binding is configured on a per-VSAN basis and can be implemented in both FICON VSANs and Fibre Channel VSANs.

If the configured database is empty, this command is not accepted

Examples

The following example copies from the active database to the config database in VSAN 1.

```
switch# fabric-binding database copy vsan 1
```

Related Commands

Command	Description
fabric-binding diff	Provides the differences between the fabric-binding databases.

fabric-binding database diff

To view the differences between the active database and the configuration database in a VSAN, use the **fabric-binding database diff** command in EXEC mode.

fabric-binding database diff {**active** | **config**} **vsan** *vsan-id*

Syntax Description

active	Provides information on the differences in the active database with respect to the configuration database.
config	Provides information on information on the differences in the configuration database with respect to the active database.
vsan *vsan-id*	Specifies the VSAN. The ID of the VSAN is from 1 to 4093.

Defaults

None

Command Modes

EXEC mode

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Extended support of fabric binding to Fibre Channel VSANs.

Usage Guidelines

Fabric binding is configured on a per-VSAN basis and can be implemented in both FICON VSANs and Fibre Channel VSANs.

Examples

The following example displays the differences between the active database and the configuration database in VSAN 1.

```
switch# fabric-binding database diff active vsan 1
```

The following example displays information on the differences between the configuration database and the active database.

```
switch# fabric-binding database diff config vsan 1
```

Related Commands

Command	Description
fabric-binding copy	Copies from the active to the config fabric binding database.

fabric-binding database vsan

To configure a user-specified fabric binding list in a VSAN, use the **fabric-binding database vsan** command in configuration mode. To disable an FC alias, use the **no** form of the command.

fabric-binding database vsan *vsan-id*
swwn *switch-wwn* **domain** *domain-id*

fabric-binding database vsan *vsan-id*
no swwn *switch-wwn* **domain** *domain-id*

no fabric-binding database vsan *vsan-id*

Syntax Description

vsan-id	Specifies the VSAN. The ID of the VSAN is from 1 to 4093.
swwn *switch-wwn*	Configures the switch WWN in dotted hex format.
domain *domain-id*	Specifies the specified domain ID. The domain ID is a number from 1 to 239.

Defaults

None

Command Modes

Configuration mode

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Extended support of fabric binding to Fibre Channel VSANs.

Usage Guidelines

Fabric binding is configured on a per-VSAN basis and can be implemented in both both FICON VSANs and Fibre Channel VSANs.

In a FICON VSAN, the fabric binding feature requires all sWWNs connected to a switch and their persistent domain IDs to be part of the fabric binding active database. In a Fibre Channel VSAN, only the sWWN is required; the domain ID is optional.

A user-specified fabric binding list contains a list of switch WWNs (sWWNs) within a fabric. If an sWWN attempts to join the fabric, and that sWWN is not on the list or the sWWN is using a domain ID that differs from the one specified in the allowed list, the ISL between the switch and the fabric is automatically isolated in that VSAN and the switch is denied entry into the fabric.

The persistent domain ID must be specified along with the sWWN. Domain ID authorization is required in FICON VSANs where the domains are statically configured and the end devices reject a domain ID change in all switches in the fabric.

Note All switches in a non-FICON VSAN must be running Cisco MDS SAN-OS Release 3.x or later.

Examples

The following example enters the fabric binding database submode and adds the sWWN and domain ID of a switch to the configured database list.

```
switch# config terminal
switch(config)# fabric-binding database vsan 5
switch(config-fabric-binding)# swwn 21:00:05:30:23:11:11:11 domain 102
```

The following example deletes a fabric binding database for the specified VSAN.

```
switch# config terminal
switch(config)# no fabric-binding database vsan 10
```

The following example deletes the sWWN and domain ID of a switch from the configured database list.

```
switch# config terminal
switch(config)# fabric-binding database vsan 5
switch(config-fabric-binding)# no swwn 21:00:15:30:23:1a:11:03 domain 101
```

Related Commands

Command	Description
fabric-binding activate	Activates fabric-binding.
fabric-binding enable	Enables fabric-binding.

fabric-binding enable

To enable fabric binding in a VSAN, use the **fabric-binding enable** command. To disable fabric binding, use the **no** form of the command.

fabric-binding enable

no fabric-binding enable

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Configuration mode

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Extended support of fabric binding to Fibre Channel VSANs.

Usage Guidelines

Fabric binding is configured on a per-VSAN basis and can be implemented in both both FICON VSANs and Fibre Channel VSANs.

The fabric binding feature must be enabled in each switch in the fabric that participate in the fabric binding.

Examples

The following examples enables fabric binding on that switch.

```
switch# config t
switch(config)# fabric-binding enable
```

The following example disables fabric binding on that switch.

```
switch# config t
switch(config)# no fabric-binding enable
```

Related Commands

Command	Description
fabric-binding activate	Activates fabric-binding.
fabric-binding database	Configures a fabric-binding database.

fcalias clone

To clone a Fibre Channel alias, use the **fcalias clone** command.

fcalias clone *origFcalias-Name cloneFcalias-Name* **vsan** *vsan-id*

Syntax Description

origFcalias-Name *cloneFcalias-Name*	Clones a Fibre Channel alias from the current name to a new name. Maximum length of names is 64 characters.
vsan	The clone Fibre Channel alias is for a VSAN.
vsan-id	The ID of the VSAN is from 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

To disable an FC alias, use the **no** form of the **fcalias name** command.

Examples

The following examples show how to clone a fcalias named origAlias to cloneAlias on VSAN 45.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# fcalias clone origAlias cloneAlias vsan 45
```

Related Commands

Command	Description
show fcalias	Displays the member name information in a Fibre Channel alias (fcalias).

fcalias name

To configure an FC alias, use the **fcalias name** command. To disable an FC alias, use the **no** form of the command.

fcalias name *alias name* **vsan** *vsan-id*

no fcalias name *alias name* **vsan** *vsan-id*

Syntax Description

alias-name	The name of the fcalias. Maximum length is 64 characters.
vsan	The fcalias is for a VSAN.
vsan-id	The ID of the VSAN is from 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

To include multiple members in any alias, use the FCID, fWWN, or pWWN values.

Examples

The following examples show how to configure an fcalias called AliasSample on VSAN 3.

```
switch# config terminal
switch(config)# fcalias name AliasSample vsan 3
switch(config-fcalias)#
```

Related Commands

Command	Description
member (fcalias configuration mode)	Configures alias member for a specified zone.

fcalias rename

To rename a Fibre Channel alias (fcalias), use the **fcalias rename** command.

fcalias rename *current-name new-name* **vsan** *vsan-id*

Syntax Description

current-name	Specifies the current fcalias name. The maximum length is 64.
new-name	Specifies the new fcalias name. The maximum length is 64.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to rename an fcalias.

```
switch# config terminal
switch(config)# fcalias rename oldalias newalias vsan 10
```

Related Commands

Command	Description
fcalias name	Configures fcalias names.
show fcalias	Displays fcalias information.

fcanalyzer

To configure the Cisco Fabric Analyzer use the **fcanalyzer** command in configuration mode.

fcanalyzer {**local** [**brief**] [**display-filter** *expression*] [**limit-captured-frames** *number*] [**limit-frame-size** *bytes*] [**write** {**slot:** | **volatile:**}] | **remote** *ip-address* [**active** [*port-number*]]}

Syntax Description

local	Begins capturing the frames locally (supervisor module).
brief	Displays the protocol summary in a brief format.
display-filter *expression*	Displays the filtered frames using the provided filter expression.
limit-frame-size *bytes*	Limits the size of the frame captures. The range is 64 to 65536 bytes.
limit-captured-frames *number*	Limits the number of frames captured to 10. The range is 0 to 2147483647 frames and the default is 100 frames. Use 0 if you do not want to limit the captured frames.
write	Saves the captured frames to a specified file.
slot:	Specifies the Flash device in slot 0.
volatile:	Specifies volatile memory.
remote	Configures the remote IP address to which the captured frames will be sent.
ip-address	Specifies IP address or histamine. Maximum length is 1024 characters.
active	Enables active mode (passive is the default) with the remote host.
port-number	Specifies port number

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can capture Fibre Channel control traffic from a switch and decode it without having to disrupt connectivity and without having to be local to the point of analysis.

Examples

The following examples shows how to configure the Cisco Fabric Analyzer.

```
switch# config terminal
switch(config)# fcanalyzer local
Capturing on eth2
switch(config)# fcanalyzer local brief
Capturing on eth2
switch(config)# fcanalyzer local display-filter SampleF
Capturing on eth2
switch(config)# fcanalyzer local limit-frame-size 64
Capturing on eth2
switch(config)# fcanalyzer local limit-captured-frames 10
Capturing on eth2
switch(config)# fcanalyzer local write SampleFile
Capturing on eth2
switch(config)# fcanalyzer remote 10.21.0.3
Capturing on eth2
switch(config)# fcanalyzer remote 10.21.0.3 active
Capturing on eth2
```

Related Commands

Command	Description
clear fcanalyzer	Clears the entire list of configured hosts.
show fcanalyzer	Displays the list of hosts configured for a remote capture.

fcc enable

To enable Fibre Channel Congestion Control (FCC), use the **fcc enable** command in configuration mode. To disable this feature, use the **no** form of the command.

fcc enable

no fcc enable

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Examples

The following example shows how to enable FCC.

```
switch# config terminal
switch(config)# fcc enable
```

Related Commands

Command	Description
show fcc	Displays FCC settings.

fcc priority

To assign the FCC priority to the entire switch, use the **fcc priority** command in configuration mode. To revert to the default, use the **no** form of the command.

fcc priority *number*

no fcc priority *number*

Syntax Description

number	The FCC priority threshold. The range is 0 to 7, where 0 is the lowest priority and 7 the highest priority.

Defaults

The default priority is 4.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

FCC reduces the congestion in the traffic without interfering with standard Fibre Channel protocol.

Examples

The following example shows how to configure the FCC priority threshold as 2.

```
switch# config terminal
switch(config)# fcc priority 2
```

Related Commands

Command	Description
show fcc	Displays FCC settings.

fcdomain

To configure the Fibre Channel domain feature, use the **fcdomain** command. To disable the FC domain, use the **no** form of the command.

fcdomain {**allowed** *domain* **vsan** *vsan-id* |
auto-reconfigure vsan *vsan-id* |
contiguous-allocation vsan *vsan-id* |
domain *id* {**preferred** | **static**} **vsan** *vsan-id* |
fabric-name *name* **vsan** *vsan-id* |
fcid {**database** | **persistent vsan** *vsan-id*} |
optimize fast-restart vsan *vsan-id* |
priority *value* **vsan** *vsan-id* |
restart [**disruptive**] **vsan** *vsan-id* |
vsan *vsan-id*}

no fcdomain {**allowed** *domain* **vsan** *vsan-id* |
auto-reconfigure vsan *vsan-id* |
contiguous-allocation vsan *vsan-id* |
domain *id* {**preferred** | **static**} **vsan** *vsan-id* |
fabric-name *name* **vsan** *vsan-id* |
fcid persistent vsan *vsan-id* |
optimize fast-restart vsan *vsan-id* |
priority *value* **vsan** *vsan-id* |
vsan *vsan-id*}

Syntax Description

allowed *domain*	Configures the allowed domain ID list ranging from 1 to 239.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
auto-reconfigure	Configures autoreconfigure.
contiguous-allocation	Configures contiguous allocation.
domain *id*	Configures the domain ID and its type. The range is 0 to 239.
preferred	Configures the domain ID as preferred. By default, the local switch accepts the domain ID assigned by the principal switch and the assigned domain ID becomes the runtime domain ID.
static	Configures the domain ID as static. The assigned domain ID is discarded, all local interfaces are isolated, and the local switch assigns itself the configured domain ID, which becomes the runtime domain ID.
fabric-name *name*	Specifies the fabric name. The name format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
fcid	Configures FC domain persistent FC IDs.
database	Enters persistent FC IDs submode.
persistent	Enables or disables FC domain persistent FC IDs.
optimize fast-restart	Enables a domain manager fast restart on a specified VSAN.
priority *value*	Specifies the FC domain priority. The range is 1 to 254.
restart	Starts a disruptive or nondisruptive reconfiguration.
disruptive	Forces the disruptive fabric reconfiguration.

Defaults

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.1(1)	This command was introduced.
2.0(1)	The **global-enable** keyword was deprecated.
3.0(2)	Added the **optimize fast-restart** option.

Usage Guidelines

You can use this command to select the principal switch, configure domain ID distribution, reconfigure the fabric, and allocate FC IDs.

We recommend using the **optimize fast-restart** option on most fabrics, especially those with a large number of logical ports (3200 or more), where a logical port is an instance of a physical port in a VSAN.

Examples

The following examples show how to configure the Fibre Channel domain feature.

```
switch# config terminal

switch(config)# fcdomain domain 3 preferred vsan 87

switch(config)# no fcdomain domain 3 preferred vsan 87

switch(config)# fcdomain domain 2 static vsan 237

switch(config)# no fcdomain domain 2 static vsan 237

switch(config)# fcdomain restart vsan 1

switch(config)# fcdomain restart disruptive vsan 1

switch(config)# fcdomain optimize fast-restart vsan 3

switch(config)# fcdomain optimize fast-restart vsan 7 - 10

switch(config)# fcdomain priority 25 VSAN 99

switch(config)# no fcdomain priority 25 VSAN 99

switch(config)# fcdomain auto-reconfigure vsan 10

switch(config)# fcdomain contiguous-allocation vsan 81-83

switch(config)# no fcdomain contiguous-allocation vsan 1030

switch(config)# fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan 3

switch(config)# no fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan 3010

switch(config)# fcdomain allowed 50-110 vsan 4

switch(config)# no fcdomain allowed 50-110 vsan 5
```

Related Commands

Command	Description
show fcdomain	Displays global information about the FC domain configurations.

fcdomain abort vsan

To flush cached data without committing and release the lock, use the **fcdomain abort vsan** command.

fcdomain abort vsan *vsan-id* |

Syntax Description

vsan-id	Specifies a VSAN ID. The range is 1 to 4093.

Defaults

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following examples show how to flush cached data.

```
switch# config terminal
switch(config)# fcdomain abort vsan 10
```

Related Commands

Command	Description
fcdomain	Configures Fibre Channel domain features.
fcdomain commit vsan	Commits cached data and releases the lock.
show fcdomain	Displays global information about the FC domain configurations.

fcdomain commit vsan

To commit cached data and release the lock, use the **fcdomain commit vsan** command.

fcdomain commit vsan *vsan-id* |

Syntax Description

vsan-id	Specifies a VSAN ID. The range is 1 to 4093.

Defaults

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following examples show how to commit cached data.

```
switch# config terminal
switch(config)# fcdomain commit vsan 10
```

Related Commands

Command	Description
fcdomain	Configures Fibre Channel domain features.
fcdomain abort vsan	Flushes cached data without committing and releases the lock.
show fcdomain	Displays global information about the FC domain configurations.

fcdomain distribute

To enable fabric distribution using Cisco Fabric Services (CFS), use the **fcdomain distribute** command. To disable fabric distribution using CFS, us the **no** form of the command.

fcdomain distribute

no fcdomain distribute

Syntax Description

This command has no arguments or keywords

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example enables fabric distribution using CFS.

```
switch# config terminal
switch(config)# fcdomain distribute
```

The following example disables fabric distribution using CFS.

```
switch(config)# no fcdomain distribute
```

Related Commands

Command	Description
fcdomain	Configures Fibre Channel domain features.
show fcdomain	Displays global information about the FC domain configurations.

fcdomain rcf-reject

To enable the RCF reject flag for a Fibre Channel or FCIP interface, use the **fcdomain** option. To disable this feature, use the **no** form of the command.

fcdomain rcf-reject vsan *number*

no fcdomain rcf-reject vsan *number*

Syntax Description

vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Defaults

Enabled

Command Modes

Interface configuration submode

Command History

Release	Modification
1.1(1a)	This command was introduced.

Usage Guidelines

Access this command from the `switch(config-if)#` submode.

Use this option to configure the RCF reject option for the selected Fibre Channel or FCIP interface.

Examples

The following examples show how to configure the FCIP RCF reject fcdomain feature.

```
switch# config terminal
switch(config)# interface fcip 1
switch(config-if)# fcdomain rcf-reject vsan 1
```

Related Commands

Command	Description
show fcdomain	Displays global information about the FC domain configurations.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

fcdroplatency

To configure the network and switch FC drop latency time, use the **fcdroplatency** command in configuration mode. To disable the FC latency time, use the **no** form of the command.

fcdroplatency {network *milliseconds* [**vsan** *vsan-id*] | **switch** *milliseconds*}

no fcdroplatency {network *milliseconds* [**vsan** *vsan-id*] | **switch** *milliseconds*

Syntax Description

network *milliseconds*	Specifies network latency. The range is 500 to 60000.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
switch *milliseconds*	Specifies switch latency. The range is 0 to 60000 milliseconds.

Defaults

2000 millisecond network latency

500 millisecond switch latency

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the network latency to 5000 milliseconds.

```
switch# config terminal
switch(config)#
switch(config)# fcdroplatency network 5000
switch(config)#
```

The following example shows how to revert to the default network latency.

```
switch(config)# no fcdroplatency network 5000
switch(config)#
```

The following example shows how to configure the switch latency to 4000 milliseconds.

```
switch(config)# fcdroplatency switch 4000
switch(config)#
```

The following example shows how to revert to the default switch latency.

```
switch(config)# no fcdroplatency switch 4000
switch(config)#
```

Related Commands

Command	Description
show fcdroplatency	Displays the configured FC drop latency parameters.

fcflow stats

To configure fcflow statistics, use the **fcflow stats** command in configuration mode. To disable the counter, use the **no** form of the command.

fcflow stats {**aggregated module** *module-number* **index** *flow-number* **vsan** *vsan-id* | **module** *module-number* **index** *flow-number destination-fcid source-fcid netmask* **vsan** *vsan-id*}

no fcflow stats {**aggregated module** *module-number* **index** *flow-number* | **module** *module-number* **index** *flow-number*}

Syntax Description

aggregated	Configures aggregated fcflow statistics.
module *module-number*	Configure fcflow statistics on a module.
index *flow-number*	Specifies a flow index. The range is 1 to 2147483647.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
destination-fcid	Enters the destination FCID in hexadecimal format.
source-fcid	Enters the source FCID in hexadecimal format.
netmask	Enters the mask for the source and destination FCID (restricted to 6 hexadecimal characters ranging from 0xff0000 to 0xffffff).

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

If you enable flow counters, you can enable a maximum of 1K entries for aggregate flow and flow statistics. Be sure to assign an unused flow index to a module for each new flow. Flow indexes can be repeated across modules. The number space for flow index is shared between the aggregate flow statistics and the flow statistics.

Examples

The following example shows how to configure aggregated fcflow statistics for module 1.

```
switch-config# fcflow stats aggregated module 1
switch-config#
```

The following example enables the aggregated flow counter.

```
switch(config)# fcflow stats aggregated module 1 index 1005 vsan 1
```

The following example disables the aggregated flow counter.

```
switch(config)# no fcflow stats aggregated module 1 index 1005
```

The following example enables the flow counter for module 1.

```
switch(config)# fcflow stats module 1 index 1 0x145601 0x5601 0xffffff vsan 1
```

The following example disables the flow counter for module 1.

```
switch(config)# no fcflow stats module 2 index 1001
```

Related Commands

Command	Description
show fcflow stats	Displays the configured FC drop latency parameters.

fcid-allocation

Use the **fcid-allocation** command to manually add a FCID to the default area company ID list. Use the **no** form of the command to remove a FCID from the default area company ID list.

fcid-allocation area company-id *company-id*

no fcid-allocation area company-id *company-id*

Syntax Description

area	Modifies the auto area list of company IDs.
company-id *company-id*	Configures the company IDs.

Defaults

None

Command Modes

Configuration mode.

Command History

Release	Modification
2.0	This command was introduced.

Usage Guidelines

Fibre Channel standards require a unique FCID to be allocated to an N port attached to a Fx port in any switch. To conserve the number of FCIDs used, Cisco MDS 9000 Family switches use a special allocation scheme.

Some HBAs do not discover targets that have FCIDs with the same domain and area. Prior to Cisco MDS SAN-OS Release 2.0, the Cisco MDS SAN-OS software maintained a list of tested company ID (also know as Organizational Unit Identifier, or OUI) which do not exhibit this behavior. These Host Bus Adapters (HBAs) were allocated with single FCIDs, and for others a full area was allocated.

The FCID allocation scheme available in Release 1.3 and earlier, allocates a full area to these HBAs. This allocation isolates them to that area and are listed with their pWWN during a fabric login. The allocated FCIDs are cached persistently and are still available in Cisco MDS SAN-OS Release 2.0 (see the “FCID Allocation for HBAs” section on page 38-22).

As of Cisco MDS SAN-OS Release 2.0, to allow further scalability for switches with numerous ports, the Cisco MDS SAN-OS software is maintaining a list of HBAs exhibiting this behavior. Each HBA is identified by its company ID used in the pWWN during a fabric log in. Hence a full area is allocated to the N ports with company IDs that are listed and for the others, a single FCID is allocated. Irrespective of the kind (whole area or single) of FCID allocated, the FCID entries remain persistent.

Examples

The following example adds a new company ID to the default area company ID list.

```
switch# config terminal
switch(config)# fcid-allocation area company-id 0x003223
```

Related Commands

Command	Description
show fcid-allocation	Displays the configured company IDs.

fcid-last-byte

Use the **fcid-last-byte** command to allocate the last byte FCID for the fabric address. To disable the configuration or to revert to factory defaults, use the **no** form of the command.

fcid-last-byte *last-byte-id*

no fcid-last-byte *last-byte-id*

Syntax Description

last-byte-fcid	Specifies the last-byte FCID range from 0 to 250.

Defaults

0

Command Modes

FICON configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	This command was deprecated.

Usage Guidelines

This is an optional configuration. If you are not sure of the EBCDIC format to be used, we recommend retaining the **us-canada** (default) option.

Examples

The following example assigns the last byte FCID for the fabric address.

```
switch# config terminal
switch(config)# ficon vsan 2
switch(config-ficon)# fcid-last-byte 12
```

The following example removes the configured last byte FCID for the fabric address and reverts to the default.

```
switch# config terminal
switch(config)# ficon vsan 2
switch(config-ficon)# no fcid-last-byte 3
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.
ficon vsan *vsan-id*	Enables FICON on the specified VSAN.

fcinterop fcid-allocation

To allocate FCIDs on the switch, use the **fcinterop fcid-allocation** command in configuration mode. To disable FCIDs on the switch, use the **no** form of the command.

fcinterop fcid-allocation {**auto** | **flat** | **none**}

no fcinterop fcid-allocation {**auto** | **flat** | **none**}

Syntax Description

auto	Assigns single FCID to compatible HBAs.
flat	Assign single FCID.
none	Assigns FCID range.

Defaults

The default is **fcinterop fcid-allocation auto**.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command defines how the switch assigns FCIDs.

Examples

```
switch# config terminal
switch(config)# fcinterop fcid-allocation none
switch(config)# fcinterop fcid-allocation flat
switch(config)# fcinterop fcid-allocation auto
```

Related Commands

Command	Description
show flogi database	Displays the fabric login (FLOGI) table.

fcinterop loop-monitor

To monitor removal of discs from a loop port, use the **fcinterop loop-monitor** command in configuration mode. To disable loop monitoring, use the **no** form of the command.

fcinterop loop-monitor

no fcinterop loop-monitor

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command detects devices that are removed from a looped port.

Examples

The following example shows how to enables monitoring of NL ports in a loop.

```
switch# config terminal
switch(config)# fcinterop loop-monitor
```

The following example shows how to disable monitoring of NL ports in a loop.

```
switch# config terminal
switch(config)# no fcinterop loop-monitor
```

Related Commands

Command	Description
show flogi database	Verify if a storage device is displayed in the Fabric login (FLOGI) table.

fcip enable

To enable the FCIP feature in any switch in the Cisco MDS Family, issue the **fcip enable** command.

fcip enable

no fcip enable

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Configuration mode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The configuration and verification commands for the iSCSI feature are only available when FCIP is enabled on a switch. When you disable this feature, all related configurations are automatically discarded.

Examples

The following command enables the FCIP feature.

```
switch(config)# fcip enable
```

The following command disables the FCIP feature (default).

```
switch(config)# no fcip enable
```

Related Commands

Command	Description
show fcip	Displays FCIP information.

fcip profile

To create and configure an FCIP profile, use the **fcip profile** command. To remove an FCIP profile, use the **no** form of the command.

fcip profile *profile-id*

no fcip profile *profile-id*

Syntax Description

profile-id	Specifies a ID range from 1 to 255.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

When you perform this command, the CLI enters FCIP profile configuration mode.

Examples

The following example shows how to configure an FCIP profile.

```
switch## config terminal
switch(config)# fcip profile 5
switch(config-profile)#
```

Related Commands

Command	Description
show fcip profile	Displays information about the FCIP profile.
interface fcip *interface_number* **use-profile** *profile-id*	Configures the interface using an existing profile ID from 1 to 255.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

fcns proxy-port

To register a name server proxy, use the **fcns proxy-port** command in configuration mode.

fcns proxy-port *wwn-id* **vsan** *vsan-id*

no fcns proxy-port *wwn-id* **vsan** *vsan-id*

Syntax Description

wwn-id	Specifies the port WWN, with the format *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

One name server can be configured to proxy another name server and name server information can be displayed using the CLI. The name server can be viewed using the CLI or the Cisco Fabric Manager.

All name server registration requests come from the same port whose parameter is registered or changed. If it does not, then the request is rejected.

Examples

The following example shows configuring a proxy port for VSAN 2.

```
switch# config terminal
switch(config)# fcns proxy-port 21:00:00:e0:8b:00:26:d vsan 2
```

Related Commands

Command	Description
show fcns	Displays the name server database and statistical information for a specified VSAN or for all VSANs.

fcns reject-duplicate-pwwn vsan

To reject duplicate Fibre Channel name server (FCNS) proxies on a VSAN, use the **fcns reject-duplicate-pwwn vsan** command in configuration mode.

fcns reject-duplicate-pwwn vsan *vsan-id*

no fcns reject-duplicate-pwwn vsan *vsan-id*

Syntax Description

vsan-id	Specifies a VSAN ID. The range is 1 to 4093.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example rejects duplicate FCNS pWWNs for VSAN 2.

```
switch# config terminal
switch(config)# fcns reject-duplicate-pwwn vsan 2
```

Related Commands

Command	Description
show fcns	Displays the name server database and statistical information for a specified VSAN or for all VSANs.

fcping

To ping an N port with a specified FCID, use the **fcping fcid** command in EXEC mode.

fcping {**device-alias** *aliasname* | **fcid** {*fc-port* | *domain-controller-id*} | **pwwn** *pwwn-id*} **vsan** *vsan-id* [**count** *number* [**timeout** *value* [**usr-priority** *priority*]]]

Syntax Description

device-alias *aliasname*	Specifies the device alias name. Maximum length is 64 characters.
fcid	The FCID of the destination N port.
fc-port	The port FCID, with the format *0xhhhhhh*.
domain-controller-id	Verifies connection to the destination switch.
pwwn *pwwn-id*	Specifies the port WWN of the destination N port, with the format *hh:hh:hh:hh:hh:hh:hh:hh*.
vsan *vsan-id*	Specifies the VSAN ID of the destination N port. The range is 1 to 4093.
count *number*	Specifies the number of frames to send. A value of 0 sends forever. The range is 0 to 2147483647.
timeout *value*	Specifies the timeout value in seconds. The range is 1 to 10.
usr-priority *priority*	Specifies the priority the frame receives in the switch fabric. The range is 0 to 1.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
1.2(1)	Allowed the domain controller ID as an FCID.
2.0(1b)	Added the **device-alias** *aliasname* option.

Usage Guidelines

To obtain the domain controller address, concatenate the domain ID with **FFFC**. For example, if the domain ID is **0xda**(218), the concatenated ID is **0xfffcda**.

Examples

The following example shows a fcping operation for the specified pWWN or the FCID of the destination. By default, five frames are sent.

```
switch# fcping fcid 0xd70000 vsan 1
28 bytes from  0xd70000  time = 730 usec
28 bytes from  0xd70000  time = 165 usec
28 bytes from  0xd70000  time = 262 usec
28 bytes from  0xd70000  time = 219 usec
28 bytes from  0xd70000  time = 228 usec
```

```
5 frames sent, 5 frames received, 0 timeouts
Round-trip min/avg/max = 165/270/730 usec
```

The following example shows the setting of the number of frames to be sent using the count option. The range is from 0 through 2147483647. A value of 0 will ping forever.

```
switch# fcping fcid 0xd70000 vsan 1 count 10
28 bytes from  0xd70000  time = 730 usec
28 bytes from  0xd70000  time = 165 usec
28 bytes from  0xd70000  time = 262 usec
28 bytes from  0xd70000  time = 219 usec
28 bytes from  0xd70000  time = 228 usec
28 bytes from  0xd70000  time = 230 usec
28 bytes from  0xd70000  time = 230 usec
28 bytes from  0xd70000  time = 225 usec
28 bytes from  0xd70000  time = 229 usec
28 bytes from  0xd70000  time = 183 usec

10 frames sent, 10 frames received, 0 timeouts
Round-trip min/avg/max = 165/270/730 usec
```

The following example shows the setting of the timeout value. The default period to wait is 5 seconds. The range is from 1 through 10 seconds.

```
switch# fcping fcid 0xd500b4 vsan 1 timeout 10
28 bytes from  0xd500b4  time = 1345 usec
28 bytes from  0xd500b4  time = 417 usec
28 bytes from  0xd500b4  time = 340 usec
28 bytes from  0xd500b4  time = 451 usec
28 bytes from  0xd500b4  time = 356 usec

5 frames sent, 5 frames received, 0 timeouts
Round-trip min/avg/max = 340/581/1345 usec
```

This command shows the `No response from the N port` message even when the N port or NL port is active. This is due to resource exhaustion at the N port or NL port. Retry the command a few seconds later.

```
switch# fcping fcid 0x010203 vsan 1
No response from the N port.

switch# fcping pwwn 21:00:00:20:37:6f:db:dd vsan 1
28 bytes from 21:00:00:20:37:6f:db:dd time = 1454 usec
28 bytes from 21:00:00:20:37:6f:db:dd time = 471 usec
28 bytes from 21:00:00:20:37:6f:db:dd time = 372 usec
28 bytes from 21:00:00:20:37:6f:db:dd time = 364 usec
28 bytes from 21:00:00:20:37:6f:db:dd time = 1261 usec

5 frames sent, 5 frames received, 0 timeouts
Round-trip min/avg/max = 364/784/1454 usec
```

The following example displays fcping operation for the device alias of the specified destination.

```
switch# fcping device-alias x vsan 1
28 bytes from 21:01:00:e0:8b:2e:80:93 time = 358 usec
28 bytes from 21:01:00:e0:8b:2e:80:93 time = 226 usec
28 bytes from 21:01:00:e0:8b:2e:80:93 time = 372 usec
```

fcroute

To configure Fibre Channel routes, use the **fcroute** command.

fcroute *fcid* [*network_mask*] **interface** {**fc** *slot*/*port* | **portchannel** *port*} **domain** *domain-id* [[**metric** *number*] **remote**] **vsan** *vsan-id*

Syntax Description

fcid	Specifies the FCID. The format is **0x***hhhhhh*.
network_mask	Specifies the FCID network mask. The format is **0x***hhhhhh*.
interface	Specifies the route for the specified interface.
fc *slot*/*port*	Specifies a Fibre Channel interface.
portchannel *port*	Specifies a PortChannel interface.
domain *domain-id*	Specifies the route for the domain of the next hop switch. The range is 1 to 239.
metric *number*	Specifies the cost of the route. The range is 1 to 65535. Default cost is 10.
remote	Configures the static route for a destination switch remotely connected.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use this command to assign forwarding information to the switch.

Examples

```
switch# config terminal
switch(config)#
switch(config)# fcroute 0x111211 interface fc1/1 domain 3 vsan 2
switch(config)#
switch(config)# fcroute 0x111211 interface port-channel 1 domain 3 vsan 4
switch(config)#
switch(config)# fcroute 0x031211 interface fc1/1 domain 3 metric 1 vsan 1
switch(config-if)#
switch(config)# fcroute 0x111112 interface fc1/1 domain 3 metric 3 remote vsan 3
```

Related Commands

Command	Description
show fcroute	Displays Fibre Channel routes.

fcrxbbcredit extended enable

To enable Fibre Channel extended buffer-to-buffer credits (BB_credits), use the **fcrxbbcredit extended enable** command in configuration mode. To disable the feature, use the **no** form of the command.

fcrxbbcredit extended enable

no fcrxbbcredit extended enable

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

Performing the **fcrxbbcredit extended enable** command enables the **switchport fcrxbbcredit extended** command.

Examples

The following example shows how to enable Fibre Channel extended BB_credits.

```
switch# config terminal
switch(config)# fcrxbbcredit extended enable
```

The following example shows how to disable Fibre Channel extended BB_credits.

```
switch# config terminal
switch(config)# no fcrxbbcredit extended enable
```

Related Commands

Command	Description
switchport fcrxbbcredit extended	Configures Fibre Channel extended BB_credits on an interface.
show interface	Displays interface information and status.

fcs plat-check-global vsan

To enable FCS platform and node name checking fabric wide, use the **fcs plat-check-global vsan** command in configuration mode. To disable this feature, use the **no** form of the command.

fcs plat-check-global vsan *vsan-id*

no fcs plat-check-global vsan *vsan-id*

Syntax Description

vsan-id	Specifies the VSAN ID for platform checking, which is from 1 to 4096.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

```
switch# config terminal
switch(config)# fcs plat-check-global vsan 2
```

Related Commands

Command	Description
show fcs	Displays fabric configuration server information.

fcs register

To register FCS attributes, use the **fcs register** command in configuration mode. To disable this feature, use the **no** form of the command.

fcs register
platform name *name* **vsan** *vsan-id*

fcs register
no platform name *name* **vsan** *vsan-id*

Syntax Description

platform name *name*	Specifies name of the platform to register. Maximum size is 255 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4096.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to register FCS attributes.

```
switch# config terminal
switch(config)# fcs register
switch(config-fcs-register)# platform Platform1 vsan 10
```

Related Commands

Command	Description
show fcs	Displays fabric configuration server information.

fcsp

To configure an Fibre Channel Security Protocol (FC-SP) authentication mode for a specific interface in a FC-SP-enabled switch, use the **fcsp** command. To disable an FC-SP on the interface, use the **no** form of the command.

fcsp {**auto-active** | **auto-passive** | **on** | **off**} [*timeout-period*]

no fcsp

Syntax Description

auto-active	Configures the auto-active mode to authenticate the specified interface.
auto-passive	Configures the auto-passive mode to authenticate the specified interface.
on	Configures the auto-active mode to authenticate the specified interface.
off	Configures the auto-active mode to authenticate the specified interface.
timeout-period	Specifies the time out period to reauthenticate the interface. The time ranges from 0 (default—no authentication is performed) to 100,000 minutes.

Defaults

Auto-passive.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

To use this command, FC-SP must be enabled using the **fcsp enable** command.

Examples

The following example turns on the authentication mode for ports 1 to 3 in Fibre Channel interface 2.

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface fc 2/1 - 3
switch(config-if)# fcsp on
switch(config-if)#
```

The following example reverts to the factory default of auto-passive for these three interfaces.

```
switch(config-if)# no fcsp
```

The following example changes these three interfaces to initiate FC-SP authentication, but does not permit reauthentication.

```
switch(config-if)# fcsp auto-active 0
```

The following example changes these three interfaces to initiate FC-SP authentication and permits reauthentication within two hours (120 minutes) of the initial authentication attempt.

```
switch(config-if)# fcsp auto-active 120
```

Related Commands

Command	Description
fcsp enable	Enable FC-SP.
show interface	Displays an interface configuration for a specified interface.

fcsp dhchap

To configure DHCHAP options in a switch, use the **fcsp dhchap** command in configuration mode. This command is only available when the FC-SP feature is enabled. Use the **no** form of the command to revert to factory defaults.

fcsp dhchap {**devicename** *switch-wwn* **password** [**0** | **7**] *password* |
dhgroup [**0** | **1**| **2** | **3** | **4**] |
hash [**md5** | **sha1**] |
password [**0** | **7**] *password* [**wwn** *wwn-id*]

no fcsp dhchap {**devicename** *switch-wwn* **password** [**0** | **7**] *password* |
dhgroup [**0** | **1**| **2** | **3** | **4**] |
hash [**md5** | **sha1**] |
password [**0** | **7**] *password* [*wwn-id*]

Syntax Description

devicename	Configures a password of another device in the fabric
switch-wwn	Provides the WWN of the device being configured
dhgroup	Configures DHCHAP Diffie-Hellman group priority list.
0	Null DH—no exchange is performed (default).
1| **2**	**3**	**4**	Specifies one or more of the groups specified by the standards.
hash	Configures DHCHAP Hash algorithm priority list in order of preference.
md5	Specifies the MD5 Hash algorithm.
sha1	Specifies the SHA-1 Hash algorithm
password	Configures DHCHAP password for the local switch.
0	Specifies a clear text password.
7	Specifies a password in encrypted text.
password	Provides the password with a maximum of 64 alphanumeric characters
wwn-id	The WWN ID with the format hh:hh:hh:hh:hh:hh:hh:hh.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

You can only see the **fcsp dhchap** command if you issue the **fcsp enable** command.

Using SHA-1 as the hash algorithm may prevent RADIUS or TACACS+ usage.

If you change the DH group configuration, ensure to change it globally for all switches in the fabric.

Examples

The following example enables FC-SP.

```
switch## config terminal
switch(config)# # fcsp enable
switch (config)#
```

The following example configures the use of only the SHA-1 hash algorithm.

```
switch(config)# fcsp dhchap hash sha1
```

The following example configures the use of only the MD-5 hash algorithm.

```
switch(config)# fcsp dhchap hash md5
```

The following example defines the use of the default hash algorithm priority list of MD-5 followed by SHA-1 for DHCHAP authentication.

```
switch(config)# fcsp dhchap hash md5 sha1
```

The following example reverts to the factory default priority list of the MD-5 hash algorithm followed by the SHA-1 hash algorithm.

```
switch(config)# no fcsp dhchap hash sha1
```

The following example prioritizes the use of DH group 2, 3, and 4 in the configured order.

```
switch(config)# fcsp dhchap group 2 3 4
```

The following example reverts to the DHCHAP factory default order of 0, 4, 1, 2, and 3 respectively.

```
switch(config)# no fcsp dhchap group 0
```

The following example configures a clear text password for the local switch.

```
switch(config)# fcsp dhchap password 0 mypassword
```

The following example configures a clear text password for the local switch to be used for the device with the specified WWN.

```
switch(config)# fcsp dhchap password 0 mypassword 30:11:bb:cc:dd:33:11:22
```

The following example removes the clear text password for the local switch to be used for the device with the specified WWN.

```
switch(config)# no fcsp dhchap password 0 mypassword 30:11:bb:cc:dd:33:11:22
```

The following example configures a password entered in an encrypted format for the local switch.

```
switch(config)# fcsp dhchap password 7 sfsfdf
```

The following example configures a password entered in an encrypted format for the local switch to be used for the device with the specified WWN.

```
switch(config)# fcsp dhchap password 7 sfsfdf 29:11:bb:cc:dd:33:11:22
```

The following example removes the password entered in an encrypted format for the local switch to be used for the device with the specified WWN.

```
switch(config)# no fcsp dhchap password 7 sfsfdf 29:11:bb:cc:dd:33:11:22
```

The following example configures a clear text password for the local switch to be used with any connecting device.

```
switch(config)# fcsp dhchap password mypassword1
```

The following example configures a password for another switch in the fabric which is identified by the Switch WWN device name.

```
switch(config)# fcsp dhchap devicename 00:11:22:33:44:aa:bb:cc password NewPassword
```

The following example removes the password entry for this switch from the local authentication database.

```
switch(config)# no fcsp dhchap devicename 00:11:22:33:44:aa:bb:cc password NewPassword
```

The following example configures a clear text password for another switch in the fabric which is identified by the Switch WWN device name.

```
switch(config)# fcsp dhchap devicename 00:11:55:66:00:aa:bb:cc password 0 NewPassword
```

The following example configures a password entered in an encrypted format for another switch in the fabric which is identified by the Switch WWN device name.

```
switch(config)# fcsp dhchap devicename 00:11:22:33:55:aa:bb:cc password 7 asdflkjh
```

Related Commands

Command	Description
fcsp enable	Enable FC-SP.
show fcsp	Displays configured FC-SP information.

fcsp enable

To enable the Fibre Channel Security Protocol (FC-SP) in a switch, use the **fcsp enable** command in configuration mode. Further FC-SP commands are available when the FC-SP feature is enabled. To disable FC-SP, use the **no** form of the command.

fcsp enable

no fcsp enable

Syntax Descriptionf

fcsp	Specifies the FC-SP feature in the switch.
enable	Enables the FC-SP feature in this switch.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example enables FC-SP.

```
switch# config terminal
switch(config)# fcsp enable
switch(config)#
```

Related Commands

Command	Description
show fcsp	Displays configured FC-SP information.

fcsp timeout

To configure the timeout value for FC-SP message, use the **fcsp timeout** command in configuration mode. Use the **no** form of the command to revert to factory defaults.

fcsp timeout *timeout-period*

no fcsp timeout *timeout-period*

Syntax Description

timeout-period	Specifies the time out period. The time ranges from 20 to 100 seconds. The default is 30 seconds.

Defaults

30 seconds

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

You can only see the **fcsp timeout** command if you issue the **fcsp enable** command.

Examples

The following example configures the FCSP timeout value.

```
switch# config terminal
switch(config)# fcsp enable
switch(config)# fcsp timeout 60
```

Related Commands

Command	Description
fcsp enable	Enable FC-SP.
show fcsp	Displays configured FC-SP information.

fctimer

To change the default Fibre Channel timers, use the **fctimer** command in configuration mode. To revert to the default values, use the **no** form of the command.

fctimer {**d_s_tov** *milliseconds* [**vsan** *vsan-id*] | **e_d_tov** *milliseconds* [**vsan** *vsan-id*] | **r_a_tov** *milliseconds* [**vsan** *vsan-id*]}

no fctimer {**d_s_tov** *milliseconds* [**vsan** *vsan-id*] | **e_d_tov** *milliseconds* [**vsan** *vsan-id*] | **r_a_tov** *milliseconds* [**vsan** *vsan-id*]}

Syntax Description

d_s_tov *milliseconds*	Specifies the distributed services time out value. The range is 5000 to 100000 milliseconds.
e_d_tov *milliseconds*	Specifies the error detect time out value. The range is 1000 to 100000 milliseconds, with a default of 2000.
r_a_tov *milliseconds*	Specifies the resolution allocation time out value. The range is 5000 to 100000 milliseconds, with a default of 10000.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4096.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The Cisco MDS 9000, Brocade, and McData FC Error Detect (ED_TOV) and Resource Allocation (RA_TOV) timers default to the same values. They can be changed if needed. In accordance with the FC-SW2 standard, these values must be the same on each switch within in the fabric.

Use the **vsan** option to configure different TOV values for VSANs with special types of links like FC or IP tunnels.

Examples

The following examples show how to change the default Fibre Channel timers.

```
switch# config terminal
switch(config)# fctimer e_d_tov 5000
switch(config)# fctimer r_a_tov 7000
```

Related Commands

Command	Description
show fctimer	Displays the configured Fibre Channel timer values.

fctimer abort

To discard a Fibre Channel timer (fctimer) Cisco Fabric Services (CFS) distribution session in progress, use the **fctimer abort** command in configuration mode.

fctimer abort

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to discard a CFS distribution session in progress.

```
switch# config terminal
switch(config)# fctimer abort
```

Related Commands

Command	Description
fctimer distribute	Enables CFS distribution for fctimer.
show fctimer	Displays fctimer information.

fctimer commit

To apply the pending configuration pertaining to the Fibre Channel timer (fctimer) Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **fctimer commit** command in configuration mode.

fctimer commit

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to commit changes to the active Fibre Channel timer configuration.

```
switch# config terminal
switch(config)# fctimer commit
```

Related Commands

Command	Description
fctimer distribute	Enables CFS distribution for fctimer.
show fctimer	Displays fctimer information.

fctimer distribute

To enable Cisco Fabric Services (CFS) distribution for Fibre Channel timer (fctimer), use the **fctimer distribute** command. To disable this feature, use the **no** form of the command.

fctimer distribute

no fctimer distribute

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Before distributing the Fibre Channel timer changes to the fabric, the temporary changes to the configuration must be committed to the active configuration using the **fctimer commit** command.

Examples

The following example shows how to change the default Fibre Channel timers.

```
switch# config terminal
switch(config)# fctimer distribute
```

Related Commands

Command	Description
fctimer commit	Commits the Fibre Channel timer configuration changes to the active configuration.
show fctimer	Displays fctimer information.

fctrace

To trace the route to an N port, use the **fctrace** command in EXEC mode.

fctrace {device-alias *aliasname* **| fcid** *fcid* **vsan** *vsan-id* [**timeout** *value*] **| pwwn** *pwwn-id* [**timeout** *seconds*]}

Syntax Description

device-alias *aliasname*	Specifies the device alias name. Maximum length is 64 characters.
fcid *fcid*	The FCID of the destination N port, with the format **0x***hhhhhh*
pwwn *pwwn-id*	The PWWN of the destination N port, with the format *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh*.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
timeout *seconds*	Configures the timeout value. The range is 1 to 10.

Defaults

By default, the period to wait before timing out is 5 seconds.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
2.0(1b)	Added the **device-alias** *aliasname* option.

Usage Guidelines

None.

Examples

The following example traces a route to the specified fcid in VSAN 1.

```
switch# fctrace fcid 0x660000 vsan 1
Route present for :  0x660000
20:00:00:05:30:00:5f:1e(0xfffc65)
Latency: 0 msec
20:00:00:05:30:00:61:5e(0xfffc66)
Latency: 0 msec
20:00:00:05:30:00:61:5e(0xfffc66)
```

The following example traces a route to the specified device alias in VSAN 1.

```
switch# fctrace device-alias x vsan 1
Route present for : 21:01:00:e0:8b:2e:80:93
20:00:00:05:30:00:4a:e2(0xfffc67)
```

fc-tunnel

To terminate a Fibre Channel tunnel in a destination switch, use the **fc-tunnel** command. To remove a configuration or revert it to factory defaults, use the **no** form of the command.

fc-tunnel {**enable** | **explicit-path** *name* [**next-address** *ip-address* {**loose** | **strict**}] | **tunnel-id-map** *tunnel-id* **interface fc** *slot-number*}

no fc-tunnel {**enable** | **explicit-path** *name* | **tunnel-id-map** *tunnel-id*}

Syntax Description

enable	Enables the FC tunnel feature
explicit-path *name*	Specifies an explicit path. Maximum length is 16 characters.
next-address *ip-address*	Specifies the IP address of the next hop switch.
loose	Specifies that a direct connection to the next hop is not required.
strict	Specifies that a direct connection to the next hop is required.
tunnel-id-map *tunnel-id*	Specifies fc-tunnel id to outgoing interface. The range is 1 to 255.
interface fc *slot/port*	Configures the Fiber Channel interface in the destination switch.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

All VSANs with RSPAN traffic must be enabled. If a VSAN containing RSPAN traffic is not enabled, it will be dropped.

The FC tunnel can only be configured in the same subnet as the VSAN interface.

The Fibre Channel tunnel feature must be enabled (the **interface fc-tunnel** command) on *each* switch in the end-to-end path of the Fibre Channel fabric in which RSPAN is to be implemented

Examples

The following example enables the FC tunnel feature.

```
switch# config terminal
switchS(config)# fc-tunnel enable
```

The following example places you at the explicit path prompt for the path named Path 1and specifies that the next hop VSAN interface IP addresses.

```
switch# config terminal
switchS(config)# fc-tunnel explicit-path Path1
switchS(config-explicit-path)# next-address 10.10.10.2 strict
switchS(config-explicit-path)# next-address 10.10.10.3 strict
switchS(config-explicit-path)# next-address 10.10.10.4 strict
```

The following example places you at the explicit path prompt for the path named Path 3 and configures a minimum cost path in which this IP address exists.

```
switchS(config)# fc-tunnel explicit-path Path3
switchS(config-explicit-path)# next-address 10.10.10.3 loose
```

The following example configures the FC tunnel (100) in the destination switch (switch D).

```
switchD(config)# fc-tunnel tunnel-id-map 100 interface fc2/1
```

The following example creates two explicit paths and configures the next hop addresses for each path in the source switch (switch S).

```
switchS# config t
switchS(config)# fc-tunnel explicit-path Path1
switchS(config-explicit-path)# next-address 10.10.10.2 strict
switchS(config-explicit-path)# next-address 10.10.10.3 strict
switchS(config-explicit-path)# next-address 10.10.10.4 strict
switchS(config-explicit-path)# exit
switchS(config)# fc-tunnel explicit-path Path3
switchS(config-explicit-path)# next-address 10.10.10.3 loose
```

The following example references the configured path in the source switch (switch S).

```
switchS# config t
switchS(config)# interface fc-tunnel 100
switchS(config)# explicit-path Path1
```

Related Commands

Command	Description
show span session	Displays all SPAN session information.
show fc-tunnel tunnel-id-map	Displays FC tunnel egress mapping information

ficon enable

To enable the FICON feature on a switch, use the **ficon enable** command in configuration mode. To disable the feature or to revert to factory defaults, use the **no** form of the command.

ficon enable

no ficon enable

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The effects of enabling the FICON feature in a Cisco MDS switch are as follows:

- You cannot disable in-order delivery for the FICON-enabled VSAN.
- You cannot disable fabric binding or static domain ID configurations for the FICON-enabled VSAN.
- The load balancing scheme is changed to Source ID (SID)—Destination ID (DID). You cannot change it back to SID—DID—OXID.
- The IPL configuration file is automatically created.

When FICON is enabled on a VSAN, it is implicitly enabled everywhere. However, when FICON is disabled on a VSAN, it remains globally enabled. You must explicitly disable FICON to disable it throughout the fabric.

Examples

The following example enables FICON on the switch.

```
switch(config)# ficon enable
```

The following example disables FICON on the switch.

```
switch(config)# no ficon enable
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.

ficon logical-port assign port-numbers

To reserve FICON port numbers for logical interfaces on the switch, use the **ficon logical-port assign port-numbers** command in configuration mode. To release the port numbers, use the **no** form of the command.

ficon logical-port assign port-numbers [*port-numbers*]

no ficon logical-port assign port-numbers [*port-numbers*]

Syntax Description

port-numbers	Specifies the range of port numbers to assign. The range can be 0 through 153 or 0x0 through 0x99.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You must reserve port numbers for logical interfaces, such as FCIP and PortChannels, if you plan to use them.

You cannot change or release port numbers for interfaces that are active. You must disable the interfaces using the **shutdown** command.

Examples

The following example reserves port numbers 230 through 249 for FCIP and PortChannel interfaces.

```
switch(config)# ficon logical-port assign port-numbers 230-249
```

The following example reserves port numbers 0xe6 through 0xf9 for FCIP and PortChannel interfaces.

```
switch(config)# ficon logical-port assign port-numbers 0xe6-0xf9
```

The following example releases the port numbers.

```
switch(config)# no ficon logical-port assign port-numbers 230-249
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.

ficon port default-state prohibit-all

To set the FICON port default state to prohibit all, use the **ficon port default-state prohibit-all** command in configuration mode. To disable the feature or to revert to factory defaults, use the **no** form of the command.

ficon port default-state prohibit-all

no ficon port default-state prohibit-all

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(2)	This command was introduced.

Usage Guidelines

You can change the default port prohibiting state to enabled in VSANs that you create and then selectively disable port prohibiting on implmeneted ports, if desired. Only the FICON configuration files created after you change the default have the new default setting.

Examples

The following example enables port prohibiting as the default for all implemented interfaces on the switch.

```
switch(config)# ficon port default-state prohibit-all
```

The following example disables port prohibiting as the default for all implemented interfaces on the switch.

```
switch(config)# no port default-state prohibit-all
```

Related Commands

Command	Description
show ficon port default-state	Displays default FICON port prohibit state.

ficon slot assign port-numbers

To reserve FICON port numbers for a slot on the switch, use the **ficon slot assign port-numbers** command in configuration mode. To release the port numbers, use the **no** form of the command.

ficon slot *slot* **assign port-numbers** [*port-numbers*]

no ficon slot *slot* **assign port-numbers** [*port-numbers*]

Syntax Description

slot	Specifies the slot number, 1 through 6.
port-numbers	Specifies the range of port numbers to assign. The range can be 0 through 153, or 0x0 through 0x99.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

A range of 255 port numbers are available for you to assign to all the ports on a switch. You can have more than 255 physical ports on a switch and the excess ports do not have ports numbers in the default numbering scheme. When you have more than 255 physical ports on your switch, you can assign unimplemented port numbers to the ports, or assign duplicate port numbers if they are not used in the same FICON VSAN. For example, you can configure port number 1 on interface fc1/1 in FICON VSAN 10 and fc10/1 in FICON VSAN 20.

FICON port numbers are not changed for ports that are active. You must first disable the interfaces using the **shutdown** command.

You can configure port numbers even when no module is installed in the slot, and before FICON is enabled on any VSAN.

For more information on assigning port numbers, refer to “FICON Port Numbering” in the *Cisco MDS 9000 Family CLI Configuration Guide* or the *Cisco MDS 9000 Family Fabric Manager Configuration Guide.*

Examples

The following example reserves FICON port numbers 0 through 15 and 48 through 63 for up to 32 interfaces in slot 3.

```
swich# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ficon slot 3 assign port-numbers 0-15, 48-63
```

The following example reserves FICON port numbers 0 through 15 for the first 16 interfaces and 0 through 15 for the second 32 interfaces in slot 3.

```
switch(config)# ficon slot 3 assign port-numbers 0-15, 0-15
```

The following example changes the reserved FICON port numbers for up to 24 interfaces in slot 3.

```
switch(config)# ficon slot 3 assign port-numbers 0-15, 56-63
```

The following example releases the port numbers.

```
switch(config)# no ficon slot 3 assign port-numbers 0-15, 56-63
```

The following example shows the switch output when there are duplicate port numbers.

```
switch(config)
switch(config)# no ficon slot 1 assign port-numbers
switch(config)# ficon slot 1 assign port-numbers 0-14, 0
WARNING: fc1/16 and fc1/1 have duplicated port-number 0 in port VSAN 99
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.

ficon swap

To enable the FICON feature in a specified VSAN, use the **ficon swap** command in configuration mode.

ficon swap {interface fc *slot* **fc** *slot* **| portnumber** *port-number port-number*} [**after swap noshut**]

Syntax Description

interface	Configures the interfaces to be swapped.
fc	Specifies the Fibre Channel interface.
slot	Specifies the slot number, 1 through 6.
portnumber	Configures the FICON port number for this interface.
port-number	Specifies the port numbers that must be swapped
after swap noshut	Initializes the port shut down after the ports are swapped.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Added the **interface** option.

Usage Guidelines

The **ficon swap portnumber** *old-port-number new port-number* command causes all configuration associated with *old-port-number* and *new port-number* to be swapped, including VSAN configurations. This command is only associated with the two ports in concerned. You must issue this VSAN-independent command from the EXEC mode.

If you specify the **ficon swap portnumber after swap noshut** command, the ports are automatically initialized.

The **ficon swap interface** *old-interface new-interface* command allows you to swap physical Fibre Channel ports, including port numbers, when there are duplicate port numbers on the switch.

If you specify the **ficon swap interface** *old-interface new-interface* **after swap noshut** command, the ports are automatically initialized.

Refer to the *Cisco MDS 9000 Family CLI Configuration Guide* for additional information.

Examples

The following example swaps the contents of ports 3 with port 15, shuts them down, and automatically initializes both ports.

```
switch# ficon swap portnumber 3 15 after swap noshut
```

The following example swaps the contents of ports 3 with port 15 and shuts them down.

```
switch# ficon swap portnumber 3 15
```

The following example swaps port 1 with port 6.

```
switch# ficon swap interface fc1/1 fc1/6
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.

ficon-tape-accelerator vsan

To enable FICON tape acceleration for the FCIP interface, use the **ficon-tape-accelerator vsan** command in interface configuration submode. To disable FICON tape acceleration for the FCIP interface, use the **no** form of the command.

ficon-tape-accelerator vsan *vsan-id*

no ficon-tape-accelerator vsan *vsan-id*

Syntax Description

vsan-id	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

Disabled.

Command Modes

Interface configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Cisco MDS SAN-OS software provides acceleration for FICON tape write operations over FCIP for the IBM VTS and tape libraries that support the 3490 command set. FICON tape read acceleration over FCIP is not supported.

FICON tape acceleration will not work if multiple inter-switch links (ISLs) are present in the VSAN.

FICON write acceleration and tape acceleration can be enabled at the same time on the FCIP interface.

Examples

The following example enables FICON tape acceleration on the FCIP interface.

```
switch# config terminal
switch(config)# interface fcip 2
switch(config-if)# ficon-tape-accelerator vsan 100
This configuration change will disrupt all traffic on the FCIP interface in all
VSANs.  Do you wish to continue? [no] y
```

The following example disables FICON tape acceleration on the FCIP interface.

```
switch(config-if)# no ficon-tape-accelerator vsan 100
This configuration change will disrupt all traffic on the FCIP interface in all
VSANs.  Do you wish to continue? [no] y
```

Related Commands

Command	Description
write-accelerator	Enables write acceleration and tape acceleration for the FCIP interface.
show fcip	Displays FCIP profile information.

ficon vsan (EXEC mode)

To configure FICON related parameters in EXEC mode, use the **ficon vsan** command. To remove the configuration or revert to the default values, use the **no** form of the command.

ficon vsan *vsan-id* | **apply file** *file-name* | **copy file** *old-file-name new-file-name* | **offline** | **online**}

Syntax Description

vsan-id	Enters the FICON configuration mode for the specified VSAN (from 1 to 4096).
apply file *file-name*	Specifies the existing FICON configuration file name after switch initialization. Maximum length is 80 characters.
copy file	Makes a copy of the specified FICON configuration file.
old-file-name	Specifies the old (existing) FICON configuration file name
new-file-name	Specifies the new name for the copied file.
offline	Logs out all ports in the VSAN that needs to be suspended.
online	Removes the offline condition and to allow ports to log on again.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

When an MDS switch is booting up with saved configuration, if FICON is enabled on a VSAN, the IPL configuration file is applied automatically by the SAN-OS software after the switch initialization is completed.

Use the **ficon vsan** *vsan-id* **copy file** *exiting-file-name save-as-file-name* command to copy an existing FICON configuration file. You can see the list of existing configuration files by issuing the **show ficon vsan** *vsan-id* command

Examples

The following example applies the configuration from the saved files to the running configuration.

```
switch# ficon vsan 2 apply file SampleFile
```

The following example copies an existing FICON configuration file called IPL and renames it to IPL3.

```
switch# ficon vsan 20 copy file IPL IPL3
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.

ficon vsan (configuration mode)

To enable the FICON feature in a specified VSAN, use the **ficon vsan** command in configuration mode. To disable the feature or to revert to factory defaults, use the **no** form of the command.

ficon vsan *vsan-id*

no ficon vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Enters the FICON configuration mode for the specified VSAN (from 1 to 4096).

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

An IPL configuration file is automatically created

Once you enable FICON, you cannot disable in-order delivery, fabric binding, or static domain ID configurations.

When you disable FICON, the FICON configuration file is also deleted.

Examples

The following example enables FICON on VSAN 2.

```
switch(config)# ficon vsan 2
```

The following example disables FICON on VSAN 6.

```
switch(config)# no ficon vsan 6
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.

file

To access FICON configuration files in a specified VSAN, use the **file** command. To disable the feature or to revert to factory defaults, use the **no** form of the command.

file *file-name*

no file *file-name*

Syntax Description

file *file-name*	Creates or accesses the FICON configuration file in the specified VSAN

Defaults

None.

Command Modes

FICON configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The configuration file submode allows you to create and edit FICON configuration files. If a specified file does not exist, it is created. Up to 16 files can be saved. Each file name is restricted to 8 alphanumeric characters.

Examples

The following example accesses the FICON configuration file called IplFile1 for VSAN 2. If this file does not exist, it is created.

```
switch# config terminal
switch(config)# ficon vsan 2
switch(config-ficon)# file IplFile1
switch(config-ficon-file)#
```

The following example deletes a previously-created FICON configuration file.

```
switch(config-ficon)# no file IplFileA
```

Related Commands

Command	Description
ficon vsan	Enable FICON for a VSAN.
show ficon	Displays configured FICON details.

find

To display a list of files on a file system, use the **find** command in EXEC mode.

find *filename*

Syntax Description

filename	Specifies a search string to match to the files in the default directory. Maximum length is 64 characters.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use the **find** (Flash file system) command to display more detail about the files in a particular file system.

Examples

The following example is sample output of all files that begin with the letter *a*:

```
switch# find a
./accountingd
./acl
./ascii_cfg_server
./arping
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
dir	Displays all files in a given file system.

format

To erase all the information on a module, use the **format** command in EXEC mode.

format {**bootflash:** | **slot0:**}

Syntax Description

bootflash:	Specifies bootflash: memory.
slot0:	Specifies the Flash device in slot 0.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The SAN-OS software only supports Cisco-certified CompactFlash devices that are formatted using Cisco MDS switches. Using uncertified CompactFlash devices may result in unpredictable consequences; formatting CompactFlash devices using other platforms may result in errors.

Examples

The following example erases all information on the bootflash memory.

```
switch# format bootflash:
```

fspf config vsan

To configure an FSPF feature for the entire VSAN, use the **fspf config vsan** command in configuration mode. To delete FSPF configuration for the entire VSAN, use the **no** form of the command.

fspf config vsan *vsan-id*
min-ls-arrival *ls-arrival-time*
min-ls-interval *ls-interval-time*
region *region-id*
spf {**hold-time** *spf-holdtime* | **static**}

fspf config vsan *vsan-id*
no min-ls-arrival
no min-ls-interval
no region
no spf {**hold-time** | **static**}

no fspf config vsan *vsan-id*

Syntax Description

vsan-id	Specifies a VSAN ID. The range is 1 to 4093.
min-ls-arrival *ls-arrival-time*	Specifies the minimum time before a new link state update for a domain will be accepted by switch. The parameter *ls-arrival-time* is an integer specifying time in milliseconds. The range is 0 to 65535.
min-ls-interval *ls-interval-time*	Specifies the minimum time before a new link state update for a domain will be generated by the switch. The parameter *ls-interval-time* is an integer specifying time in milliseconds. The range is 0 to 65535.
region *region-id*	Specifies the autonomous region to which the switch belongs. The backbone region has *region-id*=0. The parameter *region-id* is an unsigned integer value ranging from 0 to 255.
spf	Specifies parameters related to SPF route computation.
hold-time *spf-holdtime*	Specifies the time between two consecutive SPF computations. If the time is small then routing will react faster to changes but CPU usage will be more. The parameter *spf-holdtime* is an integer specifying time in milliseconds. The range is 0 to 65535.
static	Forces static SPF computation.

Defaults

In the FSPF configuration mode, the default is dynamic.

If configuring spf hold-time, the default value for FSPF is 0.

If configuring min-ls-arrival, the default value for FSPF is 1000 msecs.

If configuring min-ls-interval, the default value for FSPF is 5000 msecs.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command configures FSPF on VSANs globally.

For the commands issued in FSPF configuration mode, you do not have to specify the VSAN number every time. This prevents configuration errors that might result from specifying the wrong VSAN number for these commands.

Examples

The following example configures FSPF globally in VSAN 1, deletes the FSPF configured in VSAN 3, disables FSPF in VSAN 5, and enables FSPF in VSAN 7.

```
switch## config terminal
switch(config)##
switch(config)# fspf config vsan 1
switch-config-(fspf-config)# spf static
switch-config-(fspf-config)# exit
switch(config)#
switch(config)# no fspf config vsan 3
switch(config)#
```

Related Commands

Command	Description
show fspf interface	Displays information for each selected interface.
fspf enable	Enables FSPF routing protocol in the specified VSAN (from the `switch(config-if)#` prompt).
fspf cost	Configures the cost for the selected interface in the specified VSAN (from the `switch(config-if)#` prompt).
fspf hello-interval	Specifies the hello message interval to verify the health of a link in the VSAN (from the `switch(config-if)#` prompt).
fspf passive	Disables the FSPF protocol for the specified interface in the specified VSAN (from the `switch(config-if)#` prompt).
fspf retrasmit	Specifies the retransmit time interval for unacknowledged link state updates in specified VSAN (from the `switch(config-if)#` prompt).

fspf cost

To configure FSPF link cost for an FCIP interface, use the **fspf cost** command. To revert to the default value, use the **no** form of the command.

fspf cost *link-cost* **vsan** *vsan-id*

no fspf cost *link-cost* **vsan** *vsan-id*

Syntax Description

link-cost	Enters FSPF link cost in seconds. The range is 1 to 65535.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Defaults

1000 seconds for 1 Gbps

500 seconds for 2 Gbps

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Access this command from the `switch(config-if)#` submode.

FSPF tracks the state of links on all switches in the fabric, associates a cost with each link in its database, and then chooses the path with a minimal cost. The cost associated with an interface can be changed using the **fspf cost** command to implement the FSPF route selection.

Examples

The following example configures the FSPF link cost on an FCIP interface.

```
switch# config terminal
switch(config)# interface fcip 1
switch(config-if)# fspf cost 5000 vsan 1
```

Related Commands

Command	Description
show fspf interface	Displays information for each selected interface.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

fspf dead-interval

To set the maximum interval for which a hello message must be received before the neighbor is considered lost, use the **fspf dead-interval** command. To revert to the default value, use the **no** form of the command.

fspf dead-interval *seconds* **vsan** *vsan-id*

no fspf dead-interval *seconds* **vsan** *vsan-id*

Syntax Description

seconds	Specifies the FSPF dead interval in seconds. The rage is 2 to 65535.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Defaults

80 seconds

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Access this command from the `switch(config-if)#` submode.

Note This value must be the same in the ports at both ends of the ISL.

Caution An error is reported at the command prompt if the configured dead time interval is less than the hello time interval.

Examples

The following example configures the maximum interval of 400 seconds for a hello message before the neighbor is considered lost.

```
switch# config terminal
switch(config)# interface fcip 1
switch(config-if)# fspf dead-interval 4000 vsan 1
```

Related Commands

Command	Description
show fspf interface	Displays information for each selected interface.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

fspf enable vsan

To enable FSPF for a VSAN, use the **fspf enable** command in configuration mode. To disable FSPF routing protocols, use the **no** form of the command.

fspf enable vsan *vsan-id*

no fspf enable vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Defaults

Enabled

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command configures FSPF on VSANs globally.

Examples

The following example enables FSPF in VSAN 5 and disables FSPF in VSAN 7.

```
switch## config terminal
switch(config)# fspf enable vsan 5
switch(config)# no fspf enable vsan 7
```

Related Commands

Command	Description
fspf config vsan	Configures FSPF features for a VSAN.
show fspf interface	Displays information for each selected interface.

fspf hello-interval

To verify the health of the link, use the **fspf hello-interval** command. To revert to the default value, use the **no** form of the command.

fspf hello-interval *seconds* **vsan** *vsan-id*

no fspf hello-interval *seconds* **vsan** *vsan-id*

Syntax Description

hello-interval *seconds*	Specifies the FSPF hello-interval in seconds. The rage is 2 to 65535.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Defaults

20 seconds

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Access this command from the `switch(config-if)#` submode.

This command configures FSPF for the specified FCIP interface.

Note This value must be the same in the ports at both ends of the ISL.

Examples

The following example configures a hello interval of 3 seconds on VSAN 1.

```
switch# config terminal
switch(config)# interface fcip 1
switch(config-if)# fspf hello-interval 3 vsan 1
```

Related Commands

Command	Description
show fspf interface	Displays information for each selected interface.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

fspf passive

To disable the FSPF protocol for selected interfaces, use the **fspf passive** command. To revert to the default state, use the **no** form of the command.

fspf passive vsan *vsan-id*

no fspf passive vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Defaults

FSPF is enabled.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Access this command from the `switch(config-if)#` submode.

By default, FSPF is enabled on all E ports and TE ports. FSPF can be disabled by setting the interface as passive using the **fspf passive** command.

Note FSPF must be enabled on the ports at both ends of the ISL for the protocol to operate correctly.

Examples

The following example disables the FSPF protocol for the selected interface on VSAN 1.

```
switch# config terminal
switch(config)# interface fcip 1
switch(config-if)# fspf passive vsan 1
```

Related Commands

Command	Description
show fspf interface	Displays information for each selected interface.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

fspf retransmit-interval

To specify the time after which an unacknowledged link state update should be transmitted on the interface, use the **fspf retransmit-interval** command. To revert to the default value, use the **no** form of the command.

fspf retransmit-interval *seconds* **vsan** *vsan-id*

no spf retransmit-interval *seconds* **vsan** *vsan-id*

Syntax Description

seconds	Specifies FSPF retransmit interval in seconds. The range is 1 to 65535.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Defaults

5 seconds

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Access this command from the `switch(config-if)#` submode.

Note This value must be the same in the ports at both ends of the ISL.

Examples

The following example specifies a retransmit interval of 6 seconds after which an unacknowledged link state update should be transmitted on the interface for VSAN 1.

```
switch# config terminal
switch(config)# interface fcip 1
switch(config-if)# fspf retransmit-interval 6 vsan 1
```

Related Commands

Command	Description
show fspf interface	Displays information for each selected interface.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

CHAPTER 9

G Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "About the CLI Command Modes" section on page 1-3 to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

group

To configure a Modular Exponentiation (MODP) Diffie-Hellman (DH) group for an IKE protocol policy, use the **group** command in IKE policy configuration submode. To revert to the default, use the **no** form of the command.

group {**1** | **2** | **5**}

no group

Syntax Description

1	Specifies 768-bit MODP DH group.
2	Specifies 1024-bit MODP DH group.
5	Specifies 1536-bit MODP DH group.

Defaults

1

Command Modes

IKE policy configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Examples

The following example shows how to configure the DH group for the IKE protocol.

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# policy 1
switch(config-ike-ipsec-policy)# group 1
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
policy	Configures IKE policy parameters.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

gzip

To compress (zip) a specified file using LZ77 coding, use the **gzip** command in EXEC mode.

gzip {**bootflash:** | **slot0:** | **volatile:**} *filename*

Syntax Description

bootflash:	Source location for the file to be compressed and destination of the compressed file.
slot0:	Source location for the file to be compressed and destination of the compressed file.
volatile:	Source location for the file to be compressed and destination of the compressed file.This is the default directory.
filename	The name of the file to be compressed.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is useful in compressing large files. The output of the **show tech-support** command can directed to a file and compressed for further use. The **gzip** command replaces the source file with a compressed .gz file.

Examples

This example directs the output of the **show tech-support** command to a file (Samplefile) and then zips the file and displays the difference in the space used up in the volatile: directory:

```
switch# show tech-support > Samplefile
Building Configuration ...
switch# dir
    1525859     Jul 04 00:51:03 2003  Samplefile
Usage for volatile://
    1527808 bytes used
   19443712 bytes free
   20971520 bytes total
switch# gzip volatile:Samplefile
switch# dir
     266069     Jul 04 00:51:03 2003  Samplefile.gz
Usage for volatile://
     266240 bytes used
   20705280 bytes free
   20971520 bytes total
```

Related Commands

Command	Description
gunzip	Uncompresses LZ77 coded files.

gunzip

To uncompress (unzip) LZ77 coded files, use the **gunzip** command in EXEC mode.

gunzip {**bootflash:** | **slot0:** | **volatile:**} *filename*

Syntax Description

bootflash:	Source location for the compressed file and destination of the uncompressed file.
slot0:	Source location for the compressed file and destination of the uncompressed file.
volatile:	Source location for the compressed file and destination of the uncompressed file. This is the default directory.
filename	The name of the compressed file.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is useful in uncompressing large files. The **gunzip** command replaces the compressed.gz source file with an uncompressed file.

Examples

This example unzips a compressed file on volatile: directory and displays the space used:

```
switch# dir
     266069     Jul 04 00:51:03 2003  Samplefile.gz
Usage for volatile://
     266240 bytes used
   20705280 bytes free
   20971520 bytes total
switch# gunzip Samplefile
switch# dir
    1525859     Jul 04 00:51:03 2003 Samplefile
Usage for volatile://
    1527808 bytes used
   19443712 bytes free
   20971520 bytes total
```

Related Commands

Command	Description
gzip	Compresses a specified file using LZ77 coding.

CHAPTER 10

H Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "About the CLI Command Modes" section on page 1-3 to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

hash

To configure a hash algorithm for an IKE protocol policy, use the **hash** command in IKE policy configuration submode. To revert to the default, use the **no** form of the command.

hash {**md5** | **sha**}

no hash

Syntax Description

md5	Specifies the MD5[1] hash algorithm.
sha	Specifies the SHA[2].

1. MD5 = Message-Digest
2. SHA = Secure Hash Algorithm

Defaults

sha

Command Modes

IKE policy configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Examples

The following example shows how to configure the hash algorithm for the IKE protocol.

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# policy 1
switch(config-ike-ipsec-policy)# hash md5
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
policy	Configures IKE policy parameters.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

host

Use the **host** command to configure the switch offline state, the mainframe access control parameters, and the mainframe time stamp parameters. To disable the configuration or to revert to factory defaults, use the **no** form of the command.

host {**control** [**switch offline**] | **port control** | **set-timestamp**}

no host {**control** [**switch offline**] | **port control** | **set-timestamp**}

Syntax Description

control	Allows the host control of FICON.
switch offline	Allows the host to move the switch to an offline state and shut down the ports (default).
port control	Enables the host to configure FICON parameters.
set-timestamp	Allows the host to set the director clock

Defaults

Host offline control enabled.

Command Modes

FICON configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

By default, the clock in each VSAN is the same as the switch hardware clock. Mainframe users are allowed to change the VSAN-clock.

Examples

The following example prohibits mainframe users from moving the switch to an offline state.

```
switch# config terminal
switch(config)# ficon vsan 2
switch(config-ficon)# no host control switch offline
```

The following example allows the host to move the switch to an offline state and shut down the ports.

```
switch(config-ficon)# host control switch offline
```

The following example prohibits mainframe users to configure FICON parameters in the Cisco MDS switch (default).

```
switch(config-ficon)# no host port control
```

The following example allows mainframe users to configure FICON parameters in the Cisco MDS switch.

```
switch(config-ficon)# host port control
```

The following example prohibits mainframe users from changing the VSAN-specific clock.

```
switch(config-ficon)# no host set-timestamp
```

The following example allows the host to set the clock on this switch (default).

```
switch(config-ficon)# host set-timestamp
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.
ficon vsan *vsan-id*	Enables FICON on the specified VSAN.

hw-module logging onboard

To configure on-board failure logging (OBFL), use the **hw-module logging onboard** command. To disable this feature, use the **no** form of the command.

hw-module logging onboard [module *slot***]** [*log-type*]

no hw-module logging onboard [module *slot***]** [*log-type*]

Syntax Description

module *slot*	Configures OBFL for a specified module.
log-type	Specifies the type of events for on-board failure logging.
cpu-hog	Specifies cpu hog events.
environmental-history	Specifies environmental history events.
error-stats	Specifies error statistics events.
interrupt-stats	Specifies interrupt statistics events.
mem-leak	Specifies memory leak events.
miscellaneous-error	Specifies miscellaneous information events.
obfl-log	Specifies boot uptime, device version, and OBFL history.

Defaults

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

OBFL data uses the module's persistent logging facility to store data in its CompactFlash memory. When OBFL is disabled, the persistent logging facility discards all entries sent to it for logging.

Examples

The following example configures on-board failure logging of memory leak events on module 2.

```
switch# config terminal
switch(config)# hw-module logging onboard module 2 mem-leak
```

Related Commands

Command	Description
clear logging onboard	Clears OBFL information.
show logging onboard	Displays OBFL information.

CHAPTER 11

I Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "About the CLI Command Modes" section on page 1-3 to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

identity

To configure the identity for the IKE protocol, use the **identity** command in IKE configuration submode. To delete the identity, use the **no** form of the command.

identity {**address** | **hostname**}

no identity {**address** | **hostname**}

Syntax Description

address	Sets the IKE identity to be the IPv4 address of the switch.
hostname	Sets the IKE identity to be the host name of the switch.

Defaults

None.

Command Modes

IKE configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Before configuring a certificate for the switch, configure the host name and domain name, and set the identity to be the host name. This allows the certificate to be used for authentication.

Note The host name is the fully qualified domain name (FQDN) of the switch. To use the switch FQDN for the IKE identity, you must first configure both the switch name and the domain name. The FQDN is required for using RSA signatures for authentication.

Examples

The following example shows how to set the IKE identity to the IP address of the switch.

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# identity address 10.10.100.231
```

The following example shows how to delete the IKE identity.

```
switch(config-ike-ipsec)# no identity 10.10.100.231
```

The following example shows how to set the IKE identity to the host name.

```
switch(config-ike-ipsec)# identity hostname node1
```

The following example shows how to delete the IKE identity.

```
switch(config-ike-ipsec)# no identity hostname node1
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

in-order-guarantee

To enable in-order delivery, use the **in-order-guarantee** command in configuration mode. To disable in-order delivery, use the **no** form of the command.

in-order-guarantee [**vsan** *vsan-id*]

no in-order-guarantee [**vsan** *vsan-id*]

Syntax Description

vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

In-order delivery of data frames guarantees frame delivery to a destination in the same order that they were sent by the originator.

Examples

The following example shows how to enable in-order delivery for the entire switch.

```
switch# config terminal
switch(config) # in-order-guarantee
```

The following example shows how to disable in-order delivery for the entire switch.

```
switch(config)# no in-order-guarantee
```

The following example shows how to enable in-order delivery for a specific VSAN.

```
switch(config)# in-order-guarantee vsan 3452
```

The following example shows how to disable in-order delivery for a specific VSAN.

```
switch(config)# no in-order-guarantee vsan 101
```

Related Commands

Command	Description
show in-order-guarantee	Displays the in-order-guarantee status.

initiator

To configure the initiator version and address, use the **initiator** command IKE configuration submode. To revert to the default, use the **no** form of the command.

initiator version *version* **address** *ip-address*

no initiator version *version* **address** *ip-address*

Syntax Description

version	Specifies the protocol version number. The only valid value is 1.
address *ip-address*	Specifies the IP address for the IKE peer. The format is *A.B.C.D*.

Defaults

IKE version 2.

Command Modes

IKE configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Examples

The following example shows how initiator information for the IKE protocol.

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# initiator version 1 address 10.1.1.1
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

install all

To upgrade all modules in any Cisco MDS 9000 family switch, use the **install all** command. This upgrade can happen nondisruptively or disruptively depending on the current configuration of your switch.

install all [{**asm-sfn** | **kickstart** | **ssi** | **system**} *URL*]

Syntax Description

asm-sfn *filename*	Upgrades the ASM image.
system	Upgrades the system image.
ssi	Upgrades the SSI image.
kickstart	Upgrades the kickstart image.
URL	The location URL of the source file to be installed.

The following table lists the aliases for *URL*.

bootflash:	Source location for internal bootflash memory.
slot0:	Source location for the CompactFlash memory or PCMCIA card.
volatile:	Source location for the volatile file system.
tftp:	Source location for a Trivial File Transfer Protocol (TFTP) network server. The syntax for this URL is **tftp:[[//location]/directory]/filename**.
ftp:	Source location for a File Transfer Protocol (FTP) network server. The syntax for this URL is **ftp:[[//location]/directory]/filename**.
sftp:	Source location for a Secure Trivial File Transfer Protocol (SFTP) network server. The syntax for this URL is **sftp:[[//<username@>location]/directory]/filename**.
scp:	Source location for a Secure Copy Protocol (SCP) network server. The syntax for this URL is **scp:[[//location]/directory]/filename**.
image-filename	The name of the source image file.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(3)	This command was introduced.
1.2(2)	Added the **asm-sfn** keyword and made all keywords optional.
2.0(1b)	Added the **ssi** keyword.

Usage Guidelines

The **install all** command upgrades all modules in any Cisco MDS 9000 Family switch.

To copy a remote file, specify the entire remote path exactly as it is.

Caution If a switchover is required when you issue the **install all** command from a Telnet or SSH session, all open sessions are terminated. If no switchover is required, the session remains unaffected. The software issues a self-explanatory warning at this point and provides the option to continue or terminate the installation.

See the *Cisco MDS 9000 Family CLI Configuration Guide* for detailed procedures.

Examples

The following example displays the result of the **install all** command if the system and kickstart files are specified locally.

```
switch# install all sys bootflash:isan-1.3.1 kickstart bootflash:boot-1.3.1

Verifying image bootflash:/boot-1.3.1
[####################] 100% -- SUCCESS

Verifying image bootflash:/isan-1.3.1
[####################] 100% -- SUCCESS

Extracting "slc" version from image bootflash:/isan-1.3.1.
[####################] 100% -- SUCCESS

Extracting "ips" version from image bootflash:/isan-1.3.1.
[####################] 100% -- SUCCESS

Extracting "system" version from image bootflash:/isan-1.3.1.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image bootflash:/boot-1.3.1.
[####################] 100% -- SUCCESS

Extracting "loader" version from image bootflash:/boot-1.3.1.
[####################] 100% -- SUCCESS



Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes  non-disruptive       rolling
     2       yes      disruptive       rolling  Hitless upgrade is not supported
     3       yes      disruptive       rolling  Hitless upgrade is not supported
     4       yes  non-disruptive       rolling
     5       yes  non-disruptive         reset
     6       yes  non-disruptive         reset



Images will be upgraded according to following table:
Module       Image       Running-Version           New-Version  Upg-Required
------  ----------  --------------------  --------------------  ------------
     1         slc               1.3(2a)               1.3(1)           yes
     1        bios      v1.1.0(10/24/03)      v1.1.0(10/24/03)            no
     2         ips               1.3(2a)               1.3(1)           yes
     2        bios      v1.1.0(10/24/03)      v1.1.0(10/24/03)            no
     3         ips               1.3(2a)               1.3(1)           yes
     3        bios      v1.1.0(10/24/03)      v1.1.0(10/24/03)            no
     4         slc               1.3(2a)               1.3(1)           yes
     4        bios      v1.1.0(10/24/03)      v1.1.0(10/24/03)            no
     5      system               1.3(2a)               1.3(1)           yes
```

```
     5   kickstart              1.3(2a)             1.3(1)           yes
     5        bios      v1.1.0(10/24/03)    v1.1.0(10/24/03)          no
     5      loader               1.2(2)             1.2(2)            no
     6      system              1.3(2a)             1.3(1)           yes
     6   kickstart              1.3(2a)             1.3(1)           yes
     6        bios      v1.1.0(10/24/03)    v1.1.0(10/24/03)          no
     6      loader               1.2(2)             1.2(2)            no

Do you want to continue with the installation (y/n)?  [n] y

Install is in progress, please wait.

Syncing image bootflash:/boot-1.3.1 to standby.
[####################] 100% -- SUCCESS

Syncing image bootflash:/isan-1.3.1 to standby.
[####################] 100% -- SUCCESS
Jan 18 23:40:03 Hacienda %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from

Performing configuration copy.
[####################] 100% -- SUCCESS

Module 6: Waiting for module online.
|
Auto booting bootflash:/boot-1.3.1 bootflash:/isan-1.3.1...
Booting kickstart image: bootflash:/boot-1.3.1....
.....................................Image verification OK

Starting kernel...
INIT: version 2.78 booting
Checking all filesystems..r.r.. done.
Loading system software
Uncompressing system image: bootflash:/isan-1.3.1
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCC
INIT: Entering runlevel: 3
```

The following example displays the file output continuation of the **install all** command on the console of the standby supervisor module.

```
Hacienda(standby)#

Auto booting bootflash:/boot-1.3.1 bootflash:/isan-1.3.1...
Booting kickstart image: bootflash:/boot-1.3.1....
.....................................Image verification OK

Starting kernel...
INIT: version 2.78 booting
Checking all filesystems..r.r.. done.
Loading system software
Uncompressing system image: bootflash:/isan-1.3.1
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCC
INIT: Entering runlevel: 3


Continue on installation process, please wait.
The login will be disabled until the installation is completed.

Module 6: Waiting for module online.
Jan 18 23:43:02 Hacienda %PORT-5-IF_UP: Interface mgmt0 is up
Jan 18 23:43:19 Hacienda %LICMGR-3-LOG_LIC_NO_LIC: No license(s) present for feature
FM_SERVER_PKG. Application(s) shutdown in 53 days.
```

```
Jan 18 23:43:19 Hacienda %LICMGR-3-LOG_LIC_NO_LIC: No license(s) present for feature
ENTERPRISE_PKG. Application(s) shutdown in 50 days.
Jan 18 23:43:19 Hacienda %LICMGR-3-LOG_LIC_NO_LIC: No license(s) present for feature
SAN_EXTN_OVER_IP. Application(s) shutdown in 50 days.
Jan 18 23:43:19 Hacienda %LICMGR-3-LOG_LICAPP_NO_LIC: Application port-security running
without ENTERPRISE_PKG license, shutdown in 50 days
Jan 18 23:43:19 Hacienda %LICMGR-4-LOG_LICAPP_EXPIRY_WARNING: Application Roles evaluation
license ENTERPRISE_PKG expiry in 50 days
Jan 18 23:44:54 Hacienda %BOOTVAR-5-NEIGHBOR_UPDATE_AUTOCOPY: auto-copy supported by
neighbor, starting...

Module 1: Non-disruptive upgrading.
[#                   ]   0%Jan 18 23:44:56 Hacienda %MODULE-5-STANDBY_SUP_OK: Supervisor 5
is standby
Jan 18 23:44:55 Hacienda %IMAGE_DNLD-SLOT1-2-IMG_DNLD_STARTED:  Module image download
process. Please wait until completion...
Jan 18 23:45:12 Hacienda %IMAGE_DNLD-SLOT1-2-IMG_DNLD_COMPLETE:  Module image download
process. Download successful.
Jan 18 23:45:48 Hacienda %MODULE-5-MOD_OK: Module 1 is online
[####################] 100% -- SUCCESS

Module 4: Non-disruptive upgrading.
[#                   ]   0%Jan 18 23:46:12 Hacienda %IMAGE_DNLD-SLOT4-2-IMG_DNLD_STARTED:
Module image download process. Please wait until completion...
Jan 18 23:46:26 Hacienda %IMAGE_DNLD-SLOT4-2-IMG_DNLD_COMPLETE:  Module image download
process. Download successful.
Jan 18 23:47:02 Hacienda %MODULE-5-MOD_OK: Module 4 is online
[####################] 100% -- SUCCESS

Module 2: Disruptive upgrading.
...
-- SUCCESS

Module 3: Disruptive upgrading.
...
 -- SUCCESS

Install has been successful.

MDS Switch
Hacienda login:
```

The following example displays the result of the **install all** command if the system and kickstart files are specified remotely.

```
switch# install all system
scp://user@171.69.16.26/tftpboot/HKrel/qa/vegas/final/m9500-sf1ek9-mz.1.3.2a.bin kickstart
scp://user@171.69.16.26/tftpboot/HKrel/qa/vegas/final/m9500-sf1ek9-kickstart-mz.1.3.2a.bin
For scp://user@171.69.16.26, please enter password:
For scp://user@171.69.16.26, please enter password:

Copying image from
scp://user@171.69.16.26/tftpboot/HKrel/qa/vegas/final/m9500-sf1ek9-kickstart-mz.1.3.2a.bin
to bootflash:///m9500-sf1ek9-kickstart-mz.1.3.2a.bin.
[####################] 100% -- SUCCESS

Copying image from
scp://user@171.69.16.26/tftpboot/HKrel/qa/vegas/final/m9500-sf1ek9-mz.1.3.2a.bin to
bootflash:///m9500-sf1ek9-mz.1.3.2a.bin.
[####################] 100% -- SUCCESS

Verifying image bootflash:///m9500-sf1ek9-kickstart-mz.1.3.2a.bin
[####################] 100% -- SUCCESS
```

```
Verifying image bootflash:///m9500-sf1ek9-mz.1.3.2a.bin
[####################] 100% -- SUCCESS

Extracting "slc" version from image bootflash:///m9500-sf1ek9-mz.1.3.2a.bin.
[####################] 100% -- SUCCESS

Extracting "ips" version from image bootflash:///m9500-sf1ek9-mz.1.3.2a.bin.
[####################] 100% -- SUCCESS

Extracting "system" version from image bootflash:///m9500-sf1ek9-mz.1.3.2a.bin.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:///m9500-sf1ek9-kickstart-mz.1.3.2a.bin.
[####################] 100% -- SUCCESS

Extracting "loader" version from image bootflash:///m9500-sf1ek9-kickstart-mz.1.3.2a.bin.
[####################] 100% -- SUCCESS



Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes  non-disruptive       rolling
     2       yes      disruptive       rolling  Hitless upgrade is not supported
     3       yes  non-disruptive       rolling
     4       yes  non-disruptive       rolling
     5       yes  non-disruptive         reset
     6       yes  non-disruptive         reset
     7       yes  non-disruptive       rolling
     8       yes  non-disruptive       rolling
     9       yes      disruptive       rolling  Hitless upgrade is not supported


Images will be upgraded according to following table:
Module       Image       Running-Version           New-Version  Upg-Required
------  ----------  --------------------  --------------------  ------------
     1         slc                1.3(1)                1.3(2a)           yes
     1        bios      v1.1.0(10/24/03)      v1.0.8(08/07/03)            no
     2         ips                1.3(1)                1.3(2a)           yes
     2        bios      v1.1.0(10/24/03)      v1.0.8(08/07/03)            no
     3         slc                1.3(1)                1.3(2a)           yes
     3        bios      v1.1.0(10/24/03)      v1.0.8(08/07/03)            no
     4         slc                1.3(1)                1.3(2a)           yes
     4        bios      v1.1.0(10/24/03)      v1.0.8(08/07/03)            no
     5      system                1.3(1)                1.3(2a)           yes
     5   kickstart                1.3(1)                1.3(2a)           yes
     5        bios      v1.1.0(10/24/03)      v1.0.8(08/07/03)            no
     5      loader                1.2(2)                 1.2(2)            no
     6      system                1.3(1)                1.3(2a)           yes
     6   kickstart                1.3(1)                1.3(2a)           yes
     6        bios      v1.1.0(10/24/03)      v1.0.8(08/07/03)            no
     6      loader                1.2(2)                 1.2(2)            no
     7         slc                1.3(1)                1.3(2a)           yes
     7        bios      v1.1.0(10/24/03)      v1.0.8(08/07/03)            no
     8         slc                1.3(1)                1.3(2a)           yes
     8        bios      v1.1.0(10/24/03)      v1.0.8(08/07/03)            no
     9         ips                1.3(1)                1.3(2a)           yes
     9        bios      v1.1.0(10/24/03)      v1.0.8(08/07/03)            no

Do you want to continue with the installation (y/n)?  [n]
```

Related Commands

Command	Description
install module bios	Upgrades the supervisor or switching module BIOS.
install module loader	Upgrades the bootloader on the active or standby supervisor or modules.
show version	Displays software image version information.

install clock-module

To upgrade the EPLD images of the clock module on a Cisco MDS 9513 Switch Director, use the **install clock-module** command.

install clock-module [epld {bootflash: |slot0: | volatile:}]

Syntax Description

epld	Installs the clock module EPLD from the EPLD Image.
bootflash:	Local URI containing EPLD Image.
slot0:	Local URI containing EPLD Image.
volatile:	Local URI containing EPLD Image.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Use this command on the active supervisor to install the standby clock module EPLD from the specified EPLD image. After upgrading the clock module, power cycle the entire chassis for the change to take effect. It is not sufficient to reboot the chassis; you must turn the power off and on.

Note This command is supported only on the Cisco MDS 9513 Multilayer Switch Director.

Examples

The following example upgrades the EPLD images for the clock module.

```
switch# install clock-module epld bootflash:m9000-epld-3.0.0.278.img
Len 3031343, CS 0x58, string MDS series EPLD image, built on Fri Nov 11 01:11:09 2005
EPLD Curr Ver New Ver
------------------------------------------------------
Clock Controller 0x03 0x04
There are some newer versions of EPLDs in the image!
Do you want to continue (y/n) ? y
Proceeding to program Clock Module B.
Do you want to switchover Clock Modules after programming Clock Module B.
System Will Reset! y/n) ?n
|
Clock Module B EPLD upgrade is successful.
```

Related Commands

Command	Description
show version clock-module epld	Displays the current EPLD versions on the clock module.

install license

To program the supervisor or switching module BIOS, use the **install license** command.

install license [**bootflash:** | **slot0:** | **volatile:**] *file-name*

Syntax Description

bootflash:	Source location for the license file.
slot0:	Source location for the license file.
volatile:	Source location for the license file.
file-name	The name of the license file.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

If a target file name is provided after the source URL, the license file is installed with that name. Otherwise, the filename in the source URL is used. This command also verifies the license file before installing it.

Examples

The following example installs a file named license-file which resides in the bootflash: directory..

```
switch# install license bootflash:license-file
```

Related Commands

Command	Description
show license	Displays license information.

install module bios

To program the supervisor or switching module BIOS, use the **install module bios** command.

install module *module-number* **bios {system [bootflash: | slot0: | volatile: | *system-image*]}**

Syntax Description

module-number	From slot 1 to 9 in a Cisco MDS 9500 Series switch. From slot 1 to 2 in a Cisco MDS 9200 Series switch.
system	Specifies the system image to use (optional). If system is not specified, the current running image is used.
bootflash:	Source location for internal bootflash memory
slot0:	Source location for the CompactFlash memory or PCMCIA card.
volatile:	Source location for the volatile file system.
system-image	The name of the system or kickstart image.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(3)	This command was introduced.

Usage Guidelines

If the BIOS is upgraded, you need to reboot to make the new BIOS effective. You can schedule the reboot at a convenient time so traffic will not be impacted.

The console baud rate automatically reverts to the default rate (9600) after any BIOS upgrade.

The URL is always the system image URL in the supervisor module, and points to the bootflash: or slot0: directories.

Examples

The following example shows how to perform a nondisruptive upgrade for the system.

```
switch# install module 1 bios
Started bios programming .... please wait
###
BIOS upgrade succeeded for module 1
```

In this example, the switching module in slot 1 was updated.

install module epld

To upgrade the electrically programmable logical devices (EPLDs) module, use the **install module epld** command. This command is only for supervisor modules, not switching modules.

install module *module-number* **epld [bootflash: |ftp: | scp: | sftp: | tftp: | volatile:]**

Syntax Description

module-number	Enters the number for the standby supervisor modules or any other line card.
bootflash:	Source location for internal bootflash memory.
ftp	Local/Remote URI containing EPLD Image.
scp	Local/Remote URI containing EPLD Image.
sftp	Local/Remote URI containing EPLD Image.
tftp	Local/Remote URI containing EPLD Image.
volatile:	Source location for the volatile file system.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

Issue this command from the active supervisor module to update any other module.

If you forcefully upgrade a module that is not online, all EPLDs are forcefully upgraded. If the module is not present in the switch, an error is returned. If the module is present, the command process continues.

Do not insert or extract any modules while an EPLD upgrade or downgrade is in progress.

Examples

The following example upgrades the EPLDs for the module in slot 2.

```
switch# install module 2 epld scp://user@10.6.16.22/users/dino/epld.img

The authenticity of host '10.6.16.22' can't be established.
RSA1 key fingerprint is 55:2e:1f:0b:18:76:24:02:c2:3b:62:dc:9b:6b:7f:b7.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.6.16.22' (RSA1) to the list of known hosts.
user@10.6.16.22's password:
epld.img             100% |****************************|  1269 KB    00:00

Module Number                                       2
EPLD                              Curr Ver     New Ver
-----------------------------------------------------
Power Manager                          0x06
XBUS IO                                0x07        0x08
```

```
UD chip Fix                          0x05
Sahara                               0x05        0x05

Module 2 will be powered down now!!
Do you want to continue (y/n) ? y
\ <----------------------------------------------------------progress twirl
Module 2 EPLD upgrade is successful
```

The following example forcefully upgrades the EPLDs for the module in slot 2.

```
switch# install module 2 epld scp://user@10.6.16.22/epld-img-file-path

Module 2 is not online, Do you want to continue (y/n) ? y
cchetty@171.69.16.22's password:
epld.img             100% |****************************|  1269 KB    00:00
\ <----------------------------------------------------------progress twirl
Module 2 EPLD upgrade is successful
```

Related Commands

Command	Description
show version module *number* **epld**	Displays the current EPLD versions.
show version epld	Displays the available EPLD versions.

install module loader

To upgrade the bootloader on either the active or standby supervisor module, use the **install module loader** command. This command is only for supervisor modules, not switching modules.

install module *module-number* **loader kickstart [bootflash: | slot0: | volatile: |** *kickstart-image***]**

Syntax Description

module-number	Enters the module number for the active or standby supervisor modules (only slot 5 or 6).
kickstart	Specifies the kickstart image to use.
bootflash:	Source location for internal bootflash memory
slot0:	Source location for the CompactFlash memory or PCMCIA card.
volatile:	Source location for the volatile file system.
kickstart-image	The name of the kickstart image.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(3)	This command was introduced.

Usage Guidelines

Before issuing the **install module loader** command, be sure to read the release notes to verify compatibility issues between the boot loader and the kickstart or system images.

If you install a loader version that is the same as the currently-installed version, the loader will not be upgraded. When both the current version and the installed version are the same, use the **init system** command to force a loader upgrade.

Examples

The following example shows how to perform a non disruptive upgrade for the system.

```
switch# install module 6 loader bootflash:kickstart_image
```

This example displays the command being issued on the standby supervisor module in slot 6.

Related Commands

Command	Description
show version	Verify the output before and after the upgrade.

install ssi

To perform a nondisruptive upgrade of the SSI image on an SSM, use the **install ssi** command.

install ssi {**bootflash:** | **slot0:** | **modflash:**}*file-name* **module** *slot*

Syntax Description

bootflash:	Source location for the SSI boot image file.
slot0:	Source location for the SSI boot image file.
modflash:	Source location for the SSI boot image file.
file-name	Specifies the SSI boot image file name.
module *slot*	Specifies the module slot number.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.1(2)	This command was introduced.

Usage Guidelines

You can use the **install ssi** command to upgrade or downgrade the SSI boot image if the SSM is only configured for Fibre Channel switching. If your SSM is configured for VSFN or Intelligent Storage Services, you must use the **boot** command to reconfigure the SSI boot variable and reload the module.

The **install ssi** command implicitly sets the SSI boot variable.

Examples

The following example installs the SSI boot image on the module in slot 2.

```
switch# install ssi bootflash:lm9000-ek9-ssi-mz.2.1.2.bin module 2
```

Related Commands

Command	Description
show boot	Displays the current contents of boot variables.
show module	Verifies the status of a module.
boot	Configures the boot variables.

interface

To configure an interface on the Cisco MDS 9000 Family of switches, use the **interface** command in configuration mode.

interface {**cpp** | **fc** | **fc-tunnel** | **fcip** | **gigabitethernet** | **iscsi** | **mgmt** | **port-channel** | **svc** | **vsan**}

Syntax Description

cpp	Configures a Control Plane Process (CPP) interface.
fc	Configures a Fiber Channel interface—see the **interface fc** command.
fc-tunnel	Configures a Fiber Channel link interface—see the **interface fc-tunnel** command.
fcip	Configures a Fibre Channel over IP (FCIP) interface—see the **interface fcip** command.
gigabitethernet	Configures a Gigabit Ethernet interface—see the **interface gigabitethernet** command.
iscsi	Configures an iSCSI interface—see the **interface iscsi** command.
mgmt	Configures a management interface—see the **interface mgmt** command.
port-channel	Configures a PortChannel interface—see the **interface port-channel** command.
svc	Configures a SAN Volume Controller (SVC) interface for the Caching Services Module (CSM)—see the **interface svc** command.
vsan	Configures a VSAN interface—see the **interface vsan** command.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can specify a range of interfaces by issuing a command with the following example format:

interface fc1/1 - 5 , fc2/5 - 7

The spaces are required before and after the dash (-) and before and after the comma (,).

Examples

The following example selects the mgmt 0 interface and enters interface configuration submode.

```
switch# config terminal
switch(config)# interface mgmt 0
switch(config-if)#
```

Related Commands

Command	Description
show interface	Displays an interface configuration for a specified interface.

interface fc

To configure a Fibre Channel interface on the Cisco MDS 9000 Family of switches, use the **interface fc** command in EXEC mode. To revert to defaults, use the **no** form of the command.

interface fc *slot/port*
channel-group {*group-id* [**force**] | **auto**}
fcdomain rcf-reject vsan *vsan-id*
fspf {**cost** *link-cost* **vsan** *vsan-id* | **ficon portnumber** *portnumber* | **dead-interval** *seconds* **vsan** *vsan-id* | **hello-interval** *seconds* **vsan** *vsan-id* | **passive vsan** *vsan-id* | **retransmit-interval** *seconds* **vsan** *vsan-id*}

interface fc *slot/port*
no channel-group {*group-id* [**force**] | **auto**}
no fcdomain rcf-reject vsan *vsan-id*
no fspf {**cost** *link_cost* **vsan** *vsan-id* | **ficon portnumber** *portnumber* | **dead-interval** *seconds* **vsan** *vsan-id* | **hello-interval** *seconds* **vsan** *vsan-id* | **passive vsan** *vsan-id* | **retransmit-interval** *seconds* **vsan** *vsan-id*}

Syntax Description

slot/port	Specifies a slot number and port number.
channel-group	Adds to or removes from a Port Channel.
group-id	Specifies a Port Channel group number from 1 to 128.
force	Forcefully adds a port.
auto	Enables autocreation of port channels.
fcdomain	Enters the interface submode.
rcf-reject	Configures the rcf-reject flag.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
fspf	Configures FSPF parameters.
cost *link-cost*	Configures FSPF link cost. The range is 1 to 65535.
dead-interval *seconds*	Configures FSPF dead interval in seconds. The range is 2 to 65535.
ficon	Configures FICON parameters.
portnumber *portnumber*	Configures the FICON port number for this interface.
hello-interval *seconds*	Configures FSPF hello-interval. The range is 1 to 65535.
passive	Enables or disables FSPF on the interface.
retransmit-interval *seconds*	Configures FSPF retransmit interface in seconds. The range is 1 to 65535.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
2.0(1b)	Added the **auto** option to the **channel-group** keyword.

Usage Guidelines

You can specify a range of interfaces by issuing a command with the following example format:

interface*space***fc1/1***space***-***space***5***space***,***space***fc2/5***space***-***space***7**

Refer to the *Cisco MDS 9000 Family CLI Configuration Guide* for information on port number allocation.

Use the **no shutdown** command to enable the interface.

The **channel-group auto** command enables autocreation of port channels. If autocreation of port channels is enabled for an interface, you must first disable this configuration before downgrading to earlier software versions or before configuring the interface in a manually configured channel group.

Examples

The following example configures ports 1 to 4 in Fibre Channel interface 9.

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# int fc9/1 - 4
```

The following example enables the Fibre Channel interface.

```
switch# config terminal
switch(config)# interface fc1/1
switch(config-if)# no shutdown
```

The following example assigns the FICON port number to the selected Fibre Channel interface.

```
switch# config terminal
switch(config)# interface fc1/1
switch(config-if)# ficon portnumber 15
```

Related Commands

Command	Description
show interface	Displays an interface configuration for a specified interface.
shutdown	Disables and enables an interface.

interface fc-tunnel

To configure a Fibre Channel tunnel and facilitate RSPAN traffic in the Cisco MDS 9000 Family of switches, use the **interface fc-tunnel** command. To remove a configured tunnel or revert to factory defaults, use the **no** form of the command.

interface fc-tunnel *number*
destination *ip-address*
explicit-path *path-name*
source *ip-address*]

no interface fc-tunnel *number*
no destination *ip-address* |
no explicit-path *path-name*
no source *ip-address*

no interface fc-tunnel *number*

Syntax Description

number	Specifies a tunnel ID range form 1 to 255.
destination *ip-address*	Maps the IP address of the destination switch
explicit-path *path-name*	Specifies a name for the explicit path. Maximum length is 16 alphanumeric characters.
source *ip-address*	Maps the IP address of the source switch

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example initiates the FC tunnel (100) in the source switch (switch S).

```
switch(config)# config terminal
switch(config)# interface fc-tunnel 100
switch(config-if)#
```

The following example maps the IP address of the source switch (switch S) to the FC tunnel (100).

```
switchS(config-if)# source 10.10.10.1
```

The following example maps the IP address of the destination switch (switch D) to the FC tunnel (100).

```
switch(config-if)# destination 10.10.10.2
```

The following example enables traffic flow through this interface.

```
switch(config-if)# no shutdown
```

The following example references the configured path in the source switch (switch S).

```
switch# config t
switch(config)# interface fc-tunnel 100
switch(config)# explicit-path Path1
```

Related Commands

Command	Description
show interface fc-tunnel	Displays an FC tunnel interface configuration for a specified interface.
fc-tunnel explicit-path	Configures a new or existing next-hop path.

interface fcip

To configure a Fibre Channel over IP Protocol (FCIP) interface on the Cisco MDS 9000 Family of switches, use the **interface fcip** command. To disable a FCIP interface, use the **no** form of the command.

interface fcip *interface_number*
bport
bport-keepalives
channel-group *number* [**force**]
fcdomain rcf-reject vsan *vsan-id*
ficon portnumber *portnumber* |
fspf {**cost** *link-cost* | **dead-interval** *seconds* | **hello-interval** *seconds* | **passive** |
retransmit-interval *seconds*} **vsan** *vsan-id*
passive-mode
peer-info ipaddr *ip-address* [**port** *number*]
qos control *control-value* **data** *data-value*
special-frame peer-wwn *pwwn-id*
tcp-connections *number*
time-stamp [**acceptable-diff** *number*]
use-profile *profile-id*

interface fcip *interface_number*
no bport
no bport-keepalives
no channel-group *number* [**force**]
no fcdomain rcf-reject vsan *vsan-id*
no ficon portnumber *portnumber*
no fspf {**cost** *link-cost* | **dead-interval** *seconds* | **hello-interval** *seconds* | **passive** |
retransmit-interval *seconds*} **vsan** *vsan-id*
no qos *control-value* **data** *data-value*
no passive-mode
no peer-info ipaddr *ip-address* [**port** *number*]
no special-frame peer-wwn *pwwn-id*
no tcp-connections *number*
no time-stamp [**acceptable-diff** *number*]
no use-profile *profile-id*

Syntax Description

interface-number	Configures the specified interface from 1 to 255.
bport	Sets the B port mode.
bport-keepalives	Sets the B port keepalive responses.
channel-group *number*	Specifies a PortChannel number from 1 to 128.
force	Forcefully adds a port.
fcdomain	Enters the fcdomain mode for this FCIP interface
rcf-reject	Configures the rcf-reject flag.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
fspf	Configures FSPF parameters.
cost *link-cost*	Enters FSPF link cost. The range is 1 to 65535
dead-interval *seconds*	Specifies the dead interval in seconds. The range is 1 to 65535.

ficon	Configures FICON parameters.
portnumber *portnumber*	Configures the FICON port number for this interface.
hello-interval *seconds*	Specifies FSPF hello-interval in seconds. The range is 1 to 65535.
passive	Enables or disables FSPF on the interface.
retransmit-interval	Specifies FSPF retransmit interface in seconds. The range is 1 to 65535.
passive-mode	Configures a passive connection.
peer-info	Configures the peer information.
ipaddr *ip-address*	Specifies the peer IP address.
port *number*	Specifies the peer port number. The range is 1 to 65535.
qos	Configures the differentiated services code point (DSCP) value to mark all IP packets.
control *control-value*	Specifies the control value for DSCP.
data *data-value*	Specifies the data value for DSCP.
special-frame	Configures special frames.
peer-wwn *pwwn-id*	Specifies the peer WWN for special frames.
switchport	Configures switchport parameters.
tcp-connections *number*	Specifies the number of TCP connection attempts. Valid values are 1 or 2.
time-stamp	Configures time-stamp.
acceptable-diff *number*	Specifies the acceptable time difference for time-stamps. The range is 1 to 60000.
use-profile *profile-id*	Specifies the interface using an existing profile ID. The range is 1 to 255.

Defaults

Disabled

Command Modes

Configuration mode

Command History

Release	Modification
1.1(1)	This command was introduced.
1.3(1)	Added the **ficon portnumber** subcommand.
2.0(1b)	Added the **qos** subcommand.

Usage Guidelines

You can specify a range of interfaces by issuing a command with the following example format:

interface fcip1*space***-***space***5***space***,***space***fcip10***space***-***space***12***space*

Refer to the *Cisco MDS 9000 Family CLI Configuration Guide* for information on port number allocation.

Examples

The following example selects an FCIP interface and enters interface configuration submode.

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface fcip 1
switch(config-if)#
```

The following example assigns the FICON port number to the selected FCIP interface.

```
switch# config terminal
switch(config)# interface fcip 51
switch(config-if)# ficon portnumber 234
```

Related Commands

Command	Description
show interface fcip	Displays an interface configuration for a specified FCIP interface.

interface gigabitethernet

To configure an Gigabit Ethernet interface on the Cisco MDS 9000 Family of switches, use the **interface gigabitethernet** command. To revert to the default values, use the **no** form of the command.

interface gigabitethernet *slot/port*
cdp enable
channel-group *group-id* [**force**]
isns *profile-name*

interface gigabitethernet *slot/port*
no cdp enable
no channel-group
no isns *profile-name*

Syntax Description

slot/port	Specifies a slot number and port number.
cdp enable	Enables Cisco Discovery Protocol (CDP) configuration parameters.
channel-group *group-id*	Adds to or removes from a PortChannel. The range is 1 to 128.
force	Forcefully adds a port.
isns *profile-name*	Specifies the profile name to tag the interface. Maximum length is 64 characters.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(3a)	This command was introduced.
1.1(1a)	Added the **channel-group** subcommand.
1.3(1)	Added the **isns** subcommand.

Usage Guidelines

You can specify a range of interfaces by issuing a command with the following example format:

interface gigabitethernet1/1*space***-***space***2***space***,***space***gigabitethernet3/1***space***-***space***2**

Examples

The following example configures the Gigabit Ethernet interface at slot 4 port 1.

```
switch# config terminal
switch(config)# interface gigabitethernet 4/1
switch(config-if)#
```

The following example enters a IP address and subnet mask for the selected Gigabit Ethernet interface.

```
switch(config-if)# ip address 10.1.1.100 255.255.255.0
```

The following example changes the IP maximum transmission unit (MTU) value for the selected Gigabit Ethernet interface.

```
switch(config-if)# switchport mtu 3000
```

The following example creates a VR ID for the selected Gigabit Ethernet interface, configures the virtual IP address for the VR ID (VRRP group), and assigns a priority.

```
switch(config-if)# vrrp 100
switch(config-if-vrrp)# address 10.1.1.100
switch(config-if-vrrp)# priority 10
```

The following example adds the selected Gigabit Ethernet interface to a channel group. If the channel group does not exist, it is created, and the port is shut down.

```
switch(config-if)# channel-group 10
gigabitethernet 4/1 added to port-channel 10 and disabled
please do the same operation on the switch at the other end of the port-channel, then do
"no shutdown" at both ends to bring them up
```

Related Commands

Command	Description
show interface	Displays an interface configuration for a specified interface.

interface iscsi

To configure an iSCSI interface on the Cisco MDS 9000 Family of switches, use the **interface iscsi** command. To revert to default values, use the **no** form of the command.

interface iscsi *slot/port*
mode {**pass-thru** | **store-and-forward**}
tcp qos *value*

interface iscsi *slot/port*
no mode {**pass-thru** | **store-and-forward** | **cut-thru**}
no tcp qos *value*

no interface iscsi *slot/port*

Syntax Description

slot/port	Specifies a slot number and port number.
mode	Configures a forwarding mode.
pass-thru	Forwards one frame at a time.
store-and-forward	Forwards data in one assembled unit (default).
cut-thru	Forwards one frame at a time without waiting for the exchange to complete.
tcp qos *value*	Configures the differentiated services code point (DSCP) value to apply to all outgoing IP packets. The range is 0 to 63.

Defaults

Disabled.

The TCP QoS default is 0.

The forwarding mode default is **store-and-forward**.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.1(1)	Added the **cut-thru** option for the **mode** subcommand.

Usage Guidelines

To configure iSCSI interface, enable iSCSI using the **iscsi enable** command.

You can specify a range of interfaces by issuing a command with the following example format:
interface iscsi *space* fc1/1*space-space*5*space*,*space*fc2/5*space-space*7

Examples

The following example enables the iSCSI feature.

```
switch# config t
switch(config)# iscsi enable
```

The following example enables the store-and-forward mode for iSCSI interfaces 9/1 to 9/4.

```
switch(config)# interface iscsi 9/1 - 4
switch(config-if)# mode store-and-forward
```

The following example reverts to using the default pass-thru mode for iSCSI interface 9/1.

```
switch(config)# interface iscsi 9/1
switch(config-if)# mode pass-thru
```

Related Commands

Command	Description
iscsi enable	Enables iSCSI.
show interface	Displays an interface configuration for a specified interface.

interface mgmt

To configure a management interface on the Cisco MDS 9000 Family of switches, use the **interface mgmt** command in configuration mode.

interface mgmt *number*

Syntax Description

number	Specifies the management interface number which is 0.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

When you try to shutdown a management interface(mgmt0), a follow-up message confirms your action before performing the operation. Use the **force** option to bypass this confirmation, if required.

Examples

The following example configures the management interface, displays the options available for the configured interface, and exits to configuration mode.

```
switch# config terminal
switch(config)#
switch(config)# interface mgmt 0
switch(config-if)# exit
switch(config)#
```

The following example shuts down the interface without using the **force** option:

```
switch# config terminal
switch(config)# interface mgmt 0
switch(config-if)# shutdown
Shutting down this interface will drop all telnet sessions.
Do you wish to continue (y/n)? y
```

The following example shuts down the interface using the **force** option:

```
switch# config terminal
switch(config)# interface mgmt 0
switch(config-if)# shutdown force
switch(config-if)#
```

Related Commands

Command	Description
show interface mgmt	Displays interface configuration for specified interface.

interface port-channel

To configure a PortChannel interface on the Cisco MDS 9000 Family of switches, use the **interface port-channel** command.

interface port-channel *number*
channel mode active
fcdomain rcf-reject vsan *vsan-id*
fspf [cost *link_cost* **| dead-interval** *seconds* **| ficon portnumber** *portnumber* **| hello-interval** *seconds* **| isns** *profile-name* **| passive | retransmit-interval** *seconds***]**

interface port-channel *number*
no channel mode active
no fcdomain rcf-reject vsan *vsan-id*
no fspf [cost *link_cost* **| dead-interval** *seconds* **| ficon portnumber** *portnumber* **| hello-interval** *seconds* **| isns** *profile-name* **| passive | retransmit-interval** *seconds***]**

no interface port-channel *number*

Syntax Description

number	Enter PortChannel number. The range is 1 to 128.
channel mode active	Configures the channel mode for the PortChannel interface
fcdomain	Enter the interface submode
rcf-reject	Configure the rcf-reject flag
vsan	Specify the vsan range
vsan-id	The ID of the VSAN is from 1 to 4093.
fspf	Configure FSPF parameters
cost	Configure FSPF link cost
link_cost	Enter FSPF link cost 1-65535
dead-interval	Configure FSPF dead interval
seconds	Enter dead interval (in sec) 2-65535
ficon	Configures FICON parameters.
portnumber *portnumber*	Configures the FICON port number for this interface.
hello-interval	Configure FSPF hello-interval
seconds	Enter hello interval (in sec) 1-65535
isns	Tags this interface to the Internet Storage Name Service (iSNS) profile.
profile-name	SPecifies the profile name to tag the interface.
passive	Enable/disable FSPF on the interface
retransmit-interval	Configure FSPF retransmit interface
seconds	Enter retransmit interval (in sec) 1-65535

Defaults

Disabled

Command Modes

Configuration mode

Command History

Release	Modification
1.0(2)	This command was introduced.
1.3(1)	Added **channel mode active** subcommand.

Usage Guidelines

Refer to the *Cisco MDS 9000 Family CLI Configuration Guide* for information on port number allocation.

Examples

The following example enters configuration mode and configures a PortChannel interface.

```
switch# config terminal
switch(config)# interface port-channel 32
switch(config-if)#
```

The following example assigns the FICON port number to the selected PortChannel port.

```
switch# config terminal
switch(config)# interface Port-channel 1
switch(config-if)# ficon portnumber 234
```

Related Commands

Command	Description
show interface	Displays interface configuration for specified interface.

interface vsan

To configure a VSAN interface on the Cisco MDS 9000 Family of switches, use the **interface vsan** command. To remove a VSAN interface, use the **no** form of the command.

interface vsan *vsan-id*

no interface vsan *vsan-id*

Syntax Description

vsan-id	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example selects a VSAN interface and enters interface configuration submode.

```
switch# config terminal
switch(config)# interface vsan 1
switch(config-if)#
```

Related Commands

Command	Description
show interface	Displays interface configuration for specified interface.

ip access-group

To apply an access list to an interface, use the **ip access-group** command in interface mode. Use the **no** form of this command to negate a previously issued command or revert to factory defaults.

ip access-group *access-list-name* **[in | out]**

Syntax Description

access-list-name	Specifies the IP access list name. The maximum length is 64 alphanumeric characters and the text is case insensitive.
in	Specifies that the group is for ingress traffic.
out	Specifies that the group is for egress traffic.

Defaults

The access list is applied to both ingress and egress traffic.

Command Modes

Interface mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

The **ip access-group** command controls access to an interface. Each interface can only be associated with one access list. The access group becomes active immediately.

We recommend creating all rules in an access list, before creating the access group that uses that access list.

If you create an access group before an access list, the access list is created and all packets in that interface are dropped, because the access list is empty.

The access-group configuration for the ingress traffic applies to both local and remote traffic. The access-group configuration for the egress traffic applies only to local traffic. You can apply a different access list for each type of traffic.

Examples

The following example creates an access group called aclPermit for both the ingress and egress traffic (default)

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip access-list aclPermit permit ip any any
switch(config)# interface Gigabitethernet 3/1
switch(config-if)# ip access-group aclPermit
```

The following example deletes the access group called aclPermit.

```
switch(config-if)# no ip access-group aclPermit
```

The following example creates an access group called aclDenyTcp (if it does not already exist) for ingress traffic.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip access-list aclDenyTcp deny tcp any any
switch(config)# interface gigabitethernet 3/1
switch(config-if)# ip access-group aclDenyTcp in
```

The following example deletes the access group called aclDenyTcp for ingress traffic.

```
switch(config-if)# no ip access-group aclDenyTcp in
```

The following example creates an access list called aclPermitUdp (if it does not already exist) for local egress traffic.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip access-list aclPermitUdp permit udp 192.168.32.0 0.0.7.255 any
switch(config)# interface gigabitethernet 3/1
switch(config-if)# ip access-group aclPermitUdp out
```

The following example removes the access list called aclPermitUdp for local egress traffic.

```
switch(config-if)# no ip access-group aclPermitUdp out
```

Related Commands

Command	Description
ip access-list	Configures IP access control lists.
show ip access-list	Displays the IP-ACL configuration information.

ip access-list

To configure IP access control lists (ACLs), use the **ip access-list** command in configuration mode. To negate a previously issued command or revert to factory defaults, use the **no** form of the command.

ip access-list *list-name* {**deny** | **permit**} *ip-protocol*
{*src-addr src-wildcard*}
{*dest-addr dest-wildcard* | *operator port-value*}
[*operator* **port** *port-value]*
[**established** | **icmp-type** *icmp-value*]
[**tos** *tos-value*]
[**log-deny**]

Syntax Description

list-name	Configures an access list with this name.The maximum length is 64 characters.
deny	Denies access if the conditions match.
permit	Allows access if the conditions match.
ip-protocol	Specifies the name or number (integer range from 0 to 255) of an IP protocol. The IP protocol name can be **icmp**, **ip**, **tcp**, or **udp**.
src-addr	Specifies the network from which the packet is sent. There are two ways to specify the source: • A 32-bit quantity in four-part, dotted-decimal format • A keyword **any** as an abbreviation for a destination and a destination-wildcard of 0.0.0.0 255.255.255.255
src-wildcard	Applies the wildcard bits to the source. Each wildcard bit set to zero indicates that the corresponding bit position in the packet's IP address must exactly match the bit value in the corresponding position of the packet's ip address or it will not be considered a match to this access list. There are two ways to specify the destination wildcard: • A 32-bit quantity in four-part, dotted-decimal format • A keyword **any** as an abbreviation for a destination and a destination-wildcard of 0.0.0.0 255.255.255.255
dest-addr	Specifies the network from which the packet is sent. There are two ways to specify the destination: • A 32-bit quantity in four-part, dotted-decimal format • A keyword **any** as an abbreviation for a destination and a destination-wildcard of 0.0.0.0 255.255.255.255
dest-wildcard	Applies the wildcard bits to the destination. There are two ways to specify the destination wildcard: • A 32-bit quantity in four-part, dotted-decimal format • A keyword **any** as an abbreviation for a destination and a destination-wildcard of 0.0.0.0 255.255.255.255

operator	Compares source or destination ports to the packet and has the following options: **any** = Any destination IP **eq** = Equal source port **gt** = Greater than and including source port **lt** = Less than and including source port **range port** = Source port range *port-value*
port *port-value*	Specifies the decimal number (ranging from 0 to 65535) or one of the following names to indicate a TCP or UDP port. The TCP port names are: dns, ftp, ftp-data, http, ntp, radius, sftp, smtp, snmp, snmp-trap, ssh, syslog, tacacs-ds, telnet, wbem-http, wbem-https, and www. The UDP port names are: dns, ftp, ftp-data, http, ntp, radius, sftp, smtp, snmp, snmp-trap, ssh, syslog, tacacs-ds, telnet, tftp, wbem-http, wbem-https, and www.
icmp-type *icmp-value*	Filters ICMP packets by ICMP message type. The range is 0 to 255. The types include: echo, echo-reply, redirect, time-exceeded, traceroute, and unreachable.
established	Indicates an established connection for the TCP protocol. A match occurs if the TCP datagram has the ACK, FIN, PSH, RST, SYN or URG control bits set. The non-matching case is that of the initial TCP datagram to form a connection.
tos *tos-value*	Filters packets by the following type of service level: normal-service (0), monetary-cost (1), reliability (2), throughput (4), and delay (8).
log-deny	Sends an information logging message to the console about the packet that is denied entry.

Defaults

Denied.

Command Modes

Configuration mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

Using the **log-deny** option at the end of the individual ACL entries shows the ACL number and whether the packet was permitted or denied, in addition to port-specific information. This option causes an information logging message about the packet that matches the dropped entry (or entries).

Examples

The following example configures the an IP-ACL called aclPermit and permits IP traffic from any source address to any destination address

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip access-list aclPermit permit ip any any
```

The following example removes the IP-ACL called aclPermit.

```
switch(config-if)# no ip access-group aclPermit
```

The following example updates aclPermit to deny TCP traffic from any source address to any destination address.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip access-list aclPermit deny tcp any any
```

The following example defines an IP-ACL that permits this network. Subtracting 255.255.248.0 (normal mask) from 255.255.255.255 yields 0.0.7.255.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip access-list aclPermitUdp permit udp 192.168.32.0 0.0.7.255 any
```

The following example permits all IP traffic from and to the specified networks.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip access-list aclPermitIpToServer permit ip 10.1.1.0 0.0.0.255 172.16.1.0
0.0.0.255
```

The following example denies TCP traffic from 1.2.3.0 through source port 5 to any destination.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/
switch(config)# ip access-list aclDenyTcpIpPrt5 deny tcp 1.2.3.0 0.0.0.255 eq port 5 any
```

The following example removes this entry from the IP-ACL.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/
switch(config)# no ip access-list aclDenyTcpIpPrt5 deny tcp 1.2.3.0 0.0.0.255 eq port 5
any
```

Related Commands

Command	Description
show ip access-list	Displays the IP-ACL configuration information.

ip address (FCIP profile configuration submode)

To assign the local IP address of a Gigabit Ethernet interface to the FCIP profile, use the **ip address** command. To remove the IP address, use the **no** form of the command.

ip address *address*

no ip address *address*

Syntax Description

address	Specifies the IP address.

Defaults

Disabled

Command Modes

FCIP profile configuration submode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

To create a FCIP profile, you must assign a local IP address of a Gigabit Ethernet interface to the FCIP profile.

Examples

The following example assigns the local IP address of a Gigabit Ethernet interface to the FCIP profile.

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)# ip address 10.5.1.1
```

Related Commands

Command	Description
show fcip profile	Displays information about the FCIP profile.
interface fcip *interface_number* **use-profile** *profile-id*	Configures the interface using an existing profile ID from 1 to 255.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

ip address (interface configuration)

To assign an IP address to a Gigabit Ethernet interface, use the **ip address** command in interface configuration submode. To remove the IP address, us the **no** form of the command.

ip address *address netmask*

no ip address *address netmask*

Syntax Description

address	Specifies the IP address.
netmask	Specifies the network mask.

Defaults

None.

Command Modes

Interface configuration submode

Command History

Release	Modification
1.1(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example assigns an IP address to a Gigabit Ethernet interface.

```
switch# config terminal
switch(config)# interface gigabitethernet 1/2
switch(config-profile)# ip address 10.5.1.1 255.255.0.0
```

Related Commands

Command	Description
show fcip profile	Displays information about the FCIP profile.
interface fcip *interface_number* **use-profile** *profile-id*	Configures the interface using an existing profile ID from 1 to 255.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

ip-compression

To enable compression on the FCIP link, use the **ip-compression** command in interface configuration submode. To disable compression, use the **no** form of the command.

ip-compression [**auto** | **mode1** | **mode2** | **mode3**]

no ip-compression [**auto** | **mode1** | **mode2** | **mode3**]

Syntax Description

auto	Enables automatic compression setting.
mode1	Enables fast compression for the following high bandwidth links: — IPS-4 and IPS-8, less then 100 Mbps — MPS-14/2, up to 1 Gbps
mode2	Enables moderate compression for medium bandwidth links less then 25 Mbps.
mode3	Enables compression for bandwidth links less then 10 Mbps.

Defaults

Disabled.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.0(1b)	Changed the keywords from **high-throughput** and **high-comp-ratio** to **mode1**, **mode2**, and **mode3**.

Usage Guidelines

When no compression mode is entered in the command, the default is **auto**.

The FCIP compression feature introduced in Cisco SAN-OS Release 1.3 allows IP packets to be compressed on the FCIP link if this feature is enabled on that link. By default the FCIP compression is disabled. When enabled, the software defaults to using the auto mode (if a mode is not specified).

Cisco SAN-OS Release 2.0(1b) and later, you to configure FCIP compression using one of the following modes:

- **mode1** is a fast compression mode for high bandwidth links (> 25 Mbps)
- **mode2** is a moderate compression mode for moderately low bandwidth links (between 10 and 25 Mbps)
- **mode3** is a high compression mode for low bandwidth links (< 10 Mbps)
- **auto** (default) mode picks the appropriate compression scheme based on the bandwidth of the link (the bandwidth of the link configured in the FCIP profile's TCP parameters)

The IP compression feature behavior differs between the IPS module(s) and the MPS-14/2 module—while **mode2** and **mode3** perform software compression in both modules, **mode1** performs hardware-based compression in MPS-14/2 modules, and software compression in IPS-4 and IPS-8 modules.

In Cisco MDS SAN-OS Release 2.1(1a) and later, the **auto** mode option uses a combination of compression modes to effectively utilize the WAN bandwidth. The compression modes change dynamically to maximize the WAN bandwidth utilization.

Examples

The following example enables faster compression.

```
switch# config terminal
switch(config) interface fcip 1
switch(config-if)# ip-compression mode1
```

The following example enables automatic compression by default.

```
switch(config-if)# ip-compression
```

The following example disables compression.

```
switch(config-if)# no ip-compression
```

Related Commands

Command	Description
show interface fcip	Displays an interface configuration for a specified FCIP interface.

ip default-gateway

To configure the IP address of the default gateway, use the **ip default-gateway** command. To disable the IP address of the default gateway, use the **no** form of the command.

ip default-gateway *destination-ip-address* [**interface cpp** *slot_number*/*processor-number*/*vsan-id*]

no ip default-gateway *destination-ip-address* [**interface cpp** *slot*/*processor-number*/*vsan-id*]

Syntax Description

destination-ip-address	Specifies the IP address,
interface	Configures an interface.
cpp	Specifies a virtualization IPFC interface.
slot	Specifies a slot number of the ASM.
processor-number	Specifies the processor number for the IPFC interface. The current processor number is always 1.
vsan-id	Specifies the ID of the management VSAN. The range 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following examples configures the IP default gateway to 1.1.1.4.

```
switch# config terminal
switch(config)# ip default-gateway 1.1.1.4
```

Related Commands

Command	Description
show ip route	Displays the IP address of the default gateway.

ip default-network

To configure the IP address of the default network, use the **ip default-network** command in configuration mode. To disable the IP address of the default network, use the **no** form of the command.

ip default-network *ip-address*

no ip default-network *ip-address*

Syntax Description

ip-address	Specifies the IP address of the default network.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following examples configures the IP address of the default network to 1.1.1.4.

```
switch# config terminal
switch(config)# ip default-network 1.1.1.4
```

ip domain-list

To configure the IP domain list, use the **ip domain-list** command in configuration mode. To disable the IP domain list, use the **no** form of the command.

ip domain-list *domain-name*

no ip domain-list *domain-name*

Syntax Description

domain-name	Specifies the domain name for the IP domain list. Maximum length is 80 characters.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures the IP domain list.

```
switch# config terminal
switch(config)# ip domain MyList
```

ip domain-lookup

To enable the DNS server lookup feature, use the **ip domain-lookup** command in configuration mode. Use the **no** form of this command to disable this feature.

ip domain-lookup

no ip domain-lookup

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Instead of IP addresses, you can configure the switch using meaningful names. The configured name automatically looks up the corresponding IP address.

Examples

The following example configures a DNS server lookup feature.

```
switch# config terminal
switch(config)# ip domain-lookup
```

ip domain-name

To configure a domain name, use the **ip domain-name** command in configuration mode. To delete a domain name, use the **no** form of the command.

ip domain-name *domain-name*

no ip domain-name *domain-name*

Syntax Description

domain-name	Specifies the domain name.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures a domain name.

```
switch# config terminal
switch(config)# ip domain-name MyDomain
```

ip name-server

To configure a name server, use the **ip name-server** command in configuration mode. To disable this feature, use the **no** form of the command.

ip name-server *ip-address*

no ip name-server *ip-address*

Syntax Description

ip-address	Specifies the IP address for the name server.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can configure a maximum of six servers. By default, no server is configured.

Examples

The following example configure a name server with an IP address of 1.1.1.4.

```
switch# config terminal
switch(config)# ip name-server 1.1.1.4
```

The following example specifies the first address (15.1.0.1) as the primary server and the second address (15.2.0.0) as the secondary sever.

```
switch(config)# ip name-server 15.1.0.1 15.2.0.0
```

The following example deletes the configured server(s) and reverts to factory default.

```
switch(config)# no ip name-server
```

ip route

To configure a static route, use the **ip route** command in configuration mode.

ip route *ip-address subnet-mask* [*nexthop_ip-address*] [**interface** {**gigabitethernet** *slot /port* | **mgmt 0** | **port-channel** *channel-id* | **vsan** *vsan-id*} | **distance** *distance-number*]

no ip route *ip-address subnet-mask* [*nexthop_ip-address*] [**interface** {**gigabitethernet** *slot /port* | **mgmt 0** | **port-channel** *channel-id* | **vsan** *vsan-id*} | **distance** *distance-number*]

Syntax Description

ip-address	Specifies the IP address for the route.
subnet-mask	Specifies the subnet mask for the route.
nexthop_ip-address	Specifies the IP address of the next hop switch.
interface	Configures the interface associated with the route.
gigabitethernet *slot /port*	Specifies a Gigabit Ethernet interface at a port and slot.
mgmt 0	Specifies the managment interface (mgmt 0).
port-channel *channel-id*	Specifies a PortChannel interface. The range is 1 to 128.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
distance *distance-number*	Specifies the distance metric for this route. It can be from 0 to 32766.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following examples shows how to configure a static route.

```
switch# config terminal
switch(config)# IP route 10.0.0.0 255.0.0.0 20.20.20.10 distance 10 interface vsan 1
```

Related Commands

Command	Description
show ip route	Displays the IP address routes configured in the system.

ip routing

To enable the IP forwarding feature, use the **ip routing** command in configuration mode. To disable this feature, use the **no** form of the command.

ip routing

no ip routing

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example enables the IP forwarding feature.

```
switch# config terminal
switch(config)# ip routing
```

Related Commands

Command	Description
show ip routing	Displays the IP routing state.

ipv6 access-list

To configure an IPv6 access control list (ACL) and enter IPv6-ACL configuration submode, use the **ipv6 access-list** command in configuration mode. To discard an IPv6 ACL, use the **no** form of the command.

ipv6 access-list *list-name*

no ipv6 access-list *list-name*

Syntax Description

list-name	Specifies an IP access control list name. The maximum size is 64.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Before using the **ipv6 access-list** command to configure an IPv6 ACL on a switch, become familiar with the features of IPv6 and its extended addressing capabilities. In particular, it is important to understand the different types of IPv6 address formats, the IPv6 address prefix format, and the different IPv6 address types. For detailed information about IPv6, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

Examples

The following example configures an IPv6 access list called List1 and enters IPv6-ACL configuration submode.

```
switch # config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ipv6 access-list List1
switch(config-ipv6-acl)#
```

The following example removes the IPv6 access list called List1 and all of its entries.

```
switch(config)# no ipv6 access-list List1
switch(config)#
```

Related Commands

ipv6 route	Configures an IPv6 static route.
ipv6 routing	Enables IPv6 unicast routing.
show ipv6 access-list	Displays a summary of ACLs.
show ipv6 route	Displays the IPv6 static routes configured on the switch.
show ipv6 routing	Displays the IPv6 unicast routing configured on the switch.

ipv6 address

To enable IPv6 processing and configure an IPv6 address on the interface, use the **ipv6 address** command in interface configuration submode. To remove an IPv6 address, use the **no** form of the command.

ipv6 address *ipv6-address-prefix*

no ipv6 address *ipv6-address-prefix*

Syntax Description

ipv6-address-prefix	Specifies the IPv6 address prefix. The format is *X:X:X::X/n*.

Defaults

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can use the **ipv6 address** command to enable IPv6 processing and configure the IPv6 address on the interface. An IPv6 address must be configured on an interface for the interface to forward IPv6 traffic.

Assigning a unicast address generates a link local address and implicitly enables IPv6.

Note The *ipv6-address-prefix* argument in the **ipv6 address** command must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons. A slash mark (/) precedes a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

Examples

The following example assigns a unicast IPv6 address to the interface and enables IPv6 processing on the interface.

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface gigabitethernet 2/2
switch(config-if)# ipv6 address 2001:0DB8:800:200C::417A/64
```

Related Commands

ipv6 address autoconfig	Enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enables IPv6 processing on the interface.
ipv6 enable	Enables IPv6 processing on the interface.

ipv6 nd	Configures IPv6 neighbor discovery commands on the interface.
ipv6 traffic-filter	Configures IPv6 ACLs to filter traffic for packets on the interface.
show interface	Displays interface configuration information.

ipv6 address autoconfig

To enable automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enable IPv6 processing on the interface, use the **ipv6 address autoconfig** command in interface configuration submode. To remove the address from the interface, use the **no** form of the command.

ipv6 address autoconfig

no ipv6 address autoconfig

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can use the **ipv6 address autoconfig** command to enable IPv6 stateless autoconfiguration on the specified interface. For additional information about autoconfiguration, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

Examples

The following example assigns enables IPv6 stateless autoconfiguration on the interface.

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface gigabitethernet 2/2
switch(config-if)# ipv6 address autoconfig
```

Related Commands

ipv6 address	Enables IPv6 processing and configures an IPv6 address on an interface.
ipv6 enable	Enables IPv6 processing on the interface.
ipv6 nd	Configures IPv6 neighbor discovery commands on the interface.
ipv6 traffic-filter	Configures IPv6 ACLs to filter traffic for packets on the interface.
show interface	Displays interface configuration information.

ipv6 enable

To enable IPv6 processing and configure an IPv6 link-local address on the interface, use the **ipv6 enable** command in interface configuration submode. To disable IPv6 processing and remove the link-local address, use the **no** form of the command.

ipv6 enable

no ipv6 enable

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

When you enable IPv6 on an interface, a link local address is automatically assigned. This address is used for communication on the switch.

Examples

The following example enables IPv6 processing on the interface.

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface gigabitethernet 2/2
switch(config-if)# ipv6 enable
```

The following example disables IPv6 processing on the interface.

```
switch(config-if)# no ipv6 enable
```

Related Commands

ipv6 address	Configures the IPv6 address and enables IPv6 processing.
ipv6 nd	Configures IPv6 neighbor discovery commands on the interface.
ipv6 traffic-filter	Configures IPv6 ACLs to filter traffic for packets on the interface.
show interface	Displays interface configuration information.

ipv6 nd

To configure IPv6 neighbor discovery commands on the interface, use the **ipv6 nd** command in interface configuration submode. To remove IPv6 neighbor discovery configuration commands, use the **no** form of the command.

ipv6 nd {**dad attempts** *number* | **reachable-time** *time* | **retransmission-time** *time*}

no ipv6 nd {**dad attempts** *number* | **reachable-time** *time* | **retransmission-time** *time*}

Syntax Description

dad attempts *number*	Configures duplicate address detection (DAD) attempts. The range is 0 to 15.
reachable-time *time*	Configures reachability time. Specifies the reachability time in milliseconds. The range is 1000 to 3600000.
retransmission-time *time*	Configures the retransmission timer. Specifies the retransmission time in milliseconds. The range is 1000 to 3600000.

Defaults

DAD attempts: 0.
Reachable-time: 30000 milliseconds
Retransmission-time: 1000 milliseconds

Command Modes

Interface configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

A router must be able to determine the link-local address for each of its neighboring routers in order to ensure that the target address (the final destination) in a redirect message identifies the neighbor router by its link-local address. For static routing, the address of the next-hop router should be specified using the link-local address of the router; for dynamic routing, all IPv6 routing protocols must exchange the link-local addresses of neighboring routers.

Note A high number of DAD attempts (greater than 2) can delay address assignment.

For complete information about IPv6 neighbor discovery, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

Examples

The following example sets the duplicate address detection attempts count to 2.

```
switch# config terminal
switch(config)# interface gigabitethernet 2/2
switch(config-if)# ipv6 nd dad attempts 2
```

The following example sets the reachability time to 10000 milliseconds.

```
switch(config-if)# ipv6 nd reachability-time 10000
```

The following example sets the retransmission time to 20000 milliseconds.

```
switch(config-if)# ipv6 nd retransmission-time 20000
```

Related Commands

ipv6 address	Configures the IPv6 address and enables IPv6 processing.
ipv6 enable	Enables IPv6 processing on the interface.
ipv6 traffic-filter	Configures IPv6 ACLs to filter traffic for packets on the interface.
show interface	Displays interface configuration information.

ipv6 route

To configure an IPv6 static route, use the **ipv6 route** command in configuration mode. To remove or disable an IPv6 static route, use the **no** form of the command.

ipv6 route *destination-address-prefix next-hop-address* [**distance** *distance-metric* | **interface** {**gigabitethernet** *slot/port* | **mgmt** *number* | **port-channel** *number* | **vsan** *vsan-id*}] [**distance** *distance-metric*]

no ipv6 route *destination-address-prefix next-hop-address* [**distance** *distance-metric* | **interface** {**gigabitethernet** *slot/port* | **mgmt** *number* | **port-channel** *number* | **vsan** *vsan-id*}] [**distance** *distance-metric*]

Syntax Description

destination-address-prefix	Specifies the IPv6 destination address prefix. The format is *X:X:X::X/n*.
next-hop-address	Specifies the next hop IPv6 address. The format is *X:X:X::X*.
distance	Configures an IPv6 route metric.
distance-metric	Specifies a distance metric for the specified route. The range is 0 to 32766.
interface	Configures a next hop IPv6 address.
gigabitethernet *slot/port*	Specifies a Gigabit Ethernet slot and port number.
mgmt *number*	Specifies the management interface.
port-channel *number*	Specifies a PortChannel number. The range is 1 to 128
vsan *vsan-id*	Specifies an IPFC VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Before using the **ipv6 route** command to configure IPv6 features on a switch, become familiar with the features of IPv6 and its extended addressing capabilities. In particular, it is important to understand the different types of IPv6 address formats, the IPv6 address prefix format, and the different IPv6 address types. For detailed information about IPv6, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

Examples

The following example configures a static default IPv6 route on a Gigabit Ethernet interface.

```
switch # config terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
switch(config)# ipv6 route ::/0 gigabitethernet 3/1
```

The following example configures a fully specified static route on a Gigabit Ethernet interface.

```
switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet 3/2
```

The following example configures a recursive static route to a specified next hop address.

```
switch(config)# ipv6 route 2001:0DB8::/32 2001:0DB8:2002::1
```

The following example configures a recursive static route to a specified next hop address, from which the output interface is automatically derived, and to a specified interface.

```
switch(config)# ipv6 route 2001:0DB8::/32 2001:0DB8:2002::1 gigabitethernet 3/2
```

The following example configures a static IPv6 route with an administrative distance of 20.

```
switch(config)# ipv6 route 2001:0DB8::/32 interface gigabitethernet 2/0 distance 20
```

Related Commands

ipv6 access-list	Configures an IPv6 access control list (ACL) and enters IPv6-ACL configuration submode.
ipv6 routing	Enables IPv6 unicast routing.
show ipv6 access-list	Displays a summary of ACLs.
show ipv6 route	Displays the static IPv6 routes configured on the switch.
show ipv6 routing	Displays the IPv6 unicast routing configured on the switch.

ipv6 routing

To enable IPv6 unicast routing, use the **ipv6 routing** command in configuration mode. To disable IPv6 unicast routing, use the **no** form of the command.

ipv6 routing

no ipv6 routing

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Before using the **ipv6 routing** command to configure IPv6 features on a switch, become familiar with the features of IPv6 and its extended addressing capabilities. In particular, it is important to understand the different types of IPv6 address formats, the IPv6 address prefix format, and the different IPv6 address types. For detailed information about IPv6, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

Examples

The following example enables IPv6 routing.

```
switch # config terminal
switch(config)# ipv6 routing
```

The following example disables IPv6 routing.

```
switch(config)# no ipv6 routing
```

Related Commands

ipv6 access-list	Configures an IPv6 access control list (ACL) and enters IPv6-ACL configuration submode.
ipv6 route	Configures a static IPv6 route.
show ipv6 access-list	Displays a summary of ACLs.
show ipv6 route	Displays the static IPv6 routes configured on the switch.
show ipv6 routing	Displays the IPv6 unicast routing configured on the switch.

ipv6 traffic-filter

To configure IPv6 access control lists (ACLs) to filter traffic for packets on the interface, use the **ipv6 traffic-filter** command in interface configuration submode. To remove an IPv6-ACL traffic filter on the switch, use the **no** form of the command.

ipv6 traffic-filter *access-list-name* {**in** | **out**}

no ipv6 traffic-filter *access-list-name* {**in** | **out**}

Syntax Description

access-list-name	Specifies the name of an access control list for packets. The maximum size is 64 characters.
in	Configures inbound packets.
out	Configures outbound packets.

Defaults

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures a traffic filter, called testfilter, for inbound packets.

```
switch# config terminal
switch(config)# interface gigabitethernet 2/2
switch(config-if)# ipv6 traffic-filter testfilter in
```

Related Commands

ipv6 address	Configures the IPv6 address and enables IPv6 processing.
ipv6 enable	Enables IPv6 processing on the interface.
ipv6 nd	Configures IPv6 ACLs to filter traffic for packets on the interface.
show interface	Displays interface configuration information.

iscsi authentication

To configure the default authentication method for iSCSI, use the **iscsi authentication** command. To revert to the default, use the **no** form of the command.

iscsi authentication {**chap** | **chap-none** | **none** | **username** *username* **password** [**0** | **7**] *password*}

no iscsi authentication {**chap** | **chap-none** | **none** | **username**}

Syntax Description

chap-none	Configure either the CHAP or no authentication.
chap	Configures the Challenge Handshake Authentication Protocol (CHAP) authentication method.
none	Specifies that no authentication is required for the selected interface
username *username*	Assigns CHAP username to be used when switch is authenticated.
password	Configures the password for the username.
0	Specifies that the password is a cleartext CHAP password.
7	Specifies that the password is an encrypted CHAP password.
password	Specifies a password for the username.

Defaults

chap-none

The default password is a cleartext password.

Command Modes

Configuration mode

Command History

Release	Modification
1.1(1)	This command was introduced.
2.0(1b)	Added the **username** option.

Usage Guidelines

By default, the Cisco MDS 9000 Family switch accepts an iSCSI initiator with either no authentication or CHAP authentication. If CHAP authentication is always required, use the **iscsi authentication chap** command. If no authentication is always required, use the **iscsi authentication none** command.

Use the **chap-none** option to override the global configuration which might have been configured to allow only one option—either CHAP or none—not both.

Examples

The following example configures CHAP only for ISCSI authentication.

```
switch# config terminal
switch(config)# iscsi authentication chap
```

Related Commands

Command	Description
show iscsi global	Displays all iSCSI initiators configured by the user.

iscsi duplicate-wwn-check

To check the current running configuration for conflicts between iSCSI initiators' static WWN allocation and what the system thinks is available in its WWN pool, use the **iscsi duplicate-wwn-check** command in configuration mode.

iscsi duplicate-wwn-check

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.1(2)	This command was introduced.

Usage Guidelines

Prior to Cisco MDS SAN-OS Release 2.1(2), WWNs assigned to static iSCSI initiators by the system can be inadvertently returned to the system when an upgrade fails or the system software is manually downgraded (that is, when you manually boot up an older Cisco MDS SAN-OS release without using the **install all** command). In these instances, the system can later assign those WWNs to other iSCSI initiators (dynamic or static) and cause conflicts.

As of Cisco MDS SAN-OS Release 2.1(2), you can use the **iscsi duplicate-wwn-check** command to check for and remove any configured WWNs that belong to the system.

Examples

The following example shows how to check the current running configuration for conflicts between iSCSI initiators' static WWN allocation and what the system thinks is available in its WWN pool.

```
switch# config terminal
Enter configuration command, one per line. End with CNTL/Z.
switch(config)# iscsi duplicate-wwn-check

List of Potential WWN Conflicts:
-------------------------------
Node : iqn.test-local-nwnn:1-local-pwwn:1
    nWWN : 22:03:00:0d:ec:02:cb:02
    pWWN : 22:04:00:0d:ec:02:cb:02
```

The following example shows how to remove the conflicting nWWN and pWWN.

```
switch(config)# iscsi initiator name iqn.test-local-nwwn:1-local-pwwn:1
switch(config-iscsi-init)# no static nWWN  22:03:00:0d:ec:02:cb:02
switch(config-iscsi-init)# no static pWWN  22:04:00:0d:ec:02:cb:02
```

Related Commands

Command	Description
iscsi initiator name	Assigns an iSCSI name and changes to iSCSI initiator configuration submode.
static	Assigns persistent WWNs to an iSCSI initiator in iSCSI initiator configuration submode.
show iscsi initiator	Displays information about configured iSCSI initiators.

iscsi dynamic initiator

To configure dynamic initiator modes, use the **iscsi dynamic initiator** command in configuration mode. To revert to the default mode, use the **no** form of the command.

iscsi dynamic initiator {deny | islb}

no dynamic initiator {deny | islb}

Syntax Description

deny	Specifies that dynamic initiators are denied from logging on to the MDS switch.
islb	Specifies iSLB dynamic initiator mode.

Defaults

iSCSI.

Command Modes

Configuration mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Three dynamic initiator modes are supported:

- iSCSI—Dynamic initiators are treated as iSCSI initiators and can access dynamic virtual targets and configured iSCSI virtual targets.
- iSLB—Dynamic initiators are treated as iSLB initiators and can access dynamic virtual targets.
- Deny—Dynamic initiators are not allowed to log in to the MDS switch.

iSCSI dynamic initiator is the default mode of operation. This configuration is distributed using CFS.

Note Configuring dynamic initiator modes is supported only through the CLI, not through Device Manager or Fabric Manager.

A dynamic iSCSI initiator can be converted to a static iSCSI initiator and its WWNs can be made persistent.

A dynamic iSLB initiator can be converted to a static iSLB initiator and its WWNs can be made persistent.

Note You cannot convert a dynamic iSCSI initiator to a static iSLB initiator, or a dynamic iSLB initiator to a static iSCSI initiator.

Examples

The following command configures the dynamic initiator mode as iSLB.

```
switch(config)# iscsi dynamic initiator islb
```

The following command configures the dynamic initiator mode as deny.

```
switch(config)# iscsi dynamic initiator deny
```

The following command reverts to the default dynamic initiator mode of iSCSI.

```
switch(config)# no iscsi dynamic initiator deny
```

Related Commands

Command	Description
iscsi save-initiator	Permanently saves the automatically-assigned nWWN or pWWN mapping.
show iscsi global	Displays global iSCSI configured information.

iscsi enable

To enable the iSCSI feature in any Cisco MDS switch, issue the **iscsi enable** command. To disable this feature, use the **no** form of the command.

iscsi enable

no iscsi enable

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Configuration mode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The configuration and verification commands for the iSCSI feature are only available when iSCSI is enabled on a switch. When you disable this feature, all related configurations are automatically discarded.

Examples

The following command enables the iSCSI feature.

```
switch(config)# iscsi enable
```

The following command disables the iSCSI feature (default).

```
switch(config)# no iscsi enable
```

iscsi import target fc

To allow dynamic mapping of Fibre Channel targets, use the **iscsi import target fc** command. To disable this feature, use the **no** form of the command.

iscsi import target fc

no iscsi import target fc

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Configuration mode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command directs iSCSI to dynamically import all Fibre Channel targets into iSCSI.

Examples

The following example allows dynamic mapping of Fibre Channel targets.

```
switch# config terminal
switch(config)# iscsi import target fc
```

The following example disables dynamic mapping of Fibre Channel targets.

```
switch(config)# no iscsi import target fc
```

Related Commands

Command	Description
show iscsi global	Displays all iSCSI initiators configured by the user..

iscsi initiator idle-timeout

To configure the iSCSI initiator idle timeout, use the **iscsi initiator idle-timeout** command. To revert to the default, use the **no** form of the command.

iscsi initiator idle-timeout *seconds*

no iscsi initiator idle-timeout *seconds*

Syntax Description

seconds	Specifies the timeout in seconds. The range is 0 to 3600.

Defaults

300 seconds

Command Modes

Configuration mode

Command History

Release	Modification
1.3	This command was introduced.

Usage Guidelines

When the idle timeout value is set to 0, the initiator information is cleared immediately after the last session from the initiator terminates.

Examples

The following example configures the iSCSI initiator idle timeout to 180 seconds.

```
switch# config terminal
switch(config)# iscsi initiator idle-timeout 180
```

The following example reverts the default value of 300 seconds.

```
switch# config terminal
switch(config)# no iscsi initiator idle-timeout 240
```

Related Commands

Command	Description
show iscsi global	Displays global iSCSI configuration information.

iscsi initiator ip-address

To assign persistent WWNs to an iSCSI initiator or assign an iSCSI initiator into VSANs other than the default VSAN, use the **iscsi initiator ip-address** command. To revert to the default, use the **no** form of the command.

iscsi initiator ip-address *ipaddress*
static {**nwwn** | **pwwn**} {*wwn-id* | **system-assign** *number*}
vsan *vsan-id*

iscsi initiator ip-address *ipaddress*
no static {**nwwn** | **pwwn**} {*wwn-id* | **system-assign** *number*}
no vsan *vsan-id*

no iscsi initiator ip-address *ipaddress*

Syntax Description

ipaddress	Specifies the initiator IP address.
nwwn	Configures the inititiator node WWN hex value.
pwwn	Configures the peer WWN for special frames.
wwn-id	Enters the pWWN or nWWN ID.
system-assign *number*	Generates the nWWN value automatically. The number ranges from 1 to 64.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Defaults

Disabled.

Command Modes

Configuration mode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Under a circumstance where an iSCSI initiator needs to have a persistent binding to FC WWNs, this command should be used. Also, an iSCSI initiator can be put into multiple VSANs. An iSCSI host can become a member of one or more VSANs.

Examples

The following command configures an iSCSI initiator. using the IP address of the initiator node.

```
switch(config)# iscsi initiator ip address 10.50.1.1
```

The following command deletes the configured iSCSI initiator.

```
switch(config)# no iscsi initiator ip address 10.5.0.0
```

The following command uses the switch's WWN pool to allocate the nWWN for this iSCSI initiator and keeps it persistent.

```
switch(config-(iscsi-init))# static nWWN system-assign
```

The following command assigns the user provided WWN as nWWN for the iSCSI initiator. You can only specify one nWWN for each iSCSI node.

```
switch(config-(iscsi-init))# nWWN 20:00:00:05:30:00:59:11
```

The following command uses the switch's WWN pool to allocate two pWWNs for this iSCSI initiator and keeps it persistent.

```
switch(config-(iscsi-init))# static pWWN system-assign 2
```

The following command assigns the user provided WWN as pWWN for the iSCSI initiator.

```
switch(config-(iscsi-init))# pWWN 21:00:00:20:37:73:3b:20
```

Related Commands

Command	Description
show iscsi initiator	Displays information about configured iSCSI initiators.

iscsi initiator name

To configure an iSCSI initiator name and change to iSCSI configuration mode, use the **iscsi initiator name** command. To revert to factory defaults, use the **no** form of the command.

iscsi initiator name *name*

no iscsi initiator name *name*

Syntax Description

name	Enters the initiator name to be used. The minimum length is 16 characters and maximum is 223 characters.

Defaults

Disabled

Command Modes

Configuration mode

Command History

Release	Modification
1.3(2)	This command was introduced.

Usage Guidelines

Under a circumstance where an iSCSI initiator needs to have a persistent binding to FC WWNs, this command should be used. Also, an iSCSI initiator can be put into multiple VSANs. An iSCSI host can become a member of one or more VSANs.

Examples

The following example configures an iSCSI initiator using the iSCSI name of the initiator node.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# iscsi initiator name iqn.1987-02.com.cisco.initiator
```

Related Commands

Command	Description
show iscsi initiator	Displays information about configured iSCSI initiators.

iscsi interface vsan-membership

To configure VSAN membership for iSCSI interfaces, use the **iscsi interface vsan-membership** command. Use the **no** form of this command to disable this feature or to revert to factory defaults.

iscsi interface vsan-membership

no iscsi interface vsan-membership

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

If the **iscsi interface vsan-membership** command is disabled, you will not be able to configure iSCSI VSAN membership.

Caution Changing the VSAN membership, the forwarding mode, and the authentication of an iSCSI interface that is part of an iSLB VRRP group impacts load balancing on the interface.

For additional information, refer to the "Configuring iSCSI" chapter of the *Cisco MDS 9000 Family CLI Configuration Guide*.

Examples

The following command enables the iSCSI interface VSAN membership.

```
switch# config terminal
switch(config)# iscsi interface vsan-membership
```

The following command disables the iSCSI interface VSAN membership (default).

```
switch(config)# no iscsi interface vsan-membership
```

Related Commands

Command	Description
show iscsi initiator	Displays information about configured iSCSI initiators.

iscsi save-initiator

To permanently save the automatically-assigned nWWN/pWWN mapping, use the **iscsi save-initiator** command.

iscsi save-initiator [**ip-address** *ip-address* | **name** *name*]

Syntax Description

ip-address *ip-address*	Specifies the initiator IP address.
name *name*	Specifies the initiator name to be used from 1 to 255 characters. The minimum length is 16 characters.

Defaults

If initiator name or IP address is not specified, the nWWN/pWWN mapping for all initiators becomes permanent.

Command Modes

Configuration mode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

After executing the **iscsi save-initiator** command, issue the **copy running-config startup-config** to save the nWWN/pWWN mapping across switch reboots.

After a dynamic iSCSI initiator has logged in, you may decide to permanently save the automatically assigned nWWN/pWWN mapping so this initiator uses the same mapping the next time it logs in.

You can convert a dynamic iSCSI initiator to static iSCSI initiator and make its WWNs persistent.

Note You cannot convert a dynamic iSCSI initiator to a static iSLB initiator or a dynamic iSLB initiator to a static iSCSI initiator.

Examples

The following example shows how to save the nWWN/pWWN mapping for all the initiators.

```
switch(config)# iscsi save-initiator
```

The following example shows how to save the nWWN/pWWN mapping for an initiator named iqn.1987-02.com.cisco.initiator.

```
switch(config)# iscsi save-initiator name iqn.1987-02.com.cisco.initiator
```

Related Commands

Command	Description
iscsi initiator	Configures an iSCSI initiator.
show iscsi initiator	Displays information about configured iSCSI initiators.

iscsi virtual-target name

To create a static iSCSI virtual target, use the **iscsi virtual-target** command. To revert to the default values, use the **no** form of the command.

iscsi virtual-target name *name*
advertise interface {**gigabitethernet** *slot*/*port*[**.***subinterface*] | **port-channel** *channel-id*[**.***subinterface*]}
all-initiator-permit
initiator {*initiator-name* | **ip-address** *ipaddress* [*netmask*]} **permit**
pwwn *pwwn-id* [**fc-lun** *number* **iscsi-lun** *number* [**secondary-pwwn** *pwwn-id* [**sec-lun** *number*]] | **secondary-pwwn** *pwwn-id*]
revert-primary-port
trespass

iscsi virtual-target name *name*
no advertise interface {**gigabitethernet** *slot*/*port*[**.***subinterface*] | **port-channel** *channel-id*[**.***subinterface*]}
no all-initiator-permit
no initiator {*initiator-name* | **ip-address** *ipaddress* [*netmask*]} **permit**
no pwwn *pwwn-id* [**fc-lun** *number* **iscsi-lun** *number* [**secondary-pwwn** *pwwn-id* [**sec-lun** *number*]] | **secondary-pwwn** *pwwn-id*]
no revert-primary-port
no trespass

no iscsi virtual-target name *name*

Syntax Description

name	Enters the virtual target name to be used. The minimum length is 16 characters and maximum of 223 bytes.
advertise interface	Advertises the virtual target name on the specified interface.
gigabitethernet *slot*/*port*[**.***subinterface*]	Selects the Gigabit Ethernet interface or subinterface to configure.
port-channel *channel-id*[**.***subinterface*]	Selects the Port Channel interface or subinterface to configure.
all-initiator-permit	Enables all iSCSI initiator access to this target.
initiator	Configures specific iSCSI initiator access to this target.
initiator-name	Specifies the iSCSI initiator name to be used access a specified target. Maximum length is 255 characters.
ip-address *ip-address*	Specifies the iSCSI initiator IP address.
ip-subnet	Specifies all initiators in the subnet.
permit	Permits access to the specified target.
pwwn *pwwn-id*	Specifies the peer WWN ID for special frames.
secondary-pwwn *pwwn-id*	Specifies the secondary pWWN ID.
fc-lun *number*	Specifies the Fibre Channel Logical Unit Number (LUN).
iscsi-lun *number*	Specifies the iSCSI virtual target number.
sec-lun *number*	Specifies the secondary Fibre Channel LUN.
trespass	Moves LUNs forcefully from one port to another.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.1(1)	This command was introduced.
1.3(1)	Added **revert-to-primary** and **trespass** subcommands.

Usage Guidelines

This command is used to configure a static iSCSI target for access by iSCSI initiators. A virtual target may contain a subset of LUs of an FC target or one whole FC target.

Do not specify the LUN if you wish to map the whole Fibre Channel target to an iSCSI target. All Fibre Channel LUN targets are exposed to iSCSI.

Note The CLI interprets the LUN identifier value as a hexadecimal value whether or not the 0x prefix is included.

One iSCSI target cannot contain more than one Fibre Channel target.

Examples

The follow example creates a static virtual target and enters ISCSI target configuration submode.

```
switch# config terminal
switch(config)# iscsi virtual-target name 0123456789ABDEFGHI
switch(config-iscsi-tgt)#
```

The following command advertises the virtual target only on the specified interface. By default, it is advertised on all interfaces in all IPS modules.

```
switch(config-iscsi-tgt)# advertise interface gigabitethernet 4/1
```

The following command maps a virtual target node to a Fibre Channel target.

```
switch(config-iscsi-tgt)# pWWN 26:00:01:02:03:04:05:06
```

The following command enters the secondary pWWN for the virtual target node.

```
switch(config-iscsi-tgt)# pWWN 26:00:01:02:03:04:05:06 secondary-pwwn
66:00:01:02:03:04:05:02
```

Use the LUN option to map different Fibre Channel LUNs to different iSCSI virtual targets. If you have already mapped the whole Fibre Channel target, you will not be able to use this option.

```
switch(config-iscsi-tgt)# pWWN 26:00:01:02:03:04:05:06 fc-lun 0 iscsi-lun 0
```

The following command allows the specified iSCSI initiator node to access this virtual target. You can issue this command multiple times to allow multiple initiators.

```
switch(config-iscsi-tgt)# initiator iqn.1987-02.com.cisco.initiator1 permit
```

The following command prevents the specified initiator node from accessing virtual targets.

```
switch(config-iscsi-tgt)# no initiator iqn.1987-02.com.cisco.initiator1 permit
```

The following command allows the specified IP address to access this virtual target:

```
switch(config-iscsi-tgt)# initiator ip-address 10.50.1.1 permit
```

The following command prevents the specified IP address from accessing virtual targets:

```
switch(config-iscsi-tgt)# no initiator ip-address 10.50.1.1 permit
```

The following command allows all initiators in this subnetwork to access this virtual target:

```
switch(config-iscsi-tgt)# initiator ip-address 10.50.0.0 255.255.255.0 permit
```

The following command prevents all initiators in this subnetwork from accessing virtual targets:

```
switch(config-iscsi-tgt)# no initiator ip-address 10.50.0.0 255.255.255.0 permit
```

The following command allows all initiator nodes to access this virtual target.

```
switch(config-iscsi-tgt)# all-initiator-permit
```

The following command prevents any initiator node from accessing virtual targets.

```
switch(config-iscsi-tgt)# no all-initiator-permit
```

The following command configures a primary and secondary port and moves the LUNs from one port to the other using the **trespass** command.

```
switch# config terminal
switch(config)#iscsi virtual-target name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-tgt)# pwwn 50:00:00:a1:94:cc secondary-pwwn 50:00:00:a1:97:ac
switch(config-iscsi-tgt)# trespass
```

Related Commands

Command	Description
show iscsi virtual target	Displays information about iSCSI virtual targets.

islb abort

To discard a pending iSCSI Server Load Balancing (iSLB) configuration, use the **islb abort** command.

islb abort

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can use the **islb abort** command to discard the pending changes to the iSLB configuration and release the fabric lock. This action has no effect on the active configuration on any switch in the fabric.

The **islb abort** command can be issued only by the user who started the Cisco Fabric Services (CFS) session and only on the switch that started the CFS session.

Examples

The following example discards the pending iSLB configuration distribution.

```
switch# config t
switch(config)# islb abort
```

Related Commands

Command	Description
islb commit	Commits the iSLB configuration distribution and releases the fabric lock.
show islb cfs-session status	Displays iSLB information.
show islb pending	Displays the pending configuration changes.
show islb pending-diff	Displays the differences between the pending configuration and the current configuration.
clear islb session	Clears a pending iSLB configuration. This command can be issued on any switch by a user with admin privileges.

islb commit

To commit a pending iSCSI server load balancing (iSLB) configuration, use the **islb commit** command.

islb commit

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can use the **islb commit** command to commit the pending changes to the iSLB configuration and release the fabric lock. This action changes the active configuration on all Cisco MDS switches in the fabric.

The **islb commit** command can be issued only by the user who started the Cisco Fabric Services (CFS) session and only on the switch that started the CFS session.

Examples

The following example commits the pending iSLB configuration distribution.

```
switch# config t
switch(config)# islb commit
```

Related Commands

Command	Description
islb abort	Discards the pending iSLB configuration distribution and releases the fabric lock.
islb distribute	Enables iSLB configuration distribution.
clear islb session	Clears a pending iSLB configuration. This command can be issued on any switch by a user with admin privileges.
show islb cfs-session status	Displays iSLB information.
show islb pending	Displays the pending configuration changes.
show islb pending-diff	Displays the differences between the pending configuration and the current configuration.

islb distribute

To enable Cisco Fabric Services for iSCSI Server Load Balancing (iSLB) configuration, use the **islb distribute** command. To disable the iSLB configuration distribution, use the **no** form of the command

islb distribute

no islb distribute

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can use the **islb distribute** command to enable the distribution of iSLB configuration information to other Cisco MDS switches in the fabric using the Cisco Fabric Services (CFS) infrastructure. You can synchronize the iSLB configuration across the fabric from the console of a single MDS switch.

Note The only initiator configuration that is distributed throughout the fabric using CFS is a statically mapped, iSLB initiator configuration. Dynamically mapped and statically mapped iSCSI initiator configurations are not distributed. iSCSI initiator idle-timeout and global authentication parameters are also distributed.

If you are using both iSLB and inter-VSAN routing (IVR), ensure that the following conditions are satisfied; otherwise, traffic may be disrupted in the fabric.

- You must enable both features on at least one switch in the fabric.
- You must configure and activate zoning from the switch for normal zones, IVR zones, and and iSLB zones.

Examples

The following example enables iSLB configuration distribution.

```
switch# config t
switch(config)# islb distribute
```

The following example disables iSLB configuration distribution.

```
switch(config)# no islb distribute
```

Related Commands

Command	Description
islb abort	Discards the pending iSLB configuration distribution and releases the fabric lock.
islb commit	Commits the iSLB configuration distribution and releases the fabric lock.
clear islb session	Clears a pending iSLB configuration. This command can be issued on any switch by a user with admin privileges.

islb initiator

To configure the iSCSI server load balancing (iSLB) initiator and enter iSLB initiator configuration submode, use the **islb initiator** command. To delete the configured ISLB initiator, use the **no** form of the command.

islb initiator {ip-address {*ip-address* **|** *ipv6-address***} | name** *name***}**

no islb initiator name *name*

Syntax Description

ip-address	Specifies the iSLB initiator node IP address.
ip-address	Specifies the initiator IPv4 address.
ipv6-address	Specifies the initiator IPv6 address.
name *name*	Specifies the iSLB initiator node name. The maximum size is 223.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can use the **islb initiator** command to enter iSLB initiator configuration submode to configure static mapping for an iSLB initiator.

Examples

The following example enters iSLB initiator configuration submode to configure static mapping (using the IPv4 ip-address option) for an iSLB initiator.

```
switch# config t
switch(config)# islb initiator ipaddress 10.1.2.3
switch(config-islb-init)#
```

The following example deletes the configured iSLB initiator.

```
switch(config)# no islb initiator ipaddress 10.1.2.3
```

The following example enters iSLB initiator configuration submode to configure static mapping (using the IPv6 option) for an iSLB initiator.

```
switch# config t
switch(config)# islb initiator ipaddress 1111.2222.3333.4::5
switch(config-islb-init)#
```

The following example deletes the configured iSLB initiator.

```
switch(config)# no islb initiator ipaddress 1111.2222.3333.4::5
```

The following example enters iSLB initiator configuration submode to configure static mapping (using the name option) for an iSLB initiator.

```
switch# config t
switch(config)# islb initiator name iqn.1987-02.co..cisco.initiator
switch(config-islb-init)#
```

The following example deletes the configured iSLB initiator:

```
switch(config)# no islb initiator ipaddress name iqn.1987-02.co..cisco.initiator
```

Related Commands

Command	Description
show islb initiator configured	Displays iSLB initiator configuration information.
show islb initiator detail	Displays more detailed information about the iSLB configuration.
show islb initiator iscsi-session	Displays iSLB session details.
show islb initiator summary	Displays iSLB initiator summary information.

islb save-initiator

To permanently save the automatically-assigned nWWN/pWWN mapping for the iSLB initiator, use the **islb save-initiator** command.

islb save-initiator [**ip-address** *ip-address* | **name** *name*]

Syntax Description

ip-address *ip-address*	Specifies the initiator IP address. The format is *A.B.C.D* or *X:X:X::X*.
name *name*	Specifies the initiator name to be used from 1 to 223 characters.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Saving the automatically assigned nWWN/pWWN mapping allows the initiator to use the same mapping the next time it logs in.

You can convert a dynamic iSLB initiator to a static iSLB initiator and make its WWNs persistent.

Note You cannot convert a dynamic iSCSI initiator to a static iSLB initiator or a dynamic iSLB initiator to a static iSCSI initiator.

Note Making the dynamic mapping for iSLB initiators static is the same as for iSCSI.

Note Only a statically mapped iSLB initiator configuration is distributed throughout the fabric using CFS. Dynamically and statically configured iSCSI initiator configurations are not distributed.

Examples

The following example saves the nWWNs and pWWNs that have automatically been assigned to the iSLB initiator whose name is specified.

```
switch# config t
switch(config)# islb save-initiator name iqn.1987-02.com.cisco.initiator
```

The following example saves the nWWNs and pWWNs that have automatically been assigned to the iSLB initiator whose IPv4 address is specified.

```
switch(config)# islb save-initiator ip-address 10.10.100.11
```

The following example saves the nWWNs and pWWNs that have automatically been assigned to all the iSLB initiators.

```
switch(config)# islb save-initiator
Please execute "copy run start" to keep the WWNs persistent across switch reboots
```

Related Commands

Command	Description
show islb session	Displays detailed iSLB session information.

islb virtual-target name

To configure an iSLB virtual target and enter iSLB target configuration submode, use the **islb virtual-target name** command. To revert to the default values, use the **no** form of the command.

islb virtual-target name *name*
{all-initiator-permit |
initiator {*initiator-name* **permit | ip address {***A.B.C.D* **permit | *X:X:X::X* permit}} |**
pWWN permit |
revert-primary-port permit |
trespass permit}

islb virtual-target name *name*
{no all-initiator-permit |
no initiator {*initiator-name* **permit | ip address {***A.B.C.D* **permit | *X:X:X::X* permit}} |**
no pWWN permit |
no revert-primary-port permit |
no trespass permit}

no islb virtual-target name *name*

Syntax Description

name	Specifies the virtual target name to be used. The minimum length is 16 bytes and the maximum length is 223 bytes.
all-initiator-permit	Configures all iSLB initiators to access the target.
initiator	Configures the iSLB initiator to access the target.
initiator-name	Specifies the initiator name. The minimum length is 16 bytes and the maximum length is 223 bytes.
permit	Permits access to the specified target.
ip address *ip-address*	Specifies the initiator IP address. The format is *A.B.C.D* or *X:X:X::X*.
pWWN *pwwn-id*	Specifies the pWWN of the Fibre Channel target. The format is *hh:hh:hh:hh:hh:hh:hh:hh*.
revert-primary-port	Reverts to the primary port when it becomes active again.
trespass	Enables trespass support.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

This command is used to configure a static target for access by iSLB initiators.

Examples

The following example creates a static virtual target and enters iSLB target configuration submode.

```
switch# config terminal
switch(config)# islb virtual-target name ABCDEFGHIJ1234567890
ips-hac1(config-islb-tgt)#
```

The following example allows all iSLB initiators to access the target.

```
ips-hac1(config-islb-tgt)# all-initiator-permit
```

The following command allows the specified IP address to access this virtual target:

```
switch(config-islb-tgt)# initiator ip-address 10.50.1.1 permit
```

The following example prevents the specified IP address from accessing virtual targets:

```
switch(config-islb-tgt)# no initiator ip-address 10.50.1.1 permit
```

The following example allows all initiators in this subnetwork to access this virtual target:

```
switch(config-islb-tgt)# initiator ip-address 10.50.0.0 255.255.255.0 permit
```

The following example prevents all initiators in this subnetwork from accessing virtual targets:

```
switch(config-islb-tgt)# no initiator ip-address 10.50.0.0 255.255.255.0 permit
```

The following example maps a pWWN to a Fibre Channel target.

```
ips-hac1(config-islb-tgt)# pwwn 26:00:01:02:03:04:05:06
```

Related Commands

Command	Description
show islb virtual-target	Displays information about iSLB virtual targets.

islb vrrp

To configure iSCSI server load balancing (iSLB) on a Virtual Router Redundancy Protocol (VRRP) group, use the **islb vrrp** command. To disable the iSLB configuration on the VRRP group, use the **no** form of the command.

islb vrrp {*group-number* **load-balance** | **ipv6** *group-number* **load-balance**}

no islb vrrp {*group-number* **load-balance** | **ipv6** *group-number* **load-balance**}

Syntax Description

group-number	Specifies an IPv4 Virtual Router group number. The range is 1 to 255.
load-balance	Enables load balancing on the VRRP group.
ipv6	Specifies IPv6 on the VRRP group.
group-number	Specifies an IPv6 Virtual Router group number. The range is 1 to 255.
load-balance	Enables load balancing on the VRRP group.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The host is configured with a VRRP address as the portal address. When the VRRP master port receives the first iSCSI session from an initiator, it assigns a slave port to serve that particular host. The information is synchronized to all switches via Cisco Fabric Services (CFS) if recovery is needed when a master port fails. The initiator gets a temporary redirect iSCSI login response. The host then logs in to the slave port at its physical IP address. If the slave port goes down, the host will revert to the master port. The master port knows through CFS that the slave port has gone down and redirects the host to another slave port.

There are separate VRRP groups for IPv4 and IPv6. Each address family is allowed 256 virtual routers.

Note An initiator can also be redirected to the physical IP address of the master interface.

Tip The load balancing distribution is based on the number of initiators on a port and not on the number of sessions.

Caution A Gigabit Ethernet interface configured for iSLB can only be in one VRRP group because redirected sessions do not carry information about the VRRP IP address or group. This restriction allows the slave port to uniquely identify the VRRP group to which it belongs.

Caution Changing the VSAN membership, the forwarding mode, and the authentication of an iSCSI interface that is part of an iSLB VRRP group impacts load balancing on the interface.

For additional information, refer to the "Configuring iSCSI" chapter of the *Cisco MDS 9000 Family CLI Configuration Guide*.

Examples

The following example enables VRRP load balancing for IPv4 Virtual Router group 20.

```
switch# config t
switch(config)# islb vrrp 20 load-balance
```

The following example disables VRRP load balancing for IPv4 Virtual Router group 20.

```
switch(config)# no islb vrrp 20 load-balance
```

The following example enables VRRP load balancing for IPv6 Virtual Router group 30.

```
switch(config)# islb vrrp ipv6 30 load-balance
```

The following example disables VRRP load balancing for IPv6 Virtual Router group 30.

```
switch(config)# no islb ipv6 30 load-balance
```

Related Commands

Command	Description
show islb session	Displays detailed iSLB session information.

islb zoneset activate

To activate iSCSI server load balancing (iSLB) auto zones, use the **islb zoneset activate** command.

islb zoneset activate

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Auto-zoning of the initiator with the initiator targets is enabled by default.

A zone set must be active for a VSAN for auto-zones to be created in that VSAN. The **zoneset activate** command creates auto-zones only if at least one other change has been made to the zone set.

Examples

The following example activates an iSLB auto zone.

```
switch# config t
switch(config)# islb zoneset activate
```

Related Commands

Command	Description
show zoneset active	Displays active zone sets.

isns

To tag a Gigabit Ethernet or PortChannel interface to an Internet Storage Name Service (iSNS) profile, use the **isns** command in interface configuration submode. To untag the interface, use the **no** form of the command.

isns *profile-name*

no isns *profile-name*

Syntax Description

profile-name	Specifies the iSNS profile name.

Defaults

Disabled.

Command Modes

Interface configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, iSNS must be enabled using the **isns-server enable** command.

Use the **isns reregister** command in EXEC mode to reregister associated iSNS objects (tagged to an iSNS profile) with the iSNS server.

Examples

The following example shows how to tag a Gigabit Ethernet interface to an iSNS profile.

```
switch# config terminal
switch(config)# interface gigabitethernet 1/2
switch(config-if)# isns Profile1
```

The following example shows how to tag a PortChannel interface to an iSNS profile.

```
switch# config terminal
switch(config)# interface port-channel 2
switch(config-if)# isns Profile2
```

Related Commands

Command	Description
isns-server enable	Enables the iSNS server.
isns reregister	Reregisters the iSNS object.
show interface gigabitethernet	Displays configuration and status information for a specified Gigabit Ethernet interface.

Command	Description
show interface port-channel	Displays configuration and status information for a specified PortChannel interface.
show isns	Displays iSNS information.

isns distribute

To enable Cisco Fabric Services (CFS) distribution for Internet Storage Name Service (iSNS), use the **isns distribute** command. To disable this feature, use the **no** form of the command.

isns distribute

no isns distribute

Syntax Description

This command has no other arguments or keywords.

Defaults

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, iSNS must be enabled using the **isns-server enable** command.

You can configure the pWWN and nWWN of iSCSI initiators and permit a group of iSCSI initiators to share a given nWWN/pWWN pair by using a proxy initiator. The number of iSCSI initiators that register with the iSNS server is more than the number of iSCSI targets that register with the iSNS server. To synchronize the iSCSI initiator entries across switches, you can distribute the iSCSI initiator configuration to iSNS servers across switches.

Examples

The following example shows how to initiate iSNS information distribution.

```
switch# config terminal
switch(config)# isns distribute
```

The following example shows how to cancel iSNS information distribution.

```
switch# config terminal
switch(config)# no isns distribute
```

Related Commands

Command	Description
isns-server enable	Enables the iSNS server.
show isns	Displays iSNS information.

isns esi retries

To configure the number of entity status inquiry (ESI) retry attempts, use the **isns esi retries** command in configuration mode. To revert to the default value, use the **no** form of the command.

isns esi retries *number*

no isns esi retries *number*

Syntax Description

number	Specifies the number of retries. The range is 0 to 10.

Defaults

3 retries.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, Internet Storage Name Service (iSNS) must be enabled using the **isns-server enable** command.

The iSNS client queries the ESI port at user-configured intervals. Receipt of a response indicates that the client is still alive. Based on the configured value, the interval specifies the number of failed tries before which the client is deregistered from the server.

Examples

The following example shows how change the ESI retries limit to eight.

```
switch# config terminal
switch(config)# isns esi retries 8
```

Related Commands

Command	Description
isns-server enable	Enables the iSNS server.
show isns	Displays iSNS information.

isns profile name

To create an Internet Storage Name Service (iSNS) profile and enter iSNS profile configuration submode, use the **isns profile name** command in configuration mode. To delete the iSNS profile, use the **no** form of the command.

isns profile name *profile-name*

no isns profile name *profile-name*

Syntax Description

profile-name	Specifies the profile name. Maximum length is 64 characters.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

To use this command, iSNS must be enabled using the **isns-server enable** command.

Examples

The following example shows how to specify an iSNS profile name and enter iSNS profile configuration submode.

```
switch# config terminal
switch(config)# isns profile name UserProfile
switch(config-isns-profile)#
```

Related Commands

Command	Description
server	Configures a server IP address in an iSNS profile.
show isns	Displays iSNS information.

isns reregister

To register all Internet Storage Name Service (iSNS) objects for an interface that is already tagged to an iSNS profile, use the **isns register** command.

isns reregister {**gigabitethernet** *slot/number* | **port-channel** *channel-group*}

Syntax Description

gigabitethernet *slot/port*	Specifies tagged Gigabit Ethernet interface slot and port.
port-channel *channel-group*	Specifies tagged PortChannel group. The range is 1 to 128.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Use this command to reregister portals and targets with the iSNS server for a tagged interface.

Examples

The following command re-registers portal and targets for a tagged interface:

```
switch# isns reregister gigabitethernet 1/4
```

Related Commands

Command	Description
show isns profile	Displays details for configured iSNS profiles.

isns-server enable

To enable the Internet Storage Name Service (iSNS) server, use the **isns-server enable** command in configuration mode. To disable iSNS, use the **no** form of the command.

isns-server enable

no isns-server enable

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

Performing the **isns-server enable** command enables the commands used to configure iSNS.

Examples

The following example shows how to enable iSNS.

```
switch# config terminal
switch(config)# isns-server enable
```

The following example shows how to disable iSNS.

```
switch# config terminal
switch(config)# no isns-server enable
```

Related Commands

Command	Description
isns distribute	Enables iSNS distributed support.
isns esi retries	Configures ESI retry attempts.
isns profile name	Creates and configures iSNS profiles.
server	Configures iSNS server attributes.
show isns	Displays iSNS information.

ivr abort

To discard an Inter-VSAN Routing (IVR) CFS distribution session in progress, use the **ivr abort** command in configuration mode.

ivr abort

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to discard an IVR CFS distribution session in progress.

```
switch# config terminal
switch(config)# ivr abort
```

Related Commands

Command	Description
ivr distribute	Enables CFS distribution for IVR.
show ivr	Displays IVR CFS distribution status and other details.

ivr commit

To apply the pending configuration pertaining to the Inter-VSAN Routing (IVR) Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **ivr commit** command in configuration mode.

ivr commit

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to apply an IVR configuration to the switches in the fabric.

```
switch# config terminal
switch(config)# ivr commit
```

Related Commands

Command	Description
ivr distribute	Enables CFS distribution for IVR.
show ivr	Displays IVR CFS distribution status and other details.

ivr copy active-service-group user-configured-service-group

To copy the active service group to the user configured service group, use the **ivr copy active-service-group user-configured-service-group** command in EXEC mode.

ivr copy active-service-group user-configured-service-group

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example copies the active service group to the user defined service group.

```
switch# ivr copy active-service-group user-configured-service-group
Successfully copied active service group to user-configured service group database
```

Related Commands

Command	Description
clear ivr service-group database	Clears the IVR service group database.
show ivr service-group	Displays IVR service groups.

ivr copy active-topology user-configured-topology

To copy the active inter-VSAN routing (IVR) VSAN topology to the user configured topology, use the **ivr copy active-topology user-configured-topology** command in EXEC mode.

ivr copy active-topology user-configured-topology

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The **ivr copy active-topology user-configured-topology** command is useful if you need to edit the active IVR topology, which is not allowed. Instead you copy the active IVR topology to the user configured topology, and then edit the user configured topology.

Examples

The following example copies the active IVR topology to the user configured topology.

```
switch# ivr copy active-topology user-configured-topology
Successfully copied active VSAN-topology to user-configured topology database
```

Related Commands

Command	Description
ivr copy active-zoneset full-zoneset	Copies the active zone set to the full zone set.
ivr copy auto-topology user-configured topology	Copies the automatically discovered inter-VSAN routing (IVR) VSAN topology to the user configured topology.
show ivr vsan topology	Displays the IVR VSAN topology configuration.

ivr copy active-zoneset full-zoneset

To copy the active zone set to the full zone set, use the **ivr copy active-zoneset full-zoneset** command in EXEC mode.

ivr copy active-zoneset full-zoneset

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Copying the active zone set to the full zone set may overwrite common zone and zone set configurations in the full zoning database.

Examples

The following example copies the active zone set to the full zone set.

```
switch# ivr copy active-zoneset full-zoneset
WARNING: This command may overwrite common zones/zonesets
         in the IVR full zoneset database
Please enter yes to proceed.(y/n) [n]?
```

Related Commands

Command	Description
ivr copy active-topology user-configured topology	Copies the active inter-VSAN routing (IVR) VSAN topology to the user configured topology.
ivr copy auto-topology user-configure topology	Copies the automatically discovered inter-VSAN routing (IVR) VSAN topology to the user configured topology.
show ivr zoneset active	Displays the active IVR zone set.

ivr copy auto-topology user-configured-topology

To copy the automatically discovered inter-VSAN routing (IVR) VSAN topology to the user configured topology, use the **ivr copy auto-topology user-configured-topology** command in EXEC mode.

ivr copy auto-topology user-configured-topology

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC configuration mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

After using the **ivr copy auto-topology user-configured-topology** command to copy the automatically discovered VSAN topology into the user configured topology you must use the **ivr commit** command to apply the pending configuration changes to the IVR topology using Cisco Fabric Services (CFS) distribution.

Examples

The following example copies the automatically discovered VSAN topology into the user configured topology.

```
switch# ivr copy auto-topology user-configured-topology
```

Related Commands

Command	Description
ivr commit	Applies the changes to the IVR topology.
ivr copy active-topology user-configured topology	Copies the active inter-VSAN routing (IVR) VSAN topology to the user configured topology.
ivr copy active-zoneset full-zoneset	Copies the active zone set to the full zone set.
show ivr vsan topology	Displays the IVR VSAN topology configuration

ivr distribute

To enable Cisco Fabric Services (CFS) distribution for Inter-VSAN Routing (IVR), use the **ivr distribute** command. To disable this feature, use the **no** form of the command.

ivr distribute

no ivr distribute

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable IVR fabric distribution.

```
switch# config terminal
switch(config)# ivr distribute
```

Related Commands

Command	Description
ivr commit	Commits temporary IVR configuration changes to the active configuration.
show ivr	Displays IVR CFS distribution status and other details.

ivr enable

To enable the Inter-VSAN Routing (IVR) feature, use the **ivr enable** command in configuration mode. To disable this feature, use the **no** form of the command.

ivr enable

no ivr enable

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The IVR feature must be enabled in all edge switches in the fabric that participate in the IVR.

The configuration and display commands for the IVR feature are only available when IVR is enabled on a switch.

When you disable this configuration, all related configurations are automatically discarded.

Examples

The following command enters the configuration mode and enables the IVR feature on this switch.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr enable
```

Related Commands

Command	Description
show ivr	Displays IVR feature information.

ivr fcdomain database autonomous-fabric-num

To create IVR persistent FC IDs, use the **ivr fcdomain database autonomous-fabric-num** command. To delete the IVR fcdomain entry for a given AFID and VSAN, use the **no** form of the command.

ivr fcdomain database autonomous-fabric-num *afid-num* **vsan** *vsan-id*

no ivr fcdomain database autonomous-fabric-num *afid-num* **vsan** *vsan-id*

Syntax Description

afid-num	Specifies the current AFID. The range is 1 to 64.
vsan *vsan-id*	Specifies the current VSAN. The range is 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.1(2)	This command was introduced.

Usage Guidelines

This configuration only takes effect when NAT mode is enabled.

Examples

The following example shows how to enter IVR fcdomain database configuration submode for AFID 10 and VSAN 20.

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config) fcdomain#
```

The following example shows how to delete all persistent FC ID database entries for AFID 10 and VSAN 20.

```
switch# config t
switch(config)# no ivr fcdomain database autonomous-fabric-num 10 vsan 20
```

Related Commands

Command	Description
show ivr fcdomain database	Displays IVR fcdomain database entry information.

ivr nat

To explicitly enable Network Address Translation (NAT) functionality for Inter-VSAN Routing (IVR), use the **ivr nat** command in configuration mode. To disable this feature, use the **no** form of the command.

ivr nat

no ivr nat

SyntaxDescription

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

The **ivr nat** command allows you to explicitly enable NAT functionality of IVR. Upgrading to SAN-OS Release 2.x from SAN-OS Release 1.3.x does not automatically enable the Fibre Channel NAT functionality. This command also allows you to continue to operate in non-NAT mode even in SAN-OS Release 2.x and later.

Note You might need to operate in non-NAT mode to support proprietary protocols that embed FCIDs in the frame payloads.

Examples

The following example shows how to explicitly enable NAT functionality for IVR.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr nat
```

Related Commands

Command	Description
show ivr	Displays IVR feature information.

ivr refresh

To refresh devices being advertised by Inter-VSAN Routing (IVR), use the **ivr refresh** command in EXEC mode.

ivr refresh

SyntaxDescription

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows refresh devices being advertised by IVR.

```
switch# ivr refresh
```

Related Commands

Command	Description
ivr enable	Enables the Inter-VSAN Routing (IVR) feature.
ivr withdraw domain	Withdraws an overlapping virtual domain from a specified VSAN.

ivr service-group activate

To activate an inter-VSAN routing (IVR) service group, use the **ivr service-group activate** command in configuration mode. To disable this feature, use the **no** form of the command.

ivr service-group activate [default-sg-deny]

no ivr service-group activate [default-sg-deny]

Syntax Description

default-sg-deny	Sets the policy to deny for the default service group.

Defaults

Deactivated.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You must activate a configured IVR service group for the IVR service group to take effect. Once a configured IVR service group is activated, it replaces the currently activated service group, if there is one.

Activating an IVR service group with the **default-sg-deny** option sets the default service group policy to deny. To change the default service group policy to allow, issue the **ivr service-group activate** command again, but without the **default-sg-deny** option.

Examples

The following example activates the default IVR service group:

```
switch# config terminal
switch(config)# ivr service-group activate
```

The following example sets the default IVR service group policy to deny:

```
switch# config terminal
switch(config)# ivr service-group activate default-sg-deny
```

The following example disables the default service group:

```
switch# config terminal
switch(config)# no ivr service-group activate
```

Related Commands

Command	Description
ivr enable	Enables inter-VSAN routing (IVR).
ivr service-group name	Configures an inter-VSAN routing (IVR) service group.
show ivr service-group database	Displays an inter-VSAN routing service group database.

ivr service-group name

To configure an Inter-VSAN Routing (IVR) service group, use the **ivr service-group name** command in configuration mode. To disable this feature, use the **no** form of the command.

ivr service-group name *service-group*

no ivr service-group name *service-group*

Syntax Description

service-group	Specifies the service group name.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

In a complex network topology, you might only have a few IVR-enabled VSANs. To reduce the amount of traffic to non-IVR-enabled VSANs, you can configure a service group that restricts the traffic to the IVR-enabled VSANs. A service group is a combination of AFIDs and VSANs. Up to 16 service groups can be configured. A VSAN or AFID can belong to just one service group. When a new IVR-enabled switch is added to the network, you must update the service group to include the new VSANs.

There can be a maximum of 128 AFID/VSAN combinations in all service group. However, all 128 combinations can be in one service group.

The default service group ID is 0. The default service group is for all VSANs that are not a part of a user-defined service group.

Before configuring an IVR service group, you must enable the following:

- IVR using the **ivr commit** command
- IVR distribution using the **ivr commit** command
- Automatic IVR topology discovery using the **ivr commit auto** command.

Using the **autonomous-fabric-id (IVR topology database configuration)** command, you can restrict the IVR traffic to the AFIDs and VSANs configured in the service group.

Examples

The following example shows how to configure an IVR service group and change to IVR service group configuration mode.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr enable
switch(config)# ivr vsan-topology auto
switch(config)# ivr service-group name serviceGroup1
```

```
switch(config-ivr-sg)#
```

Related Commands

Command	Description
ivr enable	Enables the Inter-VSAN Routing (IVR) feature
ivr vsan-topology auto	Enables automatic discovery of the IVR topology.
show ivr	Displays IVR feature information.

ivr virtual-fcdomain-add

To add the Inter-VSAN Routing (IVR) virtual domains in a specific VSAN(s) to the assigned domains list in that VSAN, use the **ivr virtual-fcdomain-add** command. To delete the IVR virtual domains, use the **no** form of the command.

ivr virtual-fcdomain-add vsan-ranges *vsan-range*

no ivr virtual-fcdomain-add vsan-ranges *vsan-range*

Syntax Description

vsan-ranges *vsan-range*	Specifies the IVR VSANs or range of VSANs. The range of values for a VSAN ID is 1 to 4093.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

Use the **no ivr virtual-fcdomain-add** command to remove the currently active domains from the fcdomain manager list in a specified VSAN.

Examples

The following command adds the IVR virtual domains in VSAN 1.

```
switch# config terminal
switch(config)# ivr virtual-fcdomain-add vsan-ranges 1
```

The following command reverts to the factory default of not adding IVR virtual domains.

```
switch# config terminal
switch(config)# ivr virtual-fcdomain-add vsan-ranges 1
```

Related Commands

Command	Description
show ivr virtual-fcdomain-add-status	Displays the configured VSAN topology for a fabric.
ivr withdraw domain	Removes overlapping domains.

ivr vsan-topology

To configure manual or automatic discovery of the Inter-VSAN Routing (IVR) topology, use the **ivr vsan-topology** command in configuration mode.

ivr vsan-topology {**activate** | **auto**}

Syntax Description

activate	Configures manual discovery of the IVR topology and disables automatic discovery mode.
auto	Configures automatic discovery of the IVR topology.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.1(1a)	Added **auto** keyword.

Usage Guidelines

To use this command you must first enable IVR using the **ivr enable** command and configure the IVR database using the **ivr vsan-topology database** command.

Caution Active IVR topologies cannot be deactivated. You can only switch to automatic topology discovery mode.

Examples

The following **ivr vsan-topology activate** command activates the VSAN topology database:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr enable
switch(config)# ivr vsan-topology database
switch(config-ivr-topology-db)# autonomous-fabric-id 1 switch 20:00:00:00:30:00:3c:5e
vsan-ranges 2,2000
switch(config)# ivr vsan-topology activate
```

The following command enables VSAN topology database auto mode, which allows the switch to automatically discover the IVR topology.

```
switch(config)# ivr vsan-topology auto
```

Related Commands

Command	Description
ivr enable	Enables the Inter-VSAN Routing (IVR) feature.
autonomous-fabric-id (IVR topology database configuration)	Configure an autonomous phobic ID into the IVR topology database.
show ivr	Displays IVR feature information.

ivr vsan-topology database

To configure an Inter-VSAN Routing (IVR) topology database, use the **ivr vsan-topology database** command in configuration mode. To delete an IVR topology database, use the **no** form of the command.

ivr vsan-topology database

no ivr vsan-topology database

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

To use this command you must first enable IVR using the **ivr enable** command.

You can have up to 64 VSANs (or 128 VSANs as of Cisco MDS SAN-OS Release 2.1(1a)) in an IVR topology. Specify the IVR topology using the following information:

- The switch WWNs of the IVR-enabled switches.
- A minimum of two VSANs to which the IVR-enabled switch belongs.
- The autonomous fabric ID (AFID), which distinguishes two VSANs that are logically and physically separate, but have the same VSAN number. Cisco MDS SAN-OS Release 1.3(1) and later supports only one default AFID (AFID 1) and thus does not support non-unique VSAN IDs in the network. As of Cisco MDS SAN-OS Release 2.1(1a), you can specify up to 64 AFIDs.

Note The use of a single AFID does not allow for VSANs that are logically and physically separate but have the same VSAN number in an IVR topology.

Caution You can only configure a maximum of 128 IVR-enabled switches and 64 distinct VSANs (or 128 distinct VSANs as of Cisco MDS SAN-OS Release 2.1(1a)) in an IVR topology.

The **no ivr vsan-topology database** command only clears the configured database, not the active database. You can only delete the user-defined entries in the configured database. Auto mode entries only exist in the active database.

Examples

The following command enters configuration mode, enables the IVR feature, enters the VSAN topology database, and configures the pWWN-VSAN association for VSANs 2 and 2000:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr enable
switch(config)# ivr vsan-topology database
switch(config-ivr-topology-db)# autonomous-fabric-id 1 switch 20:00:00:00:30:00:3c:5e
vsan-ranges 2,2000
```

Related Commands

Command	Description
ivr enable	Enables the Inter-VSAN Routing (IVR) feature.
autonomous0fabric-id (IVR topology database configuration)	Configure an autonomous phobic ID into the IVR topology database
show ivr	Displays IVR feature information.

ivr withdraw domain

To withdraw overlapping virtual domain from a specified VSAN, use the **ivr withdraw domain** command in EXEC mode.

ivr withdraw domain *domain-id* **vsan** *vsan-id*

Syntax Description

domain-id	Specifies the domain id. The range is 1 to 239.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

When you enable the **ivr virtual-fcdomain-add** command, links may fail to come up due to overlapping virtual domain identifiers. If so, temporarily withdraw the overlapping virtual domain from that VSAN using the **ivr withdraw domain** command in EXEC mode.

Examples

The following command withdraws overlapping domains.

```
switch# ivr withdraw domain 10 vsan 20
```

Related Commands

Command	Description
show ivr virtual-fcdomain-add-status	Displays the configured VSAN topology for a fabric.

ivr zone name

To configure a zone for Inter-VSAN Routing (IVR), use the **ivr zone name** command. To disable a zone for IVR, use the **no** form of the command.

ivr zone name *ivzs-name*

no ivr zone name *ivz-name*

Syntax Description

ivz-name	Specifies the IVZ name. Maximum length is 59 characters.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

This command enters IVR zone configuration submode.

Examples

The following command enters the configuration mode, enables the IVR feature, creates an IVZ, and adds a pWWN-VSAN member.

```
switch# config terminal
switch(config)# ivr enable
switch(config)# ivr zone name Ivz_vsan2-3
switch(config-ivr-zone)# member pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
```

Related Commands

Command	Description
show ivr	Displays IVR feature information.

ivr zone rename

To rename an inter-VSAN routing (IVR) zone, use the **ivr zone rename** command.

ivr zone rename *current-name new-name*

Syntax Description

current-name	Specifies the current zone name. The maximum size is 64 characters.
new-name	Specifies the new zone name. The maximum size is 64 characters.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example renames the IVR zone from *east* to *west*.

```
switch# ivr zone rename east west
```

Related Commands

Command	Description
ivr zone name	Creates and configures an IVR zone.
show ivr	Displays IVR information.

ivr zoneset

To configure a zoneset for Inter-VSAN Routing (IVR), use the **ivr zoneset** command. To revert to the factory defaults, use the **no** form of the command.

ivr zoneset {**activate name** *ivzs-name* [**force**] | **name** *ivzs-name*}

no ivr zoneset {**activate name** *ivzs-name* [**force**] | **name** *ivzs-name*}

Syntax Description

activate	Activates a previously-configured IVZS.
force	Forces a IVZS activation
name *ivzs-name*	Specifies the IVZS name. Maximum length is 59 characters.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

This command enters IVR zoneset configuration submode.

Examples

The following command enters the configuration mode, enables the IVR feature, creates an IVZS, adds a IVZ member, and activates the IVZS.

```
switch# config terminal
switch(config)# ivr enable
switch(config)# ivr zoneset name Ivr_zoneset1
switch(config-ivr-zoneset)# member Ivz_vsan2-3
switch(config-ivr-zoneset)# exit
switch(config)# ivr zoneset activate name IVR_ZoneSet1
```

Related Commands

Command	Description
show ivr	Displays IVR feature information.

ivr zoneset rename

To rename an inter-VSAN routing (IVR) zone set, use the **ivr zoneset rename** command.

ivr zoneset rename *current-name new-name*

Syntax Description

current-name	Specifies the current zone set name. The maximum size is 64 characters.
new-name	Specifies the new zone set name. The maximum size is 64 characters.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example renames the IVR zone set from *north* to *south*.

```
switch# ivr zoneset rename north south
```

Related Commands

Command	Description
ivr zoneset name	Creates and configures an IVR zone set.
show ivr	Displays IVR information.

CHAPTER 12

J Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "Command Modes" section to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

job name

To assign a job to a command schedule, use the **job name** command. To remove the job, use the **no** form of the command.

job name *job-name*

no job name *job-name*

Syntax Description

job-name	Specifies the job name for the command schedule to run.

Defaults

None.

Command Modes

Scheduler schedule configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, the command scheduler must be enabled using the **scheduler enable** command.

You can configure multiple jobs in a command schedule.

Examples

The following example shows how to specified the job for a command schedule.

```
switch# config terminal
switch(config)# scheduler schedule name MySchedule
switch(config-schedule)# job name MyJob
```

Related Commands

Command	Description
scheduler enable	Enables the command scheduler.
scheduler schedule name	Configures a schedule for the command scheduler.
show scheduler	Displays scheduler information.

CHAPTER 13

K Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "Command Modes" section to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

keepalive

To configure the message keepalive interval for the IKE protocol, use the **keepalive** command in IKE configuration submode. To revert to the default, use the **no** form of the command.

keepalive *seconds*

no keepalive [*seconds*]

Syntax Description

seconds	Specifies the number of seconds for the keepalive interval. The range is 120 to 86400.

Defaults

3600 seconds or 1 hour.

Command Modes

IKE configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

The keepalive interface only applies to IKE version 2 tunnels.

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Examples

The following example shows how to configure the keepalive interval.

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# keepalive 7200
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

kernel core

Use the **kernel core** command to generate a core dump for each module. Use the **no** form of this command to negate the command or revert to its factory

kernel core {**limit** *number* | **module** *slot* {**force** | **level** {**all** | **header** | **kernel** | **ram** | **used-ram**} | **target** *ipaddress*}

no kernel core {**limit** *number* | **module** *slot* {**force** | **level** {**all** | **header** | **kernel** | **ram** | **used-ram**} | **target** *ipaddress*}

Syntax Description

limit *number*	Limits the number of modules for which the core is generated. The range is 1 to 6.
module *slot*	Configures the module requiring the core generation.
force	Forces a module to dump kernel core.
level	Specifies the core dump level for the selected module.
all	Dumps all the memory (requires 1G of space)
header	Dumps kernel header only.
kernel	Dumps all kernel memory pages.
ram	Dumps all the RAM pages.
used-ram	Dumps all the used RAM pages.
target *ipaddress*	Configures the external server IP address on the same physical LAN.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Core dumps performed on the supervisor module can lead to packet loss, even in a dual supervisor configuration.

Examples

The following example limits core generation to two modules.

```
switch(config)# kernel core limit 2
succeeded
```

The following example configures module 5 to generate cores.

```
switch(config)# kernel core module 5
succeeded
```

The following example configures module 5 to generate only header-level cores.

```
switch(config)# kernel core module 5 level header
succeeded
```

The following example configures the external server.

```
switch(config)# kernel core target 10.50.5.5
succeeded
```

Related Commands

Command	Description
show kernel	Displays configured kernel core settings.
show running-config	Displays all switch configurations saved to PSS.

key

To configure the preshared key for the IKE protocol, use the **key** command in IKE configuration submode. To revert to the default, use the **no** form of the command.

key *key-id* {**address** *ip-address* | **hostname** *name*}

no key *key-id* {**address** *ip-address* | **hostname** *name*}

Syntax Description

key-id	Specifies the ID for the preshared key. The maximum length is 128 characters.
address *ip-address*	Specifies the peer IP address. The format is *A.B.C.D*.
hostname *name*	Specifies the peer host name. The maximum length is 128 characters.

Defaults

None.

Command Modes

IKE configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.
3.0(1)	Added the **hostname** keyword.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Note The **key** command supports only the IPv4 format for IP address.

Examples

The following example shows how to configure the key.

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# key ctct address 10.10.100.231
```

The following example shows how to delete the configured key.

```
switch(config-ike-ipsec)# no key ctct address 10.10.100.231
```

The following example shows how to set the preshared key for the specified peer.

```
switch(config-ike-ipsec)# key sample hostname node1
```

The following example shows how to delete the preshared key for the specified peer.

```
switch(config-ike-ipsec)# no key sample hostname node1
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

CHAPTER 14

L Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "Command Modes" section to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

lifetime seconds

To configure the security association (SA) lifetime duration for an IKE protocol policy, use the **lifetime seconds** command in IKE policy configuration submode. To revert to the default, use the **no** form of the command.

lifetime seconds *seconds*

no lifetime [**seconds** *seconds*]

Syntax Description

seconds	Specifies the lifetime duration in seconds. The range is 600 to 86400.

Defaults

86,400 seconds.

Command Modes

IKE policy configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

The **lifetime seconds** command overrides the default.

Examples

The following example shows how to configure the SA lifetime duration for the IKE protocol.

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# policy 1
switch(config-ike-ipsec-policy)# lifetime seconds 6000
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
policy	Configures IKE protocol policy.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

line com1

To configure auxiliary COM 1 port, use the **line com1** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

line com1 -->
databits *number* |
flowcontrol hardware |
modem {**in** | **init-string** {**default** | **user-input**} | **set-string user-input** *string*} |
parity {**even** | **none** | **odd**} |
speed *speed* |
stopbits {**1** | **2**}

line com1 -->
no databits *number* |
no flowcontrol hardware |
no modem {**in** | **init-string** | **set-string user-input**} |
no parity {**even** | **none** | **odd**} |
no speed *speed* |
no stopbits {**1** | **2**}

Syntax Description

databits *number*	Specifies the number of databits per character. The range is 5 to 8.
flowcontrol hardware	Enables modem flowcontrol on the COM1 port.
modem	Enables the modem mode.
in	Enables the COM 1 port to only connect to a modem.
init-string default	Writes the default initialization string to the modem.
set-string user-input *string*	Sets the user-specified initilization string to its corresponding profile. Maximum length is 80 characters.
init-string user-default	Writes the provided initialization string to the modem.
parity	Sets terminal parity.
even	Sets even parity.
none	Sets no parity.
odd	Sets odd parity.
speed *speed*	Sets the transmit and receive speeds. The range is 110 to 115, 200 baud.
stopbits	Sets async line stopbits.
1	Sets one stop bit.
2	Sets two stop bits.

Defaults

9600 Baud

8 databits

1 stopbit

Parity none

Default init string

Command Modes

Configuration mode.

Command History

Release	Modification
1.2(2)	This command was introduced.
3.0(1)	Added an example to show the user-input initialization string for the Supervisor-2 module.

Usage Guidelines

The **line com1** command available in **config t** command mode. The **line com1** configuration commands are available in `config-com1` submode.

You can perform the configuration specified in this section only if you are connected to the console port or the COM1 port.

We recommend you use the default initialization string. If the required options are not provided in the user-input string, the initialization string is not processed.

You must first set the user-input string before initializing the string.

For additional information on the user-input initialization string for the Supervisor-1 and Supervisor-2 modules, refer to the *Cisco SAN-OS MDS 9000 Family CLI Configuration Guide*.

Examples

The following example configures a line console and sets the options for that terminal line.

```
switch## config terminal
switch(config)#
switch(config)# line com1
switch(config-com1)# databits 6
switch(config-com1)# parity even
switch(config-com1)# stopbits 1
```

The following example disables the current modem from executing its functions.

```
switch# config terminal
switch(config)# line com1
switch(config-com1)# no modem in
```

The following example enables (default) the COM1 port to only connect to a modem.

```
switch# config terminal
switch(config)# line com1
switch(config-com1)# modem in
```

The following example Writes the provides initialization string to the modem. This is the default.

```
switch# config terminal
switch(config)# line com1
switch(config-com1)# modem init-string default
```

The following example assigns the user-specified initialization string for a Supervisor-1 module to its corresponding profile.

```
switch# config terminal
switch(config)# line com1
switch(config-com1)# modem set-string user-input ATE0Q1&D2&C1S0=3\015
```

The following example assigns the user-specified initialization string for a Supervisor-2 module to its corresponding profile.

```
switch# config terminal
switch(config)# line com1
switch(config-com1)# modem set-string user-input ATE0Q0V1&D0&C0S0=1
```

The following example deletes the configured initialization string.

```
switch# config terminal
switch(config)# line com1
switch(config-com1)# no modem set-string user-input ATE0Q1&D2&C1S0=3\015
```

The following example writes the user-specified initialization string to the modem.

```
switch# config terminal
switch(config)# line com1
switch(config-com1)# modem init-string user-input
```

Related Commands

Command	Description
line console	Configure primary terminal line.
line vty	Configure virtual terminal line.
show line com1	Displays COM1 information.

line console

To configure a terminal line, use the **line console** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

line console -->
databits *number* |
exec-timeout *minutes* |
modem {**in** | **init-string** | **set-string user-input**} |
parity {**even** | **none** | **odd**} |
speed *speed* |
stopbits {**1** | **2**}

line console -->
no databits *number* |
no exec-timeout *minutes* |
no modem {**in** | **init-string** {**default** | **user-input**} | **set-string user-input** *string*} |
no parity {**even** | **none** | **odd**} |
no speed *speed* |
no stopbits {**1** | **2**}

Syntax Description

databits *number*	Specifies the number of databits per character. The range is 5 to 8.
exec-timeout *minutes*	Configure exec timeout in minutes. The range is 0 to 525,600. To disable, set to 0 minutes.
modem	Enables the modem mode.
in	Enables the COM 1 port to only connect to a modem.
init-string default	Writes the default initialization string to the modem.
set-string user-input *string*	Sets the user-specified initilization string to its corresponding profile. Maximum length is 80 characters.
init-string user-input	Writes the provided initialization string to the modem.
parity	Sets terminal parity.
even	Sets even parity.
none	Sets no parity.
odd	Sets odd parity.
speed *speed*	Sets the transmit and receive speeds. Valid values for Supervisor-1 modules are between 110 and 115,200 bps (110, 150, 300, 600, 1200, 2400, 4800, 9600, 19200, 28800, 38400, 57600, 115200). Valid values for Supervisor-2 modules are 9600, 19200, 38400, and 115200.
stopbits	Sets async line stopbits.
1	Sets one stop bit.
2	Sets two stop bits.

Defaults

9600 Baud

8 databits

1 stopbit

Parity none

Default init string

Command Modes

Configuration mode.

Command History

Release	Modification
1.2(2)	This command was introduced.
3.0(1)	Modified the **speed** option by specifying speeds for the Supervisor-1 module and Supervisor-2 module.

Usage Guidelines

The **line console** command available in **config t** command mode. The **line console** configuration commands are available in `config-console` submode.

When setting the **speed** option, be sure to specify one of the exact values.

Examples

The following example configures a line console and sets the options for that terminal line.

```
switch## config terminal
switch(config)##
switch(config)# line console
switch(config-console)# databits 60
switch(config-console)# exec-timeout 60
switch(config-console)# flowcontrol software
switch(config-console)# parity even
switch(config-console)# stopbits 1
```

The following example disables the current modem from executing its functions.

```
switch# config terminal
switch(config)# line console
switch(config-console)# no modem in
```

The following example enables (default) the COM1 port to only connect to a modem.

```
switch# config terminal
switch(config)# line console
switch(config-console)# modem in
```

The following example Writes the provides initialization string to the modem. This is the default.

```
switch# config terminal
switch(config)# line console
switch(config-console)# modem init-string default
```

The following example assigns the user-specified initialization string to its corresponding profile.

```
switch# config terminal
switch(config)# line console
switch(config-console)# modem set-string user-input ATE0Q1&D2&C1S0=3\015
```

The following example deletes the configured initialization string.

```
switch# config terminal
```

```
switch(config)# line console
switch(config-console)# no modem set-string user-input ATE0Q1&D2&C1S0=3\015
```

The following example writes the user-specified initialization string to the modem.

```
switch# config terminal
switch(config)# line console
switch(config-console)# modem init-string user-input
```

Related Commands

Command	Description
line vty	Configure virtual terminal line.
line com1	Configures the auxiliary COM 1 port
show line console	Displays console information.

line vty

To configure a virtual terminal line, use the **line vty** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

line vty -->
exec-timeout *minutes* |
session-limit *number*

line vty -->
no exec-timeout |
no session-limit *number*

Syntax Description

exec-timeout *minutes*	Configures timeout in minutes. The range is 0 to 525600. To disable, set to 0 minutes.
session-limit *number*	Configures the number of VSH sessions. The range is 1 to 64.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The **line vty** command available in **config t** command mode. **line vty** configuration commands available in config-line submode.

Examples

The following example configures a virtual terminal line and sets the timeout for that line.

```
switch## config terminal
switch(config)# line vty
switch(config-line)# exec-timeout 60
```

Related Commands

Command	Description
line console	Configure primary terminal line.
line com1	Confgiures the auxiliary COM 1 port

logging abort

To discard the logging Cisco Fabric Services (CFS) distribution session in progress, use the **logging abort** command in configuration mode.

logging abort

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to discard logging CFS distribution session in progress.

```
switch# config terminal
switch(config)# logging abort
```

Related Commands

Command	Description
show logging	Displays logging information.

logging commit

To apply the pending configuration pertaining to the logging Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **logging commit** command in configuration mode.

logging commit

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to commit changes to the active logging configuration.

```
switch# config terminal
switch(config)# logging commit
```

Related Commands

Command	Description
show logging	Displays logging information.

logging console

To set console logging, use the **logging console** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

logging console [*severity-level*]

no logging console [*severity-level*]

Syntax Description

severity-level	Specifies the maximum severity of messages logged. The range is 0 to 7, where 0 is emergency, 1 is alert, 2 is critical, 3 is error, 4 is warning, 5 is notify, 6 is informational, and 7 is debugging.

Defaults

Disabled.

The default severity level is 2.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The switch logs messages at or above the configured severity level.

Examples

The following example reverts console logging to the factory set default severity level of 2 (critical). Logging messages with a severity level of 2 or above will be displayed on the console.

```
switch# config terminal
switch(config)# logging console 2
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

logging distribute

To enable Cisco Fabric Services (CFS) distribution for logging, use the **logging distribute** command. To disable this feature, use the **no** form of the command.

logging distribute

no logging distribute

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Before distributing the Fibre Channel timer changes to the fabric, the temporary changes to the configuration must be committed to the active configuration using the **logging commit** command.

Examples

The following example shows how to change the distribute logging configuration changes.

```
switch# config terminal
switch(config)# logging distribute
```

Related Commands

Command	Description
logging commit	Commits the logging configuration changes to the active configuration.
show logging	Displays logging information.

logging level

To modify message logging facilities, use the **logging level** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

logging level *facility-name severity-level*

no logging level *facility-name severity-level*

Syntax Description

facility-name	Specifies the required facility name (for example **acl**, or **ivr**, or **port**, etc.)
severity-level	Specifies the maximum severity of messages logged. The range is 0 to 7, where 0 is emergency, 1 is alert, 2 is critical, 3 is error, 4 is warning, 5 is notify, 6 is informational, and 7 is debugging.

Defaults

Disabled

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The switch logs messages at or above the configured severity level.

Examples

Configures Telnet or SSH logging for the kernel facility at level 4 (warning). As a result, logging messages with a severity level of 4 or above will be displayed.

```
switch# config terminal
switch(config)# logging level kernel 4
```

logging logfile

To set message logging for logfile, use the **logging logfile** command.To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

logging logfile *filename severity-level* [**size** *filesize*]

no logging logfile

Syntax Description

filename	Specifies the log filename. Maximum length is 80 characters.
severity-level	Specifies the maximum severity of messages logged. The range is 0 to 7, where 0 is emergency, 1 is alert, 2 is critical, 3 is error, 4 is warning, 5 is notify, 6 is informational, and 7 is debugging.
size *filesize*	Specifies the log file size. The range is 4096 to 4194304 bytes.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The switch logs messages at or above the configured severity level.

Examples

The following example configures logging information for errors or events above a severity level of 3 (errors) to be logged in a file named ManagerLogFile. By configuring this limit, the file size is restricted to 3,000,000 bytes.

```
switch# config terminal
switch(config)# logging logfile ManagerLogFile 3 size 3000000
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

logging module

To set message logging for linecards, use the **logging module** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

logging module [*severity-level*]

no logging module [*severity-level*]

Syntax Description

severity-level	Specifies the maximum severity of messages logged. The range is 0 to 7, where 0 is emergency, 1 is alert, 2 is critical, 3 is error, 4 is warning, 5 is notify, 6 is informational, and 7 is debugging.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example sets message logging for modules at level 7.

```
switch## config terminal
switch(config)# logging module 7
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

logging monitor

To set monitor message logging, use the **logging monitor** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

logging monitor *severity level*

Syntax Description

logging monitor	Sets message logging.
severity level	0-7 0-emerg;1-alert;2-crit;3-err;4-warn;5-notif;6-inform;7-debug

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example sets terminal line (monitor) message logging at level 2.

```
switch## config terminal
switch(config)# logging monitor 2
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

logging server

To set message logging for the remote server, use the **logging server** command.

logging server [*hostname* | *ip address severity_level* | **facility auth** | **authpriv** | **cron** | **daemon** | **ftp** | **kernel** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **syslog** | **user** | **uucp**]

Syntax Description

logging server	Sets message logging for remote server.
hostname	Enters host name for remote server.
ip address	Enters the IP address for the remote server.
severity_level	Enter severity level of message. 0-emerg;1-alert;2-crit;3-err;4-warn;5-notif;6-inform;7-debug
facility	Facility to use when forwarding to server
auth	Use auth facility
authpriv	Use authpriv facility
cron	Use Cron/at facility
daemon	Use daemon facility
ftp	Use file transfer system facility
kernel	Use kernel facility
local0	Use local0 facility
local1	Use local1 facility
local2	Use local2 facility
local3	Use local3 facility
local4	Use local4 facility
local5	Use local5 facility
local6	Use local6 facility
local7	Use local7 facility
lpr	Use lpr facility
mail	Use mail facility
news	Use USENET news facility
syslog	Use syslog facility
user	Use user facility
uucp	Use Unix-to-Unix copy system facility

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

Enable message logging to the specified remote server for level 7 messages.

```
switch## config terminal
switch(config)# logging sever sanjose 7
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

logging timestamp

To set the time increment for the message logging time stamp, use the **logging timestamp** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

logging timestamp {**microseconds** | **milliseconds** | **seconds**}

no logging timestamp {**microseconds** | **milliseconds** | **seconds**}

Syntax Description

microseconds	Sets the logging time stamp to microseconds.
milliseconds	Sets the logging time stamp to milliseconds.
seconds	Sets the logging time stamp to seconds.

Defaults

Seconds.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example sets the logging time stamp to milliseconds.

```
switch## config terminal
switch(config)# logging timestamp milliseconds
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

CHAPTER 15

M Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "Command Modes" section to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

match

To configure QoS class map match criteria, use the **match** command in class map configuration submode. Remove QoS class map match criteria, use the **no** form of the command.

match {**any** | **destination-address** *fc-id* [**mask** *address-mask*] | **destination-device-alias** *name* | **destination-wwn** *wwn-id* | **input-interface fc** *slot/port* | **source-address** *fc-id* [**mask** *address-mask*] | **source-device-alias** *name* | **source-wwn** *wwn-id*}

no match {**any** | **destination-address** *fc-id* [**mask** *address-mask*] | **destination-device-alias** *name* | **destination-wwn** *wwn-id* | **input-interface fc** *slot/port* | **source-address** *fc-id* [**mask** *address-mask*] | **source-device-alias** *name* | **source-wwn** *wwn-id*}

Syntax Description

any	Enables matching of any frame.
destination-address *fc-id*	Specifies the destination FCID to match frames.
mask *address-mask*	Specifies an address mask to match frames. The range is 0x0 to 0xffffffff.
destination-device-alias *name*	Specifies the destination device alias to match frames. Maximum length is 64 characters.
destination-wwn *wwn-id*	Specifies the destination WWN to match frames.
input-interface fc *slot/port*	Specifies the source Fibre Channel interface to match frames.
source-address *fc-id*	Specifies the source FCID to match frames.
source-device-alias *name*	Specifies the source device alias to match frames. Maximum length is 64 characters.
source-wwn *wwn-id*	Specifies the source WWN to match frames.

Defaults

None.

Command Modes

Class map configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.0(1b)	Added the **destination-device-alias** and **source-device-alias** options.

Usage Guidelines

You can access this command only if you enable the QoS data traffic feature using the **qos enable** command.

Examples

The following example creates a class map called MyClass1 and places you in the class map configuration submode to match any (default) criteria specified for this class.

```
switch# config terminal
```

```
switch(config)# qos class-map MyClass1 match-any
switch(config-cmap)# match any
```

The following example specifies a destination address match for frames with the specified destination FCID.

```
switch(config-cmap)# match destination-address 0x12ee00
```

The following example specifies a source address and mask match for frames with the specified source FCID. Mask refers to a single or entire area of FCIDs.

```
switch(config-cmap)# match source-address 0x6d1090 mask 0
```

The following example specifies a destination WWN to match frames.

```
switch(config-cmap)# match destination-wwn 20:01:00:05:30:00:28:df
Operation in progress. Please check class-map parameters
```

The following example specifies a source WWN to match frames.

```
switch(config-cmap)# match source-wwn 23:15:00:05:30:00:2a:1f
Operation in progress. Please check class-map parameters
```

The following example specifies a source interface to match frames.

```
switch(config-cmap)# match input-interface fc 2/1
Operation in progress. Please check class-map parameters
```

The following example removes a match based on the specified source interface.

```
switch(config-cmap)# no match input-interface fc 3/5
```

Related Commands

Command	Description
qos enable	Enables QoS.
show qos	Displays QoS information.

match address

To configure match addresses in an IPsec crypto map with an access control list (ACL), use the **match address** command in IPsec crypto map configuration submode. To not match addresses, use the **no** form of the command.

match address *acl-name*

no match address [*acl-name*]

Syntax Description

acl-name	Specifies the ACL name. Maximum length is 64 characters.

Defaults

None.

Command Modes

IPsec crypto map configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Examples

The following example shows how to match addresses in an IPsec crypto map with an ACL.

```
switch# config terminal
switch(config)# crypto map domain ipsec x 1
switch(config-crypto-map-ip)# match address UserACL
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
show crypto map domain ipsec	Displays IPsec crypto map information.

mcast root

To configure the multicast feature, use the **mcast root** command in configuration mode. To revert to the default, use the **no** form of the command.

mcast root {**lowest** | **principal**} **vsan** *vsan-id*

no mcast root {**lowest** | **principal**} **vsan** *vsan-id*

Syntax Description

lowest	Specifies the lowest domain switch as root.
principal	Specifies the principal switch as root.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

principal

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the multicast root VSAN.

```
switch# config terminal
switch(config)# mcast root principal vsan 4001
```

Related Commands

Command	Description
show mcast	Displays multicast information.

member (fcalias configuration submode)

To add a member name to an Fibre Channel alias on a VSAN, use the **member** command in fcalias configuration submode. To remove a member name from an FC alias, use the **no** form of the command.

member {**device-alias** *aliasname* [**lun** *lun-id*] |
domain-id *domain-id* [**lun** *lun-id*] |
fcid *fc-id* [**lun** *lun-id*] |
fwwn *fwwn-id* |
interface fc *slot*/*port* [**domain-id** *domain-id* | **swwn** *swwn-id*] |
ip-address *ipv4*|*ipv6* |
pwwn *pwwn-id* [**lun** *lun-id*] |
symbolic-nodename *nodename*}

no member {**device-alias** *aliasname* [**lun** *lun-id*] |
domain-id *domain-id* [**lun** *lun-id*] |
fcid *fc-id* [**lun** *lun-id*] |
fwwn *fwwn-id* |
interface fc *slot*/*port* [**domain-id** *domain-id* | **swwn** *swwn-id*] |
ip-address *ipv4*|*ipv6* |
pwwn *pwwn-id* [**lun** *lun-id*] |
symbolic-nodename *nodename*}

Syntax Description

device-alias *aliasname*	Specifies the member device alias. Maximum length is 64 characters.
lun *lun-id*	Specifies the member LUN ID. The format is *0***x***hhhh*[**:***hhhh*[**:***hhhh*[**:***hhhh*]]], where *h* is a hexadecimal digit.
domain-id *domain-id*	Specifies the member domain ID. The range is 1 to 239.
fcid *fc-id*	Specifies the member FC ID. The format is *0***x***hhhhhh,* where *h* is a hexadecimal digit.
fwwn *fwwn-id*	Specifies the member fWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh,* where *h* is a hexadecimal digit.
interface fc *slot*/*port*	Specifies the member interface ID.
swwn *swwn-id*	Specifies the member sWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh,* where *h* is a hexadecimal digit.
ip-address *ipv4*|*ipv6*	Specifies a member IP address in either IPv4 format, *A.B.C.D*, or IPv6format, *X:X:X::X/n*.
pwwn *pwwn-id*	Specifies the member pWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh,* where *h* is a hexadecimal digit.
symbolic-nodename *nodename*	Specifies the member symbolic node name. The maximum length is 255 characters.

Defaults

None.

Command Modes

Fcalias configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to add a member to an FC alias called samplealias.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# fcalias name samplealias
switch(config-fcalias)#
```

The following example defines an IPv6 address for the member.

```
switch(switch(config-fcalias)# member ip-address 2020:dbc0:80::4076
```

The following example shows how to delete the specified member.

```
switch(config-fcalias)# no member ip-address 2020:dbc0:80::4076
```

Related Commands

Command	Description
fcalias name	Configures an FC alias.
show fcalias	Displays the member name information in an FC alias.

member (ivr zone configuration)

To add a member name to an Inter-VSAN Routing (IVR) zone, use the **member** command in IVR zone configuration submode. To remove a member name from an fcalias, use the **no** form of the command.

member {**device-alias** *aliasname* {**lun** *lun-id* **vsan** *vsan-id* **autonomous-fabric-id** *afid* |
vsan *vsan-id* **autonomous-fabric-id** *afid*} |
pwwn *pwwn-id* {**lun** *lun-id* **vsan** *vsan-id* **autonomous-fabric-id** *afid* | **vsan** *vsan-id* **autonomous-fabric-id** *afid*}}

no member {**device-alias** *aliasname* {**lun** *lun-id* **vsan** *vsan-id* **autonomous-fabric-id** *afid* |
vsan *vsan-id* **autonomous-fabric-id** *afid*} |
pwwn *pwwn-id* {**lun** *lun-id* **vsan** *vsan-id* **autonomous-fabric-id** *afid* | **vsan** *vsan-id* **autonomous-fabric-id** *afid*}}

Syntax Description

device-alias *aliasname*	Specifies the member device alias. Maximum length is 64 characters.
lun *lun-id*	Specifies the member LUN ID. The format is *0***x***hhhh*[**:***hhhh*[**:***hhhh*[**:***hhhh*]]], where *h* is a hexadecimal digit.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
autonomous-fabric-id *afid*	Specifies the AFID to the local VSAN.
pwwn *pwwn-id*	Specifies the member pWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh,* where *h* is a hexadecimal digit.

Defaults

None.

Command Modes

IVR zone configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.1(1a)	Added **lun** parameter.

Usage Guidelines

You can configure an IVR zone member based on the specified pWWN and LUN value or, based on the specified pWWN, LUN value, and AFID.

Note The CLI interprets the LUN identifier value as a hexadecimal value whether or not the 0x prefix is included.

Examples

The following example shows how to configures an IVR zone member based on the device alias VSAN, and the AFID.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr zone name IvrLunZone
switch(config-ivr-zone)# member device-alias Switch4 vsan 1 autonomous-fabric-id 14
```

The following example shows how to configures an IVR zone member based on the pWWN, VSAN, and the AFID.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr zone name IvrLunZone
switch(config-ivr-zone)# member pwwn 29:00:00:05:30:00:06:ea vsan 1 autonomous-fabric-id
14
```

Related Commands

Command	Description
show ivr zone	Displays the IVR zone information.

member (zone configuration and zoneset-zone configuration submode)

To add a member name to a Fibre Channel zone set zone member, use the **member** command in zone set zone configuration submode. To remove a member name from a zone set zones, use the **no** form of the command.

member {**device-alias** *aliasname* [**lun** *lun-id*] | **domain-id** *domain-id* **port-number** *port* | **fcalias** *alias-name* [**lun** *lun-id*] | **fcid** *fc-id* [**lun** *lun-id*] | **fwwn** *fwwn-id* | **interface fc** *slot*/*port* [**domain-id** *domain-id* | **swwn** *swwn-id*] | **ip-address** *ipv4*|*ipv6* | **pwwn** *pwwn-id* [**lun** *lun-id*] | **symbolic-nodename** *nodename*}

no member {**device-alias** *aliasname* [**lun** *lun-id*] | **domain-id** *domain-id* **port-number** *port* | **fcid** *fc-id* [**lun** *lun-id*] | **fwwn** *fwwn-id* | **interface fc** *slot*/*port* [**domain-id** *domain-id* | **swwn** *swwn-id*] | **ip-address** *ipv4*|*ipv6* | **pwwn** *pwwn-id* [**lun** *lun-id*] | **symbolic-nodename** *nodename*}

Syntax Description

device-alias *aliasname*	Specifies the member device alias. Maximum length is 64 characters.
lun *lun-id*	Specifies the member LUN ID. The format is *0***x***hhhh*[**:***hhhh*[**:***hhhh*[**:***hhhh*]]], where *h* is a hexadecimal digit.
domain-id *domain-id*	Specifies the member domain ID. The range is 1 to 239.
alias-name	The name of the fcalias. Maximum length is 64 characters.
port-number *port*	Specifies the member port number. The range is 0 to 255.
fcid *fc-id*	Specifies the member FC ID. The format is *0***x***hhhhhh,* where *h* is a hexadecimal digit.
fwwn *fwwn-id*	Specifies the member fWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh,* where *h* is a hexadecimal digit.
interface fc *slot*/*port*	Specifies the member interface ID.
swwn *swwn-id*	Specifies the member sWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh,* where *h* is a hexadecimal digit.
ip-address *ipv4*|*ipv6*	Specifies a member IP address in either IPv4 format, *A.B.C.D*, or IPv6format, *X:X:X::X/n*.
pwwn *pwwn-id*	Specifies the member pWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh,* where *h* is a hexadecimal digit.
symbolic-nodename *nodename*	Specifies the member symbolic node name. The maximum length is 255 characters.

Defaults

This command can be used in both zone configuration submode and zoneset-zone configuration submode.

Command Modes

Zone set zone configuration submode and zoneset-zone configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.
2.1(1a)	Added zoneset-zone configuration submode.
3.0(1)	Added the **IPv6** IP address format.

Usage Guidelines

Create a zone set zone member only if you need to add member to a zone from the zone set prompt.

Examples

The following example shows how to add a member to a zone called zs1 on VSAN 1.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# zone name zs1 vsan 1
switch(config-zone)# member fcid 0x111112
switch(config-zone)#
```

The following example shows how to add a zone to a zoneset called Zoneset1 on VSAN 1.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# zoneset name ZoneSet1 vsan 1
switch(config-zoneset-zone)# member fcid 0x111112
```

The following example shows how to assign an iSCSI IPv6 address-based membership into a zone.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# zoneset name ZoneSet1 vsan 1
switch(config-zoneset-zone)# member ipv6-address 2001:0DB8:800:200C::417A
```

The following example shows how to delete the specified device from a zone.

```
switch(config-zoneset-zone)# no member ipv6-address 2001:0DB8:800:200C::417A
```

Related Commands

Command	Description
zoneset (configuration submode)	Used to specify a name for a zone set.
zone name (zone set configuration submode)	Configures a zone in a zoneset.
show zoneset	Displays zone set information.

member (zoneset configuration submode)

To configure zone set zone members, use the **member** command in zone set configuration submode. To remove a zone set member, use the **no** form of the command.

member *member-name*

no member *member-name*

Syntax Description

member-name	Specifies the member name. Maximum length is 64 characters.

Defaults

None.

Command Modes

Zone set configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to add a member zone to a zone set.

```
switch# config terminal
switch(config)# zoneset name Zoneset1 vsan 10
switch(config-zoneset)# member ZoneA
```

Related Commands

Command	Description
show zone	Displays zone information.
zoneset name	Creates a zone set.

metric (iSLB initiator configuration)

To assign a load-balancing metric for an iSLB initiator, use the **metric** command in iSLB initiator configuration submode. To revert to the default load-balancing metric, use the **no** form of the command.

metric *metric*

no metric *metric*

Syntax Description

metric *metric*	Specifies a load-balancing metric. The range is 10 to 10000.

Defaults

1000

Command Modes

iSLB initiator configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can assign a load metric to each initiator for weighted load balancing. The load calculated is based on the number of initiators on a given iSCSI interface. This feature accommodates initiators with different bandwidth requirements. For example, you could assign a higher load metric to a database server than to a web server. Weighted load balancing also accommodates initiators with different link speeds.

Examples

The following example specifies a load-balancing metric for the iSLB initiator.

```
switch# config t
switch(config)# islb initiator ip-address 100.10.10.10
switch (config-islb-init)# metric 100
```

The following example reverts to the default load-balancing metric.

```
switch (config-islb-init)# no metric 100
```

Related Commands

Command	Description
islb initiator	Assigns an iSLB name and IP address to the iSLB initiator and enters iSLB initiator configuration submode.
show islb initiator configured	Displays iSLB initiator information for the specified configured initiator.
show islb initiator detail	Displays detailed iSLB initiator information.
show islb initiator summary	Displays iSLB initiator summary information.

mkdir

To create a directory in the Flash file system, use the **mkdir** command in EXEC mode.

mkdir *directory*

Syntax Description

directory	Name of the directory to create.

Defaults

None.

Command Modes

EXEC

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command is only valid on Class C Flash file systems.

You can specify whether to create the directory on bootflash:, slot0, or volatile:. If you do not specify the device, the switch creates the directory on the current directory.

Examples

The following example creates a directory called test in the slot0: directory.

```
switch# mkdir slot0:test
```

The following example creates a directory called test at the current directory level. If the current directory is slot0:mydir, this command creates a directory called slot0:mydir/test.

```
switch# mkdir test
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
rmdir	Removes an existing directory in the Flash file system.

modem connect line

To enable a modem connection when the switch is already in operation, use the **modem connect line** command in EXEC mode.

modem connect line {**com1** | **console**}

Syntax Description

com1	Connects the modem through a COM1 line connection
console	Connects the modem through a console line connection

Defaults

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(2)	This command was introduced.

Usage Guidelines

If the switch is already in operation when the modem is connected, issue this command to notify the software that a modem is going to be added.

You must issue the **modem connect line** command before setting the user-input string for initialization.

Examples

The following example announces a modem connection from the line console.

```
switch# modem connect line console
```

The following example announces a modem connection from the COM1 port.

```
switch# modem connect line com1
```

move

To remove a file from the source file and place it in the destination file, use the **move** command in EXEC mode.

move {bootflash: | slot0: | volatile:}[*directory*/]*filename*
{bootflash: | slot0: | volatile:}[*directory*/]*filename*

Syntax Description

bootflash:	Source or destination location for internal bootflash memory.
slot0:	Source or destination location for the CompactFlash memory or PCMCIA card.
volatile:	Source or destination location for volatile memory.
directory	Specifies the name of the directory.
filename	Specifies the name of the file to move or create.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

If you do not specify the directory name in the command line, the switch prompts you for it.

Examples

The following example moves the file called samplefile from the slot0 directory to the mystorage directory.

```
switch# move slot0:samplefile slot0:mystorage/samplefile
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
mkdir	Creates a directory in the Flash file system.
rmdir	Removes an existing directory in the Flash file system.

mutual-chap username (iSCSI initiator configuration and iSLB initiator configuration)

To assign a username for the initiator's challenge, use the **mutual-chap** command in iSCSI initiator configuration submode. To remove the username, use the **no** form of the command.

mutual-chap username *username* **password {0** *cleartext-password* **| 7** *encrypted-password* **|** *password***}**

no mutual-chap username *username* **password {0** *cleartext-password* **| 7** *encrypted-password* **|** *password***}**

Syntax Description

username *username*	Specifies a username. The maximum size is 32.
password	Specifies a password for the initiator's challenge.
0	Specifies that the password is a cleartext CHAP password.
7	Specifies that the password is an encrypted CHAP password.
password	Specifies a password for the username. The maximum size is 32.

Defaults

None.

Command Modes

iSCSI initiator configuration submode.
iSLB initiator configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.
3.0(1)	Added iSLB initiator configuration submode.

Usage Guidelines

The iSLB initiator can authenticate the Cisco MDS switch's initiator target during the iSCSI login phase. This authentication requires the user to configure a username and password for the switch to present to the iSLB initiator. The provided password is used to calculate a CHAP response to a CHAP challenge sent to the IPS port by the initiator.

Examples

The following example shows how to configure a username, password type, and password for an iSCSI initiator challenge (mutual CHAP).

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# iscsi initiator name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-init)# mutual-chap username userName password 0 cisco
switch(config-iscsi-init)#
```

The following example assigns a username and password to the initiator's challenge for an iSLB initiator.

```
switch# config t
switch(config)# islb initiator ip-address 100.10.10.10
switch (config-islb-init)# mutual-chap username tester password K9c4*1
```

The following example removes the username and password from the initiator's challenge for an iSLB initiator.

```
switch (config-islb-init)# no mutual-chap username tester password K9c4*1
```

Related Commands

Command	Description
iscsi initiator name	Assigns an iSCSI name and changes to iSCSI initiator configuration submode.
islb initiator	Assigns an iSLB name and IP address to the iSLB initiator and enter iSLB initiator configuration submode.
show iscsi initiator	Displays iSCSI initiator information.
show iscsi initiator configured	Displays iSCSI initiator information for the configured iSCSI initiator.
show iscsi initiator detail	Displays detailed iSCSI initiator information.
show iscsi initiator summary	Displays iSCSI initiator summary information.
show islb initiator	Displays iSLB initiator information.
show islb initiator configured	Displays iSLB initiator information for the configured iSLB initiator.
show islb initiator detail	Displays detailed iSLB initiator information.
show islb initiator summary	Displays iSLB initiator summary information.

CHAPTER 16

N Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "Command Modes" section to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

nasb module

To enable Network-Accelerated Serverless Backup (NASB) in a VSAN and map it to the Storage Services Module (SSM) where the feature is enabled, use the **nasb module** command in configuration mode. To disable this feature, use the **no** form of the command.

nasb module *slot-number* **vsan** *vsan-id* [**control [multiple] | multiple [control]**]

no nasb module *slot-number* **vsan** *vsan-id*

Syntax Description

slot-number	Specifies the slot number of the connected module.
vsan *vsan-id*	Configures up to five VSANs to be added to the database. The range is 1 to 4096.
control	Configures a single target LUN that is a Storage Array Controller (Peripheral Device Type 0x0C).
multiple	Configures up to 10 target LUNs that are the default type, Direct Access Device (Peripheral Device Type 0x00).

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.
2.1(2)	Added the **multiple** option.

Usage Guidelines

This feature must be enabled on the SSM using the **ssm enable feature** command before you can configure NASB.

Examples

The following example configures NASB on the SSM installed in slot 4 with a link to VSAN 1.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# nasb module 4 vsan 1
```

The following example configures NASB on the SSM installed in slot 4 with a link to VSAN 10, and enables a single target LUN that is a Storage Array Controller (Peripheral Device Type = 0x0C).

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# nasb module 4 vsan 10 control
```

The following example configures NASB on the SSM installed in slot 4 with a link to VSAN 10, and enables a single target LUN that is a Storage Array Controller (Peripheral Device Type = 0x0C) and up to 10 target LUNs.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# nasb module 4 vsan 10 control multiple
```

Related Commands

Command	Description
ssm enable feature	Enables the NASB feature on the Storage Services Module (SSM).
nasb module	Displays the NASB configuration on the SSM.
nasb rediscover module	Initiates the rediscovery of a target device used for NASB on an SSM where the feature is enabled.

nasb rediscover module

To initiate the rediscovery of a target device, such as a disk or tape device, used for Network-Accelerated Serverless Backup (NASB) in a VSAN on a Storage Services Module (SSM) where the feature is enabled, use the **nasb rediscover module** command in EXEC mode.

nasb rediscover module *slot-numbe*r **vsan** *vsan-id* **target-pwwn** *pwwn-id*

Syntax Description

slot-number	Specifies the slot number of the connected module.
vsan *vsan-id*	Specifies the current VSAN. The range is 1 to 4096.
target-pwwn *pwwn-id*	Specifies the pWWN for the target device. The form is *hh:hh:hh:hh:hh:hh:hh:hh*, where *h* is a hexadecimal number.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.1(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to initiate a rediscovery of a target device.

```
switch# nasb rediscover module 2 vsan 9 target-pwwn 20:02:00:a0:b8:16:a1:5f
nasb rediscovery initiated
switch#
```

Related Commands

Command	Description
nasb module	Enables the NASB feature in configuration mode and allows you to configure the Storage Array Controller and multiple LUNs.
show nasb	Displays the NASB configuration on the SSM.
ssm enable feature	Enables the NASB feature on the SSM.

native-autonomous-fabric-num

To create an IVR persistent FC ID database entry, use the **native-autonomous-fabric-num** command in fcdomain database configuration submode. To delete all IVR persistent FC ID database entries for a given AFID and VSAN, use the **no** form of the command.

native-autonomous-fabric-num *afid-num* **native-vsan** *vsan-id* **domain** *domain-id*

no native-autonomous-fabric-num *afid-num* **native-vsan** *vsan-id* **domain** *domain-id*

Syntax Description

afid-num	Specifies the native AFID. The range is 1 to 64.
native-vsan *vsan-id*	Specifies the native VSAN ID. The range is 1 to 4093.
domain *domain-id*	Specifies the domain ID. The range is 1 to 239.

Defaults

None.

Command Modes

fcdomain database configuration submode.

Command History

Release	Modification
2.1(2)	This command was introduced.

Usage Guidelines

There is only one domain ID associated with an AFID and VSAN. If you change the domain ID, all the associated FC ID mapping records are also changed.

Examples

The following example shows how to create an entry for a native AFID, VSAN, and domain.

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config-fcdomain)# native-autonomous-fabric-num 20 native-vsan 30 domain 15
switch(config-fcdomain-fcid)#
```

The following example shows how to remove all entries for a native AFID and VSAN.

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config-fcdomain)# no native-autonomous-fabric-num 20 native-vsan 30
```

Related Commands

Command	Description
ivr fcdomain database autonomous-fabric-num	Creates IVR persistent FC IDs.
show ivr fcdomain database	Displays IVR fcdomain database entry information.

npiv enable

To enable N port identifier virtualization (NPIV) for all VSANs on a switch, use the **npiv enable** command in configuration mode. To disable NPIV, use the **no** form of the command.

npiv enable

no npiv enable

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

NPIV provides a means to assign multiple port IDs to a single N port. This feature allows multiple applications on the N port to use different identifiers and allows access control, zoning, and port security to be implemented at the application level.

You must globally enable NPIV for all VSANs on the MDS switch to allow the NPIV-enabled applications to use multiple N port identifiers.

Note All of the N port identifiers are allocated in the same VSAN.

Examples

The following example enables NPIV for all VSANs on the switch.

```
switch# config terminal
switch(config)# npiv enable
```

The following example disables NPIV for all VSANs on the switch.

```
switch(config)# no npiv enable
```

Related Commands

Command	Description
show interface	Displays interface configurations.

nport pwwn

To configure the nport pWWN for the SAN extension tuner, use the **nport pwwn** command in SAN extension configuration mode. To revert to the default value, use the **no** form of the command.

nport pwwn *pwwn-id* **vsan** *vsan-id* **interface gigabitethernet** *slot*/*port*

no nport pwwn *pwwn-id* **vsan** *vsan-id* **interface gigabitethernet** *slot*/*port*

Syntax Description

pwwn-id	Specifies the port WWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
interface gigabitethernet *slot*/*port*	Specifies the Gigabit Ethernet interface slot and port.

Defaults

None.

Command Modes

SAN extension configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to add an entry to the SAN extension tuner database.

```
switch# san-ext-tuner
switch(san-ext)# nport pwwn 11:22:33:44:55:66:77:88 vsan 1 interface gigabitethernet 1/1
```

Related Commands

Command	Description
san-ext-tuner	Enters SAN extension configuration mode.
show san-ext-tuner	Shows SAN extension tuner information.

ntp

To configure NTP settings on the switch, use the **ntp** command in configuration mode.

ntp {peer *hostname* **| server | tstamp-check}**

Syntax Description

peer *hostname*	The hostname/IP address of the NTP peer (Max Size - 80).
server	The hostname/IP address of the NTP server (Max Size - 80).
tstamp-check	Enables or disables the Timestamp Check.

Defaults

This command has no default settings.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

This example forms a server association with a server.

```
switch(config)# ntp server 10.10.10.10
switch(config)#
```

This example forms a peer association with a peer. You can specify multiple associations.

```
switch(config)# ntp peer 10.20.10.0
switch(config)#
```

ntp abort

To discard the Network Time Protocol (NTP) Cisco Fabric Services (CFS) distribution session in progress, use the **ntp abort** command in configuration mode.

ntp abort

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure NTP CFS distribution session in progress.

```
switch# config terminal
switch(config)# ntp abort
```

Related Commands

Command	Description
ntp distribute	Enables CFS distribution for NTP.
show ntp	Displays NTP information.

ntp commit

To apply the pending configuration pertaining to the Network Time Protocol (NTP) Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **ntp commit** command in configuration mode.

ntp commit

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to commit changes to the active NTP configuration.

```
switch# config terminal
switch(config)# ntp commit
```

Related Commands

Command	Description
ntp distribute	Enables CFS distribution for NTP.
show ntp	Displays NTP information.

ntp distribute

To enable Cisco Fabric Services (CFS) distribution for Network Time Protocol (NTP), use the **ntp distribute** command. To disable this feature, use the **no** form of the command.

ntp distribute

no ntp distribute

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.0(2).

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

Before distributing the Fibre Channel timer changes to the fabric, the temporary changes to the configuration must be committed to the active configuration using the **ntp commit** command.

Examples

The following example shows how to distribute the active NTP configuration to the fabric.

```
switch# config terminal
switch(config)# ntp distribute
```

Related Commands

Command	Description
ntp commit	Commits the NTP configuration changes to the active configuration.
show ntp	Displays NTP information.

nwwn (DPVM database configuration submode)

To add a device to a dynamic port VSAN membership (DPVM) database using the nWWN, use the **nwwn** command in DPVM database configuration submode. To remove a device from a DPVM database using the nWWN, use the **no** form of the command.

nwwn *nwwn-id* **vsan** *vsan-id*

no nwwn *nwwn-id* **vsan** *vsan-id*

Syntax Description

nwwn-id	Specifies the node WWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

DPVM database configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

Examples

The following example shows how to add an entry to the DPVM database.

```
switch# config terminal
switch(config)# dpvm database
switch(config-dpvm-db)# nwwn 11:22:33:44:55:66:77:88 vsan 1
```

The following example shows how to delete an entry from the DPVM database.

```
switch(config-dpvm-db)# no nwwn 11:22:33:44:55:66:77:88 vsan 1
```

Related Commands

Command	Description
dpvm database	Configures the DPVM database.
show dpvm	Displays DPVM database information.

nwwn (SAN extension configuration mode)

To configure the nWWN for the SAN extension tuner, use the **nwwn** command in SAN extension configuration submode.

nwwn *nwwn-id*

Syntax Description

nwwn-id	Specifies the nWWN address. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.

Defaults

None.

Command Modes

SAN extension configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to add an entry to the SAN extension tuner database.

```
switch# san-ext-tuner
switch(san-ext)# nwwn 20:42:00:0b:46:79:f1:80
```

Related Commands

Command	Description
san-ext-tuner	Enters SAN extension configuration mode.
show san-ext-tuner	Shows SAN extension tuner information.

CHAPTER 17

O Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. Please see the Command Mode section to determine the appropriate mode for each command. For more information, see the *Cisco MDS 9000 Family CLI Configuration Guide*.

ocsp url

To configure the HTTP URL of the Online Certificate Status Protocol (OCSP) for the trust point CA, use the **ocsp url** command in trust point configuration submode. To discard the OCSP configuration, use the **no** form of the command.

ocsp url *url*

no ocsp url *url*

Syntax Description

url	Specifies the OCSP URL. The maximum size is 512 characters.

Defaults

None.

Command Modes

Trust point configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The MDS switch uses the OCSP protocol to check the revocation status of a peer certificate (presented to it during the security or authentication exchange for IKE or SSH, for example), only if the revocation checking methods configured for the trust point include OCSP as one of the methods. OCSP checks the certificate revocation status against the latest CRL on the CA using the online protocol, thereby generating network traffic and also requiring that the OCSP service of the CA be available online in the network.

On the other hand, if revocation checking is performed by the cached CRL at the MDS switch, no network traffic is generated. The cached CRL doesn't contain the latest revocation information.

You must authenticate the CA for the trust point before configuring the OCSP URL for it.

Examples

The following example shows how to specify the URL for OCSP to use to check for revoked certificates.

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# ocsp url http://admin-ca.cisco.com/ocsp
```

The following example shows how to remove the URL for OCSP.

```
switch(config-trustpoint)# no ocsp url http://admin-ca.cisco.com/ocsp
```

Related Commands

Command	Description
crypto ca crl-request	Configures a CRL or overwrites the existing one for the trust point CA.
revocation-check	Configures trust point revocation check methods.
show crypto ca crl	Displays configured CRLs.

out-of-service

To put an interface out of service, use the **out-of-service** command in interface configuration submode. To restore the interface to service, use the **no** form of the command.

out-of-service [**force**]

no out-of-service [force]

Syntax Description

force	Configures the interface that should be forced out of service.

Defaults

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Before using the **out-of-service** command, you must disable the interface using the **shutdown** command.

When an interface is out of service, all the shared resources for the interface are released, as is the configuration associated with those resources.

Caution Taking interfaces out of service releases all the shared resources to ensure that they are available to other interfaces. This causes the configuration in the shared resources to revert to default when the interface is brought back into service. Also, an interface cannot come back into service unless the default shared resources for the port are available. The operation to free up shared resources from another port is disruptive.

Examples

The following example shows how to take an interface out of service.

```
switch# config terminal
switch(config)# interface fc 1/1
switch(config-if)#shutdown
switch(config-if)# out-of-service
Putting an interface into out-of-service will cause its shared resource
configuration to revert to default
Do you wish to continue(y/n)? [n]
```

The following example makes an interface available for service.

```
switch(config-if)# no out-of-service
```

Related Commands

Command	Description
shutdown	Disables an interface.
show interface	Displays the status of an interface.

out-of-service module

To perform a graceful shutdown of an integrated crossbar on the supervisor module of a Cisco MDS 9500 Series Director, use the **out-of-service module** command in EXEC mode.

out-of-service module *slot*

Syntax Description

slot	Specifies the module number. For Cisco MDS 9506 and 9509 Directors, the range is 1 to 6. For the Cisco MDS 9513 Director, the range is 1 to 13.

Defaults

None.

Command Modes

EXEC.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Before removing a crossbar from an MDS 9500 Series Director, you must perform a graceful shutdown of the crossbar.

Enter the EXEC mode **out-of-service module** command for a graceful shutdown of the integrated crossbar on the supervisor module in a Cisco MDS 9506 or 9509 Director.

out-of-service module *slot*

The *slot* refers to the chassis slot number for Supervisor-1 module or Supervisor-2 module where the integrated crossbar is located.

Note To reactivate the integrated crossbar, you must remove and reinsert or replace the Supervisor-1 or Supervisor-2 module.

For additional information about crossbar management, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

Examples

The following example shows how to perform a graceful shutdown of the integrated crossbar.

```
switch# out-of-service module 2
```

Related Commands

Command	Description
out-of-service xbar	Performs a graceful shutdown of an external crossbar switching module in a Cisco MDS 9513 Director.
show module	Displays the status of a module.

out-of-service xbar

To perform a graceful shutdown of the external crossbar switching module of a Cisco MDS 9513 Director, use the **out-of-service xbar** command in EXEC mode.

out-of-service xbar *slot*

no out-of-service xbar *slot*

Syntax Description

slot	Specifies the external crossbar switching module slot number, either 1 or 2.

Defaults

None.

Command Modes

EXEC.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Before removing a crossbar from an MDS 9500 Series Director, you must perform a graceful shutdown of the crossbar.

The administrator must enter the EXEC mode **out-of-service xbar** command for a graceful shutdown of the external crossbar switching module in a Cisco MDS 9513 Director.

out-of-service xbar *slot*

The *slot* refers to the external crossbar switching module slot number.

Note To reactivate the external crossbar switching module, you must remove and reinsert or replace the crossbar switching module.

Caution Taking the crossbar out-of-service may cause supervisor switchover.

For additional information about crossbar management, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

Examples

The following example shows how to perform a graceful shutdown of the external crossbar switching module of a Cisco MDS 9513 Director.

```
switch# out-of-service xbar 1
```

Related Commands

Command	Description
out-of-service module	Performs a graceful shutdown of an integrated crossbar on the supervisor module of a Cisco MDS 9500 Series Director.
show module	Displays the status of a module.

CHAPTER 18

P Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "Command Modes" section to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

passive-mode

To configure the required mode to initiate an IP connection, use the **passive-mode** command. To enable passive mode for the FCIP interface, use the **no** form of the command.

passive-mode

no passive-mode

Syntax Description

This command has no keywords or arguments.

Defaults

Disabled

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Access this command from the `switch(config-if)#` submode.

By default, the active mode is enabled to actively attempt an IP connection.

If you enable the passive mode, the switch does not initiate a TCP connection and merely waits for the peer to connect to it.

Examples

The following example enables passive mode on an FCIP interface.

```
switch# config terminal
switch(config)# interface fcip 1
switch(config-if)# passive-mode
```

Related Commands

Command	Description
show interface fcip	Displays an interface configuration for a specified FCIP interface.

peer-info ipaddr

To configure the peer information for the FCIP interface, use the **peer-info ipaddr** command. To remove the peer information for the FCIP interface, use the **no** form of the command.

peer-info ipaddr *address* **[port** *number*]

no peer-info ipaddr *address* **[port** *number*]

Syntax Description

ipaddr *address*	Configures the peer IP address.
port *number*	Configures a peer port. The range is 1 to 65535.

Defaults

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Access this command from the `switch(config-if)#` submode.

The basic FCIP configuration uses the peer's IP address to configure the peer information. You can also use the peer's port number, port profile ID, or port WWN to configure the peer information. If you do not specify a port, the default 3225 port number is used to establish connection.

Examples

The following command assigns an IP address to configure the peer information. Since no port is specified, the default port number, 3225, is used.

```
switch# config terminal
switch(config)# interface fcip 10
switch(config-if)# peer-info ipaddr 10.1.1.1
```

The following command deletes the assigned peer port information.

```
switch(config-if)# no peer-info ipaddr 10.10.1.1
```

The following command assigns the IP address and sets the peer TCP port to 3000. The valid port number range is from 0 to 65535.

```
switch(config-if)# peer-info ipaddr 10.1.1.1 port 3000
```

The following command deletes the assigned peer port information.

```
switch(config-if)# no peer-info ipaddr 10.1.1.1 port 2000
```

Related Commands

Command	Description
show interface fcip	Displays an interface configuration for a specified FCIP interface.

periodic-inventory notification

To enable the periodic inventory notification message dispatches, use the **periodic-inventory notification** command Call Home configuration submode. To revert to the default state, use the **no** form of the command.

periodic-inventory notification [**interval** *days*]

no periodic-inventory notification

Syntax Description

interval *days*	Specifies the notification interval. The range is 1 to 30.

Defaults

Disabled.

The initial default interval is 7 days.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable periodic inventory notification and use the default interval.

```
switch# config terminal
switch(config)# callhome
switch(config-callhome)# periodic-inventory notification
```

The following example shows how to enable periodic inventory notification and set the interval to 10 days.

```
switch# config terminal
switch(config)# callhome
switch(config-callhome)# periodic-inventory notification interval 10
```

Related Commands

Command	Description
callhome	Enters Call Home configuration submode.
show callhome	Displays Call Home configuration information.

permit (IPv6-ACL configuration)

To configure permit conditions for an IPv6 access control list (ACL), use the **permit** command in IPv6-ACL configuration submode. To remove the conditions, use the **no** form of the command.

permit {*ipv6-protocol-number* | **ipv6**}
{*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*}
{*dest-ipv6-prefix/prefix-length* | **any** | **host** *dest-ipv6-address*}
[log-deny]

permit icmp
{*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*}
{*dest-ipv6-prefix/prefix-length* | **any** | **host** *dest-ipv6-address*}
[*icmp-type* [*icmp-code*]]
[log-deny]

permit tcp
{*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*}
[*source-port-operator source-port-number* |
range *source-port-number source-port-number*]
{*dest-ipv6-prefix/prefix-length* | **any** | **host** *dest-ipv6-address*}
[*dest-port-operator dest-port-number* |
range *dest-port-number dest-port-number*]
[established] [log-deny]

permit udp
{*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*}
[*source-port-operator source-port-number* |
range *source-port-number source-port-number*]
{*dest-ipv6-prefix/prefix-length* | **any** | **host** *dest-ipv6-address*}
[*dest-port-operator dest-port-number* |
range *dest-port-number dest-port-number*]
[log-deny]

no permit {*ipv6-protocol-number* | **ipv6** | **icmp** | **tcp** | **udp**}

Syntax Description

ipv6-protocol-number	Specifies an IPv6 protocol number. The range is 0 to 255.
ipv6	Applies the ACL to any IPv6 packet.
source-ipv6-prefix/ prefix-length	Specifies a source IPv6 network or class of networks. The format is *X:X:X::X/n*.
any	Applies the ACL to any source or destination prefix.
host *source-ipv6-address*	Applies the ACL to the specified source IPv6 host address. The format is *X:X:X::X*.
dest-ipv6-prefix/prefix-length	Specifies a destination IPv6 network or class of networks. The format is *X:X:X::X/n*.
host *dest-ipv6-address*	Applies the ACL to the specified destination IPv6 host address. The format is *X:X:X::X*.
log-deny	For packets that are dropped, creates an informational log message about the packet that matches the entry. The message includes the input interface.

icmp	Applies the ACL to any Internet Control Message Protocol (ICMP) packet.
icmp-type	Specifies an ICMP message type. The range is 0 to 255.
icmp-code	Specifies an ICMP message code. The range is 0 255.
tcp	Applies the ACL to any TCP packet.
source-port-operator	Specifies an operand that compares the source ports of the specified protocol. The operands are **lt** (less than), **gt** (greater than), and **eq** (equals).
source-port-number	Specifies the port number of a TCP or UDP port. The number can be from 0 to 65535. A range requires two port numbers.
udp	Applies the ACL to any UDP packet.
dest-port-operator	Specifies an operand that compares the destination ports of the specified protocol. The operands are **lt** (less than), **gt** (greater than), and **eq** (equals).
dest-port-operator	Specifies the port number of a TCP or UDP port. The number can be from 0 to 65535. A range requires two port numbers.
range	Specifies a range of ports to compare for the specified protocol.
established	Indicates an established connection, which is defined as a packet whole SYN flag is not set.

Defaults

None.

Command Modes

IPv6-ACL configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The following guidelines can assist you in configuring an IPv6-ACL. For complete information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

- You can apply IPv6-ACLs to VSAN interfaces, the management interface, Gigabit Ethernet interfaces on IPS modules and MPS-14/2 modules, and Ethernet PortChannel interfaces. However, if IPv6-ACLs are already configured in a Gigabit Ethernet interface, you cannot add this interface to a Ethernet PortChannel group.

Caution Do not apply IPv6-ACLs to just one member of a PortChannel group. Apply IPv6-ACLs to the entire channel group.

- Use only the TCP or ICMP options when configuring IPv6-ACLs on Gigabit Ethernet interfaces.
- Configure the order of conditions accurately. Because the IPv6-ACL filters are applied sequentially to the IP flows, the first match determines the action taken. Subsequent matches are not considered. Be sure to configure the most important condition first. If no conditions match, the software drops the packet.

Examples

The following example configures an IPv6-ACL called List, enters IPv6-ACL submode, and adds an entry that permits IPv6 traffic from any source address to any destination address.

```
switch# config terminal
switch(config)# ipv6 access-list List1
Sswitch(config-ipv6-acl)# permit tcp any any
```

The following example removes a permit condition set for any destination prefix on a specified UDP host.

```
switch# config terminal
switch(config)# ipv6 access-list List1
switch(config-ipv6-acl)# no permit udp host 2001:db8:200d::4000 any
```

The following example removes the IPv6-ACL called List1 and all its entries.

```
switch# config terminal
switch(config)# no ipv6 access-list List1
```

Related Commands

Command	Description
ipv6 access-list	Configures an IPv6 ACL and enters IPv6-ACL configuration submode.
deny	Configures deny conditions for an IPv6 ACL.

phone-contact

To configure the telephone contact number with the Call Home function, use the **phone-contact** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

phone-contact *number*

no phone-contact *number*

Syntax Description

number	(Optional) Configures the customer's phone number. Allows up to 20 alphanumeric characters in international phone format. **Note** Do not use spaces. Use the **+** prefix before the number.

Defaults

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the telephone contact number with the Call Home function.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# phone-contact +1-800-123-4567
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

ping

To diagnose basic network connectivity, use the **ping** command in EXEC mode.

ping [ipv6] [{*host-name* | *ip-address***}** **[count** *repeat-count***]** **[interface {gigabitethernet** *slot/port* **|** **mgmt** *number* **| port-channel** *number* **| vsan** *vsan-id***}] [size** *size* **[timeout** *timeout***]]**

Syntax Description

ipv6	Sends IPv6 echo messages.
host-name	Specifies the host name of system to ping. Maximum length is 64 characters.
ip-address	Specifies the address of the system to ping.
count *repeat-count*	Specifies the repeat count. The range is 0 to 64.
interface	Specifies the interface on which the ping packets are to be sent.
gigabitethernet *slot/port*	Specifies a Gigabit Ethernet slot and port number.
mgmt *number*	Specifies the management interface.
port-channel *number*	Specifies a PortChannel number. The range is 1 to 256.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
size *size*	Specifies the size. The range is 10 to 2000.
timeout *timeout*	Specifies the timeout. The range is 1 to 10.

Defaults

Prompts for input fields.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the **ipv6** argument.

Usage Guidelines

The ping (Packet Internet Groper) program sends an echo request packet to an address, and then awaits a reply. The ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

Verify connectivity to the TFTP server using the **ping** command.

To abnormally terminate a ping session, type the **Ctrl-C** escape sequence.

Examples

The following example pings the system 192.168.7.27.

```
switch# ping 192.168.7.27
PING 192.168.7.27 (192.168.7.27): 56 data bytes
64 bytes from 192.168.7.27: icmp_seq=0 ttl=255 time=0.4 ms
64 bytes from 192.168.7.27: icmp_seq=1 ttl=255 time=0.2 ms
```

```
64 bytes from 192.168.7.27: icmp_seq=2 ttl=255 time=0.2 ms
64 bytes from 192.168.7.27: icmp_seq=3 ttl=255 time=0.2 ms

--- 192.168.7.27 ping statistics ---
13 packets transmitted, 13 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.4 ms
```

The following command shows the prompts that appear when you enter the **ping** command without an IP address.

```
switch# ping
Target IP address: 10.2.2.4
Repeat count [5]: 4
Datagram size [100]: 5
Timeout in seconds [2]: 1
Extended commands [n]: 3
PING 10.2.2.4 (10.2.2.4) 5(33) bytes of data.

--- 10.2.2.4 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3017ms
```

policy

To enter IKE policy configuration and configure a policy for the IKE protocol, use the **policy** command in IKE configuration submode. To delete the policy, use the **no** form of the command.

policy *priority*

no policy *priority*

Syntax Description

priority	Specifies the priority for the IKE policy. The range is 1 to 255, where 1 is the high priority and 255 is the lowest.

Defaults

None.

Command Modes

IKE configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Examples

The following example shows how to configure a policy priority number for the IKE protocol.

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# policy 1
switch(config-ike-ipsec-policy)#
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

port

To assign the TCP port number of a Gigabit Ethernet interface to the FCIP profile or a listener peer port for a ISCSI interface, use the **port** command. Use the **no** form of the command to negate the command or revert to factory defaults.

port *number*

no port *number*

Syntax Description

port *number*	Configures a peer port. The range is 1 to 65535.

Defaults

Disabled

Command Modes

Fcip profile configuration submode.

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Associates the profile with the assigned local port number. If a port number is not assigned for a FCIP profile, the default TCP port 3225 is used.

Examples

The following example configures port 5000 on FCIP interface 5.

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)# port 5000
```

The following example configures port 4000 on ISCSI interface 2/1.

```
switch# config terminal
switch(config)# interface iscsi 2/1
switch(config-profile)# port 4000
```

Related Commands

Command	Description
show fcip profile	Displays information about the FCIP profile.
interface fcip *interface_number* **use-profile** *profile-id*	Configures the interface using an existing profile ID from 1 to 255.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

port-channel persistent

To convert an autocreated PortChannel to a persistent PortChannel, use the **port-channel persistent** command in EXEC mode.

port-channel *port-channel-id* **persistent**

Syntax Description

port-channel-id	Specifies the port channel ID. The range is 1 to 128.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

This command is not reversible. A user-created channel group cannot be converted to an autocreated channel group.When the **port-channel persistent** command is applied to an autocreated channel group, the channel group number does not change and the member ports properties change to those of a user-created channel group. The channel mode remains active.

Examples

The following example shows how to change the properties of an autocreated channel group to a persistent channel group.

```
switch# port-channel 10 persistent
```

Related Commands

Command	Description
port-channel protocol	Enables the PortChannel protocol.
show interface port-channel	Displays PortChannel interface information.
show port-channel	Displays PortChannel information.

port-security

To configure port security features and reject intrusion attempts, use the **port-security** command in configuration mode. Use the **no** form of the command to negate the command or revert to factory defaults.

port-security
{**activate vsan** *vsan-id* [**force** | **no-auto-learn**] |
auto-learn vsan *vsan-id* |
database vsan *vsan-id* {**any-wwn** | **pwwn** *wwn* | **nwwn** *wwn* | **swwn** *wwn*} [**fwwn** *wwn* |
interface {**fc** *slot/port* | **port-channel** *number*} | **swwn** *wwn* [**interface** {**fc** *slot/port* |
port-channel *number*}]]}

no port-security
{**activate vsan** *vsan-id* [**force** | **no-auto-learn**] |
auto-learn vsan *vsan-id* |
database vsan *vsan-id* {**any-wwn** | **pwwn** *wwn* | **nwwn** *wwn* | **swwn** *wwn*} [**fwwn** *wwn* |
interface {**fc** *slot/port* | **port-channel** *number*} | **swwn** *wwn* [**interface** {**fc** *slot/port* |
port-channel *number*}]]}

Syntax Description

activate	Activates a port security database for the specified VSAN and automatically enables auto-learn.
auto-learn	Enables auto-learning for the specified VSAN.
database	Enters the port security database configuration mode for the specified VSAN.
any-wwn	Specifies any WWN to login to the switch.
nwwn *wwn*	Specifies the node WWN as the Nx port connection.
pwwn *wwn*	Specifies the port WWN as the Nx port connection.
swwn *wwn*	Specifies the switch WWN as the xE port connection.
fwwn *wwn*	Specifies a fabric WWN login.
interface	Specifies the device or switch port interface through which each device is connected to the switch.
fc *slot/port*	Specifies a Fibre Channel interface by the slot and port.
port-channel *number*	Specifies a PortChannel interface. The range is 1 to 128.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
force	Forces the database activation.
no-auto-learn	Disables the autolearn feature for the port security database.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.2(1)	This command was introduced.
2.0(1b)	Add the optional **swwn** keyword to the subcommands under the **port-security database vsan** command.

Usage Guidelines

When you activate the port security feature, the **auto-learn** option is also automatically enabled. You can choose to activate the port-security feature and disable autolearn using the **port-security activate vsan** *number* **no-auto-learn** command. In this case, you need to manually populate the port security database by individually securing each port.

If the **auto-learn** option is enabled on a VSAN, you cannot activate the database for that VSAN without the **force** option.

Examples

The following example activates the port security database for the specified VSAN, and automatically enables autolearning.

```
switch# config terminal
switch(config)# port-security activate vsan 1
```

The following example deactivates the port security database for the specified VSAN, and automatically disables auto-learn.

```
switch# config terminal
switch(config)# no port-security activate vsan 1
```

The following example disables the auto-learn feature for the port security database in VSAN 1.

```
switch# config terminal
switch(config)# port-security activate vsan 1 no-auto-learn
```

The following example enables auto-learning so the switch can learn about any device that is allowed to access VSAN 1. These devices are logged in the port security active database.

```
switch# config terminal
switch(config)# port-security auto-learn vsan 1
```

The following example disables auto-learning and stops the switch from learning about new devices accessing the switch. Enforces the database contents based on the devices learnt up to this point.

```
switch# config terminal
switch(config)# no port-security auto-learn vsan 1
```

The following example enters the port security database mode for the specified VSAN.

```
switch# config terminal
switch(config)# port-security database vsan 1
switch(config-port-security)#
```

The following example configures any WWN to login through the specified interfaces.

```
switch(config-port-security)# any-wwn interface fc1/1 - fc1/8
```

The following example configures the specified pWWN to only log in through the specified fWWN.

```
switch(config-port-security)# pwwn 20:11:00:33:11:00:2a:4a fwwn 20:81:00:44:22:00:4a:9e
```

The following example deletes the specified pWWN configured in the previous step.

```
switch(config-port-security)# no pwwn 20:11:00:33:11:00:2a:4a fwwn 20:81:00:44:22:00:4a:9e
```

The following example configures the specified pWWN to only log in through the specified sWWN.

```
switch(config-port-security)# pwwn 20:11:00:33:11:00:2a:4a swwn 20:00:00:0c:85:90:3e:80
```

The following example deletes the specified pWWN configured in the previous step.

```
switch(config-port-security)# no pwwn 20:11:00:33:11:00:2a:4a swwn 20:00:00:0c:85:90:3e:80
```

The following example configures the specified nWWN to log in through the specified fWWN.

```
switch(config-port-security)# nwwn 26:33:22:00:55:05:3d:4c fwwn 20:81:00:44:22:00:4a:9e
```

The following example configures the specified pWWN to login through any port on the local switch.

```
switch(config-port-security)# pwwn 20:11:33:11:00:2a:4a:66
```

The following example configures the specified sWWN to only login through PortChannel 5.

```
switch(config-port-security)# swwn 20:01:33:11:00:2a:4a:66 interface port-channel 5
```

The following example configures any WWN to log in through the specified interface.

```
switch(config-port-security)# any-wwn interface fc3/1
```

The following example deletes the wildcard configured in the previous step.

```
switch(config-port-security)# no any-wwn interface fc2/1
```

The following example deletes the port security configuration database from the specified VSAN.

```
switch# config terminal
switch(config)# no port-security database vsan 1
switch(config)#
```

The following example forces the VSAN 1 port security database to activate despite conflicts.

```
switch(config)# port-security activate vsan 1 force
```

Related Commands

Command	Description
show port-security database	Displays configured port security information.

port-security abort

To discard the port security Cisco Fabric Services (CFS) distribution session in progress, use the **port-security abort** command in configuration mode.

port-security abort vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to discard a port security CFS distribution session in progress.

```
switch# config terminal
switch(config)# port-security abort vsan 33
```

Related Commands

Command	Description
port-security distribute	Enables CFS distribution for port security.
show port-security	Displays port security information.

port-security commit

To apply the pending configuration pertaining to the port security Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **port-security commit** command in configuration mode.

port-security commit vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to commit changes to the active port security configuration.

```
switch# config terminal
switch(config)# port-security commit vsan 13
```

Related Commands

Command	Description
port-security distribute	Enables CFS distribution for port security.
show port-security	Displays port security information.

port-security database

To copy the port security database or to view the difference within the port security database, use the **port-security database** command in EXEC mode.

port-security database {**copy** | **diff** {**active** | **config**}} **vsan** *vsan-id*

Syntax Description

port-security	Activates a port security database for the specified VSAN and automatically enables auto-learn.
database	Enters the port security database configuration mode for the specified VSAN.
copy	Copies the active database to the configuration database.
diff	Provides the difference between the active and configuration port security database.
active	Writes the active database to the configuration database.
config	Writes the configuration database to the active database.
vsan *vsan-id*	Specifies the VSAN ID. The ranges is 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

If the active database is empty, the port-security database is empty.

Use the **port-security database diff active** command to resolve conflicts.

Examples

The following example copies the active to the configured database.

```
switch# port-security database copy vsan 1
```

The following example provides the differences between the active database and the configuration database.

```
switch# port-security database diff active vsan 1
```

The following example provides information on the differences between the configuration database and the active database.

```
switch# port-security database diff config vsan 1
```

Related Commands

Command	Description
port-security database	Copies and provides information on the differences within the port security database.
show port-security database	Displays configured port security information.

port-security distribute

To enable Cisco Fabric Services (CFS) distribution for port security, use the **port-security distribute** command. To disable this feature, use the **no** form of the command.

port-security distribute

no port-security distribute

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Before distributing the Fibre Channel timer changes to the fabric, the temporary changes to the configuration must be committed to the active configuration using the **port-security commit** command.

Examples

The following example shows how to distribute the port security configuration to the fabric.

```
switch# config terminal
switch(config)# port-security distribute
```

Related Commands

Command	Description
port-security commit	Commits the port security configuration changes to the active configuration.
show port-security	Displays port security information.

port-security enable

To enable port security, use the **port-security enable** command in configuration mode. To disable port security, use the **no** form of the command.

port-security enable

no port-security enable

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

Issuing the **port-security enable** command enables the other commands used to configure port security.

Examples

The following example shows how to enable port security.

```
switch# config terminal
switch(config)# port-security enable
```

The following example shows how to disable port security.

```
switch# config terminal
switch(config)# no port-security enable
```

Related Commands

Command	Description
show port-security	Displays port security information.

port-track enable

To enable port tracking for indirect errors, use the **port-track enable** command in configuration mode. To disable this feature, use the **no** form of the command.

port-track enable

no port-track enable

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

The software brings the linked port down when the tracked port goes down. When the tracked port recovers from the failure and comes back up again, the tracked port is also brought up automatically (unless otherwise configured).

Examples

The following example shows how to enable port tracking.

```
switch# config terminal
switch(config)# port-track enable
```

The following example shows how to disable port tracking.

```
switch# config terminal
switch(config)# no port-track enable
```

Related Commands

Command	Description
show interface fc	Displays configuration and status information for a specified Fibre Channel interface.
show interface port-channel	Displays configuration and status information for a specified PortChannel interface.

port-track force-shut

To force a shutdown of a tracked port, use the **port-track force-shut** command in interface configuration submode. To reenable the port tracking, use the **no** form of the command.

port-track force-shut

no port-track force-shut

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

Use the **port-track force-shut** to keep the linked port down, even though the tracked port comes back up. You must explicitly bring the port up when required using the **no port-track force-shut** command.

Examples

The following example shows how to force the shutdown of an interface and the interfaces that it is tracking.

```
switch# config terminal
switch(config)# interface fc 1/2
switch(config-if)# no port-track force-shut
```

Related Commands

Command	Description
port-track enable	Enables port tracking.
show interface fc	Displays configuration and status information for a specified Fibre Channel interface.
show interface port-channel	Displays configuration and status information for a specified PortChannel interface.

port-track interface

To enable port tracking for specific interfaces, use the **port-track interface** command in interface configuration submode. To disable this feature, use the **no** form of the command.

port-track interface {**fc** *slot*/*port* | **fcip** *port* | **gigabitethernet** *slot*/*port* | **port-channel** *port*} [**vsan** *vsan-id*]

no port-track interface {**fc** *slot*/*port* | **fcip** *port* | **gigabitethernet** *slot*/*port* | **port-channel** *port*} [**vsan** *vsan-id*]

Syntax Description

fc *slot*/*port*	Specifies a Fibre Channel interface.
fcip *port*	Specifies a FCIP interface.
gigabitethernet *slot*/*port*	Specifies a Gigabit Ethernet interface.
port-channel *port*	Specifies a PortChannel interface. The range is 1 to 128.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

When the ports that an interface is tracking goes down, the interface also goes down. When the tracked port comes backup, the linked interface also comes back up. Use the **port-track force-shut** command to keep the linked interface down.

Examples

The following example shows how to enable port tracking for specific interfaces.

```
switch# config terminal
switch(config)# interface fc 1/2
switch(config-if)# port-track interface port-channel 2
switch(config-if)# port-track interface fcip 5
```

Related Commands

Command	Description
port-track enable	Enables port tracking.
port-track force-shut	Forcefully shuts an interface for port tracking.

Command	Description
show interface fc	Displays configuration and status information for a specified Fibre Channel interface.
show interface port-channel	Displays configuration and status information for a specified PortChannel interface.

portaddress

To enable the FICON feature in a specified VSAN, use the **ficon vsan** command in configuration mode. To disable the feature or to revert to factory defaults, use the **no** form of the command.

portaddress *portaddress*
block
name *string*
prohibit portaddress *portaddress*

portaddress *portaddress*
no block
no name *string*
no prohibit portaddress *portaddress*

Syntax Description

portnumber	Specifies the FICON port number for this interface. The range is 0 to 254.
block	Blocks a port address.
name *string*	Configures a name for the port address. Maximum length is 24 characters.
prohibit portaddress	Prohibit communication with a portaddress.

Defaults

None.

Command Modes

FICON configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The **shutdown/no shutdown** port state is independent of the **block/no block** port state. If a port is shutdown, unblocking that port will not initialize the port.

You cannot block or prohibit CUP port (0XFE).

If you prohibit ports, the specified ports are prevented from communicating with each other. Unimplemented ports are always prohibited.

Examples

The following example disables a port address and retains it in the operationally down state.

```
switch# config terminal
switch(config)# ficon vsan 2
switch(config-ficon)# portaddress 1
switch(config-ficon-portaddr)# block
```

The following example enables the selected port address and reverts to the factory default of the port address not being blocked.

```
switch(config-ficon-portaddr)# no block
```

The following example prohibits port address 1 in VSAN 2 from talking to ports 3.

```
switch(config-ficon-portaddr)# prohibit portaddress 3
```

The following example removes port address 5 from a previously-prohibited state.

```
switch(config-ficon-portaddr)# no prohibit portaddress 5
```

The following example assigns a name to the port address.

```
switch(config-ficon-portaddr)# name SampleName
```

The following example deletes a previously configured port address name.

```
switch(config-ficon-portaddr)# no name SampleName
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.

power redundancy-mode

To configure the capacity of the power supplies on the Cisco MDS 9500 Family of switches, use the **power redundancy-mode** command in configuration mode. Use the **no** form of the command to negate the command or revert to factory defaults.

power redundancy-mode {combined [force] | redundant}

no power redundancy-mode {combined [force] | redundant}

Syntax Description

combined	Configures power supply redundancy mode as combined.
force	Forces combined mode without prompting.
redundant	Configures power supply redundancy mode as redundant.

Defaults

Redundant mode.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

- If power supplies with different capacities are installed in the switch, the total power available differs based on the configured mode:
- In redundant mode, the total power is the lesser of the two power supply capacities. This reserves enough power to keep the system powered on in case of a power supply failure. This is the recommended or default mode.
- In combined mode, the total power is twice the lesser of the two power supply capacities. In case of a power supply failure, the entire system could be shut down, depending on the power usage at that time.
- When a new power supply is installed, the switch automatically detects the power supply capacity. If the new power supply has a capacity that is lower than the current power usage in the switch and the power supplies are configured in redundant mode, the new power supply will be shut down.
- When you change the configuration from combined to redundant mode and the system detects a power supply that has a capacity lower than the current usage, the power supply is shut down. If both power supplies have a lower capacity than the current system usage, the configuration is not allowed.

Examples

The following examples demonstrate how the power supply redundancy mode could be set.

```
switch(config)# power redundancy-mode combined
WARNING: This mode can cause service disruptions in case of a power supply failure.
Proceed ? [y/n] y
switch(config)# power redundancy-mode redundant
```

Related Commands

Command	Description
show environment power	Displays status of power supply modules, power supply redundancy mode, and power usage summary.
copy running-config startup-config	Copies all running configuration to the startup configuration.

poweroff module

To power off individual modules in the system, use the **poweroff module** command in configuration mode. Use the **no** form of this command to power up the specified module.

poweroff module *slot*

no poweroff module *slot*

Syntax Description

slot	Specifies the slot number for the module.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use the **poweroff module** command to power off individual modules. The **poweroff module** command cannot be used to power off supervisor modules.

Examples

The following example powers off and powers up module 1.

```
switch# config terminal
switch(config)# poweroff module 1
switch(config)#
switch(config)# no poweroff module 1
switch(config)#
```

Related Commands

Command	Description
show module	Displays information for a specified module.
copy running-config startup-config	Copies all running configuration to the startup configuration.

priority

To configure the priority in a QoS policy map class, use the **priority** command in QoS policy class map configuration submode. To disable this feature, use the **no** form of the command.

priority {**high** | **low** | **medium**}

no priority {**high** | **low** | **medium**}

Syntax Description

high	Configures the frames matching the class-map as high priority.
low	Configures the frames matching the class-map as low priority. The default.
medium	Configures the frames matching the class-map as medium priority.

Defaults

The default priority is low.

Command Modes

QoS policy map class configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Before you can configure the priority in a QoS policy map class you must first:

- Enable the QoS data traffic feature using the **qos enable** command.
- Configure a QoS class map using the **qos dwrr-q** command.
- Configure a QoS policy map using the **qos policy-map** command.
- Configure a QoS policy map class using the **class** command.

Examples

The following example shows how to select the QoS policy class-map1 and configure the frame priority as high.

```
switch(config-pmap)# class class-map1
switch(config-pmap-c)# priority high
Operation in progress. Please check class-map parameters
switch(config-pmap-c)#
```

Related Commands

Command	Description
qos enable	Enables the QoS data traffic feature on the switch.
qos class-map	Configures a QoS class map.
qos policy-map	Configure a QoS policy map.
class	Configure a QoS policy map class.
show qos	Displays the current QoS settings.

purge fcdomain fcid

To purge persistent FCIDs, use the **purge fcdomain fcid** command in EXEC mode.

purge fcdomain fcid vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Indicates that FCIDs are to be purged for a VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to purge all dynamic, unused FCIDs in VSAN 4

```
switch# purge fcdomain fcid vsan 4
switch#
```

The following example shows how to purge all dynamic, unused FCIDs in VSANs 4, 5, and 6.

```
switch# purge fcdomain fcid vsan 3-5
switch#
```

purge module

To delete configurations in the running configuration for nonexistent modules, use the **purge module** command in EXEC mode.

purge module *slot* **running-config**

Syntax Description

slot	Specifies the module slot number.
running-config	Purges the running configuration from the specified module.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command cannot be issued on a supervisor module.

Examples

The following example displays the output of the **purge module** command issued on the module in slot 8.

```
switch# purge module 8 running-config
switch#
```

pwc

To view your present working context (PWC), use the **pwc** command in any mode.

pwc

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

All.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows the present working context.

```
switch# config t
switch(config)# islb initiator ip-address 120.10.10.2
switch(config-islb-init)# pwc
(config t) -> (islb initiator ip-address 120.10.10.2)
```

Related Commands

Command	Description
pwd	Displays the current directory location.

pwd

To display the current directory location, use the **pwd** command in EXEC mode.

pwd

Syntax Description

This command has no keywords or arguments.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example changes the directory and displays the current directory.

```
switch# cd bootflash:logs
switch# pwd
bootflash:/logs
```

Related Commands

Command	Description
cd	Changes the current directory to the specified directory.
dir	Displays the contents of a directory.

pwwn (DPVM database configuration submode)

To add a device to a dynamic port VSAN membership (DPVM) database using the pWWN, use the **pwwn** command in DPVM database configuration submode. To remove a device from a DPVM database using the pWWN, use the **no** form of the command.

pwwn *pwwn-id* **vsan** *vsan-id*

no pwwn *pwwn-id* **vsan** *vsan-id*

Syntax Description

pwwn-id	Specifies the port WWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

DPVM database configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

Examples

The following example shows how to add an entry to the DPVM database.

```
switch# config terminal
switch(config)# dpvm database
switch(config-dpvm-db)# pwwn 11:22:33:44:55:66:77:88 vsan 1
```

The following example shows how to delete an entry from the DPVM database.

```
switch(config-dpvm-db)# no pwwn 11:22:33:44:55:66:77:88 vsan 1
```

Related Commands

Command	Description
dpvm database	Configures the DPVM database.
show dpvm	Displays DPVM database information.

pwwn (fcdomain database configuration submode)

To map a pWWN to a persistent FC ID for IVR, use the **pwwn** command in IVR fcdomain database configuration submode. To remove the mapping for the pWWN, use the **no** form of the command.

pwwn *pwwn-id fc-id*

no pwwn *pwwn-id*

Syntax Description

pwwn-id	Specifies the pWWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
fc-id	Specifies the FC ID of the device.

Defaults

None.

Command Modes

fcdomain database configuration submode.

Command History

Release	Modification
2.1(2)	This command was introduced.

Usage Guidelines

Only one FC ID can be mapped to a pWWN.

Examples

The following example shows how to map the pWWN to the persistent FC ID.

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config-fcdomain)# native-autonomous-fabric-num 20 native-vsan 30 domain 15
switch(config-fcdomain-fcid)# pwwn 11:22:33:44:55:66:77:88 0x123456
```

The following example shows how to remove the mapping between the pWWN and the FC ID.

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config-fcdomain)# native-autonomous-fabric-num 20 native-vsan 30 domain 15
switch(config-fcdomain-fcid)# no pwwn 11:22:33:44:55:66:77:88
```

Related Commands

Command	Description
ivr fcdomain database autonomous-fabric-num	Creates IVR persistent FC IDs.
native-autonomous-fabric-num	Creates an IVR persistent FC ID database entry.
show ivr fcdomain database	Displays IVR fcdomain database entry information.

CHAPTER 19

Q Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "Command Modes" section to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

qos class-map

To create and define a traffic class with match criteria that will be used to identify traffic, use the **qos class-map** command in configuration mode. To remove a previously-configured class, use the **no** form of the command.

qos class-map *class* [**match-all** | **match-any**]

no qos class-map *class*

Syntax Description

class-name	Specifies a class map name. Maximum length is 63 alpha-numeric characters.
match-all	Specifies a logical AND operator for all matching statements in this class. (default).
match-any	Specifies a logical OR operator for all matching statements in this class.

Defaults

match-all

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can access this command only if you enable the QoS data traffic feature using the **qos enable** command.

Examples

The following example shows how to create a QoS class map and enter class map configuration mode.

```
switch# config terminal
switch(config)# qos class-map MyClass1
switch(config-cmap)#
```

Related Commands

Command	Description
show qos	Displays configured QoS information.

qos control priority

To enable the QoS priority assignment for control traffic feature on the Cisco MDS 9000 family of switches, use the **qos control** command in configuration mode. To revert to the factory default, use the **no** form of the command.

qos control priority 0

no qos priority control 0

Syntax Description

0	Specifies the lowest priority. To revert to the highest priority, use the **no** form of the command.

Defaults

Enabled and priority 7 are the defaults.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example sets the QoS priority assignment to the highest level.

```
switch# config terminal
switch(config)# no qos control priority 0
```

Related Commands

Command	Description
show qos	Displays configured QoS information.

qos dwrr-q

To associate a weight with a deficit weighted round robin (DWRR) scheduler queue, use the **qos dwrr-q** command in configuration mode. To remove a previously-configured class, use the **no** form of the command.

qos dwrr-q {**high** | **low** | **medium**} **weight** *value*

no qos dwrr-q {**high** | **low** | **medium**} **weight** *value*

Syntax Description

high	Assigns the DWRR queue high option to DWRR queues.
low	Assigns the DWRR queue low option to DWRR queues.
medium	Assigns the DWRR queue medium option to DWRR queues.
weight *value*	Specifies DWRR queue weight

Defaults

10

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

You can access this command only if you enable the QoS data traffic feature using the **qos enable** command.

Examples

The following example specifies the DWRR queue priority.

```
switch# config terminal
switch(config)# qos dwrr-q high weight 50
```

The following example reverts to the default value of 10.

```
switch(config)# no qos dwrr-q high weight 50
```

Related Commands

Command	Description
show qos	Displays configured QoS information.

qos enable

To enable the QoS priority assignment for data traffic feature on the Cisco MDS 9000 family of switches, use the **qos enable** command in configuration mode. To disable the QoS priority assignment for control traffic feature, use the **no** form of the command.

qos enable

no qos enable

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example disables the QoS priority assignment feature.

```
switch# config terminal
switch(config)# qos enable
```

Related Commands

Command	Description
show qos	Displays configured QoS information.

qos policy-map

To specify the class of service, use the **qos policy-map** command in configuration mode. To remove a previously configured class, use the **no** form of the command.

qos policy-map *policy-name*

no qos policy-map *policy-name*

Syntax Description

policy-name	Specifies a policy map name. Maximum length is 63 alphanumeric characters.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

You can access this command only if you enable the QoS data traffic feature using the **qos enable** command.

As an alternative, you can map a classmap to a Differentiated Services Code Point (DSCP).The DSCP is an indicator of the service level for a specified frame. The DSCP value ranges from 0 to 63. A dscp value of 46 is disallowed.

Examples

The following example creates a policy map called MyPolicy and places you in the policy-map submode.

```
switch(config)# qos policy-map MyPolicy
switch(config-pmap)#
```

Related Commands

Command	Description
qos enable	Enables the QoS data traffic feature on the switch.
show qos	Displays configured QoS information.

qos priority

To configure the quality of server (QoS) priority attribute in a zone attribute group, use the **qos priority** command in zone attribute configuration submode. To revert to the default, use the **no** form of the command.

qos priority {**high** | **low** | **medium**}

no qos priority {**high** | **low** | **medium**}

Syntax Description

high	Specifies high priority.
low	Specifies low priority.
medium	Specifies medium priority.

Defaults

Low.

Command Modes

Zone attribute configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to set the QoS priority attribute for a zone attribute group.

```
switch# config terminal
switch(config)# zone-attribute-group name admin-attributes vsan 10
switch(config-attribute-group)# qos priority medium
```

Related Commands

Command	Description
show zone-attribute-group	Displays zone attribute group information.
zone-attribute-group name	Configures zone attribute groups.

qos service

To apply a service policy, use the **qos service** command in configuration mode. To remove a previously-configured class, use the **no** form of the command.

qos service policy *policy-name* **vsan** *vsan-id*

no qos service policy *policy-name* **vsan** *vsan-id*

Syntax Description

policy *policy-name*	Associates a policy map with the VSAN.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

You can access this command only if you enable the QoS data traffic feature using the **qos enable** command.

Examples

The following example applies a configured policy to VSAN 3.

```
switch(config)# qos service policy MyPolicy vsan 3
Operation in progress. Please check policy-map parameters
```

The following example deletes a configured policy that was applied to VSAN 7.

```
switch(config)# no qos service policy OldPolicy vsan 7
Operation in progress. Please check policy-map parameters
```

Related Commands

Command	Description
show qos	Displays configured QoS information.

quiesce

To gracefully shut down an ISL in a PortChannel, use the **quiesce** command in configuration mode. To disable this feature, use the **no** form of the command.

quiesce interface fc *slot/port*

no queisce interface fc *slot/port*

Syntax Description

interface fc *slot/port*	Specifies the interface to be quiesced.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.0(2b)	This command was deprecated and the functionality integrated into the **shutdown** command.

Usage Guidelines

The following conditions return an error:

- The interface is not part of port-channel
- The interface is not up
- The interface is the last operational interface in the PortChannel

Examples

The following example gracefully shuts down the one end of the ISL link in a PortChannel.

```
switchA# quiesce interface fc 2/1
WARNING: this command will stop forwarding frames to the specified interfaces. It is
intended to be used to gracefully shutdown interfaces in a port-channel. The procedure is:
1. quiesce the interfaces on both switches.
2. shutdown the interfaces administratively.
Do you want to continue? (y/n)  [n] y
```

Related Commands

Command	Description
show interface	Displays interface configuration and status information.

CHAPTER 20

R Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "Command Modes" section to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

radius abort

To discard a RADIUS Cisco Fabric Services (CFS) distribution session in progress, use the **radius abort** command in configuration mode.

radius abort

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to discard a RADIUS CFS distribution session in progress.

```
switch# config terminal
switch(config)# radius abort
```

Related Commands

Command	Description
radius distribute	Enables CFS distribution for RADIUS.
show radius	Displays RADIUS CFS distribution status and other details.

radius commit

To apply the pending configuration pertaining to the RADIUS Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **radius commit** command in configuration mode.

radius commit

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to apply a RADIUS configuration to the switches in the fabric.

```
switch# config terminal
switch(config)# radius commit
```

Related Commands

Command	Description
radius distribute	Enables CFS distribution for RADIUS.
show radius	Displays RADIUS CFS distribution status and other details.

radius distribute

To enable Cisco Fabric Services (CFS) distribution for RADIUS, use the **radius distribute** command. To disable this feature, use the **no** form of the command.

radius distribute

no radius distribute

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable RADIUS fabric distribution.

```
switch# config terminal
switch(config)# radius distribute
```

Related Commands

Command	Description
radius commit	Commits temporary RADIUS configuration changes to the active configuration.
show radius	Displays RADIUS CFS distribution status and other details.

radius-server deadtime

To set a periodic time interval where a nonreachable (nonresponsive) RADIUS server is monitored for responsiveness, use the **radius-server deadtime** command. To disable the monitoring of the nonresponsive RADIUS server, use the **no** form of the command.

radius-server deadtime *time*

no radius-server deadtime *time*

Syntax Description

time	Specifies the time interval in minutes. The range is 1 to 1440.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Setting the time interval to zero disables the timer. If the dead time interval for an individual RADIUS server is greater than zero (0), that value takes precedence over the value set for the server group.

When the dead time interval is 0 minutes, RADIUS server monitoring is not performed unless the RADIUS server is part of a server group and the dead time interval for the group is greater than 0 minutes.

Examples

The following example shows how to set a duration of 10 minutes.

```
switch# config terminal
switch(config)# radius-server deadtime 10
```

Related Commands

Command	Description
deadtime	Sets a time interval for monitoring a nonresponsive RADIUS server.
show radius-server	Displays all configured RADIUS server parameters.

radius-server directed-request

To specify a RADIUS server to send authentication requests to when logging in, use the **radius-server directed-request** command. To revert to sending the authentication request to the configured group, use the **no** form of the command.

radius-server directed-request

no radius-server directed-request

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The user can specify the username@servername during login. The user name is sent to the server name for authentication.

Examples

The following example shows how to specify a RADIUS server to send authentication requests to when logging in.

```
switch# config terminal
switch(config)# radius-server directed-request
```

Related Commands

Command	Description
show radius-server	Displays all configured RADIUS server parameters.
show radius-server directed request	Displays a directed request RADIUS server configuration.

radius-server host

To configure RADIUS server parameters, use the **radius-server host** command. Use the **no** form of this command to revert to the factory defaults.

radius-server host {*server-name* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret*] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

no radius-server host {*server-name* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret*] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

Syntax Description

server-name	Specifies the RADIUS server DNS name. Maximum length is 256 characters.
ipv4-address	Specifies the RADIUS server IP address in the format *A.B.C.D*.
ipv6-address	Specifies the RADIUS server IP address in the format *X:X::X*.
auth-port *port-number*	Configures the RADIUS server port for authentication.
acct-port *port-number*	Configures the RADIUS server port for accounting.
authentication	Configures authentication.
accounting	Configures accounting.
key	Configures the RADIUS server shared secret key.
0	Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the RADIUS client and server. This is the default.
7	Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the RADIUS client and server.
shared-secret	Configures a preshared key to authenticate communication between the RADIUS client and server.
retransmit *count*	Configures the number of times the switch tries to connect to a RADIUS server(s) before reverting to local authentication. The range is 1 to five times and the default is 1 time.
test	Configures parameters to send test packets to the RADIUS server.
idle-time *time*	Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.
password *password*	Specifies a user password in the test packets. The maximum size is 32.
username *name*	Specifies a user name in the test packets. The maximum size is 32.
timeout *seconds*	Specifies the timeout (in seconds) between retransmissions to the RADIUS server. The default is 1 second and the valid range is 1 to 60 seconds.

Defaults

Idle-time is not set. Server monitoring is turned off.
Timeout is 1 second.
Username is test.
Password is test.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the *ipv6-address* argument and the **test** option.

Usage Guidelines

When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

Examples

The following example configures RADIUS server authentication parameters.

```
switch# config terminal
switch(config)# radius-server host 10.10.2.3 key HostKey
switch(config)# radius-server host 10.10.2.3 auth-port 2003
switch(config)# radius-server host 10.10.2.3 acct-port 2004
switch(config)# radius-server host 10.10.2.3 accounting
switch(config)# radius-server host radius2 key 0 abcd
switch(config)# radius-server host radius3 key 7 1234
switch(config)# radius-server host 10.10.2.3 test idle-time 10
switch(config)# radius-server host 10.10.2.3 test username tester
switch(config)# radius-server host 10.10.2.3 test password 2B9ka5
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server key

To configure a global RADIUS shared secret, use the **radius-server key** command. Use the **no** form of this command to removed a configured shared secret.

radius-server key [0 | 7] *shared-secret*

no radius-server key [0 | 7] *shared-secret*

Syntax Description

0	Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the RADIUS client and server. This is the default.
7	Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the RADIUS client and server.
shared-secret	Configures a preshared key to authenticate communication between the RADIUS client and server.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You need to configure the RADIUS preshared key to authenticate the switch to the RADIUS server. The length of the key is restricted to 65 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all RADIUS server configurations on the switch. You can override this global key assignment by explicitly using the **key** option in the **radius-server host** command.

Examples

The following examples provide various scenarios to configure RADIUS authentication.

```
switch# config terminal
switch(config)# radius-server key AnyWord
switch(config)# radius-server key 0 AnyWord
switch(config)# radius-server key 7 public
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server retransmit

To globally specify the number of times the switch should try a request with a RADIUS server, use the **radius-server retransmit** command. To revert to default value, use the **no** form of the command.

radius-server retransmit *count*

no radius-server retransmit *count*

Syntax Description

count	Configures the number of times the switch tries to connect to a RADIUS server(s) before reverting to local authentication. The range is 1 to 5 times.

Defaults

1 retransmission

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures the number of retransmissions to 3.

```
switch# config terminal
switch(config)# radius-server retransmit 3
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server timeout

To specify the time between retransmissions to the RADIUS servers, use the **radius-server timeout** command. You can revert the retransmission time to its default by issuing the **no** form of the command.

radius-server timeout *seconds*

no radius-server timeout *seconds*

Syntax Description

seconds	Specifies the time (in seconds) between retransmissions to the RADIUS server. The range is 1 to 60 seconds.

Defaults

1 second

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures the timeout value to 30 seconds.

```
switch# config terminal
switch(config)# radius-server timeout 30
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

reload

To reload the entire switch, an active supervisor module, a standby supervisor module, or a specific module, or to force a netboot on a given module, use the **reload** command in EXEC mode.

reload [**module** *module-number* **force-dnld**]

Syntax Description

module *module-number*	Reloads a specific module or active/standby supervisor module.
force-dnld	Reloads, initiates netboot, and forces the download of the latest module firmware version to a specific module.

Defaults

Reboots the entire switch.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use the **reload** command to reboot the system, or to reboot a specific module, or to force a netboot on a specific module. The **reload** command used by itself, powers down all the modules and reboots the supervisor modules.

Use the **reload module** *module-number* command, if the given slot has a module or standby supervisor module, to power-cycle that module. If the given slot has an active supervisor module, then it causes the currently active supervisor module to reboot and the standby supervisor module becomes active.

The **reload module** *module-number* **force-dnld** command is similar to the previous command. This command forces netboot to be performed. If the slot contains a module, then the module netboots with the latest firmware and updates its corresponding flash with this image.

Examples

The following example uses **reload** to reboot the system.

```
switch# reload
This command will reboot the system. (y/n)? y
```

The following example uses **reload** to initiate netboot on a specific module.

```
switch# reload module 8 force-dnld
```

The following example uses **reload** to reboot a specific module.

```
switch# reload module 8
reloading module 8 ...
```

The following example uses **reload** to reboot an active supervisor module.

```
switch# reload module 5
This command will cause supervisor switchover. (y/n)? y
```

Related Commands

Command	Description
install	Installs a new software image.
copy system:running-config nvram:startup-config	Copies any file from a source to a destination.

read command-id

To configure a SCSI read command for a SAN tuner extension N port, use the **read command-id** command.

read command-id *cmd-id* **target** *pwwn* **transfer-size** *bytes* [**outstanding-ios** *value* [**continuous** | **num-transactions** *number*]]

Syntax Description

cmd-id	Specifies the command identifier. The range is 0 to 2147483647.
target *pwwn*	Specifies the target port WWN. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
transfer-size *bytes*	Specifies the transfer size in multiples of 512 bytes. The range is 512 to 8388608.
outstanding-ios *value*	Specifies the number of outstanding I/Os. The range is 1 to 1024.
continuous	Specifies that the command is performed continuously.
num-transactions *number*	Specifies a number of transactions. The range is 1 to 2147483647.

Defaults

None.

Command Modes

SAN extension N port configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To stop a SCSI read command in progress, use the **stop** command.

Examples

The following example configures a continuous SCSI read command.

```
switch# san-ext-tuner
switch(san-ext)# nWWN 10:00:00:00:00:00:00:00
switch(san-ext)# nport pwwn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2
switch(san-ext-nport)# read command-id 100 target 22:22:22:22:22:22:22:22 transfer-size
512000 outstanding-ios 2 continuous
```

Related Commands

Command	Description
nport pwwn	Configures a SAN extension tuner N port.
san-ext-tuner	Enables the SAN extension tuner feature.
show san-ext-tuner	Displays SAN extension tuner information.
stop	Cancels a SCSI command in progress on a SAN extension tuner N port.

read-only

To configure the read-only attribute in a zone attribute group, use the **read-only** command in zone attribute configuration submode. To revert to the default, use the **no** form of the command.

read-only

no read-only

Syntax Description

This command has no other arguments or keywords.

Defaults

Read-write.

Command Modes

Zone attribute configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

This command only configures the read-only attribute for enhanced zoning. To enable broadcast zoning for basic mode, use the **attribute read-only** subcommand after entering zone configuration mode using the **zone name** command.

Examples

The following example shows how to set the read-only attribute for a zone attribute group.

```
switch# config terminal
switch(config)# zone-attribute-group name admin-attributes vsan 10
switch(config-attribute-group)# read-only
```

Related Commands

Command	Description
show zone-attribute-group	Displays zone attribute group information.
zone mode enhanced vsan	Enables enhanced zoning for a VSAN.
zone name	Configures zone attributes.
zone-attribute-group name	Configures zone attribute groups.

revocation-check

To configure trust point revocation check methods, use the **revocation-check** command in trust point configuration submode. To discard the revocation check configuration, use the **no** form of the command.

revocation-check {crl [none | ocsp [none]] | none | ocsp [crl [none] | none]}

no revocation-check {crl [none | ocsp [none]] | none | ocsp [crl [none] | none]}

Syntax Description

crl	Specifies the locally stored certificate revocation list (CRL) as the place to check for revoked certificates.
none	Specifies that no checking be done for revoked certificates.
ocsp	Specifies the Online Certificate Status Protocol (OCSP) for checking for revoked certificates.

Defaults

By default, the revocation checking method for a trust point is CRL.

Command Modes

Trust point configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You must authenticate the CA and configure the OCSP URL before configuring OCSP as a revocation checking method.

The revocation checking configuration allows one or more of the methods to be specified as an ordered list for revocation checking. During peer certificate verification, each method is tried in the specified order until one method succeeds by providing the revocation status. When none is specified as the method, it means there is no need to check the revocation status, which thereby treats the peer certificate as not revoked. If none is the first method specified in the method list, subsequent methods are not allowed to be specified as checking is not required.

Examples

The following example shows how to check for revoked certificates using OCSP on a URL that must have been previously configured.

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# revocation-check oscp
```

The following example shows how to check for revoked certificates in the locally stored CRL.

```
switch(config-trustpoint)# revocation-check crl
```

The following example shows how to check revocation status first using locally cached CRL and then, if needed, using OCSP. If CRL is not yet cached locally, only OCSP checking is attempted.

```
switch(config-trustpoint)# revocation-check crl ocsp
```

The following example shows how to do no checking for revoked certificates.

```
switch(config-trustpoint)# revocation-check none
```

Related Commands

Command	Description
crypto ca crl-request	Configures a CRL or overwrites the existing one for the trust point CA.
ocsp url	Configures details of the trust point OSCP.
show crypto ca crl	Displays configured CRLs.

rmdir

To delete an existing directory from the Flash file system, use the **rmdir** command in EXEC mode.

rmdir [**bootflash: | slot0: | volatile:**]*directory*

Syntax Description

bootflash:	Source or destination location for internal bootflash memory.
slot0:	Source or destination location for the CompactFlash memory or PCMCIA card.
volatile:	Source or destination location for volatile file system.
directory	Name of the directory to remove.

Defaults

Uses the current default directory.

Command Modes

EXEC Mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command is only valid on Flash file systems.

The **rmdir** command deletes an existing directory at the current directory level or at a specified directory level. The directory must be empty to be deleted.

Examples

The following example deletes the directory called test in the slot0 directory.

```
switch# rmdir slot0:test
```

The following example deletes the directory called test at the current directory level. If the current directory is slot0:mydir, this command deletes the slot0:mydir/test directory.

```
switch# rmdir test
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
mkir	Creates a new directory in the Flash file system.

rmon alarm

To configure a remote monitoring (RMON) alarm, use the **rmon alarm** command in configuration mode. To delete an RMON alarm, use the **no** form of the command.

rmon alarm *alarm-number mib-object sample-interval* {**absolute** | **delta**} **rising-threshold** *value* [*rising-event*] **falling-threshold** *value* [*falling-event*] [**owner** *alarm-owner*]

no rmon alarm *alarm-number*

Syntax Description

alarm-number	Specifies the RMON alarm number. The range is 1 to 65535.
mib-object	Specifies the MIB object to monitor. Maximum length is 80 characters. **Note** The MIB object identifier must be fully numbered, dotted-decimal notation, not the text string description.
sample-interval	Specifies the sample interval in seconds. The range is 1 to 2147483647.
absolute	Tests each sample directly.
delta	Tests the delta (or difference) between samples.
rising-threshold *value*	Specifies the rising threshold value. The range is –2147483648 to 2147483647.
rising-event	Specifies the event to trigger on rising threshold crossing. The range is 1 to 65535.
falling-threshold *value*	Specifies the falling threshold value. The range is –2147483648 to 2147483647.
failing-event	Specifies the event to trigger on rising threshold crossing. The range is 1 to 65535.
owner *alarm-owner*	Specifies an owner for the alarm. Maximum size is 80 characters.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

The events that can be triggered are configured using the **rmon event** command.

Examples

The following example configures an RMON alarm.

```
switch# config terminal
switch(config)# rmon alarm 20 1.3.6.1.2.1.2.2.1.14.16777216 900 delta rising-threshold 15
1 falling-threshold 0 owner test
```

Related Commands

Command	Description
rmon event	Configures an RMON event.
show rmon	Displays RMON configuration information.

rmon event

To configure a remote monitoring (RMON) event, use the **rmon event** command in configuration mode. To delete an RMON event, use the **no** form of the command.

rmon event *event-number* [**description** *text* [**owner** *owner-name*] | **log** [**trap** *trap-name*] [**description** *text*] [**owner** *owner-name*] | **owner** *owner-name* | **trap** *community-string* [**description** *text*] [**owner** *owner-name*]]

no rmon event *event-number*

Syntax Description

event-number	Specifies the RMON event number. The range is 1 to 65535.
description *text*	Specifies a description of the event. Maximum length is 80 characters.
owner *owner-name*	Specifies an owner for the alarm. Maximum length is 80 characters
log	Generates an RMON log entry when the event is triggered by an alarm.
trap *community-string*	Generates an SNMP notification when event is triggered by an alarm. Maximum length is 32 characters.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

The events created by this command can be triggered by alarms configured using the **rmon alarm** command.

Examples

The following example configures an RMON event.

```
switch# config terminal
switch(config)# rmon event 2 log trap eventtrap description CriticalErrors owner Test2
```

Related Commands

Command	Description
rmon alarm	Configures an RMON alarm.
show rmon	Displays RMON configuration information.

role abort

To discard an authorization role Cisco Fabric Services (CFS) distribution session in progress, use the **role abort** command in configuration mode.

role abort

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to discard an authorization role CFS distribution session in progress.

```
switch# config terminal
switch(config)# role abort
```

Related Commands

Command	Description
role distribute	Enables CFS distribution for authorization roles.
show role	Displays authorization role information.

role commit

To apply the pending configuration pertaining to the authorization role Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **role commit** command in configuration mode.

role commit

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to apply an authorization role configuration to the switches in the fabric.

```
switch# config terminal
switch(config)# role commit
```

Related Commands

Command	Description
role distribute	Enables CFS distribution for authorization roles.
show role	Displays authorization roles information.

role distribute

To enable Cisco Fabric Services (CFS) distribution for authorization roles, use the **role distribute** command. To disable this feature, use the **no** form of the command.

role distribute

no role distribute

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable fabric distribution for authorization roles.

```
switch# config terminal
switch(config)# role distribute
```

Related Commands

Command	Description
role commit	Commits temporary to the authorization role configuration changes to the active configuration.
show role	Displays authorization role information.

role name

To configure and assign users to a new role or to modify the profile for an existing role, use the **role name** command in configuration mode. Use the **no** form of this command to delete a configured role.

role name *name* **[description** *user description***] [rule** *number* **permit clear feature** *name* **|permit config feature** *name* **| permit debug feature** *name* **| permit show feature** *name***] [rule** *number* **deny clear feature** *name* **| deny config feature** *name* **| deny debug feature** *name* **| deny exec feature** *name* **| deny show feature** *name***]**

no role name *name* **[description** *user description***] [rule** *number* **permit clear feature** *name* **| permit config feature** *name* **| permit debug feature** *name* **| permit show feature** *name***] [rule** *number* **deny clear feature** *name* **| deny config feature** *name* **| deny debug feature** *name* **| deny exec feature** *name* **| deny show feature** *name***]**

Syntax Description

name	Adds RADIUS server. The maximum size is 32.
description	Add a description for the role. The maximum size is 80.
user description	Add description of users to the role.
exit	Exit from this submode
no	Negate a command or set its defaults
rule	Enter the rule keyword.
number	Enter the rule number 1-16.
permit	Add commands to the role.
deny	Remove commands from the role.
clear	Clear commands
config	Configuration commands
debug	Debug commands
show	Show commands
feature	Enter the feature name
exec	Exec commands
name	Enter the feature name (Max Size - 32)

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Roles are assigned rules. Roles are a group of rules defining a user's access to certain commands. Users are assigned roles. The rules within roles can be assigned to permit or deny access to the following commands:

clear Clear commands
config Configuration commands
debug Debug commands
exec EXEC commands
show Show commands

These commands can have **permit** or **deny** options within that command line.

Examples

The following example shows how to assign users to a new role.

```
switch# config terminal
switch(config)# role name techdocs
switch(config-role)#
switch(config)# no role name techdocs
switch(config)#
switch(config-role)# description Entire Tech. Docs. group
switch(config-role)# no description
switch# config terminal
switch(config)# role name sangroup
switch(config-role)#
switch(config-role)# rule 1 permit config
switch(config-role)# rule 2 deny config feature fspf
switch(config-role)# rule 3 permit debug feature zone
switch(config-role)# rule 4 permit exec feature fcping
switch(config-role)# no rule 4

Role: network-operator
Description: Predefined Network Operator group. This role cannot be modified
Access to Show commands and selected Exec commands
```

Related Commands

Command	Description
show role	Displays all roles configured on the switch including the rules based on each role.

rsakeypair

To configure and associate the RSA key pair details to a trust point, use the **rsakeypair** command in trust point configuration submode. To disassociate the RSA key pair from the trust point, use the **no** form of the command.

rsakeypair *key-pair-label* [*key-pair-size*]

no rsakeypair *key-pair-label* [*key-pair-size*]

Syntax Description

key-pair-label	Specifies a name for the RSA key pair. The maximum size is 64 characters.
key-pair-size	Specifies a size for the RSA key pair. The size can range from 512 to 2048.

Defaults

The default key pair size is 512 if the key pair is not already generated.

Command Modes

Trust point configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Only one RSA key pair can be associated with a trust point CA, even though the same key pair can be associated with many trust point CAs. This association must occur before enrolling with the CA to obtain an identity certificate. If the key pair had been generated previously (using the **crypto key generate** command), then the key pair size, if specified, should be the same as that was used during generation. If the specified key pair is not yet generated, it will be generated during enrollment using the **crypto ca enroll** command.

The **no** form of the **rsakeypair** command disassociates (but never destroys) the key pair from the trust point. Before issuing the **no rsakeypair** command, first remove the identity certificate, if present, from the trust point C. Doing so ensures the consistency of the association between the identity certificate and the key pair for a trust point

Examples

The following example shows how to associate an RSA key pair to a trust point.

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# rsakeypair adminid-key
```

The following example shows how to disassociate an RSA key pair from a trust point.

```
switch(config-trustpoint)# no rsakeypair adminid-key
```

Related Commands

Command	Description
crypto ca enroll	Requests certificates for the switch's RSA key pair created for the trust point CA.
crypto key generate rsa	Configures RSA key pair information.
show crypto key mypubkey rsa	Displays information about configured RSA key pairs.

rscn

To configure a registered state change notification (RSCN), a Fibre Channel service that informs Nx ports about changes in the fabric, use the **rscn** command in configuration mode.

rscn {multi-pid | suppress domain-swrscn} vsan *vsan-id*

Syntax Description

multi-pid	Sends RSCNs in multi-PID format.
suppress domain-swrscn	Suppresses transmission of domain format SW-RCSNs.
vsan *vsan-id*	Configures VSAN information or membership. The ID of the VSAN is from 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures RSCNs in multi-PID format.

```
switch# config terminal
switch(config)# rscn multi-pid vsan 1
```

Related Commands

Command	Description
show rscn src-table	Displays state change registration table,
show rscn statistics	Displays RSCN statistics.

rscn abort vsan

To cancel a Registered State Change Notification (RSCN) configuration on a VSAN, use the **rscn abort vsan** command in configuration mode. To reverse the cancellation, use the **no** form of the command.

rscn abort vsan *vsan-id*

no rscn abort vsan *vsan-id*

Syntax Description

vsan-id	Specifies a VSAN where the RSCN configuration should be cancelled. The ID of the VSAN is from 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example cancels an RSCN configuration on VSAN 1.

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn abort vsan 1
```

Related Commands

Command	Description
rscn commit vsan	Commits a pending RSCN configuration on a specified VSAN.
rscn distribute	Enables the distribution of an RSCN configuration.
rscn event-tov	Configures an RSCN event timeout.
clear rscn session vsan	Clears the RSCN session for a specified VSAN.
show rscn	Displays RSCN configuration information.

rscn commit vsan

To apply a pending Registered State Change Notification (RSCN) configuration, use the **rscn commit vsan** command in configuration mode. To discard a pending RSCN configuration, use the **no** form of the command.

rscn commit vsan *vsan-id*

no rscn commit vsan *vsan-id*

Syntax Description

vsan-id	Specifies a VSAN where the RSCN configuration should be committed. The ID of the VSAN is from 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

If you commit the changes made to the active database, the configuration is committed to all the switches in the fabric. On a successful commit, the configuration change is applied throughout the fabric and the lock is released.

Examples

The following example commits an RSCN configuration on VSAN 1.

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn commit vsan 1
```

Related Commands

Command	Description
rscn abort vsan	Cancels a pending RSCN configuration on a specified VSAN.
rscn distribute	Enables the distribution of an RSCN configuration.
rscn event-tov	Configures an RSCN event timeout.
clear rscn session vsan	Clears the RSCN session for a specified VSAN.
show rscn	Displays RSCN configuration information.

rscn distribute

To enable distribution of a Registered State Change Notification (RSCN) configuration, use the **rscn distribute** command in configuration mode. To disable the distribution, use the **no** form of the command.

rscn distribute

no rscn distribute

Syntax Description

This command has no arguments or keywords.

Defaults

RSCN timer distribution is disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The RSCN timer configuration must be the same on all switches in the VSAN; otherwise, the link will not come up. Cisco Fabric Service (CFS) automatically distributes the RSCN timer configuration to all switches in a fabric. Only the RSCN timer configuration distributed.

Note For the CFS distribution to operate correctly for the RSCN timer configuration, all switches in the fabric must be running Cisco SAN-OS Release 3.0(1) or later.

Examples

The following example enables the distribution of an RSCN configuration.

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn distribute
```

Related Commands

Command	Description
rscn abort vsan	Cancels a pending RSCN configuration on a specified VSAN.
rscn commit vsan	Applies a pending RSCN configuration.
rscn event-tov	Configures an RSCN event timeout.
clear rscn session vsan	Clears the RSCN session for a specified VSAN.
show rscn	Displays RSCN configuration information.

rscn event-tov

To configure an event timeout value for a Registered State Change Notification (RSCN) on a specified VSAN, use the **rscn event-tov** command in configuration mode. To cancel the event timeout value and restore the default value, use the **no** form of the command.

rscn event-tov *timeout* **vsan** *vsan-id*

no rscn event-tov *timeout* **vsan** *vsan-id*

Syntax Description

timeout	Specifies an event timeout value in milliseconds. The range is 0 to 2000.
vsan-id	Specifies a VSAN where the RSCN event timer should be used. The ID of the VSAN is from 1 to 4093.

Defaults

The default timeout values are 2000 milliseconds for Fibre Channel VSANs and 1000 milliseconds for FICON VSANs.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Before changing the timeout value, you must enable RSCN configuration distribution using the **rscn distribute** command.

The RSCN timer is registered with Cisco Fabric Services (CFS) during initialization and switchover. For high availability, if the RSCN timer distribution crashes and restarts or a switchover occurs, it resumes normal functionality from the state prior to the crash or switchover.

Note You can determine configuration compatibility when downgrading to an earlier Cisco MDS SAN-OS release using the **show incompatibility system** command. You must disable RSCN timer distribution support before downgrading to an earlier release.

Examples

The following example configures an RSCN event timeout value on VSAN 1.

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn event-tov 20 vsan 1
Successful. Commit should follow for command to take effect.
```

Related Commands

Command	Description
rscn abort vsan	Cancels a pending RSCN configuration on a specified VSAN.
rscn commit vsan	Applies a pending RSCN configuration.
rscn distribute	Enables distribution of an RSCN configuration.
clear rscn session vsan	Clears the RSCN session for a specified VSAN.
show rscn	Displays RSCN configuration information.

run-script

To execute the commands specified in a file, use the **run-script** command.

run-script [**bootflash:** | **slot0:** | **volatile:**]*filename*

Syntax Description

bootflash:	Source or destination location for internal bootflash memory.
slot0:	Source or destination location for the CompactFlash memory or PCMCIA card.
volatile:	Source or destination location for volatile file system.
filename	Name of the file containing the commands.

Defaults

Uses the current default directory.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Updated the Usage Guidelines and Examples with information about user-defined variables.

Usage Guidelines

To use this command, be sure to create the file and specify commands in the required order.

The **run-script** command accepts user-defined variables as parameters.

Examples

The following example executes the CLI commands specified in the testfile that resides in the slot0 directory.

```
switch# show file slot0:testfile
conf t
interface fc 1/1
no shutdown
end
sh interface fc1/1
```

In response to the **run-script** command, this is the file output:

```
switch# run-script slot0:testfile
'conf t'
Enter configuration commands, one per line. End with CNTL/Z.

'interface fc 1/1'

'no shutdown'

'end'
```

```
'sh interface fc1/1'
fc1/1 is down (Fcot not present)
    Hardware is Fibre Channel
    Port WWN is 20:01:00:05:30:00:48:9e
    Admin port mode is auto, trunk mode is on
    vsan is 1
    Beacon is turned off
    Counter Values (current):
      0 frames input, 0 bytes, 0 discards
      0 runts, 0 jabber, 0 too long, 0 too short
      0 input errors, 0 CRC, 0 invalid transmission words
      0 address id, 0 delimiter
      0 EOF abort, 0 fragmented, 0 unknown class
      0 frames output, 0 bytes, 0 discards
      Received 0 OLS, 0 LRR, 0 NOS, 0 loop inits
      Transmitted 0 OLS, 0 LRR, 0 NOS, 0 loop inits
    Counter Values (5 minute averages):
      0 frames input, 0 bytes, 0 discards
      0 runts, 0 jabber, 0 too long, 0 too short
      0 input errors, 0 CRC, 0 invalid transmission words
      0 address id, 0 delimiter
      0 EOF abort, 0 fragmented, 0 unknown class
      0 frames output, 0 bytes, 0 discards
      Received 0 OLS, 0 LRR, 0 NOS, 0 loop inits
      Transmitted 0 OLS, 0 LRR, 0 NOS, 0 loop inits
```

The following example shows how you can pass user-defined variables to the **run-script** command.

```
switch# run-script bootflash:test2.vsh var1="fc1/1" var2="brief"
switch # show interface $(var1) $(var2)
--------------------------------------------------------------------------------
Interface Vsan Admin Admin Status SFP Oper Oper Port
Mode Trunk Mode Speed Channel
Mode (Gbps)
--------------------------------------------------------------------------------
fc1/1 1 auto on sfpAbsent -- -- --
```

rspan-tunnel

To associate and bind the SPAN tunnel (ST) port with the RSPAN tunnel, use the **rspan-tunnel** command.

rspan-tunnel interface fc-tunnel *tunnel-id*

rspan-tunnel

Syntax Description

rspan-tunnel	Configures the remote SPAN (RSPAN) tunnel.
interface	Specifies the interface to configure this tunnel.
fc-tunnel *tunnel-id*	Specifies the FC tunnel interface. The range is 1 to 255.

Defaults

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

The interface is not operationally up until the Fibre Channel tunnel mapping is configured in the source and destination switches.

Examples

The following example configures an interface to associate and bind the ST port with the RSPAN tunnel and enables traffic flow trough this interface..

```
switchS# config t
switchS(config)# interface fc2/1
switchS(config-if)# rspan-tunnel interface fc-tunnel 100
switchS(config-if)# no shutdown
```

CHAPTER 21

S Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "Command Modes" section to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

santap module

To configure the mapping between the Storage Services Module (SSM) and the VSAN where the appliance is configured, use the **santap module** command in configuration mode. To disable this feature, use the **no** form of the command.

santap module *slot-number* {**appl-vsan** *vsan-id* [**cvt-name** *cvt-name*] |
dvt target-pwwn *target-pwwn* **target-vsan** *target-vsan-id* **dvt-name** *dvt-name* **dvt-vsan** *dvt-vsan-id* [**dvt-port** *port-number*] [**lun-size-handling** *enable/disable*] [**io-timeout** *timeout-value*]}

no santap module *slot-number* {**appl-vsan** *vsan-id* [**cvt-name** *cvt-name*] |
dvt target-pwwn *target-pwwn*}

Syntax Description

slot-number	Specifies the slot number of the SSM where the control virtual target (CVT) is created.
appl-vsan *vsan-id*	Specifies the appliance VSAN identification number used to communicate with the appliance. The range is 1 to 4093.
cvt-name *cvt-name*	Specifies the control virtual target (CVT) name. The maximum size is 80 characters.
dvt	Configures the data virtual target (DVT).
target-pwwn *target-pwwn*	Specifies the target pWWN for the DVT. The format is *hh:hh:hh:hh:hh:hh:hh:hh.*
target-vsan *target-vsan-id*	Specifies the target VSAN for the DVT. The range for the real *target-vsan-id* is 1 through 4093.
dvt-name *dvt-name*	Specifies the DVT name. The maximum size is 80 characters.
dvt-vsan *dvt-vsan-id*	Specifies the DVT VSAN. The range for the *dvt-vsan-id* is 1 through 4093.
dvt-port *port-number*	Specifies the DVT port. The range for the port number is 1 through 32.
lun-size-handling *enable/disable*	Enables or disables LUN size handling. Specify 1 to enable or 0 to disable LUN size handling, with the default being enable.
io-timeout *timeout-value*	Specifies the I/O timeout value. The range is 10 to 200 seconds, with the default being 10 seconds.

Defaults

Disabled.
Io-timeout: 10 seconds.
Lun-size-handling: Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.
3.0(1)	Added the following options: **cvt-name**, **dvt**, **target-pwwn**, **target-vsan**, **dvt-name**, **dvt-vsan**, **dvt-port**, **lun-size-handling**, and **io-timeout**.

Usage Guidelines

To access this command, you must first enable the SANTap feature on the SSM using the **ssm enable feature** command.

When the **lun-size-handling** option is set (enabled), the maximum logical block addressing (LBA) for DVT LUN is set to 2 TB. As a result, there is no issue with LUN resizing.

Note You can delete **dvt target-pwwn** using the **no santap module** *slot* **dvt target-pwwn** command. Other **dvt** options are not supported by the **no** form of the command.

Examples

The following example shows the configuration of the SSM where the SANTap feature is enabled and the VSAN used to communicate with the appliance.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# santap module 1 appl-vsan 1
```

Related Commands

Command	Description
ssm enable feature	Enables the SANTap feature on the SSM.
show santap module	Displays the configuration and statistics of the SANTap feature.

scsi-flow distribute

To enable SCSI flow distribution through CFS, use the **scsi-flow distribute** command. To disable the SCSI flow distribution, use the **no** form of the command.

scsi-flow distribute

no scsi-flow distribute

Syntax Description

This command has no arguments or keywords.

Defaults

Distribution is enabled by default.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(2)	This command was introduced.

Usage Guidelines

You must enable the SCSI flow feature on the Storage Services Module (SSM) before you can configure a SCSI flow. Use the **ssm enable feature module** *slot-number* command to enable the SCSI flow feature on the SSM.

Examples

The following example enables distribution of SCSI flow services using CFS.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# scsi-flow distribute
```

The following example disables distribution of SCSI flow services.

```
switch(config)# no scsi-flow distribute
```

Related Commands

Command	Description
ssm enable feature	Enables the SCSI flow feature on the SSM.
show santap module	Displays SCSI flow configuration and status.

scsi-flow flow-id

To configure SCSI flow services, use the **scsi-flow flow-id** command. To disable the SCSI flow services, use the **no** form of the command.

scsi-flow flow-id *flow-id* {**initiator-vsan** *vsan-id* **initiator-pwwn** *wwn* **target-vsan** *vsan-id*
target-pwwn *wwn* |
statistics |
write-acceleration [**buffers** *count*]}

no scsi-flow flow-id *flow-id* [**statistics** | **write-acceleration**]

Syntax Description

flow-id	Configures the SCSI flow identification number. The range is 1 to 65535.
initiator-vsan *vsan-id*	Specifies the initiator VSAN identification number. The range is 1 to 4093.
initiator-pwwn *wwn*	Configures initiator side PWWN.
target-vsan *vsan-id*	Configures target VSAN identification number of the SCSI flow.
target-pwwn *wwn*	Configures the target side PWWN.
write-acceleration	Enables write acceleration.
statistics	Enables statistics gathering.
buffers *count*	Configures the write acceleration buffer count. The range is 1 to 40000 and the default is 1024.

Defaults

Disabled

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(2)	This command was introduced.

Usage Guidelines

You must enable the SCSI flow feature on the Storage Services Module (SSM) before you can configure a SCSI flow. Use the **ssm enable feature module** *slot-number* command to enable the SCSI flow feature on the SSM.

Examples

The following example configures a SCSI flow with a flow identifier of 4 and the following attributes:

- Initiator VSAN number—101
- Initiator port WWN—21:00:00:e0:8b:05:76:28
- Target VSAN number—101
- Target port—WWN 21:00:00:20:37:38:67:cf

```
switch# config terminal
switch(config)# scsi-flow flow-id 4 initiator-vsan 101 initiator-pwwn
21:00:00:e0:8b:05:76:28 target-vsan 101 target-pwwn 21:00:00:20:37:38:67:cf
```

The following example disables a SCSI flow with a flow identifier of 4.

```
switch(config)# no scsi-flow flow-id 4
```

The following example configures SCSI flow 4 to gather statistics about the SCSI flow.

```
switch(conf)# scsi-flow flow-id 4 statistics
```

The following example disables the statistics gathering feature on SCSI flow 4.

```
switch(conf)# no scsi-flow flow-id 4 statistics
```

The following example configures SCSI flow 4 with write acceleration.

```
switch(conf)# scsi-flow flow-id 4 write-acceleration
```

The following example configures SCSI flow 4 with write acceleration and buffers of 1024 credits.

```
switch(conf)# scsi-flow flow-id 4 write-acceleration buffer 1024
```

The following example disables the write acceleration feature on SCSI flow 4.

```
switch(conf)# no scsi-flow flow-id 4 write-acceleration
```

Related Commands

Command	Description
ssm enable feature	Enables the SCSI flow feature on the SSM.
show scsi-flow	Displays SCSI flow configuration and status.

send

To send a message to all active CLI users currently using the switch, use the **send** command in EXEC mode.

send *message-text*

Syntax Description

message-text	The text of your message.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This message is restricted to 80 alphanumeric characters with spaces.

Examples

The following example sends a warning message to all active users about the switch being shut down.

```
switch# send Shutting down the system in 2 minutes. Please log off.

Broadcast Message from admin@excal-112
        (/dev/pts/3) at 16:50 ...

Shutting down the system in 2 minutes. Please log off.
```

server

To add a server in an Internet Storage Name Service (iSNS) profile, use the **server** command in iSNS profile configuration submode. To delete a server from an iSNS profile, use the **no** form of the command.

server *server-id*

no server *server-id*

Syntax Description

server-id	Specifies the server address. The format is *A.B.C.D*.

Defaults

None.

Command Modes

iSNS profile configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

An iSNS profile can have only one server address. To change the server address, you must delete the current server and add the new one.

Examples

The following example shows how to add a server address to an iSNS profile.

```
switch# config terminal
switch(config)# isns profile name UserProfile
switch(config-isns-profile)# server 10.1.1.1
```

The following example shows how to delete a server address from an iSNS profile.

```
switch# config terminal
switch(config)# isns profile name AdminProfile
switch(config-isns-profile)# no server 10.2.2.2
```

Related Commands

Command	Description
isns-server enable	Enables the iSNS server.
isns profile name	Creates iSNS profiles.
show isns	Displays iSNS information.

server (radius configuration)

To configure a RADIUS server, use the **server** command in RADIUS configuration submode. To discard the configuration, use the **no** form of the command.

server [*ipv4-address* | *ipv6-address* | *dns-name*]

no server [*ipv4-address* | *ipv6-address* | *dns-name*]

Syntax Description

ipv4-address	Specifies the RADIUS server IP address in the format *A.B.C.D*.
ipv6-address	Specifies the RADIUS server IP address in the format *X:X::X*.
name	Specifies the RADIUS DNS server name. The maximum size is 255.

Defaults

None.

Command Modes

RADIUS configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Added the *ipv6-address* argument.

Usage Guidelines

None.

Examples

The following example shows the **server** command in RADIUS configuration submode.

```
switch# config terminal
switch(config)# aaa group server radius testgroup
switch(config-radius)# server myserver
```

Related Commands

Command	Description
radius-server host	Configures RADIUS server parameters.
show radius-server	Displays RADIUS server configuration parameters.

server (tacacs+ configuration)

To configure a TACACS+ server, use the **server** command in TACACS+ configuration submode. To discard the configuration, use the **no** form of the command.

server [*ipv4-address* | *ipv6-address* |*dns-name*]

no server [*ipv4-address* | *ipv6-address* |*dns-name*]

Syntax Description

ipv4-address	Specifies the TACACS+ server IP address in the format *A.B.C.D*.
ipv6-address	Specifies the TACACS+ server IP address in the format *X:X::X*.
dns-name	Specifies the TACACS+ DNS server name. The maximum size is 255.

Defaults

None.

Command Modes

TACACS+ configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Added the *ipv6-address* argument.

Usage Guidelines

None.

Examples

The following example shows the **server** command in RADIUS configuration submode.

```
switch# config terminal
switch(config)# aaa group server tacacs+ testgroup
switch(config-tacacs+)# server myserver
```

Related Commands

Command	Description
tacacs-server host	Configures TACACS+ server parameters.
show tacacs-server	Displays TACACS+ server configuration parameters.

set (IPsec crypto map configuration submode)

To configure attributes for IPsec crypto map entries, use the **set** command in IPsec crytpo map configuration submode. To revert to the default values, use the **no** form of the command.

set {**peer** {*ip-address* | **auto-peer**} | **pfs** [**group1** | **group14** | **group2** | **group5**] | **security-association lifetime** {**gigabytes** *number* | **kilobytes** *number* | **megabytes** *number* | **seconds** *number*} | **transform-set** {*set-name* | *set-name-list*}}

no set {**peer** {*ip-address* | **auto-peer**} | **pfs** | **security-association lifetime** {**gigabytes** | **kilobytes** | **megabytes** | **seconds**} | **transform-set**}

Syntax Description

peer	Specifies an allowed encryption/decryption peer.
ip-address	Specifies a static IP address for the destination peer.
auto-peer	Specifies automatic assignment of the address for the destination peer.
pfs	Specifies the perfect forwarding secrecy.
group1	Specifies PFS DH Group1 (768-bit MODP).
group14	Specifies PFS DH Group14 (2048-bit MODP).
group2	Specifies PFS DH Group2 (1024-bit MODP).
group5	Specifies PFS DH Group5 (1536-bit MODP).
security-association lifetime	Specifies the security association lifetime in traffic volume or time in seconds.
gigabytes *number*	Specifies a volume-based key duration in gigabytes. The range is 1 to 4095.
kilobytes *number*	Specifies a volume-based key duration in kilobytes. The range is 2560 to 2147483647.
megabytes *number*	Specifies a volume-based key duration in megabytes. The range is 3 to 4193280.
seconds *number*	Specifies a time-based key duration in seconds. The range is 120 to 86400.
transform-set	Configures the transform set name or set name list.
set-name	Specifies a transform set name. Maximum length is 63 characters.
set-name-list	Specifies a comma-separated transform set name list. Maximum length of each name is 63 characters. You can specified a maximum of six lists.

Defaults

None.

PFS is disabled by default. When it is enabled without a group parameter, the default is group1.

The security association lifetime defaults to global setting configured by the **crypto global domain ipsec security-association lifetime** command.

Command Modes

IPsec crypto map configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, IPsec must be enabled using the **crypto ipsec enable** command.

Examples

The following example shows how to configure IPsec crypto map attributes.

```
switch# config terminal
switch(config)# crypto map domain ipsec x 1
switch(config-crypto-map-ip)# set peer auto-peer
```

Related Commands

Command	Description
crypto global domain ipsec security-association lifetime	Configures the global security association lifetime value.
crypto ipsec enable	Enables IPsec.
show crypto map domain ipsec	Displays IPsec crypto map information.

setup

To enter the switch setup mode, use the **setup** command in EXEC mode.

setup

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Refer to the *Cisco MDS 9000 Family CLI Configuration Guide* for more information on using the **setup** command.

The setup utility guides you through the basic configuration process. Type **Ctrl-c** at any prompt to skip the remaining configuration options and proceed with what is configured until that point.

If you do not wish to answer a previously-configured question, or if you wish to skip answers to any questions press **Enter**. If a default answer is not available (for example switch name), the switch uses what is previously configured and skips to the next question.

Examples

The following example shows how to enter switch setup mode.

```
switch# setup
---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

*Note: setup always assumes a predefined defaults irrespective
of the current system configuration when invoked from CLI.

Press Enter incase you want to skip any dialog. Use ctrl-c at anytime
to skip away remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes
```

setup ficon

To enter the automated FICON setup mode, use the **setup ficon** command in EXEC mode.

setup ficon

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Refer to the *Cisco MDS 9000 Family CLI Configuration Guide* for more information on using the **setup ficon** command.

The setup utility guides you through the basic configuration process. Type **Ctrl-c** at any prompt to skip the remaining configuration options and proceed with what is configured until that point.

If you do not wish to answer a previously-configured question, or if you wish to skip answers to any questions press **Enter**. If a default answer is not available (for example switch name), the switch uses what is previously configured and skips to the next question.

Examples

The following example shows how to enter switch setup mode.

```
switch# setup ficon
---- Basic System Configuration Dialog ----

--- Ficon Configuration Dialog ---

This setup utility will guide you through basic Ficon Configuration
on the system.

Press Enter if you want to skip any dialog. Use ctrl-c at anytime
to skip all remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes
```

shutdown

To disable an interface, use the **shutdown** command. To enable an interface, use the **no** form of the command.

shutdown [**force**]

no shutdown [**force**]

Syntax Description

force	Forces the shutdown of the mgmt 0 interface to avoid the confirmation.

Defaults

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.0(1)	This command was introduced.

Usage Guidelines

The default state for interfaces is shutdown. Use the **no shutdown** command to enable an interface to carry traffic.

When you try to shutdown a management interface(mgmt0), a follow-up message confirms your action before performing the operation. Use the **force** option to bypass this confirmation, if required.

Examples

The following example shows how to enable an interface.

```
switch# config terminal
switch(config)# interface fc 1/2
switch(config-if)# no shutdown
```

The following example shows how to disable an interface.

```
switch# config terminal
switch(config)# interface mgmt 0
switch(config-if)# shutdown
```

The following example shows how to forcefully disable the mgmt 0 interface.

```
switch# config terminal
switch(config)# interface mgmt 0
switch(config-if)# shutdown force
```

Related Commands

Command	Description
interface	Specifies an interface and enters interface configuration submode.
show interface	Displays interface information.

site-id

To configure the site ID with the Call Home function, use the **site-id** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

site-id *site-number*

no site-id *site-number*

Syntax Description

site-number	(Optional) Identifies the unit to the outsourced throughput. Allows up to 256 alphanumeric characters in free format.

Defaults

None.

Command Modes

Call Home configuration submode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the site ID in the Call Home configuration.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# site-id Site1ManhattanNY
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

sleep

To delay an action by a specified number of seconds, use the **sleep** command.

sleep *seconds*

Syntax Description

seconds	The number of seconds to delay an action.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command is useful within scripts. For example, if you create a script called test-script:

```
switch# show file slot0:test-script
discover scsi-target remote
sleep 10
show scsi-target disk

switch# run-script slot0:test-script
```

When you execute the slot0:test-script, the switch software executes the **discover scsi-target remote** command, and then waits for 10 seconds before executing the **show scsi-target disk command**.

Examples

The following example shows how to delay the switch prompt return.

```
switch# sleep 30
```

You will see the switch prompt return after 30 seconds.

snmp port

Use the **snmp port** command to enable SNMP control of FICON configurations. To disable the configuration or to revert to factory defaults, use the **no** form of the command.

snmp port control

no snmp port control

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled.

Command Modes

FICON configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

By default, SNMP users can configure FICON parameters through the Fabric Manager application. You can prohibit this access, if required, by issuing the **no snmp port control** command.

Examples

The following example prohibits SNMP users from configuring FICON parameters.

```
switch(config)# ficon vsan 2
switch(config-ficon)# no snmp port control
```

The following example allows SNMP users to configure FICON parameters (default).

```
switch(config-ficon)# snmp port control
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.
ficon vsan *vsan-id*	Enables FICON on the specified VSAN.

snmp-server

To configure the SNMP server information, switch location, and switch name, use the **snmp-server** command in configuration mode. To remove the system contact information, use the **no** form of the command.

snmp-server {**community** *string* [**group** *group-name* | **ro** | **rw**] | **contact** [*name*] | **location** [*location*]}

no snmp-server {**community** *string* [**group** *group-name* | **ro** | **rw**] | **contact** [*name*] | **location** [*location*]}

Syntax Description

community *string*	Specifies SNMP community string. Maximum length is 32 characters.
group *group-name*	Specifies group name to which the community belongs. Maximum length is 32 characters.
ro	Sets read-only access with this community string.
rw	Sets read-write access with this community string.
contact	Configures system contact.
name	Specifies the name of the contact. Maximum length is 80 characters.
location	Configures system location.
location	Specifies system location. Maximum length is 80 characters.

Defaults

The default community access is read-only (**ro**).

Command Modes

Configuration mode

Command History

Release	Modification
1.0(3)	This command was introduced.
2.0(1b)	Added **group** option.

Usage Guidelines

None.

Examples

The following example sets the contact information, switch location, and switch name.

```
switch# config terminal
switch(config)# snmp-server contact NewUser
switch(config)# no snmp-server contact NewUser
switch(config)# snmp-server location SanJose
switch(config)# no snmp-server location SanJose
switch(config)# snmp-server name NewName
switch(config)# no snmp-server name NewName
switch(config)# no snmp-server user usernameA
```

Related Commands

Command	Description
show snmp	Displays SNMP information.

snmp-server enable traps

To enable SNMP server notifications (informs and traps), use the **snmp-server enable traps** command. To disable the SNMP server notifications, use the **no** form of the command.

snmp-server enable traps [**entity** [**fru**] | **fcc** | **fcdomain** | **fcns** | **fdmi** | **fspf** | **license** | **link** [**cisco** | **ietf** [**cisco**] | **ietf-extended** [**cisco**]] | **port-security** | **rscn** [**els** | **ils**] | **snmp** [**authentication**] | **vrrp** | **zone** [**default-zone-behavior-change** | **merge-failure** | **merge-success** | **request-reject**]

no snmp-server enable traps [**entity** [**fru**] | **fcc** | **fcdomain** | **fcns** | **fdmi** | **fspf** | **license** | **link** [**cisco** | **ietf** [**cisco**] | **ietf-extended** [**cisco**]] | **port-security** | **rscn** [**els** | **ils**] | **snmp** [**authentication**] | **vrrp** | **zone** [**default-zone-behavior-change** | **merge-failure** | **merge-success** | **request-reject**]

Syntax Description

entity	Enables all SNMP entity notifications.
fru	Enables only SNMP entity FRU notifications.
fcc	Enables SNMP Fibre Channel congestion control notifications.
fcdomain	Enables SNMP Fibre Channel domain notifications.
fcns	Enables SNMP Fibre Channel name server notifications.
fdmi	Enables SNMP Fabric Device Management Interface notifications.
fspf	Enables SNMP Fabric Shortest Path First notifications.
license	Enables SNMP license manager notifications.
link	Enables SNMP link traps.
cisco	Enables Cisco cieLinkUp/cieLinkDown.
ietf	Enables standard linkUp/linkDown trap.
ietf-extended	Enables standard linkUp/linkDown trap with extra varbinds.
port-security	Enables SNMP port security notifications.
rscn	Enables all SNMP Registered State Change Notification notifications.
els	Enables only SNMP RSCN ELS notifications.
ils	Enables only SNMP RSCN ILS notifications.
snmp	Enables all SNMP agent notifications.
authentication	Enables only SNMP agent authentication notifications.
vrrp	Enables SNMP Virtual Router Redundancy Protocol notifications
zone	Enables all SNMP zone notifications.
default-zone-behavior-change	Enables only SNMP zone default zone behavior change notifications.
merge-failure	Enables only SNMP zone merge failure notifications.
merge-success	Enables only SNMP zone merge success notifications.
request-reject	Enables only SNMP zone request reject notifications.

Defaults

All the notifications listed in the Syntax Description table are disabled by default except for the following: **entity fru**, **vrrp**, **license**, **link**, and any notification not listed (including the generic notifications such as **coldstart**, **warmstart**, and **linkupdown**).

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.
2.1(2)	• Added the **link** option. • Renamed the **standard** option to **ietf**. • Renamed the **standard-extended** option to **ietf-extended**.

Usage Guidelines

If the **snmp-server enable traps** command is entered without keywords, all notifications (informs and traps) are enabled.

As of Cisco MDS SAN-OS Release 2.1(2), you can configure the linkUp/linkDown notifications that you want to enable on the interfaces. You can enable the following types of linkUp/linkDown notifications:

- Cisco—Only traps (cieLinkUp, cieLinkDown) defined in CISCO-IF-EXTENSION-MIB.my are sent for an interface, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface.
- IETF—Only traps (linkUp, linkDown) defined in IF-MIB are sent for an interface, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. Only the varbinds defined in the trap definition are sent with the traps.
- IETF extended—Only traps (linkUp, linkDown) defined in IF-MIB are sent for an interface, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. In addition to the varbinds defined in the trap definition, varbinds defined in the IF-MIB specific to the Cisco Systems implementation are sent. This is the default setting.
- IETF cisco—Traps (linkUp, linkDown) defined in IF-MIB and traps (cieLinkUp, cieLinkDown) defined in CISCO-IF-EXTENSION-MIB.my are sent for an interface, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. Only the varbinds defined in the trap definition are sent with the linkUp and linkDown traps.
- IETF extended cisco—Traps (linkUp, linkDown) defined in IF-MIB and traps (cieLinkUp, cieLinkDown) defined in CISCO-IF-EXTENSION-MIB.my are sent for an interface, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. In addition to the varbinds defined in the linkUp and linkDown trap definition, varbinds defined in the IF-MIB specific to the Cisco Systems implementation are sent with the linkUp and linkDown traps.

Note For more information on the varbinds defined in the IF-MIB specific to the Cisco Systems implementation, refer to the *Cisco MDS 9000 Family MIB Quick Reference.*

Examples

The following example enables all the SNMP notifications listed in the Syntax Description table.

```
switch# config terminal
switch(config)# snmp-server traps
```

The following example enables all SNMP entity notifications.

```
switch# config terminal
switch(config)# snmp-server traps entity
```

To following example enables (default) only standard extended linkUp/linkDown notifications.

```
switch# config t
switch(config)# snmp-server enable traps link
```

The following example enables only Cisco Systems defined cieLinkUp/cieLinkDown notifications.

```
switch# config terminal
switch(config)# snmp-server enable traps link cisco
```

Related Commands

Command	Description
show snmp	Displays SNMP information.
snmp-server host	Configures SNMP server host information.

snmp-server host

To specify the recipient of an Simple Network Management Protocol notification operation, use the **snmp-server host** global configuration command. To remove the specified host, use the no form of the command.

snmp-server host *host-address* **[traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}]** *community-string* **[udp-port port] [notification-type]**

no snmp-server host *host-address* **[traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}]** *community-string* **[udp-port port] [notification-type]**

Syntax Description

host-address	Specifies the name or IP address of the host (the targeted recipient).
traps	Sends SNMP traps to this host.
informs	Sends SNMP informs to this host.
version	Specifies the version of the Simple Network Management Protocol (SNMP) used to send the traps. Version 3 is the most secure model, as it allows packet encryption with the **priv** keyword.
1	SNMPv1 (default). This option is not available with informs.
2c	SNMPv2C.
3	SNMPv3 has three optional keywords (**auth**, **no auth** (default), or **priv**).
auth	Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication
noauth	Specifies the noAuthNoPriv security level.
priv	Enables Data Encryption Standard (DES) packet encryption (privacy).
community-string	Sends a password-like community string with the notification operation.
udp-port	Specifies the port UDP port of the host to use. The default is 162.

Defaults

Sends SNMP traps.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(3)	This command was introduced.

Usage Guidelines

If you use the version keyword, one of the following must be specified: **1**, **2c**, or **3**.

Examples

The following example specify the recipient of an SNMP notification.

```
switch# config terminal
switch(config)# snmp-server host 10.1.1.1 traps version 2c abcddsfsf udp-port 500
```

snmp-server user

To configure SNMP user information, use the **snmp-server user** command in configuration mode. To disable the configuration or to revert to factory defaults, use the **no** form of the command.

snmp-server user *username* [*group-name*] [**auth** {**md5** | **sha**} *password* [**priv** [*password* [**auto** | **localizedkey** [**auto**]]] | **aes-128** *password* [**auto** | **localizedkey** [**auto**] | **auto** | **localizedkey** [**auto**]]]

no snmp-server user *name* [*group-name* | **auth** {**md5** | **sha**} *password* [**priv** [*password* [**auto** | **localizedkey** [**auto**]]] | **aes-128** *password* [**auto** | **localizedkey** [**auto**] | **auto** | **localizedkey** [**auto**]]]

Syntax Description

username	Specifies the user name. Maximum length is 32 characters.
group-name	Specifies role group to which the user belongs. Maximum length is 32 characters.
auth	Sets authentication parameters for the user.
md5	Sets HMAC MD5 algorithm for authentication.
sha	Uses HMAC SHA algorithm for authentication.
password	Specifies user password. Maximum length is 64 characters.
priv	Sets encryption parameters for the user.
aes-128	Sets 128-byte AES algorithm for privacy.
auto	Specifies whether the user is autocreated (volatile).
localizedkey	Sets passwords in localized key format.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
1.0(3)	Added the **localizedkey** option.
2.0(1b)	Added the **auto** and **aes128** options.

Usage Guidelines

The localized keys are not portable across devices as they contain information on the engine ID of the device. If a configuration file is copied into the device, the passwords may not be set correctly if the configuration file was generated at a different device. We recommend that passwords be explicitly configured to the desired passwords after copying the configuration into the device.

SNMP Version 3 is the most secure model, as it allows packet encryption with the **priv** keyword.

To assign multiple roles to a user, perform multiple **snmp-server user** *username group-name* commands. The *group-name* is defined by the **role name** command.

Examples

The following example sets the user information.

```
switch# config terminal
switch(config)# snmp-server user joe network-admin auth sha abcd1234
switch(config)# snmp-server user sam network-admin auth md5 abcdefgh
switch(config)# snmp-server user Bill network-admin auth sha abcd1234 priv abcdefgh
switch(config)# no snmp-server user usernameA
switch(config)# snmp-server user user1 network-admin auth md5 0xab0211gh priv 0x45abf342
localizedkey
```

Related Commands

Command	Description
role name	Configures role profiles.
show snmp	Displays SNMP information.
snmp-server host	Configures SNMP server host information.

source

To configure a switched port analyzer (SPAN) source, use the **source** command in SPAN session configuration submode. To disable this feature, use the **no** form of the command.

source {
filter vsan *vsan-id* |
interface {
fc *slot/port* [**rx [traffic-type** {**initiator** | **mgmt** | **target**}] | **tx [traffic-type** {**initiator** | **mgmt** | **target**}] | **traffic-type** {**initiator** | **mgmt** | **target**}] |
fcip *fcip-i***d** |
fv *slot/dpp-number/fv-port* |
iscsi *slot/port* [**rx** [**traffic-type** {**initiator** | **mgmt** | **target**}] | **tx [traffic-type** {**initiator** | **mgmt** | **target**}] | **traffic-type** {**initiator** | **mgmt** | **target**}]|
port-channel *channel-number* [**rx** [**traffic-type** {**initiator** | **mgmt** | **target**}] | **tx [traffic-type** {**initiator** | **mgmt** | **target**}] | **traffic-type** {**initiator** | **mgmt** | **target**}] |
sup-fc *number* [**rx [traffic-type** {**initiator** | **mgmt** | **target**}] | **tx [traffic-type** {**initiator** | **mgmt** | **target**}] | **traffic-type** {**initiator** | **mgmt** | **target**}]} |
vsan *vsan-id*}

no source {
filter vsan *vsan-id* |
interface {
fc *slot/port* [**rx [traffic-type** {**initiator** | **mgmt** | **target**}] | **tx [traffic-type** {**initiator** | **mgmt** | **target**}] | **traffic-type** {**initiator** | **mgmt** | **target**}] |
fcip *fcip-id* |
fv *slot/dpp-number/fv-port* |
iscsi *slot/port* **[rx [traffic-type** {**initiator** | **mgmt** | **target**}] | **tx [traffic-type** {**initiator** | **mgmt** | **target**}] | **traffic-type** {**initiator** | **mgmt** | **target**}]|
port-channel *channel-number* [**rx [traffic-type** {**initiator** | **mgmt** | **target**}] | **tx** [**traffic-type** {**initiator** | **mgmt** | **target**}] | **traffic-type** {**initiator** | **mgmt** | **target**}] |
sup-fc *number* [**rx** [**traffic-type** {**initiator** | **mgmt** | **target**}] | **tx** [**traffic-type** {**initiator** | **mgmt** | **target**}] | **traffic-type** {**initiator** | **mgmt** | **target**}]} |
vsan *vsan-id*}

Syntax Description

filter	Configures SPAN session filter.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
interface	Specifies the interface type.
fc *slot/port*	Specifies the Fibre Channel interface ID at a slot and port.
fcip *fcip-id*	Specifies the FCIP interface ID. The range is 1 to 255.
fv *slot/dpp-number/fv-port*	Specifies a virtual F port (FV port) interface in the specified slot along with the data path processor (DPP) number and the FV port number.
iscsi *slot/port*	Configures the iSCSI interface in the specified slot/port.
port-channel *channel-number*	Specifies the PortChannel interface ID. The range is 1 to 128.
sup-fc *number*	Specifies the inband interface, which is 0.
rx	Specifies SPAN traffic in ingress direction.
traffic-type	Configures the SPAN traffic type.

initiator	Specifies initiator traffic.
mgmt	Specifies management traffic.
target	Specifies target traffic.
tx	Specifies SPAN traffic in egress direction.

Defaults

Disabled.

Command Modes

SPAN session configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to create a SPAN session, then configures the SPAN traffic at all sources in VSAN 1.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# span session 1
switch(config-span)# source vsan 1
```

The following example shows how to configure the SPAN source interface as PortChannel 1.

```
switch(config-span)# source interface port-channel 1
```

The following example shows how to configure the SPAN source interface as FC 9/1 with an egress filter for VSAN 1.

```
switch(config-span)# source interface fc9/1 tx filter vsan 1
```

The following example shows how to configure the SPAN source interface as FCIP 51.

```
switch(config-span)# source interface fcip 51
```

The following example shows how to configure the SPAN source interface as iSCSI interface 4/1.

```
switch(config-span)# source interface iscsi 4/1
```

The following example shows how to disable configure the SPAN source interface as FC 9/1 with an egress filter for VSAN 1.

```
switch(config-span)# no source interface fc9/1 tx filter vsan 1
```

Related Commands

Command	Description
switchport	Configures the switch port mode on the Fibre Channel interface.
span session	Selects or configures the SPAN session and changes to SPAN configuration submode.
destination interface	Configures a SPAN destination interface.
suspend	Suspends a SPAN session.
show span session	Displays specific information about a SPAN session

span session

To configure a SPAN session, use the **span session** command. To remove a configured SPAN feature or revert it to factory defaults, use the **no** form of the command.

span session *session-id*

no span session *session-id*

Syntax Description

session-id	Enter SPAN session ID from 1 to 16.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure a SPAN session.

```
switch# config terminal
switch(config)# span session 1
switch(config-span)#
```

The following example shows how to delete a SPAN session.

```
switch(config)# no span session 1
```

Related Commands

Command	Description
switchport	Configures the switch port mode on the Fibre Channel interface.
span session	Selects or configures the SPAN session and changes to SPAN configuration submode.
destination interface	Configures a SPAN destination interface.
source	Configures a SPAN source.
suspend	Suspends a SPAN session.
show span session	Displays specific information about a SPAN session

special-frame

To enable or disable special frames for the FCIP interface, use the **special-frame** command. To disable the passive mode for the FCIP interface, use the **no** form of the command.

special-frame peer-wwn *pwwn-id* [**profile-id** *profile-number*]

no special-frame peer-wwn *pwwn-id*

Syntax Description

peer-wwn *pwwn-id*	Specifies the peer WWN ID for special frames.
profile-id *profile-number*	Specifies the peer profile ID. The range is 1 to 255.

Defaults

Disabled.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Access this command from the `switch(config-if)#` submode.

When a new TCP Connection is established, an FCIP special frame (if enabled) makes one round trip from the FCIP profile and initiates the TCP connect operation to the FCIP profile receiving the TCP connect request and back. Use these frames to identify the FCIP link endpoints, to learn about the critical parameters shared by Fibre Channel and FCIP profile pairs involved in the FCIP link, and to perform configuration discovery

Examples

The following example configures the special frames.

```
switch# config terminal
switch(config)# interface fcip 1
switch(config)# special-frame peer-pwwn 11:11:11:11:11:11:11:11
switch(config)# special-frame peer-pwwn 22:22:22:22:22:22:22:22 profile-id 10
```

Related Commands

Command	Description
show interface fcip	Displays an interface configuration for a specified FCIP interface.

ssh

To initiate a Secure Shell (SSH) session, use the **ssh** command in EXEC mode.

ssh {*hostname* | *userid*@*hostname*}

Syntax Description

hostname	Specifies the name or IP address of the host to access. If no user name is specified, the default is “admin”.
userid	Specifies a user name on a host.

Defaults

The default user name is “admin”.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to initiate an SSH session using a host name.

```
switch# ssh host1

admin@1host1's password:
```

The following example shows how to initiate an SSH session using a host IP address.

```
switch# ssh 10.2.2.2

admin@10.1.1.1's password:
```

The following example shows how to initiate an SSH session using a user name host name.

```
switch# ssh user1@host1

user1@1host1's password:
```

Related Commands

Command	Description
show ssh key	Displays SSH key information.
ssh server enable	Enables SSH server.

ssh key

To generate an SSH key, use the **ssh key** command in configuration mode. To delete the SSH keys, use the **no** form of the command.

ssh key {dsa [*bits*] **| rsa** [*bits*] **| rsa1** [*bits*]} [**force**]

no ssh key

Syntax Description

dsa [*bits*]	Generates a DSA key. The range for the number of bits is 768 to 1856.
rsa [*bits*]	Generates an RSA key. The range for the number of bits is 768 to 2048.
rsa1 [*bits*]	Generates an RSA1 key. The range for the number of bits is 768 to 2048.
force	Forces the generation of keys even when previous keys are present.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to generate an SSH key.

```
switch# config terminal
switch(config)# ssh key rsa1 1024
generating rsa1 key.....
generated rsa1 key
switch(config)#
switch(config)# ssh key dsa 1024
generating dsa key.....
generated dsa key
switch(config)#
switch(config)# ssh key rsa 1024
generating rsa key.....
generated rsa key
switch(config)#
switch(config)# no ssh key
cleared RSA keys
switch(config)#
```

Related Commands

Command	Description
show ssh key	Displays SSH key information.
ssh server enable	Enables SSH server.

ssh server enable

To enable the SSH server, use the **ssh server enable** command in configuration mode. To disable the SSH service, use the **no** form of the command.

ssh server enable

no ssh server enable

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example enables the SSH server.

```
switch# config terminal
switch(config)# ssh server enable
updated
switch(config)# no ssh server enable
updated
```

Related Commands

Command	Description
show ssh server	Displays SSH server information.
ssh key	Generates an SSH key.

ssm enable feature

To enable a feature on the Storage Services Module (SSM), use the **ssm enable feature** command. To disable the feature on the module, use the **no** form of the command.

ssm enable feature {
invista {**bootflash:** *uri* | **force module** *slot-number* | **modflash:** *uri* | **module** *slot-number* | **slot0:** *uri*} |
nasb {**force module** *slot-number* | **interface fc** *slot*/*port-port*} | **module** *slot-number*} |
nsp {**bootflash:** *uri* | **force module** *slot-number* | **modflash:** *uri* | **module** *slot-number* | **slot0:** *uri*} |
santap {**force module** *slot-number* | **interface fc** *slot*/*port-port* | **module** *slot-number*} |
scsi-flow {**force module** *slot-number* | **interface fc** *slot*/*port-port* | **module** *slot-number*}}

no ssm enable feature {
invista {**bootflash:** *uri* | **force module** *slot-number* | **modflash:** *uri* | **module** *slot-number* | **slot0:** *uri*} |
nasb {**force module** *slot-number* | **interface fc** *slot*/*port-port*} | **module** *slot-number*} |
nsp {**bootflash:** *uri* | **force module** *slot-number* | **modflash:** *uri* | **module** *slot-number* | **slot0:** *uri*} |
santap {**force module** *slot-number* | **interface fc** *slot*/*port-port* | **module** *slot-number*} |
scsi-flow {**force module** *slot-number* | **interface fc** *slot*/*port-port* | **module** *slot-number*}}

Syntax Description

invista	Enables the Invista feature on the SSM.
nasb	Enables the Network-Accelerated Serverless Backup (NASB) feature on the SSM.
nsp	Enables the Network Storage Processor (NSP) feature on the SSM.
santap	Enables the SANTap feature on the SSM.
scsi-flow	Enables the SCSI flow feature on the SSM.
force	Forces an immediate configuration change.
module *slot-number*	Specifies the slot number of the SSM.
bootflash: *uri*	Specifies the source location for internal bootflash with image name.
modflash: *uri*	Specifies the source location for internal modflash with image name.
slot0:*uri*	Specifies the source location for the CompactFlash memory or PC Card with image name.
interface	Specifies the interface to be configured.
fc *slot*/*port*	Configures the Fibre Channel interface.
fc *slot*/*port-port*	Configures the Fibre Channel interface range of ports. See the usage guidelines for this command for a list of interface range restrictions.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(2b)	This command was introduced.
2.1(1a)	Added **emcsr**, **nasb**, and **santap** options.
3.0(1)	Changed the name of the **emcsr** option to **invista**.

Usage Guidelines

Use the **ssm enable feature scsi-flow** command to enable the SCSI flow feature on an SSM.

The features **invista** and **nsp** can only be provisioned on a module basis. The features **nasb**, **santap**, and **scsi-flow** can be provisioned on either a module or a range of interfaces.

The image must be specified when configuring the **invista** and **nsp** features.

Caution The **force** option is only applicable when unprovisioning (using the **no** parameter). Using the **force** parameter without the **no** keyword causes the SSM to reload.

For Release 2.1 and later images, intelligent services can be configured on a range of interfaces with the following restrictions:

- The minimum range is four interfaces.
- The range of interfaces must be specified in multiples of four interfaces. For example, 4, 8, 12, 16, 20, 24, 28, 32.
- Ranges start at the following specific ports: 1, 5, 9, 13, 17, 21, 25, and 29.

Examples

The following example enables the Invista feature on the SSM in slot 4.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config) ssm enable feature invista module 4
```

The following example enables the Invista feature using the bootflash image name.

```
switch(config) ssm enable feature invista bootflash:image_name
```

The following example enables the Invista feature using the image name found on the PC card Flash module in slot0.

```
switch(config) ssm enable feature invista slot0:image_name
```

The following example disables the Invista feature on the SSM in slot 4.

```
switch(config) no ssm enable feature invista force module 4
```

The following example enables the NASB feature on the SSM in slot 4.

```
switch(config) ssm enable feature nasb module 4
```

The following example enables the NASB feature on the specific Fibre Channel interface range 1 to 4.

```
switch(config) ssm enable feature nasb interface fc 4/1-4
```

The following example enables the NSP feature on the SSM in slot 4.

```
switch(config) ssm enable feature nsp module 4
```

The following example enables the SANTap feature on the SSM in slot 4.

```
switch(config) ssm enable feature santap module 4
```

The following example enables the SCSI flow feature on the SSM in slot 4.

```
switch(config) ssm enable feature scsi-flow module 4
```

Related Commands

Command	Description
scsi-flow distribute	Configures the SCSI flow services.
show scsi-flow	Displays SCSI flow configuration and status.

static (iSCSI initiator configuration and iSLB initiator configuration)

To assign persistent WWNs to an iSCSI initiator or iSLB initiator, use the **static** command in iSCSI initiator configuration submode or iSLB initiator configuration submode. To disable this feature, use the **no** form of the command.

static {**nwwn** | **pwwn**} {*wwn-id* | **system-assign**}

no static {**nwwn** | **pwwn**} {*wwn-id* | **system-assign**}

Syntax Description

nwwn	Configures the initiator node WWN hex value.
pwwn	Configures the peer WWN for special frames.
wwn-id	Specifies the pWWN or nWWN ID.
system-assign	Generates the pWWN or nWWN value automatically.

Defaults

None.

Command Modes

iSCSI initiator configuration submode.
iSLB initiator configuration submode.

Command History

Release	Modification
1.3(2)	This command was introduced.
3.0(1)	Added iSBL initiator configuration submode.

Usage Guidelines

We recommend using the **system-assign** option. If you manually assign a WWN, you must ensure its uniqueness. You should not use any previously-assigned WWN.

If you use **system-assign** option to configure WWNs for an iSLB initiator, when the configuration is saved to an ASCII file, the system-assigned WWNs are also saved. If you subsequently perform a write erase, you must manually delete the WWN configuration from the ASCII file. Failing to do so can cause duplicate WWN assignments if the ASCII configuration file is reapplied on the switch.

Examples

The following example uses the switch WWN pool to allocate the nWWN for this iSCSI initiator and to keep it persistent.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# iscsi initiator name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-init)# static nWWN system-assign
```

The following example uses the switch WWN pool to allocate two pWWNs for this iSCSI initiator and to keep it persistent.

```
switch(config-iscsi-init)# static pWWN system-assign 2
```

The following example shows a system-assigned pWWN for an iSLB initiator.

```
switch# config t
switch(config)# islb initiator ip-address 100.10.10.10
ips-hac2(config-islb-init)# static pwwn system-assign ?
  <1-64>  Enter the number of pWWN(s)

ips-hac2(config-islb-init)# static pwwn system-assign 4 ?
  <cr>  Carriage return.
```

The following example removes the system-assigned pWWN for the iSLB initiator.

```
switch (config-islb-init)# no static pwwn system-assign 4
```

Related Commands

Command	Description
iscsi initiator name	Assigns an iSCSI name and changes to iSCSI initiator configuration submode.
show iscsi initiator	Displays information about configured iSCSI initiators.
show iscsi initiator configured	Displays iSCSI initiator information for the configured iSCSI initiator.
show iscsi initiator detail	Displays detailed iSCSI initiator information.
show iscsi initiator summary	Displays iSCSI initiator summary information.
islb initiator	Assigns an iSLB name and IP address to the iSLB initiator and enters iSLB initiator configuration submode.
show islb initiator	Displays iSLB initiator information.
show islb initiator configured	Displays iSLB initiator information for the specified configured initiator.
show islb initiator detail	Displays detailed iSLB initiator information.
show islb initiator summary	Displays iSLB initiator summary information.

stop

To stop SCSI commands in progress on a SAN tuner extension N port, use the **stop** command.

stop {**all** | **command-id** *cmd-id*}

Syntax Description

all	Stops all SCSI commands.
command-id *cmd-id*	Stop a specific SCSI command identified by the command number. The range is 0 to 2147483647.

Defaults

None.

Command Modes

SAN extension N port configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example stops all SCSI command on a SAN extension tuner N port.

```
switch# san-ext-tuner
switch(san-ext)# nWWN 10:00:00:00:00:00:00:00
switch(san-ext)# nport pwwn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2
switch(san-ext-nport)# stop all
```

The following example stops a specific SCSI command on a SAN extension tuner N port.

```
switch# san-ext-tuner
switch(san-ext)# nWWN 10:00:00:00:00:00:00:00
switch(san-ext)# nport pwwn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2
switch(san-ext-nport)# stop command-id 100
```

Related Commands

Command	Description
nport pwwn	Configures a SAN extension tuner N port.
read command-id	Configures a SCSI read command for a SAN extension tuner N port.
san-ext-tuner	Enables the SAN extension tuner feature.
show san-ext-tuner	Displays SAN extension tuner information.
write command-id	Configures a SCSI write command for a SAN extension tuner N port.

streetaddress

To configure the street address with the Call Home function, use the **streetaddress** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

streetaddress *street-address*

no streetaddress *street-address*

Syntax Description

street-address	(Optional). Configures the customer's street address where the equipment is located. Allows up to 256 alphanumeric characters in free format for the street number, city, state, and zip (combined).

Defaults

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the street address in the Call Home configuration.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# streetaddress 1234 Picaboo Street, AnyCity, AnyState, 12345
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

suspend

To suspend a switched port analyzer (SPAN) session, use the **suspend** command in SPAN session configuration submode. To disable the suspension, use the **no** form of the command.

suspend

no suspend

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

SPAN session configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to suspend a SPAN session.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# span session 1
switch(config-span)# suspend
switch(config-span)# do show span session 1
Session 1 (admin suspended)
   Destination is not configured
   No session filters configured
   Ingress (rx) sources are
     fc3/13,
   Egress (tx) sources are
     fc3/13,

switch(config-span)#
```

The following example shows how to disable the suspension of the SPAN session.

```
switch(config-span)# no suspend
```

Related Commands

Command	Description
switchport	Configures the switch port mode on the Fibre Channel interface.
span session	Selects or configures the SPAN session and changes to SPAN configuration submode.
destination interface	Configures a SPAN destination interface.
source	Configures a SPAN source.
show span session	Displays specific information about a SPAN session.

switch-priority

To configure the switch priority with the Call Home function, use the **switch-priority** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

switch-priority *priority-value*

no switch-priority *priority-value*

Syntax Description

priority-value	(Optional). Configures the switch priority. Specifies a priority value. 0 is the highest priority and 7 the lowest.

Defaults

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the switch priority in the Call Home configuration.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# switch-priority 0
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

switch-wwn

To configure a switch WWN in an autonomous fabric ID (AFID) database, use the **switch-wwn** command in AFID database configuration submode. To disable this feature, use the **no** form of this command.

switch-wwn *wwn-id* {**autonomous-fabric-id** *fabric-id* **vsan-ranges** *vsan-range* | **default-autonomous-fabric-id** *fabric-id* **vsan-ranges** *vsan-range*}

no switch-wwn *wwn-id* {**autonomous-fabric-id** *fabric-id* **vsan-ranges** *vsan-range* | **default-autonomous-fabric-id** *fabric-id* **vsan-ranges** *vsan-range*}

Syntax Description

wwn-id	Specifies the port WWN, with the format *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
autonomous-fabric-id *fabric-id*	Specifies the fabric ID for the IVR topology.
vsan-ranges *vsan-range*	Specifies the IVR VSANs or range of VSANs. The range of values for a VSAN ID is 1 to 4093.
default-autonomous-fabric-id *fabric-id*	Specifies the default fabric ID for the IVR topology.

Defaults

Disabled.

Command Modes

AFID database configuration submode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

Using the **default-autonomous-fabric-id** keyword configures the default AFID for all VSANs not explicitly associated with an AFID.

Examples

The following example shows adds a switch WWN, AFID, and range of VSANs to the AFID database.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr vsan-topology auto
switch(config)# autonomous-fabric-id database
switch(config-afid-db)# switch-wwn 28:1d:00:05:30:00:06:ea autonomous-fabric-id 14
vsan-ranges 1-4
```

The following example shows adds a switch WWN and the default AFID to the AFID database.

```
switch(config-afid-db)# switch-wwn 28:1d:00:05:30:00:06:ea default-autonomous-fabric-id 16
```

Related Commands

Command	Description
autonomous-fabric-id-database	Enters AFID database configuration submode.
show autonomous-fabric-id-database	Displays the contents of the AFID database.

switchname

To change the name of the switch, use the **switchname** command in configuration mode. To revert the switch name to the default name, use the **no** form of the command.

switchname *name*

no switchname

Syntax Description

name	Specifies a switch name. Maximum length is 32 characters.

Defaults

switch

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example changes the name of the switch to myswitch1.

```
switch# config terminal
switch(config)# switchname myswitch1
myswitch1(config)#
myswitch1(config)# no switchname
switch(config)#
```

Related Commands

Command	Description
snmp-server	Sets the contact information, switch location, and switch name within the limit of 20 characters (without spaces).

switchport

To configure a switch port parameter on a Fibre Channel, Gigabit Ethernet, or management interface, use the **switchport** command in interface configuration submode. To discard the configuration, use the **no** form of the command.

Fibre Channel Interface

switchport {**beacon** |
description *text* |
encap eisl |
fcbbscn |
fcrxbbcredit {*credit* [**mode** {**E** | **Fx**}] | **default** | **extended** *credit* | **performance-buffers** {*buffers* | **default**}} |
fcrxbufsize *size* |
mode {**auto** | **E** | **F** | **FL** | **Fx** | **SD** | **ST** | **TL**} |
rate-mode {**dedicated** | **shared**} |
speed {**1000** | **2000** | **4000** | **auto** [**max 2000**]} |
trunk {**allowed vsan** {[**add**] *vsan-id* | **all**} | **mode** {**auto** | **off** | **on**}}}

no switchport {**beacon** | **description** *text* | **encap eisl** | **fcrxbbcredit** [**extended** *credit*] | **fcrxbufsize** *size* | **mode** | **rate-mode** | **speed** | **trunk allowed vsan** [[**add**] *vsan-id* | **all**]}

Gigabit Ethernet Interface

switchport {**auto-negotiate** |
beacon |
description *text* |
mtu |
promiscuous-mode {**off** | **on**}}

no switchport {**auto-negotiate** | **beacon** | **description** *text* | **mtu** | **promiscuous-mode**}

Management Interface

switchport {**description** *text* |
duplex {**auto** | **full** | **half**} |
speed {**10** | **100** | **1000**}}

no switchport {**description** *text* | **duplex** | **speed**}

Syntax Description

beacon	Enables the beacon for the interface.
description *text*	Specifies the interface description. Maximum length is 80 characters.
encap eisl	Configures extended ISL (EISL) encapsulation for the interface.
fcbbscn	Enables or disables buffer-to-buffer state change notification.
fcrxbbcredit	Configures receive BB_credit for the port.
credit	Specifies receive BB_credit. The range is 1 to 255
mode	Configures receive BB_credit for the specific port mode.
E	Configures receive BB_credit for E or TE port mode.
Fx	Configures receive BB_credit for F or FL port mode.

default	Configures default receive BB_credits depending on the port mode and capabilities.
extended *credit*	Specifies extended receive BB_credits. The range is 256 to 4095.
performance-buffers {*buffers* | **default**}	Specifies receive BB_credit performance buffers. The range is 1 to 145. The default value is determined by a built-in algorithm.
fcrxbufsize *size*	Specifies receive data field size for the interface. The range is 256 to 2112 bytes.
mode	Configures the port mode.
auto	Configures autosense mode.
E	Configures E port mode.
F	Configures F port mode.
FL	Configures FL port mode.
Fx	Configures Fx port mode.
SD	Configures SD port mode.
ST	Configures ST port mode.
TL	Configures TL port mode.
rate-mode	Configures the rate mode for an interface.
dedicated	Specifies dedicated bandwidth for the port.
shared	Specifies shared bandwidth for the port.
speed	Configures the port speed.
1000	Configures 1000-Mbps speed.
2000	Configures 2000-Mbps speed.
4000	Configures 4000-Mbps speed.
auto	Configures autosense speed.
max 2000	Configures 2-Gbps as the maximum bandwidth reserved in auto mode for 24-port and 48-port 4-Gbps switching module interfaces.
trunk	Configures trunking parameters on the interface.
allowed	Specifies the allowed list for interface(s).
vsan	Configures the VSAN range.
add	Adds the VSAN ID to the range of allowed VSAN list
vsan-id	Specifies the VSAN ID. The range is 1 to 4093.
all	Adds all the VSANs to allowed VSAN list.
mode	Configures the trunking mode.
auto	Configures automatic trunking mode.
off	Disables the trunking mode.
on	Enables the trunking mode.
auto-negotiate	Configures the switch to use the negotiation protocol on the interface.
mtu	Configures the maximum transmission unit (MTU) for the port.
promiscuous-mode	Configures promiscuous mode for the port.
off	Disables promiscuous mode.
on	Enables promiscuous mode.
duplex	Configures the port duplex mode.

auto	Configures auto negotiate duplex mode.
full	Specifies full duplex mode
half	Configures half duplex mode.
10	Configures 10-Mbps port speed.
100	Configures 100-Mbps port speed.
1000	Configures 1000-Mbps port speed.

Defaults

The beacon is disabled.

The EISL encapsulation is disabled.

The default receive data buffer size is 2112 bytes.

The port mode is **auto**.

The speed is **auto**.

The maximum auto speed is **2000**.

The trunk mode is **on**.

The rate mode is **shared**.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.
2.0(1b)	Added the **extended** option to the **fcrxbbcredit** keyword.
3.0(1)	• Added the **fcbbscn** option. • Added the **ST** option to the **mode** keyword. • Added the **4000** option to the **speed** keyword. • Added the **auto max 2000** option to the **speed** keyword. • Added the **rate-mode** keyword. • Added the Gigabit Ethernet interface syntax. • Added the management interface syntax.

Usage Guidelines

You can specify a range of interfaces by issuing a command with the following example format:

interface*space***fc1/1***space***-***space***5***space***,***space***fc2/5***space***-***space***7**

Tip The **shutdown** or **no shutdown** command for the FCIP or iSCSI interfaces is automatically issued when you change the MTU size—you do not need to explicitly issue this command.

You must perform the **fcrxbbcredit extended enable** command in configuration mode to use the **switchport fcrxbbcredit extended** command in interface configuration submode to enable extended BB_credits on a Fibre Channel interface.

The port speed on an interface, combined with the rate mode, determines the amount of shared resources available to the ports in the port group. Especially in the case of dedicated rate mode, the port group resources are reserved even though the bandwidth is not used. For example, if an interface is configured for autosensing (**auto**), then 4 Gbps of bandwidth is reserved even though the maximum operating speed is 2 Gbps. For the same interface, if autosensing with a maximum speed of 2 Gbps (**auto max 2000**) is configured, then only 2 Gbps of bandwidth is reserved and the unused 2 Gbps is shared with the other interface in the port group.

Note The 4-port 10-Gbps switching module only supports 10-Gbps traffic.

Table 21-1 lists the default configurations, credits, and buffers for switching modules.

Table 21-1 Default Configurations, Credits, and Buffers

Switching Module	Speed	Port Mode	Rate Mode	Credits Min/Max/Default
12 port	Auto[1]	Auto[2]	Dedicated	2/250/250
24 port	Auto[1]	Fx	Shared	1/16/16
			Dedicated	1/250/16
		Auto	Dedicated	2/250/250
48 port	Auto[1]	Fx	Shared	1/16/16
			Dedicated	1/250/16
		Auto	Dedicated	2/250/125
4 port	Auto[3]	Auto[2]	Auto	2/250/250

1. Auto speed negotiates to 1-, 2-, or 4-Gbps.
2. Auto port mode can operate as an E, TE, or Fx port.
3. Auto speed for a 4-port module negotiates to 10-Gbps.

When configuring port modes, observe the following guidelines:

- Auto port mode and E port mode cannot be configured in shared rate mode.
- The 4-port 10-Gbps module does not support FL port mode.
- Generation 2 modules do not support TL port mode.
- Shared to dedicated ports should be configured in this order: speed, rate mode, port mode, credit.
- Dedicated to shared ports should be configured in this order: credit, port mode, rate mode, speed.

When configuring PortChannels, observe the following guidelines:

- When an interface is out-of-service, it cannot be part of a PortChannel.
- The 24-port module and the 48-port module support making ports out-of-service. In a shared resource configuration, an out-of-service port reverts to its default values when it comes back into service.
- The maximum number of PortChannels for Generation-2 modules is 256.

- The maximum number of PortChannels for a mixture of Generation-1 and Generation-2 modules is 128.
- The number of PortChannels is independent of the type of supervisor module.
- When adding a PortChannel to a configuration that uses both Generation-1 and Generation-2 modules, configure the PortChannel and Generation-2 interface speed to **auto max 2000**.
- When using the force option to add a PortChannel to a configuration that uses both Generation-1 and Generation-2 modules, follow these guidelines:
  - Configure the PortChannel interface speed to **auto max 2000**, or add the Generation-1 interfaces followed by the Generation-2 interfaces.
  - Generation-1 interfaces do not support the **auto max 2000** speed.
  - The force addition can fail for a Generation-2 interface if resources are unavailable.

Examples

The following example configures switch port parameters for a Fibre Channel interface.

```
switch# config terminal
switch(config)# interface fc 1/23
switch(config-if)# switchport description techdocsSample
switch(config-if)# switchport mode E
switch(config-if)# switchport trunk mode auto
switch(config-if)# switchport trunk allowed vsan all
switch(config-if)# switchport trunk allowed vsan 3
switch(config-if)# switchport trunk allowed vsan add 2
switch(config-if)# switchport encap eisl
switch(config-if)# switchport fcrxbbcredit performance-buffers 45
switch(config-if)# switchport proxy-initiator nWWN 11:11:11:11:11:11:11:11 pwwn
22:22:22:22:22:22:22:22
switch(config-if)# no switchport proxy-initiator nWWN 11:11:11:11:11:11:11:11 pwwn
22:22:22:22:22:22:22:22
switch(config-if)# switchport fcrxbbcredit extended 2000
```

The following example configures the port speed of a Fibre Channel interface and enables autosensing on the interface.

```
switch# config terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport speed 4000
switch(config-if)# switchport speed auto
```

The following example reserves dedicated bandwidth for the interface.

```
switch(config-if)# switchport rate-mode dedicated
```

The following example reserves shared (default) bandwidth for the interface.

```
switch(config-if)# switchport rate-mode shared
```

Related Commands

Command	Description
fcrxbbcredit extended enable	Enables extended BB_credits on the switch.
show interface	Displays an interface configuration for a specified interface.

switchport auto-negotiate

To configure auto-negotiation in Gigabit Ethernet interfaces, use the **switchport auto-negotiate** command in configuration mode. Use the **no** form of the command to delete the configured switch port information.

switchport auto-negotiate

no switchport auto-negotiate

Syntax Description

switchport	Configures switch port parameters.
auto-negotiate	Automatically negotiates the speed, pause method, and duplex of incoming signals based on the link partner.

Defaults

Enabled

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

You can configure the **auto-negotiate** option for a specified Gigabit Ethernet interface. By default, the port is configured to auto-negotiate. By configuring auto-negotiation, the port automatically detects the speed or pause method, and duplex of incoming signals and synchronizes with them.

Access this command from the `switch(config-if)#` submode for Gigabit Ethernet interfaces.

Examples

The following example configures auto-negotiation on a Gigabit Ethernet interface.

```
switch# config t
switch(config)# interface gigabitethernet 8/1
switch(config-if)# switchport auto-negotiate
```

The following example disable auto-negotiation on a Gigabit Ethernet interface.

```
switch(config-if)# no switchport auto-negotiate
```

Related Commands

Command	Description
show interface gigabitethernet	Displays an interface configuration for a specified Gigabit Ethernet interface.

switchport ignore bit-errors

To prevent the detection of bit error threshold events from disabling the interface, use the **switchport ignore bit-errors** command. To revert to the default, use the **no** form of the command.

switchport ignore bit-errors

no switchport ignore bit-errors

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

The bit error rate threshold is used by the switch to detect an increased error rate before performance degradation seriously affects traffic.

Bit errors can occur for the following reasons:

- Faulty or bad cable
- Faulty or bad GBIC or SFP
- GBIC or SFP is specified to operate at 1 Gbps but is used at 2 Gbps
- Short haul cable is used for long haul or long haul cable is used for short haul
- Momentary sync loss
- Loose cable connection at one or both ends
- Improper GBIC or SFP connection at one or both ends

A bit error rate threshold is detected when 15 error bursts occur in a 5-minute period. By default, the switch disables the interface when the threshold is reached. You can issue a **shutdown/no shutdown** command sequence to reenable the interface.

Note Regardless of the setting of the **switchport ignore bit-errors** command, the switch generates a syslog message when bit error threshold events are detected.

Examples

The following example shows how to prevent the detection of bit error events from disabling the interface.

```
switch# config t
switch(config)# interface fc1/1
switch(config-if)# switchport ignore bit-errors
```

The following example shows how to allow the detection of bit error events from disabling the interface.

```
switch# config t
switch(config)# interface fc1/1
switch(config-if)# no switchport ignore bit-errors
```

Related Commands

Command	Description
show interface	Displays interface information.

switchport ingress-rate

To configure the port rate limit for a specified interface, use the **switchport ingress-rate** command in interface configuration mode. Use the **no** form of the command to delete the configured switch port information.

switchport ingress-rate *limit*

no switchport ingress-rate *limit*

Syntax Description

limit	Specifies the ingress rate limit as a percentage. The range is 1 to 100.

Defaults

Disabled

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Access this command from the `switch(config-if)#` submode. This command is only available if the following conditions are true:

- The QoS feature is enabled using the **qos enable** command.
- The command is issued in a Cisco MDS 9100 series switch.

Examples

The following example configures the ingress rate limit on a Fibre Channel interface.

```
switch# config terminal
switch(config)# interface fc 2/5
switch(config-if)# switchport ingress-rate 5
```

Related Commands

Command	Description
show interface fc	Displays an interface configuration for a specified Fibre Channel interface.

switchport initiator id

To configure the iSCSI initiator ID mode, use the **switchport initiator id** command in interface configuration submode. To delete the configured switch port information, use the **no** form of the command.

switchport initiator id {**ip-address** | **name**]

no switchport initiator id {**ip-address** | **name**}

Syntax Description

ip-address	Identifies initiators using the IP address.
name	Identifies initiators using the specified name.

Defaults

Disabled

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Access this command from the `switch(config-if)#` submode.

Examples

The following example configures the switch port initiator ID mode for a iSCSI interface.

```
switch# config terminal
switch(config)# interface iscsi 2/5
switch(config-if)# switchport initiator id ip-address
switch(config-if)# switchport initiator name
```

Related Commands

Command	Description
show interface iscsi	Displays an interface configuration for a specified iSCSI interface.

switchport promiscuous-mode

To configure the promiscuous-mode in Gigabit Ethernet interfaces, use the **switchport promiscuous-mode** command in interface configuration submode. Use the **no** form of the command to delete the configured switch port information.

switchport promiscuous-mode {**off** | **on**}

no switchport promiscuous-mode

Syntax Description

off	Disables promiscuous mode.
on	Enables promiscuous mode.

Defaults

Disabled

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Access this command from the `switch(config-if)#` submode for Gigabit Ethernet interfaces.

Examples

The following example enables promiscuous mode on a Gigabit Ethernet interface.

```
switch# config terminal
switch(config)# interface gigabitethernet 8/1
switch(config-if)# switchport promiscuous-mode on
```

The following example disables promiscuous mode on a Gigabit Ethernet interface.

```
switch(config-if)# switchport promiscuous-mode off
```

The following example disables promiscuous mode on a Gigabit Ethernet interface.

```
switch(config-if)# no switchport promiscuous-mode
```

Related Commands

Command	Description
show interface gigabitethernet	Displays an interface configuration for a specified Gigabit Ethernet interface.

switchport proxy-initiator

To configure the iSCSI proxy initiator mode, use the **switchport proxy-initiator** command in interface configuration submode. To delete the configured switch port proxy initiator mode, use the **no** form of the command.

switchport proxy-initiator [**nwwn** *wwn* **pwwn** *wwn*]

no switchport proxy-initiator [**nwwn** *wwn* **pwwn** *wwn*]

Syntax Description

nwwn *wwn*	Specifies the node WWN.
pwwn *wwn*	Specifies the port WWN.

Defaults

Disabled.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Access this command from the `switch(config-if)#` submode.

When you do not include the WWNs in the command, the IPS port dynamically assigns a pWWN and nWWN to the proxy initiator.

Caution Enabling proxy initiator mode on an iSCSI interface that is part of an iSLB VRRP group impacts load balancing on the interface.

Examples

The following example configures the switch port proxy initiator mode for a iSCSI interface using WWNs.

```
switch# config terminal
switch(config)# interface iscsi 2/5
switch(config-if)# switchport proxy-initiator nwwn 11:11:11:11:11:11:11:11 pwwn
22:22:22:22:22:22:22:22
```

The following example configures the switch port proxy initiator mode for a iSCSI interface without WWNs.

```
switch# config terminal
switch(config)# interface iscsi 2/5
switch(config-if)# switchport proxy-initiator
```

The following example deletes the switch port proxy initiator mode for a iSCSI interface.

```
switch(config-if)# switchport proxy-initiator
```

Related Commands

Command	Description
show interface iscsi	Displays an interface configuration for a specified iSCSI interface.

system cores

To enable copying the core and log files periodically, use the **system cores** command in configuration mode. To revert the switch to factory defaults, use the **no** form of the command.

system cores {**slot0:** | **tftp:**}

no system cores

Syntax Description

slot0	Selects destination file system.
tftp:	Selects destination file system.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Create any required directory before issuing this command. If the directory specified by this command does not exist, the switch software logs a syslog message each time a copy cores is attempted.

Examples

The following example enables periodic copying core and log files.

```
switch# config terminal
switch(config)# system cores slot0:coreSample
```

The following example disables periodic copying core and log files.

```
switch(config)# no system cores
switch(config)#
```

Related Commands

Command	Description
show system cores	Displays the currently configured scheme for copying cores.

system default switchport

To configure default values for various switch port attributes, use the **system default switchport** command in configuration mode. To revert to the default, use the **no** form of the command.

system default switchport {shutdown | trunk {mode auto | off | on}}

no system default switchport shutdown

Syntax Description

shutdown	Disables or enables switch ports by default.
trunk	Configures trunking parameters as a default.
mode	Configures trunking mode.
auto	Sets autosense trunking.
off	Disables trunking.
on	Enables trunking.

Defaults

Enabled

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Attributes configured using this command are applied globally to all future switch port configurations, even if you do not individually specify them at that time.

Examples

The following example configures default values for switch port attributes.

```
switch# config terminal
switch(config)# system default switchport shutdown
switch(config-if)#
switch(config)# no system default switchport shutdown
switch(config-if)#
switch(config)# system default switchport trunkmode auto
switch(config-if)#
```

Related Commands

Command	Description
show system default switchport	Displays default values for switch port attributes.

system default zone default-zone permit

To configure default values for a zone, use the **system default zone default-zone permit** command in configuration mode. To revert to the defaults, use the **no** form of the command.

system default zone default-zone permit

no system default zone default-zone permit

Syntax Description

This command has no arguments or keywords.

Defaults

Default zone: deny.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

This command defines the default values for the default zone for all VSANs. The default values are used when you initially create a VSAN and it becomes active. If you do not want to use the default values, use the **zone default-zone permit vsan** command to define the operational values for the default zone.

The **system default zone default-zone permit** command should only be used in conjunction with VSANs that have not yet been created; it has no effect on existing VSANs.

Note Because VSAN 1 is the default VSAN and is always present, this command has no effect on it.

Examples

The following example sets the default zone to use the default values.

```
switch# config terminal
switch(config)# system default zone default-zone permit
```

The following example restores the default setting (deny).

```
switch(config)# no system default zone default-zone permit
```

Related Commands

Command	Description
zone default-zone permit vsan	Defines whether a default zone (nodes not assigned a created zone) permits or denies access to all in the default zone.
show system default zone	Displays default values for the default zone.

system default zone distribute full

To configure default values for distribution to a zone set, use the **system default zone distribute full** command in configuration mode. To revert to the defaults, use the **no** form of the command.

system default zone distribute full

no system default zone distribute full

Syntax Description

This command has no arguments or keywords.

Defaults

Distribute: active only.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

This command distributes the default values for the default zone to all VSANs. The default values are used when you initially create a VSAN and it becomes active. If you do not want to use the default values, use the **zoneset distribute full vsan** command to distribute the operational values for the default zone.

The **system default zone distribute full** command should only be used in conjunction with VSANs that have not yet been created; it has no effect on existing VSANs.

Note Because VSAN 1 is the default VSAN and is always present, this command has no effect on it.

Examples

The following example distributes the default values to the full zone set.

```
switch# config terminal
switch(config)# system default zone distribute full
```

The following example distributes default values to the active zone set only (default).

```
switch(config)# no system default zone distribute full
```

Related Commands

Command	Description
zoneset distribute full vsan	Distributes the operational values for the default zone to all zone sets.
show system default zone	Displays default values for the default zone.

system hap-reset

To configure the HA reset policy, use the **system hap-reset** command in EXEC mode. Use the **no** form of this command to disable this feature.

system hap-reset

system no hap-reset

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can disable the HA policy supervisor reset feature (enabled by default) for debugging and troubleshooting purposes.

Examples

The following example enables the supervisor reset HA policy.

```
switch# system hap-reset
```

system health

To configure Online Health Management System (OHMS) features for a specified interface or for the entire switch, use the **system health** command. To disable this feature, use the **no** form of the command.

system health [**failure-action** | **interface** {**fc** *slot*/*port* | **iscsi** *slot*/*port*} | **loopback** {**frame-length** {*bytes* | **auto**} | **frequency** *seconds*}]

no system health [**failure-action** | **interface** {**fc** *slot*/*port* | **iscsi** *slot*/*port*}]

Syntax Description

failure-action	Prevents the SAN-OS software from taking any OHMS action for the entire switch.
interface	Configures an interface.
fc *slot*/*port*	Specifies the Fibre Channel interface to configure by slot and port number.
iscsi *slot*/*port*	Specifies the iSCSI interface to configure by slot and port number.
loopback	Configures the OHMS loopback test.
frame-length *bytes*	Specifies the frame-length in bytes ranging from 0 to 128 bytes for the loopback test.
auto	Configures the frame-length to auto for the loopback test.
frequency *seconds*	Specifies the loopback frequency in seconds ranging from 5 seconds (default) to 255 seconds.

Defaults

Enabled.
Frame-length: Auto-size (which could be 0 to 128).

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(4)	This command was introduced.
3.0(1)	Added the **frame-length** and **auto** options to the **loopback** keyword.

Usage Guidelines

If you do not configure the loopback frequency value, the default frequency of 5 seconds is used for all modules in the switch.

Note The **no** form of the command is not supported for the **frame-length**, **auto**, and **frequency** options.

Examples

The following example disables OHMS in this switch.

```
switch# config terminal
switch(config)# no system health
System Health is disabled.
```

The following example enables (default) OHMS in this switch.

```
switch(config)# system health
System Health is enabled.
```

The following example enables OHMS in this interface.

```
switch(config)# no system health interface fc8/1
System health for interface fc8/13 is enabled.
```

The following example disables OHMS in this interface.

```
switch(config)# system health interface fc8/1
System health for interface fc8/13 is disabled.
```

The following example configures the loopback frequency to be 50 seconds for any port in the switch.

```
switch(config)# system health loopback frequency 50
The new frequency is set at 50 Seconds.
```

The following example configures the loopback frame-length to auto.

```
switch(config)# system health loopback frame-length auto
Loopback frame-length auto-size mode is now enabled.
```

The following example prevents the switch from taking any failure action.

```
switch(config)# system health failure-action
System health global failure action is now enabled.
```

The following example prevents the switch configuration from taking OHMS action (default) in case of a failure.

```
switch(config)# no system health failure-action
System health global failure action now disabled.
```

Related Commands

Command	Description
system health external-health	Explicitly runs an external Online Health Management System (OHMS) loopback test on demand for a specified interface or module.
system health internal-loopback	Explicitly runs an internal OHMS loopback test on demand for a specified interface or module.
system health serdes-loopback	To explicitly run an internal OHMS Serializer/Deserializer (Serdes) loopback test on demand for a Fibre Channel interface.

system health clear-errors

To clear previous error conditions stored in the Online Health Management System (OHMS) application's memory, use the **system health clear-errors** command.

system health clear-errors interface {**fc** *slot/port* | **iscsi** *slot/port*}

system health clear-errors module *slot* [**battery-charger** | **bootflash** | **cache-disk** | **eobc** | **inband** | **loopback** | **mgmt**]

Syntax Description

interface	Specifies the interface to be configured.
fc *slot/port*	Configures the Fiber Channel interface.
iscsi *slot/port*	Selects the iSCSI interface to configure.
module *slot*	Specifies the required module in the switch,
battery-charger	Configure the OHMS battery-charger test on the specified module
bootflash	Configures the OHMS bootflash test on the specified module.
cache-disk	Configures the OHMS cache-disk test on the specified module.
eobc	Configures the OHMS EOBC test on the specified module.
inband	Configures the OHMS inband test on the specified module.
loopback	Configures the OHMS loopback test on the specified module.
mgmt	Configures the OHMS management port test on the specified module.

Defaults

Enabled

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

You can clear the error history for Fibre Channel interfaces, iSCSI interfaces, for an entire module, or one particular test for an entire module. The **battery-charger**, the **bootflash**, the **cache-disk**, the **eobc**, the **inband**, the **loopback**, and the **mgmt** test options can be individually specified for a given module.

The management port test cannot be run on a standby supervisor module.

Examples

The following example clears the error history for the specified Fibre Channel interface:

```
switch# system health clear-errors interface fc 3/1
```

The following example clears the error history for the specified module:

```
switch# system health clear-errors interface module 3
```

The following example clears the management port test error history for the specified module:

```
switch# system health clear-errors module 2 mgmt
```

system health external-loopback

To explicitly run an external Online Health Management System (OHMS) loopback test on demand (when requested by the user) for a specified interface or module, use the **system health external-loopback** command.

system health external-loopback {interface fc *slot*/*port* **| source interface fc** *slot*/*port* **destination fc** *slot*/*port*} [**frame-length** *bytes* **[frame-count** *number*] **| frame-count** *number*] **[force**]

Syntax Description

interface	Configures an interface.
fc *slot*/*port*	Configures the Fibre Channel interface specified by the slot and port.
source	Specifies the source Fibre Channel interface.
destination	Specifies the destination Fibre Channel interface.
frame-length *bytes*	Configures the specified length of the loopback test frame in bytes. The range is 0 to 128 bytes.
frame-count *number*	Configures the specified number of frames for the loopback test. The number of frames can range from 1 to 32.
force	Directs the software to use the non-interactive loopback mode.

Defaults

Loopback: disabled.
Frame-length: 0.
Frame-count: 1.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.
3.0(1)	Added the **source** and **destination** keywords and the **frame-count** and **frame-length** options.

Usage Guidelines

Use this command to run this test on demand for the external devices connected to a switch that are part of a long haul network.

Examples

The following example displays an external loopback command for a Fibre Channel interface.

```
switch# system health external-loopback interface fc 3/1
This will shut the requested interfaces Do you want to continue (y/n)?  [n] y
External loopback test on interface fc3/1 was  successful.
```

The following example displays the effect of the **force** option when implementing a forced loopback.

```
switch# system health external-loopback interface fc 3/1 force
External loopback test on interface fc3/1 was  successful.
```

Related Commands

Command	Description
system health	Configures Online Health Management System (OHMS) features for a specified interface or for the entire switch.
system health internal-loopback	Explicitly runs an internal OHMS loopback test on demand for a specified interface or module.
system health serdes-loopback	To explicitly run an internal OHMS Serializer/Deserializer (Serdes) loopback test on demand for a Fibre Channel interface.

system health internal-loopback

To explicitly run an internal Online Health Management System (OHMS) loopback test on demand (when requested by the user) for a specified interface or module, use the **system health internal-loopback** command.

system health internal-loopback interface {**fc** *slot*/*port* | **iscsi** *slot*/*port*} [**frame-length** *bytes* [**frame-count** *number*] | **frame-count** *number*]

Syntax Description

interface	Configures an interface.
fc *slot*/*port*	Configures the Fibre Channel interface specified by the slot and port.
iscsi *slot*/*port*	Specifies the iSCSI interface to configure by slot and port.
frame-length *bytes*	Configures the specified length of the loopback test frame in bytes. The range is 0 to 128 bytes.
frame-count *number*	Configures the specified number of frames for the loopback test. The number of frames can range from 1 to 32.

Defaults

Loopback: disabled.
Frame-length: 0.
Frame-count: 1.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.
3.0(1)	Added the **frame-count** and **frame-length** options.

Usage Guidelines

Internal loopback tests send and receive FC2 frames to and from the same ports and provide the round trip time taken in microseconds for the Fibre Channel interface.

Examples

The following example performs the internal loopback test for a Fibre Channel interface.

```
switch# system health internal-loopback interface iscsi 8/1
Internal loopback test on interface iscsi 8/1 was successful.
Round trip time taken is 79 useconds
```

Related Commands

Command	Description
system health	Configures Online Health Management System (OHMS) features for a specified interface or for the entire switch.
system health external-loopback	Explicitly runs an external OHMS loopback test on demand for a specified interface or module.
system health serdes-loopback	To explicitly run an internal OHMS Serializer/Deserializer (Serdes) loopback test on demand for a Fibre Channel interface.

system health module

To configure Online Health Management System (OHMS) features for a specified module, use the **system health module** command. Use the **no** form of this command to disable this feature.

system health module *slot*
[**battery-charger** [**failure-action** | **frequency** *seconds*] |
bootflash [**failure-action** | **frequency** *seconds*] |
cache-disk [**failure-action** | **frequency** *seconds*] |
eobc [**failure-action** | **frequency** *seconds*] |
failure-action |
inband [**failure-action** | **frequency** *seconds*] |
loopback [**failure-action**] |
mgmt [**failure-action** | **frequency** *seconds*]]

no system health module *slot*
[**battery-charger** [**failure-action** | **frequency** *seconds*] |
bootflash [**failure-action** | **frequency** *seconds*] |
cache-disk [**failure-action** | **frequency** *seconds*] |
eobc [**failure-action** | **frequency** *seconds*] |
failure-action |
inband [**failure-action** | **frequency** *seconds*] |
loopback [**failure-action**] |
mgmt [**failure-action** | **frequency** *seconds*]]

Syntax Description

module *slot*	Specifies the required module in the switch,
battery-charger	Configure the OHMS battery-charger test on the specified module
frequency *seconds*	Specifies the loopback frequency in seconds loopback frequency ranging from 5 seconds (default) to 255 seconds. **Note** The frequency range for bootflash is 10 seconds (default) to 255 seconds. This range applies only to the bootflash test.
failure-action	Prevents the SAN-OS software from taking any OHMS action for the specified module.
bootflash	Configures the OHMS bootflash test on the specified module.
cache-disk	Configures the OHMS cache-disk test on the specified module.
eobc	Configures the OHMS EOBC test on the specified module.
inband	Configures the OHMS inband test on the specified module.
loopback	Configures the OHMS loopback test on the specified module.
mgmt	Configures the OHMS management port test on the specified module.

Defaults

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

If you do not configure the loopback frequency value, the default frequency of 5 seconds is used for all modules in the switch.

Examples

The following example enables the battery-charger test on both batteries in the CSM module residing in slot 6. If the switch does not have a CSM, this message is issued,

```
switch# config terminal
switch(config)# system health module 6 battery-charger
battery-charger test is not configured to run on module 6.
```

The following example enables the cache-disk test on both disks in the CSM module residing in slot 8. If the switch does not have a CSM, this message is issued,

```
switch(config)# system health module 6 cache-disk
cache-disk test is not configured to run on module 6.
```

The following example enables the bootflash test on Module 6.

```
switch(config)# system health module 6 bootflash
System health for module 6 Bootflash is already enabled.
```

The following example enables you to prevent the SAN-OS software from taking any OHMS action if any component fails in Module 6.

```
switch(config)# system health module 6 bootflash failure-action
System health failure action for module 6 Bootflash test is now enabled.
```

The following example enables an already-enabled bootflash test on Module 6.

```
switch(config)# system health module 6 bootflash failure-action
System health failure action for module 6 Bootflash test is already enabled.
```

The following example disables the bootflash test configuration on Module 6.

```
switch(config)# no system health module 6 bootflash failure-action
System health failure action for module 6 Bootflash test is now disabled.
```

The following example sets the new frequency of the bootflash test on module 6 to 200 seconds.

```
switch(config)# system health module 6 bootflash frequency 200
The new frequency is set at 200 Seconds.
```

The following example enables the EOBC test on Module 6.

```
switch(config)# system health module 6 eobc
System health for module 6 EOBC is now enabled.
```

The following example enables the inband test on Module 6.

```
switch(config)# system health module 6 inband
System health for module 6 EOBC is now enabled.
```

The following example enables the loopback test on Module 6.

```
switch(config)# system health module 6 loopback
System health for module 6 EOBC is now enabled.
```

The following example enables the management test on Module 6.

```
switch(config)# system health module 6 management
System health for module 6 EOBC is now enabled.
```

system health serdes-loopback

To explicitly run an internal Online Health Management System (OHMS) Serializer/Deserializer (Serdes) loopback test on demand (when requested by the user) for a Fibre Channel interface, use the **system health serdes-loopback** command.

system health serdes-loopback interface fc *slot/port* **[frame-length** *bytes* **[frame-count** *number***]** **| frame-count** *number***] [force]**

Syntax Description

interface	Configures an interface.
fc *slot/port*	Configures the Fiber Channel interface specified by the slot and port.
force	Directs the software to use the non-interactive loopback mode.
frame-length *bytes*	Configures the specified length of the loopback test frame in bytes. The range is 0 to 128 bytes.
frame-count *number*	Configures the specified number of frames for the loopback test. The number of frames can range from 1 to 32.

Defaults

Loopback: disabled.
Frame-length: 0.
Frame-count: 1.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example performs a Serdes loopback test within ports for an entire module.

```
switch# system health serdes-loopback interface fc 4/1
This will shut the requested interfaces Do you want to continue (y/n)?  [n] y
Serdes loopback test on interface fc 4/1 was successful.
```

The following example performs a Serdes loopback test within ports for the entire module and overrides the frame count configured on the switch.

```
switch# system health serdes-loopback interface fc 3/1 frame-count 10
This will shut the requested interfaces Do you want to continue (y/n)? [n] y
Serdes loopback test passed for module 3 port 1
```

Related Commands

Command	Description
system health	Configures Online Health Management System (OHMS) features for a specified interface or for the entire switch.
system health external-loopback	Explicitly runs an external OHMS loopback test on demand for a specified interface or module.
system health internal-loopback	To explicitly run an internal OHMS loopback test on demand for a specified interface or module.

system heartbeat

To enable system heartbeat checks, use the **system heartbeat** command in EXEC mode. Use the **no** form of this command to disable this feature.

system heartbeat

system no heartbeat

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can disable the heartbeat checking feature (enabled by default) for debugging and troubleshooting purposes like attaching a GDB to a specified process.

Examples

The following example enables the system heartbeat checks.

```
switch# system heartbeat
```

system memlog

To collect system memory statistics, use the **system memlog** command in EXEC mode.

system memlog

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use this command for debugging and troubleshooting purposes.

Examples

The following example enables system memory logging.

```
switch# system memlog
```

system startup-config

To release a system startup configuration lock, use the **system startup-config** command in EXEC mode.

system startup-config unlock *lock-id*

Syntax Description

unlock *lock-id*	Configures the system startup-config unlock ID number. The range is 0 to 65536.

Defaults

Disabled.

Command Modes

EXEC.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

The **system startup-config** command allows you to unlock or release the rr_token lock. To determine the *lock-id,* use the **show system internal sysmgr startup-config locks** command

Examples

The following example releases the system configuration lock with identifier 1.

```
switch# system startup-config unlock 1
```

Related Commands

Command	Description
show system	Displays system information.

system statistics reset

To reset the high availability statistics collected by the system, use the **system statistics reset** command in EXEC mode.

system statistics reset

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can disable the system statistics reset feature (enabled by default) for debugging and troubleshooting purposes.

Examples

The following example resets the HA statistics.

```
switch# system statistics reset
```

system switchover (EXEC mode)

To specifically initiate a switchover from an active supervisor module to a standby supervisor module, use the **system switchover** command in EXEC mode.

system switchover

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Any switchover function is nonrevertive. Once a switchover has occurred and the failed processor has been replaced or successfully restarted, you cannot switch back to the original, active supervisor module (unless there is a subsequent failure or you issue the **system switchover** command).

Examples

The following example initiates a HA switchover from an active supervisor module to a standby supervisor module.

```
switch# system switchover
```

Related Commands

Command	Description
show version compatibility	Determines version compatibility between switching modules.
show module	Displays the HA-standby state for the standby supervisor module.
show system redundancy status	Determines whether the system is ready to accept a switchover.

system switchover (configuration mode)

To enable a switchover for the system, use the **system switchover** command in configuration mode. To revert to the factory default setting, use the **no** form of the command.

system switchover {**ha** | **warm**}

no system switchover

Syntax Description

ha	Specifies HA switchover.
warm	Specifies warm switchover.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example enables a HA switchover from an active supervisor module to a standby supervisor module.

```
switch# config terminal
switch(config)# system switchover ha
```

system trace

To configure the system trace level, use the **system trace** command in configuration mode. To disable this feature, use the **no** form of the command.

system trace *bit-mask*

no system trace

Syntax Description

bit-mask	Specifies the bit mask to change the trace level.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command is used for debugging purposes.

Examples

The following example shows how to configure the system trace level.

```
switch# config terminal
switch(config)# system trace 0xff
```

system watchdog

To enable watchdog checks, use the **system watchdog** command in EXEC mode. To disable this feature, use the **no** form of the command.

system watchdog

system no watchdog

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

If a watchdog is not logged at every 8 seconds by the software, the supervisor module reboots the switch.

You can disable the watchdog checking feature (enabled by default) for debugging and troubleshooting purposes like attaching a GDB or a kernel GDB (KGDB) to a specified process.

Examples

The following example enables the supervisor reset HA policy.

```
switch# system watchdog
```

CHAPTER 22

Show Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "Command Modes" section to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

show aaa accounting

To display the accounting configuration, use the **show aaa accounting** command.

show aaa accounting

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays accounting log configuration.

```
switch# show aaa accounting
         default: local
```

Related Commands

Command	Description
aaa accounting default	Configure the default accounting method

show aaa authentication

To display configured authentication information, use the **show aaa authentication** command.

show aaa authentication [**login** {**error-enable** | **mschap**}]

Syntax Description

login error-enable	Displays the authentication login error message enable configuration.
login mschap	Displays the authentication login MS-CHAP enable configuration.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.0(1b)	Added the **login error-enable** option.
3.0(1)	Added the **login mschap** option.

Usage Guidelines

None.

Examples

The following example displays the configured authentication parameters.

```
switch# show aaa authentication
         default: group TacServer local none
         console: local
         iscsi: local
         dhchap: local
```

The following example displays the authentication login error message enable configuration.

```
switch# show aaa authentication login error-enable
disabled
```

The following example displays the authentication login MS-CHAP enable configuration.

```
switch# show aaa authentication login mschap
disabled
```

show aaa groups

To display configured server groups, use the **show aaa groups** command.

show aaa groups

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

None.

Examples

To display configured server groups.

```
switch# show aaa groups
radius
TacServer
```

show accounting log

To display the accounting log contents, use the **show accounting log** command.

show accounting log [*size*]

Syntax Description

size	Specifies the size of the log to display in bytes. The range is 0 to 250000.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the entire accounting log.

```
switch# show accounting log
2002:stop:snmp_1033151784_171.71.49.83:admin:
Fri Sep 27 18:36:24 2002:start:_1033151784:root
Fri Sep 27 18:36:28 2002:update:::fcc configuration requested
Fri Sep 27 18:36:33 2002:start:snmp_1033151793_171.71.49.83:admin
Fri Sep 27 18:36:33 2002:stop:snmp_1033151793_171.71.49.83:admin:
Fri Sep 27 18:39:28 2002:start:snmp_1033151968_171.71.49.96:admin
Fri Sep 27 18:39:28 2002:stop:snmp_1033151968_171.71.49.96:admin:
Fri Sep 27 18:39:28 2002:start:_1033151968:root
Fri Sep 27 18:39:31 2002:update:::fcc configuration requested
Fri Sep 27 18:39:37 2002:start:snmp_1033151977_171.71.49.96:admin
Fri Sep 27 18:39:37 2002:stop:snmp_1033151977_171.71.49.96:admin:
Fri Sep 27 18:39:37 2002:start:snmp_1033151977_171.71.49.96:admin
Fri Sep 27 18:42:12 2002:start:snmp_1033152132_171.71.49.96:admin
Fri Sep 27 18:42:12 2002:stop:snmp_1033152132_171.71.49.96:admin:
Fri Sep 27 18:42:12 2002:start:snmp_1033152132_171.71.49.96:admin
Fri Sep 27 18:42:40 2002:start:snmp_1033152160_171.71.49.96:admin
...
```

The following example displays the 400 bytes of the accounting log.

```
switch# show accounting log 400

Tue Dec  8 22:06:59 1981:start:/dev/pts/2_376697219:admin:
Tue Dec  8 22:07:03 1981:stop:/dev/pts/2_376697219:admin:shell terminated
Tue Dec  8 22:07:13 1981:start:/dev/pts/2_376697233:admin:
Tue Dec  8 22:07:53 1981:stop:/dev/pts/2_376697233:admin:shell terminated
Tue Dec  8 22:08:15 1981:update:/dev/ttyS0_376628597:admin:iSCSI Interface Vsan Enabled
```

Related Commands

Command	Description
clear accounting log	Clears the accounting log.

show arp

To display Address Resolution Protocol (ARP) entries, use the **show arp** command.

show arp

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

This displays the ARP table.

```
switch# show arp
Protocol Address           Age (min)      Hardware Addr  Type  Interface
Internet  171.1.1.1        0              0006.5bec.699c  ARPA  mgmt0
Internet  172.2.0.1        4              0000.0c07.ac01  ARPA  mgmt0
```

Related Commands

Command	Description
clear arp-cache	Clears the arp-cache table entries.

show autonomous-fabric-id database

To display the contents of the AFID database, use the **show autonomous-fabric-id database** command in EXEC mode.

show autonomous-fabric-id database

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows contents of the AFID database.

```
switch# show autonomous-fabric-id database
SWITCH WWN                      Default-AFID
------------------------------------------------------------
20:00:00:0c:91:90:3e:80            5


Total:   1 entry in default AFID table

SWITCH WWN                      AFID     VSANS
------------------------------------------------------------
20:00:00:0c:91:90:3e:80           10     1,2,5-8


Total: 1 entry in AFID table
```

Related Commands

Command	Description
autonomous-fabric-id (IVR topology database configuration)	Configures an autonomous fabric ID into the Inter-VSAN Routing (IVR) topology database.

Command	Description
autonomous-fabric-id (IVR service group configuration)	Configures an autonomous fabric ID into the IVR service group.
autonomous-fabric-id-database	Configures an autonomous fabric ID (AFID) database

show banner motd

To display a configured message of the day (MOTD) banner, use the **show banner moted** command.

show banner motd

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

The configured MOTD banner is displayed before the login prompt on the terminal whenever a user logs in to a Cisco MDS 9000 Family switch.

Examples

The following example displays the configured banner message.

```
switch# show banner motd
 Testing the MOTD Feature
```

The configured message is visible the next time you log in to the switch:

```
 Testing the MOTD Feature
switch login:
```

Related Commands

Command	Description
banner motd	Configures the required banner message.

show boot

To display the boot variables or modules, use the **show boot** command.

show boot [**module** [*slot* | *variable-name*] | **sup-1** | **sup-2** | **variables**]

Syntax Description

module	Displays the boot variables for modules.
slot	Specifies a module by the slot number.
variable-name	Specifies the variable. Maximum length is 80 characters.
sup-1	Displays the upper sup configuration.
sup-2	Displays the lower sup configuration.
variables	Displays the list of boot variables.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the current contents of the boot variable.

```
switch# show boot
kickstart variable = bootflash:/kickstart-image
system variable = bootflash:/system-image
Module 2
asm-sfn variable = bootflash:/asm-image
```

The following example displays the images on the specified module.

```
switch# show boot module
Module 2
asm-sfn variable = bootflash:/asm-image
```

The following example displays a list of all boot variables.

```
switch# show boot variables
List of boot variables are:
     asm-sfn
     system
     kickstart
```

show boot auto-copy

To display state of the auto-copy feature, use the **show boot auto-copy** command.

show boot auto-copy [**list**]

Syntax Description

list	Displays the list of files to be auto-copied

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows the message that displays on the console when you enable the auto-copy feature:

```
switch(config)# boot auto-copy
Auto-copy administratively enabled
```

The following example shows the message that displays on the console when you disable the auto-copy feature:

```
switch(config)# boot auto-copy
Auto-copy administratively disabled
```

The following example displays the current state of the auto-copy feature when it is enabled.

```
switch# show boot auto-copy
Auto-copy feature is enabled
```

The following example displays the current state of the auto-copy feature when it is disabled.

```
switch# show boot auto-copy
Auto-copy feature is disabled
```

The following example displays the ilc1.bin image being copied to the standby supervisor module's bootflash, and once this is successful, the next file will be lasilc1.bin. This command only displays files on the active supervisor module.

```
switch# show boot auto-copy list
File: /bootflash/ilc1.bin
Bootvar: ilce

File:/bootflash/lasilc1.bin
Bootvar: lasilc
```

The following example displays a typical message when the auto-copy option is disabled or if no files are copied.

```
switch# show boot auto-copy list
No file currently being auto-copied
```

show callhome

To display Call Home information configured on a switch, use the **show callhome** command.

show callhome [**destination-profile** [**profile** {*profile* | **full-txt-destination** | **short-txt-destination** | **XML-destination**}] | **last** {**action status** | **merge status**} | **pending** | **pending-diff** | **transport-email** | **user-def-cmds**]

Syntax Description

destination-profile	Displays the Call Home destination profile information.
profile	Specifies the destination profile.
profile	Specifies a user-defined destination profile.
full-txt-destination	Specifies the full text destination profile.
short-txt-destination	Specifies the short text destination profile.
XML-destination	Specifies the XML destination profile.
last action status	Displays the status of the last CFS commit or discard operation.
last merge status	Displays the status of the last CFS merge operation.
pending	Displays the status of pending Call Home configuration.
pending-diff	Displays the difference between running and pending Call Home configurations.
transport-email	Displays the Call Home e-mail transport information.
user-def-cmds	Displays the CLI commands configured for each alert group.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
2.0(1b)	Added **last action status**, **pending**, and **pending-diff** options.
3.0(1)	Added the **user-def-cmds** argument.

Usage Guidelines

None.

Examples

The following example displays configured Call Home information.

```
switch# show callhome
callhome enabled
Callhome Information:
contact person name:who@where
contact person's email:person@place.com
contact person's phone number:310-408-4000
```

```
street addr:1234 Picaboo Street, Any city, Any state, 12345
site id:Site1ManhattanNewYork
customer id:Customer1234
contract id:Andiamo1234
switch priority:0
duplicate message throttling : enabled
periodic inventory : disabled
periodic inventory time-period : 7 days
distribution of callhome configuration data using cfs : disabled
```

The following example displays all destination profile information.

```
switch# show callhome destination-profile
XML destination profile information
maximum message size:250000
email addresses configured:
findout@.cisco.com

Short-txt destination profile information
maximum message size:4000
email addresses configured:
person1@epage.company.com

full-txt destination profile information
maximum message size:250000
email addresses configured:
person2@company2.com
```

The following example displays the full-text destination profile.

```
switch# show callhome destination-profile profile full-txt-destination
full-txt destination profile information
maximum message size:250000
email addresses configured:
person2@company2.com
```

The following example displays the short-text destination profile.

```
switch# show callhome destination-profile profile short-txt-destination
Short-txt destination profile information
maximum message size:4000
email addresses configured:
person2@company2.com
```

The following example displays the XML destination profile.

```
switch# show callhome destination-profile profile XML-destination
XML destination profile information
maximum message size:250000
email addresses configured:
findout@.cisco.com
```

The following example displays e-mail and SMTP information.

```
switch# show callhome transport-email
from email addr:user@company1.com
reply to email addr:pointer@company.com
return receipt email addr:user@company1.com
smtp server:server.company.com
smtp server port:25
```

The following example displays user-defined CLI commands for the alert groups.

```
switch# show callhome user-def-cmds
User configured commands for alert groups :
alert-group test user-def-cmd "show version"
```

Related Commands

Command	Description
alert-group	Customizes a Call Home alert group with user-defined **show** commands.
callhome	Configures Call Home.
callhome test	Sends a dummy test message to the configured destination(s).

show cdp

To display CDP parameters configured globally or for a specific interface, use the **show cdp** command.

show cdp {**all** | **entry** [**all** | **name** *cdp-name*] | **global** | **interface** [**gigabitethernet** *slot/port* | **mgmt 0**] | **neighbors** [**detail** | **interface** (**gigabitethernet** *slot/port* | **mgmt 0**)] | **traffic interface** [**gigabitethernet** *slot/port* | **mgmt 0**]}

Syntax Description

all	Displays all enabled CDP interfaces.
entry	Displays CDP database entries.
all	Displays all CDP entries in the database
name *cdp-name*	Displays CDP entries that match a specified name. Maximum length is 256 characters.
global	Displays global CDP parameters.
interface	Displays CDP parameters for an interface.
gigabitethernet *slot/port*	Specifies the Gigabit Ethernet interface at the slot number and port number separated by a slash (/).
mgmt 0	Specifies the Ethernet management interface.
neighbors	Displays all CDP neighbors.
detail	Displays detailed information for all CDP neighbors
interface	Displays CDP information for neighbors on a specified interface.
traffic	Displays CDP traffic statistics for an interface.

Defaults

None

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is allowed only on the active supervisor module in the Cisco MDS 9500 Series.

Examples

The following example displays all CDP capable interfaces and parameters.

```
switch# show cdp all
GigabitEthernet4/1 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
GigabitEthernet4/8 is down
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
mgmt0 is up
    CDP enabled on interface
    Sending CDP packets every 100 seconds
    Holdtime is 200 seconds
```

The following example displays all CDP neighbor entries.

```
switch# show cdp entry all
----------------------------------------
Device ID:069038747(Kiowa3)
Entry address(es):
    IP Address: 172.22.92.5
Platform: WS-C5500, Capabilities: Trans-Bridge Switch
Interface: mgmt0, Port ID (outgoing port): 5/22
Holdtime: 136 sec

Version:
WS-C5500 Software, Version McpSW: 2.4(3) NmpSW: 2.4(3)
Copyright (c) 1995-1997 by Cisco Systems

Advertisement Version: 1
```

The following example displays the specified CDP neighbor.

```
switch# show cdp entry name 0
----------------------------------------
Device ID:0
Entry address(es):
    IP Address: 0.0.0.0
Platform: DS-X9530-SF1-K9, Capabilities: Host
Interface: GigabitEthernet4/1, Port ID (outgoing port): GigabitEthernet4/1
Holdtime: 144 sec

Version:
1.1(0.144)

Advertisement Version: 2
Duplex: full
```

The following example displays global CDP parameters.

```
switch# show cdp global
Global CDP information:
    CDP enabled globally
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is enabled
```

The following example displays CDP parameters for the management interface.

```
switch# show cdp interface mgmt 0
mgmt0 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
```

The following example displays CDP parameters for the Gigabit Ethernet interface.

```
switch# show cdp interface gigabitethernet 4/1
GigabitEthernet4/1 is up
    CDP enabled on interface
    Sending CDP packets every 80 seconds
    Holdtime is 200 seconds
```

The following example displays CDP Neighbors (brief).

```
switch# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce   Hldtme  Capability  Platform      Port ID
0                Gig4/1          135     H           DS-X9530-SF1- Gig4/1
069038732(Kiowa2 mgmt0           132     T S         WS-C5500      8/11
069038747(Kiowa3 mgmt0           156     T S         WS-C5500      6/20
069038747(Kiowa3 mgmt0           158     T S         WS-C5500      5/22
```

The following example displays CDP neighbors (detail).

```
switch# show CDP neighbor detail
----------------------------------------
Device ID:0
Entry address(es):
    IP Address: 0.0.0.0
Platform: DS-X9530-SF1-K9, Capabilities: Host
Interface: GigabitEthernet4/1, Port ID (outgoing port): GigabitEthernet4/1
Holdtime: 162 sec

Version:
1.1(0.144)

Advertisement Version: 2
Duplex: full
----------------------------------------
Device ID:069038732(Kiowa2)
Entry address(es):
    IP Address: 172.22.91.5
Platform: WS-C5500, Capabilities: Trans-Bridge Switch
Interface: mgmt0, Port ID (outgoing port): 8/11
Holdtime: 132 sec

Version:
WS-C5500 Software, Version McpSW: 2.4(3) NmpSW: 2.4(3)
Copyright (c) 1995-1997 by Cisco Systems

Advertisement Version: 1
```

The following example displays the specified CDP neighbor (detail).

```
switch# show CDP neighbors interface gigabitethernet 4/1 detail
----------------------------------------
Device ID:0
Entry address(es):
    IP Address: 0.0.0.0
Platform: DS-X9530-SF1-K9, Capabilities: Host
Interface: GigabitEthernet4/1, Port ID (outgoing port): GigabitEthernet4/1
Holdtime: 144 sec

Version:
1.1(0.144)

Advertisement Version: 2
Duplex: full
```

The following example displays CDP traffic statistics for the management interface.

```
switch# show cdp traffic interface mgmt 0
----------------------------------------
Traffic statistics for mgmt0
Input Statistics:
    Total Packets: 1148
    Valid CDP Packets: 1148
        CDP v1 Packets: 1148
        CDP v2 Packets: 0
    Invalid CDP Packets: 0
        Unsupported Version: 0
        Checksum Errors: 0
        Malformed Packets: 0

Output Statistics:
    Total Packets: 2329
        CDP v1 Packets: 1164
        CDP v2 Packets: 1165
    Send Errors: 0
```

The following example displays CDP traffic statistics for the Gigabit Ethernet interface

```
switch# show cdp traffic interface gigabitethernet 4/1
----------------------------------------
Traffic statistics for GigabitEthernet4/1
Input Statistics:
    Total Packets: 674
    Valid CDP Packets: 674
        CDP v1 Packets: 0
        CDP v2 Packets: 674
    Invalid CDP Packets: 0
        Unsupported Version: 0
        Checksum Errors: 0
        Malformed Packets: 0

Output Statistics:
    Total Packets: 674
        CDP v1 Packets: 0
        CDP v2 Packets: 674
    Send Errors: 0
```

show cfs

To display Cisco Fabric Services (CFS) information, use the **show cfs** command.

show cfs {**application** [**name** *app-name*] | **lock** [**name** *app-name*] | **merge status name** *app-name*] | **peers** [**name** *app-name*] | **status** [**name** *app-name*]}

Syntax Description

application	Displays locally registered applications.
name *app-name*	Specifies a local application information by name. Maximum length is 64 characters.
lock	Displays the state of application logical or physical locks.
merge status	Displays CFS merge information.
peers	Displays logical or physical CFS peers.
status	Displays if CFS distribution is enabled or disabled. Enabled is the default configuration.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.
2.1(1a)	• Added **status** keyword. • Replaced `vsan` with `fctimer` for the fctimer application in the Application field in the command output.
3.0(1)	Modified the **show cfs application** example with output that shows which applications support CFS distribution over IP and Fibre Channel and those that support only CFS distribution over Fibre Channel.

Usage Guidelines

None.

Examples

The following example shows how to display CFS physical peer information for all applications.

```
switch# show cfs peers

Physical Fabric
-------------------------------------------------
 Switch WWN               IP Address
-------------------------------------------------
 20:00:00:05:30:00:61:de  172.22.46.223   [Local]
 20:00:00:0d:ec:08:66:c0  172.22.46.233
 20:00:00:05:30:00:f1:e2  172.22.46.225
 20:00:00:05:30:00:eb:46  172.22.46.222
```

```
 20:00:00:05:30:00:cb:56  172.22.46.224
 20:00:00:05:30:00:5b:5e  172.22.46.182
 20:00:00:05:30:00:34:9e  172.22.46.220

Total number of entries = 7
```

The following example shows how to display CFS information for all applications on the switch.

```
switch# show cfs application

-----------------------------------------------
 Application    Enabled   Scope
-----------------------------------------------
ntp             No        Physical-all
fscm            Yes       Physical-fc
role            No        Physical-all
rscn            No        Logical
radius          No        Physical-all
fctimer         No        Physical-fc
syslogd         No        Physical-all
callhome        No        Physical-all
fcdomain        Yes       Logical
device-alias    Yes       Physical-fc

Total number of entries = 10
```

Note The **show cfs application** command displays only those applications that are registered with CFS. Conditional services that use CFS do not appear in the output unless those services are running.

The following example shows how to display CFS information for the device alias application.

```
switch# show cfs application name device-alias

 Enabled        : Yes
 Timeout        : 5s
 Merge Capable  : Yes
 Scope          : Physical
```

The following example shows how to display CFS merge operation information for the device alias application.

```
switch# show cfs merge status device-alias

Physical  Merge Status: Success
 Local Fabric
------------------------------------------------------------
 Switch WWN               IP Address
------------------------------------------------------------
 20:00:00:05:30:00:34:9e  172.22.46.220   [Merge Master]
 20:00:00:05:30:00:5b:5e  172.22.46.182
 20:00:00:05:30:00:61:de  172.22.46.223
 20:00:00:05:30:00:cb:56  172.22.46.224
 20:00:00:05:30:00:eb:46  172.22.46.222
 20:00:00:05:30:00:f1:e2  172.22.46.225
```

The following example shows whether or not CFS distribution is enabled.

```
switch# show cfs status
Fabric distribution Enabled
switch#
```

To enable CFS distribution, use the **cfs distribute** command.

show cimserver

To display the Common Information Models (CIM) configurations and settings, use the **show cimserver** command.

show cimserver [**certificateName** | **HttpsStatus** | **HttpStatus** | **status**]

Syntax Description

certificateName	Displays the installed Secure Socket Layer (SSL) certificate.
HttpsStatus	Displays the HTTP (non-secure) protocol settings for the CIM server.
HttpStatus	Displays the HTTPS (secure) protocol for the CIM server.
status	Displays the CIM server status

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays CIM server certificate files.

```
switch# show cimserver certificateName
cimserver certificate file name is servcert.pem
```

The following example displays the CIM server configuration.

```
switch# show cimserver
 cimserver is enabled
 cimserver Http is not enabled
 cimserver Https is enabled
 cimserver certificate file name is servcert.pem
```

The following example displays the CIM server HTTPS status.

```
switch# show cimserver httpsstatus
 cimserver Https is enabled
```

The following example displays the CIM server HTTP status.

```
switch# show cimserver httpstatus
 cimserver Http is not enabled
```

show cli alias

To display configured aliases on a switch, use the **show cli alias** command.

show cli alias [name *name***]**

Syntax Description

name *name*	Specifies an alias name. The maximum size of the name is 31 characters.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The **show cli alias** command shows the default alias and other user-defined aliases. The default alias is **alias**, which means **show cli alias**.

Examples

The following example displays CLI aliases.

```
switch# show cli alias
CLI alias commands
==================
alias  :show cli alias
env    :show environment
clock  :show clock
```

The following example displays a specific alias by name.

```
switch# show cli alias name qos
qos :show qos
```

Related Commands

Command	Description
cli alias name	Defines a command alias name.

show cli variables

To display user-defined session and persistent CLI variables, use the **show cli variables** command.

show cli variables

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The **show CLI variables** command shows all available CLI variables, including user-defined session CLI variables, user-defined persistent CLI variables, and system-defined CLI variables. There is no distinction between the types of CLI variables in the output.

Examples

The following example displays CLI variables.

```
switch# show cli variables
VSH Variable List
-----------------
TIMESTAMP="2005-10-24-21.29.33"
testinterface="fc 1/1"
```

Note The TIMESTAMP variable shown in the output in the preceding example is a predefined variable supported by Cisco MDS SAN-OS. For more information about the TIMESTAMP variable, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

Related Commands

Command	Description
cli var name	Defines a CLI session variable.
cli var name (configuration)	Defines a CLI persistent variable.

show clock

To display the system date and time and verify the time zone configuration, use the **show clock** command.

show clock

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system date, time, and time zone configuration.

```
switch# show clock
Fri Mar 14 01:31:48 UTC 2003
```

show cloud discovery

To display discovery information about the cloud, use the **show cloud discovery** command.

show cloud discovery {config | stats | status}

Syntax Description

config	Displays global discovery configuration information.
stats	Displays discovery statistics information.
status	Displays discovery status information.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows information about a cloud.

```
switch# show cloud discovery config
Auto discovery: Enabled
```

The following example shows statistics about a cloud.

```
sswitch# show cloud discovery stats
Global statistics
    Number of Auto Discovery                      = 4
    Number of Manual (demand) Discovery                    = 0
    Number of cloud discovery (ping) messages sent = 17
    Number of cloud discovery (ping) success       = 1
```

Related Commands

Command	Description
cloud discover	Initiates manual, on-demand cloud discovery.
cloud discovery	Configures cloud discovery.
cloud-discovery	Enables discovery of cloud memberships.
show cloud membership	Displays information about members of a cloud.

show cloud membership

To display membership information about the cloud, use the **show cloud membership** command.

show cloud membership [all | interface {gigabitethernet *slot/port* **| port-channel** *number***} | unresolved]**

Syntax Description

all	Displays all clouds and cloud members.
interface	Displays all members of a cloud containing a specified interface.
gigabitethernet *slot/port*	Specifies a Gigabit Ethernet interface by slot and port number. The range is 1 to 6.
port-channel *number*	Specifies a PortChannel interface. The range is 1 to 128.
unresolved	Displays unresolved members of the cloud.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the members of clouds.

```
switch# show cloud membershp
Undiscovered Cloud
    port-channel 1[20:00:00:05:30:00:a7:9e] IP Addr fe80::205:30ff:fe00:a412
    port-channel 1.250[20:00:00:05:30:00:a7:9e] IP Addr 3000:2::1
    port-channel 1.250[20:00:00:05:30:00:a7:9e] IP Addr fe80::205:30ff:fe00:a412
  #members=3
Cloud 2
    port-channel 1[20:00:00:05:30:00:a7:9e] IP Addr 3000:1::1
  #members=1
Cloud 3
    GigabitEthernet1/1[20:00:00:05:30:00:a7:9e] IP Addr 10.10.10.1
  #members=1
Cloud 4
    GigabitEthernet1/2[20:00:00:05:30:00:a7:9e] IP Addr 10.10.60.1
  #members=1
```

Related Commands

Command	Description
cloud discover	Initiates manual, on-demand cloud discovery.
cloud discovery	Configures cloud discovery.
cloud-discovery enable	Enables discovery of cloud memberships.
show cloud discovery	Displays discovery information about a cloud.

show cores

To display all the cores presently available for upload from active sup, use the **show cores** command.

show cores

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

In the following example, an FSPF core was generated on the active supervisor (slot 5), an FCC core on the standby supervisor (slot 6) and acltcam and fib on module (slot 8).

```
switch# show cores

Module-num     Process-name       PID     Core-create-time
----------     ------------       ---     ----------------
5               fspf             1524     Jan 9 03:11
6               fcc               919     Jan 9 03:09
8               acltcam           285     Jan 9 03:09
8               fib               283     Jan 9 03:08
```

show crypto ca certificates

To display configured trust point certificates, use the **show crypto ca certificates** command.

show crypto ca certificates *trustpoint-label*

Syntax Description

trustpoint-label	Specifies the name of the trust point. The maximum size is 64 characters.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

This command displays the important fields in the identity certificate, if present, followed by those in the CA certificate (or each CA certificate if it is a chain, starting from the lowest to the self-signed root certificate), or the trust point. If the trust point name is not specified, all trust point certificate details are displayed.

Examples

The following example displays configured trust point certificates.

```
switch# show crypto ca certificates
Trustpoint: admin-ca
certificate:
subject= /CN=switch160
issuer= /C=US/O=cisco/CN=Aparna CA2
serial=6CDB2D9E000100000006
notBefore=Jun  9 10:51:45 2005 GMT
notAfter=May  3 23:10:36 2006 GMT
MD5 Fingerprint=0A:22:DC:A3:07:2A:9F:9A:C2:2C:BA:96:EC:D8:0A:95
purposes: sslserver sslclient ike

CA certificate 0:
subject= /C=US/O=cisco/CN=Aparna CA2
issuer= /emailAddress=amandke@cisco.com/C=IN/ST=Maharashtra/L=Pune/O=cisco/OU=ne
tstorage/CN=Aparna CA1
serial=14A3A877000000000005
notBefore=May  5 18:43:36 2005 GMT
notAfter=May  3 23:10:36 2006 GMT
MD5 Fingerprint=32:50:26:9B:16:B1:40:A5:D0:09:53:0A:98:6C:14:CC
purposes: sslserver sslclient ike

CA certificate 1:
subject= /emailAddress=amandke@cisco.com/C=IN/ST=Maharashtra/L=Pune/O=cisco/OU=n
etstorage/CN=Aparna CA1
issuer= /emailAddress=amandke@cisco.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/OU
=netstorage/CN=Aparna CA
```

```
serial=611B09A1000000000002
notBefore=May  3 23:00:36 2005 GMT
notAfter=May  3 23:10:36 2006 GMT
MD5 Fingerprint=65:CE:DA:75:0A:AD:B2:ED:69:93:EF:5B:58:D4:E7:AD
purposes: sslserver sslclient ike

CA certificate 2:
subject= /emailAddress=amandke@cisco.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/O
U=netstorage/CN=Aparna CA
issuer= /emailAddress=amandke@cisco.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/OU
=netstorage/CN=Aparna CA
serial=0560D289ACB419944F4912258CAD197A
notBefore=May  3 22:46:37 2005 GMT
notAfter=May  3 22:55:17 2007 GMT
MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
purposes: sslserver sslclient ike
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the certificate of the CA.
show ca trustpoints	Displays trust point configurations.

show crypto ca crl

To display configured certificate revocation lists (CRLs), use the **show crypto ca crl** command.

show crypto ca crl *trustpoint-label*

Syntax Description

trustpoint-label	Specifies the name of the trust point. The maximum size is 64 characters.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

This command lists serial numbers of revoked certificates in the CRL of the specified trust point.

Examples

The following example displays a configured CRL.

```
switch# show crypto ca crl admin-ca
Trustpoint: admin-ca
CRL:
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: /emailAddress=rviyyoka@cisco.com/C=IN/ST=Kar/L=Bangalore/O=Cisco
 Systems/OU=1/CN=cisco-blr
        Last Update: Sep 22 07:05:23 2005 GMT
        Next Update: Sep 29 19:25:23 2005 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
            keyid:CF:72:E1:FE:14:60:14:6E:B0:FA:8D:87:18:6B:E8:5F:70:69:05:3F

            1.3.6.1.4.1.311.21.1:
                ...
Revoked Certificates:
    Serial Number: 1E0AE838000000000002
        Revocation Date: Mar 15 09:12:36 2005 GMT
    Serial Number: 1E0AE9AB000000000003
        Revocation Date: Mar 15 09:12:45 2005 GMT
    Serial Number: 1E721E50000000000004
        Revocation Date: Apr  5 11:04:20 2005 GMT
    Serial Number: 3D26E445000000000005
        Revocation Date: Apr  5 11:04:16 2005 GMT
    Serial Number: 3D28F8DF000000000006
        Revocation Date: Apr  5 11:04:12 2005 GMT
    Serial Number: 3D2C6EF3000000000007
        Revocation Date: Apr  5 11:04:09 2005 GMT
```

```
Serial Number: 3D4D7DDC000000000008
    Revocation Date: Apr  5 11:04:05 2005 GMT
Serial Number: 5BF1FE87000000000009
    Revocation Date: Apr  5 11:04:01 2005 GMT
Serial Number: 5BF22FB300000000000A
    Revocation Date: Apr  5 11:03:45 2005 GMT
Serial Number: 5BFA4A4900000000000B
    Revocation Date: Apr  5 11:03:42 2005 GMT
Serial Number: 5C0BC22500000000000C
    Revocation Date: Apr  5 11:03:39 2005 GMT
Serial Number: 5C0DA95E00000000000D
    Revocation Date: Apr  5 11:03:35 2005 GMT
Serial Number: 5C13776900000000000E
    Revocation Date: Apr  5 11:03:31 2005 GMT
Serial Number: 4864FD5A00000000000F
    Revocation Date: Apr  5 11:03:28 2005 GMT
Serial Number: 48642E2E000000000010
    Revocation Date: Apr  5 11:03:24 2005 GMT
Serial Number: 486D4230000000000011
    Revocation Date: Apr  5 11:03:20 2005 GMT
Serial Number: 7FCB75B9000000000012
    Revocation Date: Apr  5 10:39:12 2005 GMT
Serial Number: 1A7519000000000013
    Revocation Date: Apr  5 10:38:52 2005 GMT
Serial Number: 20F1B0000000000014
    Revocation Date: Apr  5 10:38:38 2005 GMT
Serial Number: 436E43A9000000000023
    Revocation Date: Sep  9 09:01:23 2005 GMT
    CRL entry extensions:
        X509v3 CRL Reason Code:
        Cessation Of Operation
Serial Number: 152D3C5E000000000047
    Revocation Date: Sep 22 07:12:41 2005 GMT
Serial Number: 1533AD7F000000000048
    Revocation Date: Sep 22 07:13:11 2005 GMT
Serial Number: 1F9EB8EA00000000006D
    Revocation Date: Jul 19 09:58:45 2005 GMT
    CRL entry extensions:
        X509v3 CRL Reason Code:
        Cessation Of Operation
Serial Number: 1FCA9DC600000000006E
    Revocation Date: Jul 19 10:17:34 2005 GMT
    CRL entry extensions:
        X509v3 CRL Reason Code:
        Cessation Of Operation
Serial Number: 2F1B5E2E000000000072
    Revocation Date: Jul 22 09:41:21 2005 GMT
    CRL entry extensions:
        X509v3 CRL Reason Code:
        Cessation Of Operation
Signature Algorithm: sha1WithRSAEncryption
    4e:3b:4e:7a:55:6b:f2:ec:72:29:70:16:2a:fd:d9:9a:9b:12:
    f9:cd:dd:20:cc:e0:89:30:3b:4f:00:4b:88:03:2d:80:4e:22:
    9f:46:a5:41:25:f4:a5:26:b7:b6:db:27:a9:64:67:b9:c0:88:
    30:37:cf:74:57:7a:45:5f:5e:d0
```

Related Commands

Command	Description
crypto ca crl request	Configures a CRL or overwrites the existing one for the trust point CA.

show crypto ca trustpoints

To display trust point configurations, use the **show crypto ca trustpoints** command.

show crypto ca trustpoints

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays configured trust points.

```
switch# show crypto ca trustpoints
trustpoint: CAname; key:
revokation methods:  crl
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the certificate of the CA.
crypto ca trustpoint	Declares the trust point certificate authority that the switch should trust.
show crypto ca certificates	Displays configured trust point certificates.

show crypto global domain ipsec

To display global IPsec crypto map set information, use the **show crypto global domain ipsec** command.

show crypto global domain ipsec [**interface gigabitethernet** *slot/port* | **security-association lifetime**]

Syntax Description

interface gigabitethernet *slot/port*	Displays crypto IPsec domain information for the specified Gigabit Ethernet interface slot and port.
security-association lifetime	Displays crypto IPsec domain security association lifetime parameters.

Defaults

Displays IPsec global statistics.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, IPsec must be enabled using the **crypto ipsec enable** command.

Examples

The following example shows how to display crypto global domain IPsec statistics.

```
switch# show crypto global domain ipsec
IPSec global statistics:
        Number of crypto map sets: 2
```

The following example shows how to display crypto global domain IPsec statistics for an interface.

```
switch# show crypto global domain ipsec interface gigabitethernet 1/2
IPSec interface statistics:
        IKE transaction stats: 0 num
        Inbound SA stats: 0 num, 512 max
        Outbound SA stats: 0 num, 512 max
```

The following example shows how to display crypto global domain IPsec security association lifetime parameters.

```
switch# show crypto global domain ipsec security-association lifetime
Security Association Lifetime: 4500 megabytes/3600 seconds
```

Related Commands

Command	Description
crypto global domain ipsec security-association lifetime	Configures global attributes for IPsec.
crypto ipsec enable	Enables IPsec.

show crypto ike domain ipsec

To display IKE protocol information, use the **show crypto ike domain ipsec** command.

show crypto ike domain ipsec [**initiator** [**address** *ip-address*] | **keepalive** | **key** [**address** *ip-address*] | **policy** [*policy-number*] | **sa**]

Syntax Description

initiator	Displays initiator configuration information.
address *ip-address*	Specifies the initiator peer IP address.
keepalive	Displays keepalive for the IKE protocol in seconds
key	Displays pre-shared authentication keys.
policy [*policy-number*]	Displays IKE configuration policies for IPsec. The range is 1 to 255.
sa	Displays IKE Security Associations for IPsec.

Defaults

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Examples

The following example shows how to display IKE keepalive value configuration information.

```
switch# show crypto ike domain ipsec keepalive
keepalive 3600
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.

show crypto key mypubkey rsa

To display any RSA public key configurations, use the **show crypto key mypubkey rsa** command.

show crypto key mypubkey rsa

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays RSA public key configurations.

```
switch# show crypto key mupubkey rsa
key label: myrsa
key size: 512
exportable: yes
```

Related Commands

Command	Description
crypto ca enroll	Requests certificates for the switch's RSA key pair.
crypto key generate rsa	Generate an RSA key pair.
rsakeypair	Configure trust point RSA key pair details

show crypto map domain ipsec

To map configuration information for IPsec, use the **show crypto map domain ipsec** command.

show crypto map domain ipsec [**interface gigabitethernet** *slot/port* | **tag** *tag-name*]

Syntax Description

interface gigabitethernet *slot/port*	Displays IPsec map information for a specific Gigabit Ethernet interface.
tag *tag-name*	Displays IPsec map information for a specific tag name. The maximum length is 63 characters.

Defaults

Displays all IPsec map information.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, IPsec must be enabled using the **crypto ipsec enable** command.

Examples

The following example shows how to display IPsec crypto map information.

```
switch# show crypto map domain ipsec
Crypto Map "cm10" 1 ipsec
        Peer = 10.10.10.4
        IP ACL = aclmds10
            permit ip 10.10.10.1 255.255.255.255 10.10.10.4 255.255.255.255
        Transform-sets: 3des-md5, 3des-sha, des-md5, des-sha,
        Security Association Lifetime: 450 gigabytes/3600 seconds
        PFS (Y/N): N
Crypto Map "cm10" 2 ipsec
        Peer = Auto Peer
        IP ACL = acl10
            permit ip 10.10.10.0 255.255.255.0 10.10.10.0 255.255.255.0
        Transform-sets: 3des-md5, 3des-sha, des-md5, des-sha,
        Security Association Lifetime: 450 gigabytes/3600 seconds
        PFS (Y/N): N
Crypto Map "cm11" 1 ipsec
        Peer = 10.10.11.2
        IP ACL = aclany
            permit ip any any
        Transform-sets: 3des-md5, 3des-sha, des-md5, des-sha,
        Security Association Lifetime: 450 gigabytes/3600 seconds
        PFS (Y/N): N
```

```
Crypto Map "cm50" 1 ipsec
        Peer = 10.10.50.2
        IP ACL = aclany
            permit ip any any
        Transform-sets: 3des-md5,
        Security Association Lifetime: 450 gigabytes/3600 seconds
        PFS (Y/N): N
Interface using crypto map set cm50:
    GigabitEthernet1/2.1

Crypto Map "cm51" 1 ipsec
        Peer = 10.10.51.2
        IP ACL = aclany
            permit ip any any
        Transform-sets: 3des-md5,
        Security Association Lifetime: 450 gigabytes/3600 seconds
        PFS (Y/N): N
Interface using crypto map set cm51:
    GigabitEthernet1/2.2

Crypto Map "cm60" 1 ipsec
        Peer = 10.10.60.2
        IP ACL = acl60
            permit ip 10.10.60.0 255.255.255.0 10.10.60.0 255.255.255.0
        Transform-sets: 3des-md5,
        Security Association Lifetime: 450 gigabytes/3600 seconds
        PFS (Y/N): N
Interface using crypto map set cm60:
    GigabitEthernet1/2

Crypto Map "cm100" 1 ipsec
        Peer = 10.10.100.221
        IP ACL = aclmds100
            permit ip 10.10.100.231 255.255.255.255 10.10.100.221 255.255.255.255
        Transform-sets: 3des-md5, 3des-sha, des-md5, des-sha,
        Security Association Lifetime: 450 gigabytes/3600 seconds
        PFS (Y/N): N
Crypto Map "cm100" 2 ipsec
        Peer = Auto Peer
        IP ACL = acl100
            permit ip 10.10.100.0 255.255.255.0 10.10.100.0 255.255.255.0
        Transform-sets: 3des-md5, 3des-sha, des-md5, des-sha,
        Security Association Lifetime: 450 gigabytes/3600 seconds
        PFS (Y/N): N
```

Related Commands

Command	Description
crypto ipsec enable	Enables IPsec.
crypto map domain ipsec	Enters IPsec map configuration mode.

show crypto sad domain ipsec

To display IPsec security association database information, use the **show crypto sad domain ipsec** command.

show crypto sad domain ipsec [**interface gigabitethernet** *slot/port* [{**inbound** | **outbound**} **sa-index** *index*]]

Syntax Description

interface gigabitethernet *slot/port*	Displays IPsec security association information for a specific Gigabit Ethernet interface.
inbound	Specifies the inbound association.
outbound	Specifies the outbound association.
sa-index *index*	Specifies the security association index. The range is 0 to 2147483647.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, IPsec must be enabled using the **crypto ipsec enable** command.

Examples

The following example shows how to display IPsec security association information.

```
switch# show crypto sad domain ipsec
interface: GigabitEthernet4/1
    Crypto map tag: cm10, local addr. 10.10.10.1
    protected network:
    local ident (addr/mask): (10.10.10.0/255.255.255.0)
    remote ident (addr/mask): (10.10.10.4/255.255.255.255)
    current_peer: 10.10.10.4
      local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.4
      mode: tunnel, crypto algo: esp-3des, auth algo: esp-md5-hmac
    current outbound spi: 0x30e000f (51249167), index: 0
      lifetimes in seconds:: 120
      lifetimes in bytes:: 423624704
    current inbound spi: 0x30e0000 (51249152), index: 0
      lifetimes in seconds:: 120
      lifetimes in bytes:: 423624704
```

Related Commands

Command	Description
crypto ipsec enable	Enables IPsec.

show crypto spd domain ipsec

To display the security policy database (SPD), use the **show crypto spd domain ipsec** command.

show crypto spd domain ipsec [**interface gigabitethernet** *slot/port* [**policy** *number*]]

Syntax Description

interface gigabitethernet *slot/port*	Displays SPD information for a specific Gigabit Ethernet interface.
policy *number*	Specifies a SPD policy number.

Defaults

Displays all SPD information.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, IPsec must be enabled using the **crypto ipsec enable** command.

Examples

The following example shows how to display the SPD.

```
switch# show crypto spd domain ipsec
Policy Database for interface: GigabitEthernet1/1, direction: Both
#   0:      deny  udp any port eq 500 any
#   1:      deny  udp any any port eq 500
#   2:      permit ip any any
#  63:      deny  ip any any
Policy Database for interface: GigabitEthernet1/2, direction: Both
#   0:      deny  udp any port eq 500 any
#   1:      deny  udp any any port eq 500
#   3:      permit ip 10.10.50.1 255.255.255.255 10.10.50.2 255.255.255.255
#   4:      permit ip 10.10.51.1 255.255.255.255 10.10.51.2 255.255.255.255
#  63:      deny  ip any any
```

Related Commands

Command	Description
crypto ipsec enable	Enables IPsec.

show crypto transform-set domain ipsec

To display transform set information for IPsec, use the **show crypto transform-set domain ipsec** command.

show crypto transform-set domain ipsec [*set-name*]

Syntax Description

set-name	Specifies the transform set name. Maximum length is 63 characters.

Defaults

Displays information for all transform sets.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, IPsec must be enabled using the **crypto ipsec enable** command.

Examples

The following example shows how to display information for all IPsec transform sets.

```
switch# show crypto transform-set domain ipsec
Transform set: ipsec_default_transform_set {esp-aes-256-ctr esp-aes-xcbc-mac}
    will negotiate {tunnel}
```

Related Commands

Command	Description
crypto ipsec enable	Enables IPsec.
crypto transform-set domain ipsec	Configures IPsec transform set information.

show debug

To display the **debug** commands configured on the switch, use the **show debug** command in EXEC mode.

show debug all [**aaa** | **acl** | **arbiter** | **ascii-cfg** | **bootvar** | **callhome** | **capability** | **cdp** | v | **cimserver** | **cloud** | **confcheck** | **core** | **device-alias** | **dstats** | **epp** | **ethport** | **exceptionlog** | **fabric_start_cfg_mgr** | **fc-tunnel** | **fc2** | **fc2d** | **fcc** | **fcdomain** | **fcfwd** | **fcns** | **fcs** | **fdmi** | **flogi** | **fs-daemon** | **fspf** | **fvp** | **idehsd** | **ilc_helper** | **ipacl** | **ipconf** | **ipfc** | **kadb** | **kipfc** | **klm-scsi-target** | **license** | **logfile** | **mcast** | **mip** | **module** | **ntp** | **platform** | **port** | **port-channel** | **qos** | **radius** | **rdl** | **redundancy** | **rib** | **rlir** | **rscn** | **scsi-flow** | **scsi-target** | **security** | **sensor** | **snmp** | **span** | **system** | **SystemHealth** | **tcap** | **tlport** | **ttyd** | **vni** | **vp** | **vrrp** | **vsan** | **vshd** | **wwn** | **xbar** | **xbc** | **zone**]

Syntax Description

aaa	Displays debugging flags of 301.
acl	Displays debugging flags of ACL manager.
arbiter	Displays Arbiter debugging flags of arbiter.
ascii-cfg	Displays all debugging flags of ascii-cfg.
bootvar	Displays debugging flags of bootvar.
callhome	Displays debugging flags of Call Home.
capability	Displays all debugging flags of capability.
cdp	Displays debugging flags of the Cisco Discovery Protocol (CDP).
cfs	Displays debugging flags of Cisco Fabric Services (CFS).
cimserver	Displays debugging flags of the CIM server.
cloud	Displays debugging flags of cloud.
confcheck	Displays all debugging flags of confcheck.
core	Displays debugging flags for feature manager.
device-alias	Displays debugging flags of Distributed Device Alias Services.
dstats	Displays debugging flags of delta statistics.
epp	Displays debugging flags of EPP.
ethport	Displays debugging flags of Ethernet port.
exceptionlog	Displays all debugging flags of exception logger.
fabric_start_cfg_mgr	Displays debugging flags of fabric startup configuration manager.
fc-tunnel	Displays all debugging flags of MPLS tunnel.
fc2	Displays all debugging flags of of FC2.
fc2d	Displays debugging flags of FC2D.
fcc	Displays all debugging flags of FCC.
fcdomain	Displays internal debugging flags of FC domain.
fcfwd	Displays all debugging flags of FCFWD.
fcns	Displays name server debug flags.
fcs	Displays debugging flags of Fabric Config server.
fdmi	Displays all debugging flags of FDMI.
flogi	Displays debugging flags of F port server.

fs-daemon	Displays debugging flags of file server daemon.
fspf	Displays all debugging flags of FSPF.
fvp	Displays all debugging flags of FVP manager.
idehsd	Displays debugging flags of IDEHSD.
ilc_helper	Displays debugging flags of ilc_helper.
ipacl	Displays all debugging flags of IP-ACL.
ipconf	Displays debugging flags of IP configuration.
ipfc	Displays all debugging flags of IPFC.
kadb	Displays debugging flags of Kernel ADB.
kipfc	Displays debugging flags of IPFC kernel.
klm-scsi-target	Displays debug flags of SCSI-target driver.
license	Displays debugging flags for licensing.
logfile	Displays contents of the logfile.
mcast	Displays all debugging flags of mcast.
mip	Displays debugging flags of mip kernel.
module	Displays all debugging flags of module.
ntp	Displays the state of NTP debug settings.
platform	Displays all debugging flags of platform manager.
port	Displays debugging flags of port.
port-channel	Displays all debugging flags of port-channel.
qos	Displays debugging flags. of QoS
radius	Displays debugging flags of RADIUS.
rdl	Displays debugging flags of RDL.
redundancy	Displays debugging flags of Redundancy drivers.
rib	Displays all debugging flags of rib.
rlir	Displays all debugging flags of RLIR.
rscn	Displays all debugging flags of RSCN.
scsi-flow	Displays debugging flags of SCSI flow.
scsi-target	Displays debugging flags for SCSI target daemon.
security	Displays debugging flags of security and accounting
sensor	Displays all debugging flags of sensor manager.
snmp	Displays all debugging flags of SNMP server.
span	Displays debugging flags of SPAN.
system	Displays all debugging flags of system.
SystemHealth	Displays all debugging flags of system health.
tcap	Displays all debugging flags of exception logger.
tlport	Displays debugging flags of TL Port.
ttyd	Displays all debugging flags of TTYD.
vni	Displays debugging flags of the virtual network interface.
vp	Displays all debugging flags of VP manager.
vrrp	Displays the debugging flags of VRRP.

vsan	Displays debugging flags of VSAN manager.
vshd	Displays all debugging flags of VSHD.
wwn	Displays all debugging flags of WWN manager.
xbar	Displays all debugging flags of XBAR.
xbc	Displays all debugging flags of XBC.
zone	Displays zone server debug elements.

Defaults

Displays all configured debugging flags.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the **cloud** option.

Usage Guidelines

None.

Examples

The following example shows all debug commands configured on the switch.

```
switch# show debug
Show Debug all

ILC helper:
 ILC_HELPER errors debugging is on

SCSI Flow Manager:
 Error debugging is on
switch#
```

The following example displays the debug messages in the specified debug log file.

```
switch# show debug logfile SampleFile
2004 Jun 28 00:14:17 snmpd[2463]: header_fspfLinkEntry : Sending GETNEXT request
 for fspfLsrTable for vsanIndex  =0,fspfLsrDomainId = 0, fspfLsrType = 0
2004 Jun 28 00:14:17 snmpd[2463]: header_fspfLinkEntry : Sending GETNEXT request
 for fspfLsrTable for vsanIndex  =0,fspfLsrDomainId = 0, fspfLsrType = 0
2004 Jun 28 00:14:17 snmpd[2463]: header_fspfLinkEntry : Recd rsp for GETNEXT fo
r entry (vsanIndex=1,fspfLsrDomainId = 10, fspfLsrType=0, fspfLinkIndex = 1,fspf
LinkNbrDomainId = 84, fspfLinkPortIndex = 67331,fspfLinkNbrPortIndex = 66064, fs
pfLinkType = 1,fspfLinkCost = 500
2004 Jun 28 00:14:17 snmpd[2463]: header_fspfLinkEntry : Sending GETNEXT request
 for fspfLsrTable for vsanIndex  =1,fspfLsrDomainId = 209, fspfLsrType = 0
2004 Jun 28 00:14:17 snmpd[2463]: header_fspfLinkEntry : Sending GETNEXT request
 for fspfLsrTable for vsanIndex  =16777216,fspfLsrDomainId = 3506438144, fspfLsr
Type = 0
2004 Jun 28 00:14:17 snmpd[2463]: header_fspfLinkEntry : Sending GETNEXT request
 for fspfLsrTable for vsanIndex  =33554432,fspfLsrDomainId = 4009754624, fspfLsr
Type = 16777216
```

show device-alias

To display the device name information, use the **show device-alias** command.

show device-alias {**database** [**pending** | **pending-diff**] | **name** *device-name* [**pending**] | **pwwn** *pwwn-id* [**pending**] | **statistics** | **status**]

Syntax Description

database	Displays the entire device name database.
pending	Displays the pending device name database information.
pending-diff	Displays the pending differences in the device name database information.
name *device-name*	Displays device name database information for a specific device name.
pwwn *pwwn-id*	Displays device name database information for a specific pWWN. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
statistics	Displays device name database statistics.
status	Displays device name database status.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To make use of fcaliases as device names instead of using the cryptic device name, add only one member per fcalias.

Examples

The following example shows how to display the contents of the device alias database.

```
switch# show device-alias database
device-alias name efg pwwn 21:00:00:20:37:9c:48:e5
device-alias name fred pwwn 10:00:00:00:c9:2d:5a:de
device-alias name myalias pwwn 21:21:21:21:21:21:21:21
device-alias name test pwwn 21:00:00:20:37:6f:db:bb
device-alias name test2 pwwn 21:00:00:20:37:a6:be:35

Total number of entries = 5
```

The following example shows how to display all global fcaliases and all VSAN dependent fcaliases.

```
switch# show device-alias name efg
device-alias name efg pwwn 21:00:00:20:37:9c:48:e5
```

The following example shows how to display all global fcaliases and all VSAN dependent fcaliases.

```
switch# show device-alias statistics
        Device Alias Statistics
========================================
Lock requests sent: 1
Database update requests sent: 1
Unlock requests sent: 1
Lock requests received: 0
Database update requests received: 0
Unlock requests received: 0
Lock rejects sent: 0
Database update rejects sent: 0
Unlock rejects sent: 0
Lock rejects received: 0
Database update rejects received: 0
Unlock rejects received: 0
Merge requests received: 5
Merge request rejects sent: 0
Merge responses received: 0
Merge response rejects sent: 0
Activation requests received: 5
Activation request rejects sent: 0
Activation requests sent: 0
Activation request rejects received: 0
v_226# pwwn 21:00:00:20:37:6f:dc:0e
```

Related Commands

Command	Description
device-alias name	Configures device alias names.
device-alias database	Configures device alias information.
device-alias distribute	Enables device alias CFS distribution.

show dpvm

To display dynamic port VSAN membership (DPVM) information, use the **show dpvm** command.

show dpvm {**database** [**active**] | **pending** | **pending-diff** | **ports** [**vsan** *vsan-id*] | **status**}

Syntax Description

database	Displays both the configured and active DPVM databases.
active	Displays only the active DPVM database.
pending	Displays pending DPVM operations.
pending-diff	Displays differences between the pending DPVM operations and the active DPVM database.
ports	Displays DPVM information for the ports.
vsan *vsan-id*	Specifies a VSAN ID. The range is from 0 to 4093.
status	Displays DPVM status information.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

Examples

The following example shows how to display DPVM database information.

```
switch# show dpvm database
pwwn 00:00:00:00:00:00:00:01 vsan 1
pwwn 00:00:00:00:00:00:00:02 vsan 1
[Total 2 entries]
```

Related Commands

Command	Description
dpvm database	Configures the DPVM database.

show environment

To display all environment-related switch information (status of chassis clock, chassis fan modules, power supply modules, power supply redundancy mode and power usage summary, module temperature thresholds and alarm status, use the **show environment** command.

show environment [**clock** | **fan** | **power** | **temperature**]

Syntax Description

clock	Displays status of chassis clock modules
fan	Displays status of chassis fan modules
power	Displays status of power supply modules, power supply redundancy mode and power usage summary.
temperature	Displays module temperature thresholds and alarm status of temperature sensors.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the status and alarm states of the clock, fan, power supply and temperature sensors.

```
switch# show environment
switch-180# show env
Clock:
--------------------------------------------------------------
Clock           Model                Hw         Status
--------------------------------------------------------------
A               DS-C9500-CL          0.0        ok/active
B               DS-C9500-CL          0.0        ok/standby


Fan:
-----------------------------------------------------
Fan             Model                Hw         Status
-----------------------------------------------------
Chassis         WS-9SLOT-FAN         0.0        ok
PS-1            --                   --         ok
PS-2            --                   --         ok
```

```
Temperature:
-----------------------------------------------------------------
Module   Sensor   MajorThresh   MinorThres   CurTemp     Status
                  (Celsius)     (Celsius)    (Celsius)
-----------------------------------------------------------------
1        Outlet   75            60           38          ok
1        Intake   65            50           35          ok

5        Outlet   75            60           36          ok
5        Intake   65            50           36          ok

6        Outlet   75            60           40          ok
6        Intake   65            50           33          ok

9        Outlet   75            60           28          ok
9        Intake   65            50           40          ok

Power Supply:
-----------------------------------------------------
PS  Model                Power     Power       Status
                         (Watts)   (Amp @42V)
-----------------------------------------------------
1   DS-CAC-2500W         1153.32   27.46       ok
2   WS-CAC-2500W         1153.32   27.46       ok

Mod Model                Power     Power       Power     Power       Status
                         Requested Requested   Allocated Allocated
                         (Watts)   (Amp @42V)  (Watts)   (Amp @42V)
--- -------------------  -------   ----------  --------- ----------  ----------
1    DS-X9016            220.08    5.24        220.08    5.24        powered-up
5    DS-X9530-SF1-K9     220.08    5.24        220.08    5.24        powered-up
6    DS-X9530-SF1-K9     220.08    5.24        220.08    5.24        powered-up
9    DS-X9016            220.08    5.24        220.08    5.24        powered-up

Power Usage Summary:
--------------------
Power Supply redundancy mode:                 non-redundant (combined)

Total Power Capacity                          2306.64  W

Power reserved for Supervisor(s)[-]           440.16   W
Power reserved for Fan Module(s)[-]           210.00   W
Power currently used by Modules[-]            440.16   W

                                              -------
Total Power Available                         1216.32  W
                                              -------
```

Related Commands

Command	Description
show hardware	Displays all hardware components on a system.

show fabric-binding

To display configured fabric binding information, use the **show fabric-binding** command in EXEC mode.

show fabric-binding {**database** [**active**] [**vsan** *vsan-id*] | **efmd statistics** [**vsan** *vsan-id*] | **statistics** [**vsan** *vsan-id*] | **status** [**vsan** *vsan-id*] | **violations** [**last** *number*]}

Syntax Description

database	Displays configured database information.
active	Displays the active database configuration information.
vsan *vsan-id*	Specifies the FICON-enabled VSAN ID. The range is 1 to 4093.
efmd statistics	Displays Exchange Fabric Membership Data (EFMD) statistics.
statistics	Displays fabric binding statistics.
status	Displays fabric binding status
violations	Displays violations in the fabric binding configuration.
last *number*	Specifies between 1 and 100 recent violations.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays configured fabric binding database information.

```
switch# show fabric-binding database
-------------------------------------------------
Vsan   Logging-in Switch WWN     Domain-id
-------------------------------------------------
1      21:00:05:30:23:11:11:11   0x66(102)
1      21:00:05:30:23:1a:11:03    0x19(25)
1      20:00:00:05:30:00:2a:1e   0xea(234)
4      21:00:05:30:23:11:11:11   0x66(102)
4      21:00:05:30:23:1a:11:03    0x19(25)
61     21:00:05:30:23:1a:11:03    0x19(25)
61     21:00:05:30:23:11:11:11   0x66(102)
[Total 7 entries]
```

The following example displays active fabric binding information.

```
switch# show fabric-binding database active
-------------------------------------------------
Vsan   Logging-in Switch WWN     Domain-id
-------------------------------------------------
1      21:00:05:30:23:11:11:11   0x66(102)
1      21:00:05:30:23:1a:11:03    0x19(25)
1      20:00:00:05:30:00:2a:1e   0xea(234)
61     21:00:05:30:23:1a:11:03    0x19(25)
61     21:00:05:30:23:11:11:11   0x66(102)
61     20:00:00:05:30:00:2a:1e   0xef(239)
```

The following example displays active VSAN-specific fabric binding information.

```
switch# show fabric-binding database active vsan 61
-------------------------------------------------
Vsan   Logging-in Switch WWN     Domain-id
-------------------------------------------------
61     21:00:05:30:23:1a:11:03    0x19(25)
61     21:00:05:30:23:11:11:11   0x66(102)
61     20:00:00:05:30:00:2a:1e   0xef(239)
[Total 3 entries]
```

The following example displays configured VSAN-specific fabric binding information.

```
switch# show fabric-binding database vsan 4
-------------------------------------------------
Vsan   Logging-in Switch WWN     Domain-id
-------------------------------------------------
4      21:00:05:30:23:11:11:11   0x66(102)
4      21:00:05:30:23:1a:11:03    0x19(25)
[Total 2 entries]
```

The following example displays fabric binding statistics.

```
switch# show fabric-binding statistics
Statistics For VSAN: 1
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 4
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 61
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 345
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
```

```
Statistics For VSAN: 346
------------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 347
------------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 348
------------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 789
------------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 790
------------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
```

The following example displays fabric binding status for each VSAN.

```
switch# show fabric-binding status
VSAN 1 :Activated database
VSAN 4 :No Active database
VSAN 61 :Activated database
VSAN 345 :No Active database
VSAN 346 :No Active database
VSAN 347 :No Active database
VSAN 348 :No Active database
VSAN 789 :No Active database
VSAN 790 :No Active database
```

The following example displays EFMD statistics.

```
switch# show fabric-binding efmd statistics

EFMD Protocol Statistics for VSAN 1
---------------------------------------
Merge Requests -> Transmitted : 0 , Received : 0
Merge Accepts  -> Transmitted : 0 , Received : 0
Merge Rejects  -> Transmitted : 0 , Received : 0
Merge Busy     -> Transmitted : 0 , Received : 0
Merge Errors   -> Transmitted : 0 , Received : 0

EFMD Protocol Statistics for VSAN 4
---------------------------------------
Merge Requests -> Transmitted : 0 , Received : 0
```

```
Merge Accepts  -> Transmitted : 0 , Received : 0
Merge Rejects  -> Transmitted : 0 , Received : 0
Merge Busy     -> Transmitted : 0 , Received : 0
Merge Errors   -> Transmitted : 0 , Received : 0

EFMD Protocol Statistics for VSAN 61
---------------------------------------
Merge Requests -> Transmitted : 0 , Received : 0
Merge Accepts  -> Transmitted : 0 , Received : 0
Merge Rejects  -> Transmitted : 0 , Received : 0
Merge Busy     -> Transmitted : 0 , Received : 0
Merge Errors   -> Transmitted : 0 , Received : 0
```

The following example displays EFMD statistics for a specified VSAN.

```
switch# show fabric-binding efmd statistics vsan 4

EFMD Protocol Statistics for VSAN 4
---------------------------------------
Merge Requests -> Transmitted : 0 , Received : 0
Merge Accepts  -> Transmitted : 0 , Received : 0
Merge Rejects  -> Transmitted : 0 , Received : 0
Merge Busy     -> Transmitted : 0 , Received : 0
Merge Errors   -> Transmitted : 0 , Received : 0
```

The following example displays fabric binding violations.

```
switch# show fabric-binding violations
--------------------------------------------------------------------------------
VSAN Switch WWN [domain] Last-Time [Repeat count] Reason
--------------------------------------------------------------------------------
3 20:00:00:05:30:00:4a:1e [*] Nov 25 05:44:58 2003 [2] sWWN not found
3 20:00:00:05:30:00:4a:1e [0xeb] Nov 25 05:46:14 2003 [2] Domain mismatch
4 20:00:00:05:30:00:4a:1e [*] Nov 25 05:46:25 2003 [1] Database mismatch
```

show fc-tunnel

To display configured Fibre Channel tunnel information, use the **show fc-tunnel** command.

show fc-tunnel [**explicit-path** [*name*] | **tunnel-id-map**]

Syntax Description

explicit-path	Displays all configured explicit paths.
name	Specifies the explicit path name. Maximum length is 16 characters.
tunnel-id-map	Displays the mapping information for the outgoing interface.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

Multiple tunnel IDs can terminate at the same interface.

Examples

The following example displays the FC tunnel status

```
switch# show fc-tunnel
fc-tunnel is enabled
```

The following example displays the FC tunnel egress mapping information.

```
switch# show fc-tunnel tunnel-id-map
tunnel id egress interface
    150    fc3/1
    100    fc3/1
```

The following example displays explicit mapping information of the FC tunnel.

```
switch# show fc-tunnel explicit-path
Explicit path name: Alternate1
       10.20.1.2 loose
       10.20.1.3 strict
Explicit path name: User2
       10.20.50.1 strict
       10.20.50.4 loose
```

show fc2

To display FC2 information, use the **show fc2** command.

show fc2 {bind | classf | exchange | exchresp | flogi | nport | plogi | plogi_pwwn | port [brief] | socket | sockexch | socknotify | socknport | vsan}

Syntax Description

bind	Displays FC2 socket bindings.
classf	Displays FC2 classf sessions.
exchange	Displays FC2 active exchanges.
exchresp	Displays FC2 active responder exchanges.
flogi	Displays FC2 FLOGI table.
nport	Displays FC2 local N ports.
plogi	Displays FC2 PLOGI sessions.
plogi_pwwn	Displays FC2 PLOGI pWWN entries.
port [**brief**]	Displays FC2 physical port table.
socket	Displays FC2 active sockets.
sockexch	Displays FC2 active exchanges for each socket.
socknotify	Displays FC2 local N port PLOGI/LOGO notifications for each socket.
socknport	Displays FC2 local nports per each socket.
vsan	Displays FC2 VSAN table.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays FC2 active socket information.

```
switch# show fc2 socket
SOCKET   REFCNT PROTOCOL      PID   RCVBUF  RMEM_USED     QLEN    NOTSK
b2a64b20        2        0     1421    65535          0        0        0
b2a647e0        3        0     1418   262142          0        0        0
b2a644a0        3        0     1417    65535          0        0        0
b2a64160        3        0     1417   262142          0        0        0
b294b180        3        0     1411    65535          0        0        0
b294ae40        3        0     1411    65535          0        0        0
b294a7c0        3        0     1410    65535          0        0        0
b294a480        2        7     1410    65535          0        0        0
b294a140        3        0     1409   262142          0        0        0
b278bb20        3        0     1409   262142          0        0        0
b278b4a0        3        0     1407    65535          0        0        0
b278b160        3        0     1407   256000          0        0        0
b278ae20        3        0     1407    65535          0        0        0
b1435b00        3        0     1408    65535          0        0        0
b1434e00        3        0     1406    65535          0        0        0
b1434ac0        3        0     1406   131072          0        0        0
b1434780        3        0     1406    65535          0        0        0
b1434440        2        0     1405   131072          0        0        0
b1434100        3        0     1405   262142          0        0 b1434440
b22e2420        2        0     1372    65535          0        0        0
...
```

The following example displays FC2 socket binding information.

```
switch# show fc2 bind
  SOCKET RULE   SINDEX   VSAN     D_ID     MASK TYPE  SUBTYPE M_VALUES
b23ba0c0   16  6081000      1        0        0    0 00:00:00 00:00:00:00:00:00:00:00
b2a647e0    7 ffffffff  65535   fffffd   ffffff   22 03:01:00 14:15:16:00:00:00:00:00
b294b180    7 ffffffff  65535   fffffd   ffffff    1 02:01:00 61:62:00:00:00:00:00:00
b294ae40    7 ffffffff  65535   fffc00   ffff00   22 01:01:00 1b:00:00:00:00:00:00:00
b294a7c0    7 ffffffff  65535   fffffd   ffffff    1 01:01:00 10:00:00:00:00:00:00:00
...
```

The following example displays FC2 local N port information.

```
switch# show fc2 nport
REF   VSAN   D_ID   MASK   FL   ST  IFINDEX   CF   TC 2-SO   IC   RC   RS   CS
 EE 3-SO   IC   RC   RS   CS   EE
  1  65535 fffffd ffffff    3    0 ffffffff c800 0128 8000 0000 0000 2112 0064 0
008 8000 0000 0000 2112 0064 0000
  6  65535 fffc00 ffff00  18b    0 ffffffff c800 0128 8000 0000 0000 2112 0064 0
008 8000 0000 0000 2112 0064 0000
  2  65535 fffffa ffffff    3    0 ffffffff c800 0128 8000 0000 0000 2112 0064 0
008 8000 0000 0000 2112 0064 0000
  1  65535 fffffc ffffff    3    0 ffffffff c800 0128 8000 0000 0000 2112 0064 0
008 8000 0000 0000 2112 0064 0000
...
```

The following example displays FC2 PLOGI session information.

```
switch# show fc2 plogi
HIX  ADDRESS   VSAN   S_ID   D_ID  IFINDEX   FL  STATE   CF   TC 2-SO   IC   RC
  RS   CS   EE 3-SO   IC   RC   RS   CS   EE EECNT TCCNT 2CNT 3CNT REFCNT
2157 af364064      1 fffc6c 123400 ffffffff 0000      0 0000 0001 8000 0000 2000
 0256 0001 0001 8000 0000 2000 0256 0001 0000     0     0    0    0      1
```

The following example displays FC2 physical port information.

```
switch# show fc2 port
 IX ST MODE EMUL   TXPKTS    TXDROP     TXERR    RXPKTS    RXDROP  R_A_TOV  E_D_TOV
F-SO   RC   RS   CS    EE 2-SO   RS 3-SO   RS
  0  D    1    0        0        0        0        0         0    10000     2000
8000 0000 2112 0001 0001 8000 0256 8000 0256
  1  D    1    0        0        0        0        0         0    10000     2000
8000 0000 2112 0001 0001 8000 0256 8000 0256
  2  D    1    0        0        0        0        0         0    10000     2000
8000 0000 2112 0001 0001 8000 0256 8000 0256
  3  D    1    0        0        0        0        0         0    10000     2000
8000 0000 2112 0001 0001 8000 0256 8000 0256
  4  D    1    0        0        0        0        0         0    10000     2000
8000 0000 2112 0001 0001 8000 0256 8000 0256
...
```

The following example displays FC2 local N port PLOGI notifications for each socket.

```
switch# show fc2 socknotify
  SOCKET  ADDRESS REF   VSAN   D_ID   MASK   FL   ST  IFINDEX
b2a64160 b27f01e4   6  65535 fffc00 ffff00  18b    0 ffffffff
b294a7c0 b27f01e4   6  65535 fffc00 ffff00  18b    0 ffffffff
af8a3a60 b27f01e4   6  65535 fffc00 ffff00  18b    0 ffffffff
```

The following example displays FC2 local N ports for each socket.

```
switch# show fc2 socknport
  SOCKET  ADDRESS REF   VSAN   D_ID   MASK   FL   ST  IFINDEX
b2a64160 b27f01e4   6  65535 fffc00 ffff00  18b    0 ffffffff
b294b180 b27f0294   1  65535 fffffd ffffff    3    0 ffffffff
b294a7c0 b27f01e4   6  65535 fffc00 ffff00  18b    0 ffffffff
b278ae20 b27f0134   2  65535 fffffa ffffff    3    0 ffffffff
b1434e00 b27f0134   2  65535 fffffa ffffff    3    0 ffffffff
b1434780 b27f0084   1  65535 fffffc ffffff    3    0 ffffffff
af8a3a60 b27f01e4   6  65535 fffc00 ffff00  18b    0 ffffffff
```

The following example displays FC2 VSAN table.

```
switch# show fc2 vsan
  VSAN      X_ID  E_D_TOV  R_A_TOV                      WWN
     1         4     2000    10000  20:01:00:05:30:00:58:1f
     2         1     2000    10000  20:02:00:05:30:00:58:1f
     3         1     2000    10000  20:03:00:05:30:00:58:1f
     4         1     2000    10000  20:04:00:05:30:00:58:1f
     5         1     2000    10000  20:05:00:05:30:00:58:1f
     6         1     2000    10000  20:06:00:05:30:00:58:1f
     7         1     2000    10000  20:07:00:05:30:00:58:1f
     8         1     2000    10000  20:08:00:05:30:00:58:1f
     9         1     2000    10000  20:09:00:05:30:00:58:1f
    10         1     2000    10000  20:0a:00:05:30:00:58:1f
    11         1     2000    10000  20:0b:00:05:30:00:58:1f
    12         1     2000    10000  20:0c:00:05:30:00:58:1f
    13         1     2000    10000  20:0d:00:05:30:00:58:1f
    14         1     2000    10000  20:0e:00:05:30:00:58:1f
    15         1     2000    10000  20:0f:00:05:30:00:58:1f
    16         1     2000    10000  20:10:00:05:30:00:58:1f
    17         1     2000    10000  20:11:00:05:30:00:58:1f
    18         1     2000    10000  20:12:00:05:30:00:58:1f
....
```

show fcalias

To display the member name information in a Fibre Channel alias (fcalias), use the **show fcalias** command.

show fcalias [**name** *fcalias-name*] [**pending**] [**vsan** *vsan-id*]

Syntax Description

name *fcalias-name*	Displays fcalias information for a specific name. The maximum length is 64.
pending	Displays pending fcalias information.
vsan *vsan-id*	Displays fcalias information for a VSAN. The range is 1 to 4093.

Defaults

Displays a list of all global fcaliases and all VSAN dependent fcaliases.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
2.0(1b)	Added the **pending** keyword.

Usage Guidelines

To make use of fcaliases as device names instead of using the cryptic device name, add only one member per fcalias.

Examples

The following example displays fcalias configuration information.

```
switch# show fcalias vsan 1
fcalias name Alias2 vsan 1

fcalias name Alias1 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:9c:48:e5
```

Related Commands

Command	Description
fcalias name	Configures fcalias names.

show fcanalyzer

To display the list of hosts configured for a remote capture, use the **show fcanalyzer** command.

show fcanalyzer

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The `DEFAULT` keyword shown with an `ActiveClient` entry specifies that the default port is used in attempting the connection to the client.

Examples

Displays Configured Hosts

```
switch# show fcanalyzer
PassiveClient = 10.21.0.3
PassiveClient = 10.21.0.3
ActiveClient = 10.21.0.3, DEFAULT
```

show fcc

To view FCC settings, use the **show fcc** commands.

show fcc [**statistics interface** {**fc** *slot*/*port* | **fcip** *fcip-id* | **iscsi** *slot*/*port*}]

Syntax Description

statistics interface	Displays FCC statistics for a specified interface.
fc *slot*/*port*	Specifies a Fibre Channel interface.
fcip *fcip-id*	Specifies an FCIP interface. The range is 1 to 255.
iscsi *slot*/*port*	Specifies an iSCSI interface.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

Displays configured FCC information

```
switch# show fcc
fcc is disabled
fcc is applied to frames with priority up to 4
```

show fcdomain

To display the Fibre Channel domain (fcdomain) information, use the **show fcdomain** command.

show fcdomain [**address-allocation** [**cache**] |
allowed |
domain-list |
fcid persistent [**unused**] |
pending [**vsan** *vsan-id*] |
pending-diff [**vsan** *vsan-id*] |
session-status [**vsan** *vsan-id*] |
statistics [**interface** {**fc** *slot/port* [**vsan** *vsan-id*] | **fcip** *fcip-id* [**vsan** *vsan-id*] | **iscsi** *slot/port*} |
port-channel [**vsan** *vsan-id*]] |
status |
vsan *vsan-id*]

Syntax Description

address-allocation	Displays statistics for the FC ID allocation.
cache	Reassigns the FC IDs for a device (disk or host) that exited and reentered the fabric for the principal switch. In the cache content, VSAN refers to the VSAN that contains the device, WWN refers to the device that owned the FC IDs, and mask refers to a single or entire area of FC IDs.
allowed	Displays a list of allowed domain IDs.
domain-list	Displays a list of domain IDs granted by the principal switch.
fcid persistent	Displays persistent FC IDs (across reboot)
pending	Displays the pending configuration.
pending-diff	Displays the difference between the running configuration and the pending configuration.
session-status	Displays the last action performed by FC domain.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093).
statistics interface	Displays the statistics of FC domain
fc *slot/port*	Specifies a Fibre Channel interface.
fcip *fcip-id*	Specifies an FCIP interface. The range is 1 to 255.
iscsi *slot/port*	Specifies an iSCSI interface.
port-channel *number*	Specifies a PortChannel interface. The range is 1 to 128.
status	Displays all VSAN-independent information in FC domain.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
2.1(1a)	The **domain-list** display was modified to include a virtual IVR description.
3.0(1)	Added the **pending**, **pending-diff**, **session-status**, and **status** options.

Usage Guidelines

Issuing the **show fcdomain** with no arguments displays all VSANs. The VSANs should be active or you will get an error.

Examples

The following example displays the fcdomain information for VSAN 1.

```
switch# show fcdomain vsan 1
The local switch is a Subordinated Switch.

Local switch run time information:
        State: Stable
        Local switch WWN:    20:01:00:05:30:00:51:1f
        Running fabric name: 10:00:00:60:69:22:32:91
        Running priority: 128
        Current domain ID: 0x64(100) ß verify domain id

Local switch configuration information:
        State: Enabled
        Auto-reconfiguration: Disabled
        Contiguous-allocation: Disabled
        Configured fabric name: 41:6e:64:69:61:6d:6f:21
        Configured priority: 128
        Configured domain ID: 0x64(100) (preferred)

Principal switch run time information:
        Running priority: 2

Interface               Role          RCF-reject
----------------    -------------    ------------
fc2/1               Downstream       Disabled
fc2/2               Downstream       Disabled
fc2/7               Upstream         Disabled
----------------    -------------    ------------
```

The following example displays the fcdomain domain-list information for VSAN 76.

```
switch# show fcdomain domain-list vsan 76

Number of domains: 3
Domain ID              WWN
---------    -----------------------
0xc8(200)    20:01:00:05:30:00:47:df [Principal]
 0x63(99)    20:01:00:0d:ec:08:60:c1 [Local]
 0x61(97)    50:00:53:0f:ff:f0:10:06 [Virtual (IVR)]
```

Table 22-1 describes the significant fields shown in the **show fcdomain domain-list** command output.

Table 22-1 show fcdomain Field Descriptions

Field	Description
Domain ID	Lists the domain IDs corresponding to the WWN.
WWN	Indicates the WWN of the switch (physical or virtual) that requested the corresponding domain ID.
Principal	Indicates which row of the display lists the WWN and domain ID of the principal switch in the VSAN.
Local	Indicates which row of the display lists the WWN and domain ID of the local switch (the switch where you entered the **show fcdomain domain-list** command).
Virtual (IVR)	Indicates which row of the display lists the WWN of the virtual switch used by the Inter-VSAN Routing (IVR) manager to obtain the domain ID.

The following example displays the allowed domain ID lists.

```
switch# show fcdomain allowed vsan 1
Assigned or unallowed domain IDs: 1-96,100,111-239.
[Interoperability Mode 1] allowed domain IDs: 97-127.
[User] configured allowed domain IDs: 50-110.
```

The following example shows the status of CFS distribution for allowed domain ID lists.

```
switch# show fcdomain status
CFS distribution is enabled
```

The following example displays pending configuration changes.

```
switch# show fcdomain pending vsan 10

Pending Configured Allowed Domains
---------------------------------
VSAN 10
Assigned or unallowed domain IDs: 1-9,24,100,231-239.
[User] configured allowed domain IDs: 10-230.
```

The following example displays the differences between the pending configuration and the current configuration.

```
switch# show fcdomain pending-diff vsan 10

Current Configured Allowed Domains
---------------------------------
VSAN 10
Assigned or unallowed domain IDs: 24,100.
[User] configured allowed domain IDs: 1-239.
Pending Configured Allowed Domains
---------------------------------
VSAN 10
Assigned or unallowed domain IDs: 1-9,24,100,231-239.
[User] configured allowed domain IDs: 10-230.
```

The following example displays the status of the distribution session.

```
switch# show fcdomain session-status vsan 1
Last Action: Distribution Enable
Result: Success
```

Related Commands

Command	Description
fcdomain	Configures the Fibre Channel domain feature.

show fcdroplatency

To display the configured Fibre Channel latency parameters, use the **show fcdroplatency** command.

show fcdroplatency [**network** | **switch**]

Syntax Description

network	Network latency in milliseconds.
switch	Switch latency in milliseconds.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the configured Fibre Channel latency parameters.

```
switch# show fcdroplatency
switch latency value:4000 milliseconds
network latency value:5000 milliseconds
```

show fcflow stats

To display the configured Fibre Channel flow (fcflow) information, use the **show fcflow stats** command.

show fcflow stats [**aggregated** | **usage**] **module** *slot* [**index** *flow-index*]

Syntax Description

aggregated	Displays aggregated fcflow statistics.
usage	Displays flow index usage
module *slot*	Displays fcflow statistics for a module in the specified slot.
index *flow-index*	Specifies a fcflow index.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays aggregated fcflow details for the specified module.

```
switch# show fcflow stats aggregated module 2
Idx  VSAN # frames # bytes
---- ---- -------- -------
0000 4    387,653  674,235,875
0001 6    34,402   2,896,628
```

The following example displays fcflow details for the specified module.

```
switch# show fcflow stats module 2
Idx  VSAN D ID        S ID        mask      # frames # bytes
---- ---- ----------- ----------- -----     -------- -------
0000 4    032.001.002 007.081.012 ff.ff.ff   387,653  674,235,875
0001 6    004.002.001 019.002.004 ff.00.00   34,402   2,896,628
```

The following example displays fcflow index usage for the specified module.

```
switch# show fcflow stats usage module 2
2 flows configured
configured flow : 3,7
```

show fcfwd

To display the configured fcfwd tables and statistics, use the **show fcfwd** command.

show fcfwd {idxmap [**interface-toport** | **port-to-interface** | **statistics**] | **pcmap** [**interface**] | **sfib** [**multicast** | **statistics** | **unicast**] | **spanmap** [**rx** | **tx**]**}**

Syntax Description

idxmap	Displays FC forward index tables.
interface-to-port	Displays interface index to port index table.
port-to-interface	Displays port index to interface index table.
statistics	Displays index table statistics.
pcmap	Displays FC forward PortChannel table.
interface	Displays PortChannel table for an interface.
sfib	Displays software forwarding tables.
multicast	Displays multicast software forwarding tables.
statistics	Displays software forwarding statistics.
unicast	Displays unicast software forwarding tables.
spanmap	Displays SPAN map tables.
rx	Displays SPAN map table in ingress -rx direction.
tx	Displays SPAN map table in egress -tx direction.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays fcfwd SPAN map receive information.

```
switch# show fcfwd spanmap rx
SPAN source information: size [c8]
dir source               vsan   bit   drop_thresh destination
```

show fcid-allocation

Use the **show fcid allocation** command to display the Fibre Channel area list of company IDs.

show fcid-allocation area company-id [*company-id]*

Syntax Description

area	Selects the auto area list of company IDs.
company-id	Selects company ID list.
company-id	Selects the individual company ID (also know as Organizational Unit Identifier, or OUI) to display.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0	New command

Examples

The following example shows the Fibre Channel area company list of company IDs.

```
switch# show fcid-allocation area company-id

Fcid area allocation company id info:

    00:50:2E
    00:50:8B
    00:60:B0
    00:A0:B8
    00:E0:69
    00:E0:8B
    00:32:23 +


Total company ids: 7
+ - Additional user configured company ids.
* - Explicitly deleted company ids from default list.
switch#
```

Table 22-2 describes the significant fields shown in the display.

Table 22-2 show fcid-allocation area company Field Descriptions

Field	Description
+	Indicates a company ID added to the default list.
–	Indicates a company ID deleted from the default list.

show fcip

To display FCIP profile information, use the **show fcip** command.

show fcip {**host-map** *fcip-id* | **profile** [*profile-id* | **all**] | **summary** | **tape-session** {**summary** | **tunnel** *tunnel-id* {**host-end** | **target-end**}} | **target-map** *fcip-id* | **wa-login-list** *tunnel-id*}

Syntax Description

host-map *fcip-id*	Displays the information for a specified map. The range is 1 to 255.
profile	Displays the information for a profile.
profile-id	Specifies the profile ID. The range is 1 to 255.
all	Specifies all profile IDs.
summary	Displays summary information.
tape-session	Displays tape session information.
tunnel *tunnel-id*	Displays information for a specified FCIP tunnel ID. The range is 1 to 255.
host-end	Displays information for the host end.
target-end	Displays information for the target end.
target-map *fcip-id*	Displays information for a specified target map. The range is 1 to 255.
wa-login-list *tunnel-id*	Displays the write acceleration login list for a specified FCIP tunnel ID. The range is 1 to 255.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.
2.0(1b)	Added the **host-map**, **summary**, and **target-map** keywords.
3.0(1)	Added the **tape-session**, **tunnel**, **host-end**, **target-end**, and **wa-login-list** keywords.

Usage Guidelines

None.

Examples

The following example displays all FCIP profiles.

```
switch# show fcip profile all
-------------------------------------------------
ProfileId       Ipaddr          TcpPort
-------------------------------------------------
1               41.1.1.2        3225
2               10.10.100.154   3225
3               43.1.1.2        3225
4               44.1.1.100      3225
```

```
6               46.1.1.2        3225
7               47.1.1.2        3225
```

The following example displays information for a specified FCIP profile.

```
switch# show fcip profile 7
FCIP Profile 7
    Internet Address is 47.1.1.2 (interface GigabitEthernet4/7)
    Listen Port is 3225
    TCP parameters
        SACK is disabled
        PMTU discovery is enabled, reset timeout is 3600 sec
        Keep alive is 60 sec
        Minimum retransmission timeout is 300 ms
        Maximum number of re-transmissions is 4
        Send buffer size is 0 KB
        Maximum allowed bandwidth is 1000000 kbps
        Minimum available bandwidth is 15000 kbps
        Estimated round trip time is 1000 usec
```

The following example displays FCIP summary information.

```
switch# show fcip summary
sw172-22-46-223# show fcip summary

--------------------------------------------------------------------------------
Tun prof    Eth-if    peer-ip       Status T W T Enc Comp  Bandwidth   rtt
                                           E A A            max/min    (us)
--------------------------------------------------------------------------------
1   1    GE1/1      10.10.11.2       DOWN  N N N  N    N   1000M/500M  1000
2   2    GE1/2      10.10.60.2       DOWN  N N N  N    N   1000M/500M  1000
```

Table 22-3 describes the significant fields shown in the previous display.

Table 22-3 show fcip summary Field Descriptions

Field	Description
Tun	Tunnel number for the row. For example, a number 1 indicates tunnel fcip1 and a number 2 indicates fcip2.
prof	Tunnel profile.
Eth-if	Ethernet interface to which this tunnel is bound.
peer-ip	IP address of the tunnel peer port on the far end of the tunnel.
Status	State of the tunnel (UP or DOWN).
TE	Tunnel operating in TE mode (**Y**es or **N**o).
WA	Write acceleration enabled (**Y**es or **N**o).
TA	Tape acceleration enabled (**Y**es or **N**o).
Enc	Encryption enabled (**Y**es or **N**o).
Bandwidth max/min	Maximum and minimum bandwidth configured in the profile to which this tunnel is bound.
rtt (us)	Round trip time (RTT) in microseconds.

Related Commands

Command	Description
fcip enable	Configures FCIP parameters.

show fcns database

To display the results of the discovery, or to display the name server database for a specified VSAN or for all VSANs, use the **show fcns database** command.

show fcns database {detail [**vsan** *vsan-id*] | **domain** *domain-id* [**detail**] [**vsan** *vsan-range*] | **fcid** *fcid-id* [**detail**] **vsan** *vsan-range* | **local** [**detail**] [**vsan** *vsan-range*] | **vsan** *vsan-id*}

Syntax Description

detail	Displays all objects in each entry.
vsan *vsan-id*	Displays entries for a specified VSAN ID. The range is 1 to 4093.
domain *domain-id*	Displays entries in a domain.
fcid *fcid-id*	Displays entry for the given port.
local	Displays local entries.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(2)	This command was introduced.

Usage Guidelines

The discovery can take several minutes to complete, especially if the fabric is large fabric or if several devices are slow to respond.

Virtual enclosure ports can be viewed using the **show fcns database** command.

Examples

The following example displays the contents of the FCNS database:

```
switch# show fcns database
VSAN 1:
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x020101    N     22:04:00:05:30:00:35:e1 (Cisco)         scsi-fcp:init isc..w <--iSCSI
0x020102    N     22:02:00:05:30:00:35:e1 (Cisco)         scsi-fcp:init isc..w initiator
0x0205d4    NL    21:00:00:04:cf:da:fe:c6 (Seagate)       scsi-fcp:target
0x0205d5    NL    21:00:00:04:cf:e6:e4:4b (Seagate)       scsi-fcp:target
0x0205d6    NL    21:00:00:04:cf:e6:21:ac (Seagate)       scsi-fcp:target
0x0205d9    NL    21:00:00:04:cf:e6:19:9b (Seagate)       scsi-fcp:target
0x0205da    NL    21:00:00:04:cf:e6:19:62 (Seagate)       scsi-fcp:target
0x0205dc    NL    21:00:00:04:cf:e6:e9:82 (Seagate)       scsi-fcp:target
0x0205e0    NL    21:00:00:04:cf:e6:21:06 (Seagate)       scsi-fcp:target
0x0205e1    NL    21:00:00:04:cf:e6:e0:eb (Seagate)       scsi-fcp:target

Total number of entries = 10
```

```
VSAN 2:
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0xef0001    N     22:02:00:05:30:00:35:e1 (Cisco)         scsi-fcp:init isc..w

Total number of entries = 1

VSAN 3:
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0xed0001    N     22:02:00:05:30:00:35:e1 (Cisco)         scsi-fcp:init isc..w

Total number of entries = 1
```

The following example displays the detailed contents of the FCNS database.

```
switch# show fcns database detail
------------------------
VSAN:1     FCID:0x020101
------------------------
port-wwn (vendor)     :22:04:00:05:30:00:35:e1 (Cisco)
node-wwn              :22:03:00:05:30:00:35:e1
class                 :2,3
node-ip-addr          :10.2.2.12
ipa                   :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name    :
symbolic-node-name    :iqn.1991-05.com.microsoft:oasis2-dell
port-type             :N
port-ip-addr          :0.0.0.0
fabric-port-wwn       :22:01:00:05:30:00:35:de
hard-addr             :0x000000
------------------------
VSAN:1     FCID:0x020102
------------------------
port-wwn (vendor)     :22:02:00:05:30:00:35:e1 (Cisco)
node-wwn              :22:01:00:05:30:00:35:e1
class                 :2,3
node-ip-addr          :10.2.2.11
ipa                   :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name    :
symbolic-node-name    :iqn.1987-05.com.cisco.01.14ac33ba567f986f174723b5f9f2377
port-type             :N
port-ip-addr          :0.0.0.0
fabric-port-wwn       :22:01:00:05:30:00:35:de
hard-addr             :0x000000

...
Total number of entries = 10
==========================================================================
------------------------
VSAN:2     FCID:0xef0001
------------------------
port-wwn (vendor)     :22:02:00:05:30:00:35:e1 (Cisco)
node-wwn              :22:01:00:05:30:00:35:e1
class                 :2,3
node-ip-addr          :10.2.2.11
ipa                   :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name    :
symbolic-node-name    :iqn.1987-05.com.cisco.01.14ac33ba567f986f174723b5f9f2377
```

```
port-type             :N
port-ip-addr          :0.0.0.0
fabric-port-wwn       :22:01:00:05:30:00:35:de
hard-addr             :0x000000

Total number of entries = 1


...
```

The following example displays the management VSAN (VSAN 2).

```
switch# show fcns database vsan 2
VSAN 2:
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x6d0001    N     10:00:00:05:30:00:94:9f (Cisco)         ipfc
0x6d0002    N     10:00:00:05:30:00:94:a0 (Cisco)         ipfc virtual:..c_port
0x6d0003    N     24:15:00:05:30:00:94:a0 (Cisco)         virtual:volume_owner
...
Total number of entries = 24
```

The following example displays the database for all configured VSANs.

```
switch# show fcns database
VSAN 2:
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x6d0001    N     10:00:00:05:30:00:94:9f (Cisco)         ipfc
0x6d0002    N     10:00:00:05:30:00:94:a0 (Cisco)         ipfc virtual:..c_port
0x6d0003    N     24:15:00:05:30:00:94:a0 (Cisco)         virtual:volume_owner
...
Total number of entries = 24
VSAN 3:
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x650001    N     24:0c:00:05:30:00:94:a0 (Cisco)         scsi-fcp:init vir..t
...
0x720101    NL    21:00:00:20:37:65:1c:cb (Company)       scsi-fcp
...
Total number of entries = 30
VSAN 4:
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x6b0001    N     23:26:00:05:30:00:59:20 (Cisco)         scsi-fcp:init vir..t
...
0x7800b5    NL    22:00:00:20:37:46:78:97 (Company)       scsi-fcp
...
0x780100    N     50:06:04:82:bf:d0:cf:4b (Company)           scsi-fcp 250
...
Total number of entries = 27
VSAN 5:
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x6f0001    N     23:43:00:05:30:00:59:20 (Cisco)         scsi-fcp:target vi..
...
```

Related Commands

Command	Description
asm mgmt-vsan	Displays the CPP interface configuration for a specified interface.

show fcns statistics

To display the statistical information for a specified VSAN or for all VSANs, use the **show fcns statistics** command.

show fcns statistics [**detail**] [**vsan** *vsan-id*]

Syntax Description

detail	Displays detailed statistics.
vsan *vsan-id*	Displays statistics for the specified VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays statistical information for a specified VSAN.

```
switch# show fcns statistics
registration requests received = 27
deregistration requests received = 0
queries received = 57
queries sent = 10
reject responses sent = 14
RSCNs received = 0
RSCNs sent = 0
switch#
```

show fcroute

Use the **show fcroute** command to view specific information about existing Fibre Channel and FSPF configurations.

show fcroute {**distance** | **label** [*label*] **vsan** *vsan-id* | **multicast** [*fc-id* **vsan** *vsan-id* | **vsan** *vsan-id*] | **summary** [**vsan** *vsan-id*] | **unicast** [[**host**] *fc-id fc-mask* **vsan** *vsan-id* | **vsan** *vsan-id*]}

Syntax Description

distance	Displays FC route preference.
label	Displays label routes.
multicast	Displays FC multicast routes.
summary	Displays FC routes summary.
unicast	Displays FC unicast routes.
vsan *vsan-id*	The ID of the VSAN (from 1 to 4093).
fcid-id	The Fibre Channel ID.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

When the number of routes are displayed in the command output, both visible and hidden routes are included in the total number of routes.

Examples

The following example displays administrative distance.

```
switch# show fcroute distance

        Route
UUID    Distance        Name
----    --------        ----
10      20              RIB
22      40              FCDOMAIN
39      80              RIB-CONFIG
12      100             FSPF
17      120             FLOGI
21      140             TLPM
14      180             MCAST
64      200             RIB-TEST
```

The following example displays multicast routing information.

```
switch# show fcroute multicast
VSAN FC ID    # Interfaces
---- -------- ------------
1    0xffffff 0
2    0xffffff 1
3    0xffffff 1
4    0xffffff 0
5    0xffffff 0
6    0xffffff 0
7    0xffffff 0
8    0xffffff 0
9    0xffffff 0
10   0xffffff 0
```

The following example displays FCID information for a specified VSAN.

```
switch# show fcroute multicast vsan 3

VSAN FC ID    # Interfaces
---- -------- ------------
3    0xffffff 1
```

The following example displays FCID and interface information for a specified VSAN.

```
switch# show fcroute multicast 0xffffff vsan 2

VSAN FC ID    # Interfaces
---- -------- ------------
2    0xffffff 1
  fc1/1
```

The following example displays unicast routing information.

```
switch# show fcroute unicast
D:direct R:remote P:permanent V:volatile A:active N:non-active
                                                  # Next
Protocol VSAN    FC ID/Mask     RCtl/Mask Flags Hops   Cost
-------- ---- -------- -------- ---- ---- ----- ------ ----
static   1    0x010101 0xffffff 0x00 0x00 D P A 1      10
static   2    0x111211 0xffffff 0x00 0x00 R P A 1      10
fspf     2    0x730000 0xff0000 0x00 0x00 D P A 4      500
fspf     3    0x610000 0xff0000 0x00 0x00 D P A 4      500
static   4    0x040101 0xffffff 0x00 0x00 R P A 1      103
static   4    0x040102 0xffffff 0x00 0x00 R P A 1      103
static   4    0x040103 0xffffff 0x00 0x00 R P A 1      103
static   4    0x040104 0xffffff 0x00 0x00 R P A 1      103
static   4    0x111211 0xffffff 0x00 0x00 D P A 1      10
```

The following example displays unicast routing information for a specified VSAN.

```
switch# show fcroute unicast vsan 4

D:direct R:remote P:permanent V:volatile A:active N:non-active
                                                  # Next
Protocol VSAN    FC ID/Mask     RCtl/Mask Flags Hops   Cost
-------- ---- -------- -------- ---- ---- ----- ------ ----
static   4    0x040101 0xffffff 0x00 0x00 R P A 1      103
static   4    0x040102 0xffffff 0x00 0x00 R P A 1      103
static   4    0x040103 0xffffff 0x00 0x00 R P A 1      103
static   4    0x040104 0xffffff 0x00 0x00 R P A 1      103
static   4    0x111211 0xffffff 0x00 0x00 D P A 1      10
```

The following example displays unicast routing information for a specified FCID.

```
switch# show fcroute unicast 0x040101 0xffffff vsan 4

D:direct R:remote P:permanent V:volatile A:active N:non-active
                                                    # Next
Protocol VSAN    FC ID/Mask     RCtl/Mask Flags Hops   Cost
-------- ---- -------- -------- ---- ---- ----- ------ ----
static   4    0x040101 0xffffff 0x00 0x00 R P A 1      103
  fc1/2 Domain 0xa6(166)
```

The following example displays route database information.

```
switch# show fcroute summary

FC route database created Tue Oct 29 01:24:23 2002
VSAN    Ucast   Mcast   Label   Last Modified Time
----    -----   -----   -----   ------------------
1       2       1       0       Tue Oct 29 18:07:02 2002
2       3       1       0       Tue Oct 29 18:33:24 2002
3       2       1       0       Tue Oct 29 18:10:07 2002
4       6       1       0       Tue Oct 29 18:31:16 2002
5       1       1       0       Tue Oct 29 01:34:39 2002
6       1       1       0       Tue Oct 29 01:34:39 2002
7       1       1       0       Tue Oct 29 01:34:39 2002
8       1       1       0       Tue Oct 29 01:34:39 2002
9       1       1       0       Tue Oct 29 01:34:39 2002
10      1       1       0       Tue Oct 29 01:34:39 2002
Total   19      10      0
```

The following example displays route database information for a specified VSAN.

```
switch# show fcroute summary vsan 4

FC route database created Tue Oct 29 01:24:23 2002
VSAN    Ucast   Mcast   Label   Last Modified Time
----    -----   -----   -----   ------------------
4       6       1       0       Tue Oct 29 18:31:16 2002
Total   6       1       0
```

show fcs

Use the **show fcs** commands to display the status of the fabric configuration.

show fcs {database [vsan *vsan-id*] | **ie** [**nwwn** *wwn*] **vsan** *vsan-id* | **platform** [**name** *string*] **vsan** *vsan-id* | **port** [**pwwn** *wwn*] **vsan** *vsan-id*] | **statistics vsan** *vsan-id* | **vsan}**

Syntax Description

database	Displays local database of FCS.
ie	Displays Interconnect Element Objects Information.
nwwn *wwn*	Specifies a node WWN id. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
platform	Displays Platform Objects Information.
name *string*	Specifies a platform name. Maximum length is 255 characters.
port	Displays Port Objects Information.
pwwn *wwn*	Specifies a port WWN id. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
statistics	Displays statistics for FCS packets.
vsan	Displays list of all the VSANs and plat-check-mode for each.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays FCS database information.

```
switch# show fcs database

FCS Local Database in VSAN: 1
------------------------------
Switch WWN               : 20:01:00:05:30:00:16:df
Switch Domain Id         : 0x7f(127)
Switch Mgmt-Addresses    : snmp://172.22.92.58/eth-ip
                           http://172.22.92.58/eth-ip
Fabric-Name              : 20:01:00:05:30:00:16:df
Switch Logical-Name      : 172.22.92.58
Switch Information List  : [Cisco Systems*DS-C9509*0*20:00:00:05:30:00
Switch Ports:
--------------------------------------------------------------------
Interface  pWWN                      Type     Attached-pWWNs
```

```
-------------------------------------------------------------------
fc2/1      20:41:00:05:30:00:16:de  TE       20:01:00:05:30:00:20:de
fc2/2      20:42:00:05:30:00:16:de  Unknown  None
fc2/17     20:51:00:05:30:00:16:de  TE       20:0a:00:05:30:00:20:de

FCS Local Database in VSAN: 5
------------------------------
Switch WWN               : 20:05:00:05:30:00:12:5f
Switch Domain Id         : 0xef(239)
Switch Mgmt-Addresses    : http://172.22.90.171/eth-ip
                           snmp://172.22.90.171/eth-ip
                           http://10.10.15.10/vsan-ip
                           snmp://10.10.15.10/vsan-ip
Fabric-Name              : 20:05:00:05:30:00:12:5f
Switch Logical-Name      : 172.22.90.171
Switch Information List  : [Cisco Systems*DS-C9509**20:00:00:05:30:00:12:5e]
Switch Ports:
-------------------------------------------------------------------
Interface  pWWN                     Type     Attached-pWWNs
-------------------------------------------------------------------
fc3/1      20:81:00:05:30:00:12:5e  TE       22:01:00:05:30:00:12:9e
fc3/2      20:82:00:05:30:00:12:5e  TE       22:02:00:05:30:00:12:9e
fc3/3      20:83:00:05:30:00:12:5e  TE       22:03:00:05:30:00:12:9e
```

The following example displays Interconnect Element object information for a specific VSAN.

```
switch# show fcs ie vsan  1

IE List for VSAN: 1
-------------------------------------------------------------------
IE-WWN                  IE-Type                          Mgmt-Id
-------------------------------------------------------------------
20:01:00:05:30:00:16:df  Switch (Local)                  0xfffc7f
20:01:00:05:30:00:20:df  Switch (Adjacent)               0xfffc64
[Total 2 IEs in Fabric]
```

This command displays Interconnect Element object information for a specific WWN.

```
switch# show fcs ie nwwn 20:01:00:05:30:00:16:df vsan 1
IE Attributes
-------------
Domain-Id = 0x7f(127)
Management-Id = 0xfffc7f
Fabric-Name = 20:01:00:05:30:00:16:df
Logical-Name = 172.22.92.58
Management Address List =
        snmp://172.22.92.58/eth-ip
        http://172.22.92.58/eth-ip
Information List:
        Vendor-Name = Cisco Systems
        Model Name/Number = DS-C9509
        Release-Code = 0
```

This command displays platform information.

```
switch# show fcs platform name SamplePlatform vsan 1
Platform Attributes
-------------------
Platform Node Names:
        11:22:33:44:55:66:77:88
Platform Type = Gateway
Platform Management Addresses:
        1.1.1.1
```

This command displays platform information within a specified VSAN.

```
switch# show fcs platform vsan 1
Platform List for VSAN: 1
Platform-Names
--------------
SamplePlatform
[Total 1 Platforms in Fabric]
```

This command displays FCS port information within a specified VSAN.

```
switch# show fcs port vsan 24
Port List in VSAN: 24
                -- IE WWN: 20:18:00:05:30:00:16:df  --
------------------------------------------------------------------------
Port-WWN                 Type      Module-Type            Tx-Type
------------------------------------------------------------------------
20:41:00:05:30:00:16:de  TE_Port   SFP with Serial Id      Shortwave Laser

20:51:00:05:30:00:16:de  TE_Port   SFP with Serial Id      Shortwave Laser

[Total 2 switch-ports in IE]
                -- IE WWN: 20:18:00:05:30:00:20:df  --
------------------------------------------------------------------------
Port-WWN                 Type      Module-Type            Tx-Type
------------------------------------------------------------------------
20:01:00:05:30:00:20:de  TE_Port   SFP with Serial Id      Shortwave Laser

20:0a:00:05:30:00:20:de  TE_Port   SFP with Serial Id      Shortwave Laser

[Total 2 switch-ports in IE]
```

This command displays ports within a specified WWN.

```
switch# show fcs port pwwn 20:51:00:05:30:00:16:de vsan 24
Port Attributes
---------------
Port Type = TE_Port
Port Number = 0x1090000
Attached-Port-WWNs:
        20:0a:00:05:30:00:20:de
Port State = Online
```

This command displays FCS statistics.

```
switch# show fcs statistics

FCS Statistics for VSAN: 1
---------------------------
FCS Rx Get Reqs   :2
FCS Tx Get Reqs   :7
FCS Rx Reg Reqs   :0
FCS Tx Reg Reqs   :0
FCS Rx Dereg Reqs :0
FCS Tx Dereg Reqs :0
FCS Rx RSCNs      :0
FCS Tx RSCNs      :3
FCS Rx RJTs       :3
FCS Tx RJTs       :0
FCS Rx ACCs       :4
FCS Tx ACCs       :2
FCS No Response   :0
FCS Retransmit    :0

FCS Statistics for VSAN: 30
---------------------------
FCS Rx Get Reqs   :2
FCS Tx Get Reqs   :2
FCS Rx Reg Reqs   :0
FCS Tx Reg Reqs   :0
FCS Rx Dereg Reqs :0
FCS Tx Dereg Reqs :0
FCS Rx RSCNs      :0
FCS Tx RSCNs      :0
FCS Rx RJTs       :0
FCS Tx RJTs       :0
FCS Rx ACCs       :2
FCS Tx ACCs       :2
FCS No Response   :0
FCS Retransmit    :0
```

show fcsp

To display the status of the Fibre Channel Security Protocol (FC-SP) configuration, use the **show fcsp** commands.

show fcsp [**asciiwwn** *ascii-wwn* | **dhchap** [**database**] | **interface fc** *slot/port* [**statistics** | **wwn**] | **fcip** *interface-number* [**statistics** | **wwn**]]

Syntax Description

asciiwwn *ascii-wwn*	Displays the ASCII representation of the WWN used with AAA server.
dhchap	Displays the DHCHAP hash algorithm status.
database	Displays the contents of the local DHCHAP database.
interface	Displays the FC-SP settings for a FC or FCIP interface.
fc *slot/port*	Displays the Fibre Channel interface in the specified slot and port.
fcip *interface-number*	Displays the description of the specified FCIP interface from 1 to 255.
statistics	Displays the statistics for the specified interface.
wwn	Displays the FC-SP identity of the other device.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays DHCHAP configurations in FC interfaces.

```
switch# show fcsp interface fc1/9

fc1/9:
        fcsp authentication mode:SEC_MODE_ON
        Status: Successfully authenticated
```

The following example displays DHCHAP statistics for a FC interfaces.

```
switch# show fcsp interface fc1/9 statistics

fc1/9:
        fcsp authentication mode:SEC_MODE_ON
        Status: Successfully authenticated
        Statistics:
        FC-SP Authentication Succeeded:5
        FC-SP Authentication Failed:0
        FC-SP Authentication Bypassed:0
```

The following example displays the FC-SP WWN of the device connected through a specified interface.

```
switch# show fcsp interface fc 2/1 wwn

fc2/1:
        fcsp authentication mode:SEC_MODE_ON
        Status: Successfully authenticated
        Other device's WWN:20:00:00:e0:8b:0a:5d:e7
```

The following example displays hash algorithm and DHCHAP groups configured for the local switch.

```
switch# show fcsp dhchap
Supported Hash algorithms (in order of preference):
DHCHAP_HASH_MD5
DHCHAP_HASH_SHA_1

Supported Diffie Hellman group ids (in order of preference):
DHCHAP_GROUP_NULL
DHCHAP_GROUP_1536
DHCHAP_GROUP_1024
DHCHAP_GROUP_1280
DHCHAP_GROUP_2048
```

The following example displays the DHCHAP local password database.

```
switch# show fcsp dhchap database
DHCHAP Local Password:
        Non-device specific password:********
        Password for device with WWN:29:11:bb:cc:dd:33:11:22 is ********
        Password for device with WWN:30:11:bb:cc:dd:33:11:22 is ********

Other Devices' Passwords:
        Password for device with WWN:00:11:22:33:44:aa:bb:cc is ********
```

The following example displays he ASCII representation of the device WWN.

```
switch# show fcsp asciiwwn 30:11:bb:cc:dd:33:11:22
Ascii representation of WWN to be used with AAA servers:0x_3011bbccdd331122
```

Related Commands

Command	Description
fcsp enable	Enables the FC-SP feature for this switch.

show fctimer

To view the Fibre Channel timers (fctimer), use the **show fctimer** command.

show fctimer [**d_s_tov** [**vsan** *vsan-id*] | **distribution status** | **e_d_tov** [**vsan** *vsan-id*] | **f_s_tov** [**vsan** *vsan-id*] | **last action status** | **pending** | **pending-diff** | **r_a_tov** [**vsan** *vsan-id*] | **session-status** | **vsan** *vsan-id*]

Syntax Description

d_s_tov	Displays the distributed services time out value (D_S_TOV) in milliseconds.
distribution status	Displays Cisco Fabric Services (CFS) distribution status information.
e_d_tov	Displays the error detection time out value (E_D_TOV) in milliseconds.
f_s_tov	Displays the fabric stability time out value (F_S_TOV) in milliseconds.
last action status	Displays the status of the last CFS commit or discard operation.
pending	Displays the status of pending fctimer commands.
pending-diff	Displays the difference between pending database and running config.
r_a_tov	Displays the resource allocation time out value (R_A_TOV) in milliseconds.
session-status	Displays the state of fctimer CFS session.
vsan *vsan-id*	Displays information for a VSAN. The range is 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.0(1b)	Added the **distribution status**, **last action status**, **pending**, **pending-diff**, and **session-status** keywords.

Usage Guidelines

None.

Examples

The following example displays configured global TOVs.

```
switch# show fctimer
F_S_TOV    D_S_TOV    E_D_TOV    R_A_TOV
----------------------------------------
5000 ms    5000 ms    2000 ms    10000 ms
```

The following example displays configured TOVs for a specified VSAN.

```
switch# show fctimer vsan 10
vsan no.  F_S_TOV    D_S_TOV    E_D_TOV    R_A_TOV
-------------------------------------------------
10        5000 ms    5000 ms    3000 ms    10000 ms
```

Related Commands

Command	Description
fctimer	Configures fctimer parameters.

show fdmi

To display the Fabric-Device Management Interface (FDMI) database information, use the **show fdmi** command.

show fdmi database [**detail** [**hba-id** [*hba-id* **vsan** *vsan-id* | **vsan** *vsan-id*] | **vsan** *vsan-id*]

Syntax Description

fdmi	Accesses the FDMI commands.
database	Displays the FDMI database contents.
detail	Specifies detailed FDMI information.
hba-id	Displays detailed information for the specified HBA entry.
hba-id	Displays detailed information for the specified HBA entry.
vsan *vsan-id*	Specifies FDMI information for the specified VSAN ranging from 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays all HBA management servers.

```
switch# show fdmi database
Registered HBA List for VSAN 1
  10:00:00:00:c9:32:8d:77
  21:01:00:e0:8b:2a:f6:54
switch# show fdmi database detail
Registered HBA List for VSAN 1
-------------------------------
HBA-ID: 10:00:00:00:c9:32:8d:77
-------------------------------
Node Name         :20:00:00:00:c9:32:8d:77
Manufacturer      :Emulex Corporation
Serial Num        :0000c9328d77
Model             :LP9002
Model Description:Emulex LightPulse LP9002 2 Gigabit PCI Fibre Channel Adapter
Hardware Ver      :2002606D
Driver Ver        :SLI-2 SW_DATE:Feb 27 2003, v5-2.20a12
ROM Ver           :3.11A0
Firmware Ver      :3.90A7
OS Name/Ver       :Window 2000
CT Payload Len    :1300000
  Port-id: 10:00:00:00:c9:32:8d:77
```

```
------------------------------
HBA-ID: 21:01:00:e0:8b:2a:f6:54
------------------------------
Node Name        :20:01:00:e0:8b:2a:f6:54
Manufacturer     :QLogic Corporation
Serial Num       :\74262
Model            :QLA2342
Model Description:QLogic QLA2342 PCI Fibre Channel Adapter
Hardware Ver     :FC5010409-10
Driver Ver       :8.2.3.10 Beta 2 Test 1 DBG (W2K VI)
ROM Ver          :1.24
Firmware Ver     :03.02.13.
OS Name/Ver      :500
CT Payload Len   :2040
  Port-id: 21:01:00:e0:8b:2a:f6:54
```

The following example displays VSAN1-specific FDMI information.

```
switch# show fdmi database detail vsan 1
Registered HBA List for VSAN 1
------------------------------
HBA-ID: 10:00:00:00:c9:32:8d:77
------------------------------
Node Name        :20:00:00:00:c9:32:8d:77
Manufacturer     :Emulex Corporation
Serial Num       :0000c9328d77
Model            :LP9002
Model Description:Emulex LightPulse LP9002 2 Gigabit PCI Fibre Channel Adapter
Hardware Ver     :2002606D
Driver Ver       :SLI-2 SW_DATE:Feb 27 2003, v5-2.20a12
ROM Ver          :3.11A0
Firmware Ver     :3.90A7
OS Name/Ver      :Window 2000
CT Payload Len   :1300000
  Port-id: 10:00:00:00:c9:32:8d:77
------------------------------
HBA-ID: 21:01:00:e0:8b:2a:f6:54
------------------------------
Node Name        :20:01:00:e0:8b:2a:f6:54
Manufacturer     :QLogic Corporation
Serial Num       :\74262
Model            :QLA2342
Model Description:QLogic QLA2342 PCI Fibre Channel Adapter
Hardware Ver     :FC5010409-10
Driver Ver       :8.2.3.10 Beta 2 Test 1 DBG (W2K VI)
ROM Ver          :1.24
Firmware Ver     :03.02.13.
OS Name/Ver      :500
CT Payload Len   :2040
  Port-id: 21:01:00:e0:8b:2a:f6:54
```

The following example displays details for the specified HBA entry.

```
switch# show fdmi database detail Hba-id 21:01:00:e0:8b:2a:f6:54 vsan 1

Node Name        :20:01:00:e0:8b:2a:f6:54
Manufacturer     :QLogic Corporation
Serial Num       :\74262
Model            :QLA2342
Model Description:QLogic QLA2342 PCI Fibre Channel Adapter
Hardware Ver     :FC5010409-10
Driver Ver       :8.2.3.10 Beta 2 Test 1 DBG (W2K VI)
ROM Ver          :1.24
Firmware Ver     :03.02.13.
OS Name/Ver      :500
CT Payload Len   :2040
  Port-id: 21:01:00:e0:8b:2a:f6:54
```

show ficon

To display configured FICON information, use the **show ficon** command.

show ficon [**control-device sb3** [**vsan** *vsan-id*] |
first-available port-number |
port default-state |
port-numbers {**assign** [*slot* | **logical-port** | **slot** *slot*] | **interface**} |
stat |
vsan *vsan-id* [**allegiance** | **directory-history** [**key-counter** *value*] | **file** {**all** | **name** *filename* [**portaddress** *port*]} | **interface** {**fc** *slot*/*port* | **fcip** *fcip-id* | **port-channel** *port*} | **portaddress** [*port* [**counters**] | **portnumber** [*port-numbers* | **duplicate** | **undefined**] [**brief**] [**installed**]]

Syntax Description

control-device sb3	Displays FICON control device information.
vsan *vsan-id*	Specifies FICON information for the specified VSAN ranging from 1 to 4093.
first-available port-number	Displays the available port numbers.
port default-state	Displays the default FICON port prohibit state.
port-numbers	Displays FICON port numbers.
assign *slot*	Displays the FICON port numbers assigned to the specified slot, 1 though 6.
logical port	Displays FICON port numbers assigned to logical interfaces.
slot *slot*	Displays the FICON port numbers assigned to the specified slot, 1 though 6.
stat	Displays information about FICONSTAT.
allegiance	Displays FICON device allegiance information.
directory-history	Displays FICON directory history.
key-counter *value*	Specifies a key counter.
file	Displays FICON information for a file.
all	Specifies all files.
name *filename*	Specifies the name for a file.
portaddress *port*	Specifies a port address for a file.
interface	Displays FICON information for an interface.
fc *slot*/*port*	Specifies a Fibre Channel interface.
fcip *fcip-id*	Specifies an FC IP interface.
port-channel *port*	Specifies a PortChannel interface.
counters	Displays counter information for the port address.
portnumber *port-numbers*	Displays FICON information for a port number in the specified range, 0 through 153 or 0x0 through 0x99.
duplicate	Displays FICON interfaces with duplicate port numbers and port addresses.
undefined	Displays FICON interfaces without port numbers and port addresses.
brief	Displays brief FICON information for the port address.
installed	Displays FICON information for the installed port address.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	• Added the **port-numbers** and **stat** options. • Added the **portnumber** keyword.
3.0(2)	Added the **port default-state** option.

Usage Guidelines

If FICON is not enabled on a VSAN, you will not be able to view FICON configuration information for that VSAN.

Examples

The following example displays configured FICON information

```
switch# show ficon
Ficon information for VSAN 20
  Ficon is online
  VSAN is active
  Host port control is Enabled
  Host offline control is Enabled
  User alert mode is Enabled
  SNMP port control is Enabled
  Host set director timestamp is Enabled
  Active=Saved is Disabled
  Number of implemented ports are 240
  Key Counter is 73723
  FCID last byte is 0
  Date/Time is set by host to Sun Jun 26 00:04:06.991999 1904
  Device allegiance is locked by Host
  Codepage is us-canada
  Saved configuration files
    IPL
    _TSIRN00
```

The following example displays the default prohibit state.

```
switch# show ficon port default-state
Port default state is allow-all
```

The following example displays assigned FICON port numbers.

```
switch# show ficon port-numbers assign
ficon slot 1 assign port-numbers 0-31
ficon slot 2 assign port-numbers 32-63
ficon slot 3 assign port-numbers 64-95
ficon slot 4 assign port-numbers 96-127
ficon logical-port assign port-numbers 128-153
```

The following example displays port address information

```
switch# show ficon vsan 2 portaddress
Port Address 1 is not installed in vsan 2
    Port number is 1, Interface is fc1/1
    Port name is
    Port is not admin blocked
    Prohibited port addresses are 0,241-253,255

Port Address 2 is not installed in vsan 2
    Port number is 2, Interface is fc1/2
    Port name is
    Port is not admin blocked
    Prohibited port addresses are 0,241-253,255

...
Port Address 239 is not installed in vsan 2
    Port name is
    Port is not admin blocked
    Prohibited port addresses are 0,241-253,255

Port Address 240 is not installed in vsan 2
    Port name is
    Port is not admin blocked
    Prohibited port addresses are 0,241-253,255
```

The following example displays port address information in a brief format.

```
switch# show ficon vsan 2 portaddress 50-55 brief
--------------------------------------------------------------------------------
Port    Port    Interface          Admin     Status           Oper   FCID
Address Number                     Blocked                    Mode
--------------------------------------------------------------------------------
50      50      fc2/18             on     fcotAbsent       --     --
51      51      fc2/19             off       fcotAbsent       --     --
52      52      fc2/20             off       fcotAbsent       --     --
53      53      fc2/21             off       fcotAbsent       --     --
54      54      fc2/22             off       notConnected     --     --
55      55      fc2/23             off       up               FL     0xea0000
56     55                       off       up               FL     0xea0000
```

The following example displays port address counter information.

```
switch# show ficon vsan 20 portaddress 8 counters
Port Address 8(0x8) is up in vsan 20
    Port number is 8(0x8), Interface is fc1/8
    Version presented 1, Counter size 32b
    242811 frames input, 9912794 words
      484 class-2 frames, 242302 class-3 frames
      0 link control frames, 0 multicast frames
      0 disparity errors inside frames
      0 disparity errors outside frames
      0 frames too big, 0 frames too small
      0 crc errors, 0 eof errors
      0 invalid ordered sets
      0 frames discarded c3
      0 address id errors
    116620 frames output, 10609188 words
      0 frame pacing time
    0 link failures
    0 loss of sync
    0 loss of signal
    0 primitive seq prot errors
    0 invalid transmission words
    1 lrr input, 0 ols input, 5 ols output
```

```
    0 error summary
```

The following example displays the contents of the specified FICON configuration file

```
switch# show ficon vsan 3 file IPL
FICON configuration file IPL      in vsan 3
    Port address 1
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,81-253,255

    Port address 2
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,81-253,255

    Port address 3
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,81-253,255

    Port address 4
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,81-253,255

...
Port address 80
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,81-253,255

    Port address 254
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,81-253,255
```

The following example displays all FICON configuration files

```
switch# show ficon vsan 2
Ficon information for VSAN 2
  Ficon is enabled
  VSAN is active
  Host control is Enabled
  Host offline control is Enabled
  Clock alert mode is Disabled
  User alert mode is Disabled
  SNMP control is Disabled
  Active=Saved is Disabled
  Number of implemented ports are 240
  Key Counter is 9
  FCID last byte is 0
  Date/Time is same as system time (Sun Dec 14 01:26:30.273402 1980)
  Device Allegiance not locked
  Codepage is us-canada
  Saved configuration files
    IPL
    IPLFILE1
```

The following example displays the specified port addresses for a FICON configuration file

```
switch# show ficon vsan 2 file iplfile1 portaddress 1-7
FICON configuration file IPLFILE1 in vsan 2
    Port address 1
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,241-253,255

    Port address 2
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,241-253,255

    Port address 3
        Port name is P3
        Port is not blocked
        Prohibited port addresses are 0,241-253,255
...
    Port address 7
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,241-253,255
```

The following example displays the specified port address when FICON is enabled

```
switch# show ficon vsan 2 portaddress 55
Port Address 55 is not installed in vsan 2
    Port number is 55, Interface is fc2/23
    Port name is
    Port is not admin blocked
    Prohibited port addresses are 0,241-253,255
    Admin port mode is FL
    Port mode is FL, FCID is 0xea0000
```

The following example displays two port addresses configured with different states

```
switch# show ficon vsan 2 portaddress 2
Port Address 2(0x2) is not installed in vsan 2
    Port number is 2(0x2), Interface is fc1/2
    Port name is
    Port is not admin blocked
    Prohibited port addresses are 0,241-253,255(0,0xf1-0xfd,0xff)
    Admin port mode is auto
    Peer was type model manufactured by

switch# show ficon vsan 2 portaddress 1
Port Address 2(0x2) is not installed in vsan 2
    Port number is 2(0x2), Interface is fc1/2
    Port name is
    Port name is SampleName
    Port is admin blocked
    Prohibited port addresses are 0,241-253,255(0,0xf1-0xfd,0xff)
    Admin port mode is auto
    Peer was type model manufactured by
```

The following example displays control unit information.

```
switch# show ficon control-device sb3
Control Unit Image:0x80b9c2c
VSAN:20 CU:0x20fe00 CUI:0 CUD:0 CURLP:(nil)
ASYNC LP:(nil) MODE:1 STATE:1 CQ LEN:0 MAX:0
PRIMARY LP:   VSAN:0 CH:0x0 CHI:0 CU:0x0 CUI:0
ALTERNATE LP: VSAN:0 CH:0x0 CHI:0 CU:0x0 CUI:0
```

```
Logical Path:0x80b9fb4
VSAN:20 CH:0x200600 CHI:15 CU:0x20fe00 CUI:0 STATE:1 FLAGS:0x1
LINK: OH:0x0 OC:0x0 IH:0x0 IC:0x0
DEV:  OH:0x0 OC:0x0 IH:0x0 IC:0x0
SENSE: 00 00 00 00 00 00 00 46
       30 20 00 00 00 00 00 00
       00 00 00 00 00 00 00 00
       00 00 00 00 00 00 00 00
IUI:0x0 DHF:0x0 CCW:0x0 TOKEN:0x0 PCCW:0x0 FCCW:0x0 PTOKEN:0x0 FTOKEN:0x0
CMD:0x0 CCW_FLAGS:0x0 CCW_COUNT:0 CMD_FLAGS:0x0 PRIO:0x0 DATA_COUNT:0
STATUS:0x0 FLAGS:0x0 PARAM:0x0 QTP:0x0 DTP:0x0
CQ LEN:0 MAX:0 DESTATUS:0x0
```

The following example displays the history buffer for the specified VSAN

```
switch# show ficon vsan 20 director-history
Director History Buffer for vsan 20
-------------------------------------------
Key Counter           Ports Address
                      Changed
-------------------------------------------
74556                 43
74557                 44
74558                 45
74559                 46
74560                 47
74561                 48
74562                 49
74563                 50
74564                 51
74565                 52
74566                 53
74567                 54
74568                 55
74569                 56
74570                 57
74571                 58
74572                 59
74573                 60
74574                 61
74575                 62
74576                 63
74577                 64
74578
74579
74580                 1-3,5,10,12,14-16,34-40,43-45,47-54,56-57,59-64
74581                 3,5
74582                 64
74583
74584                 1-3,10,12,14-16,34-40,43-45,47-54,56-57,59-64
74585                 1
74586                 2
74587                 3
```

The following example displays the running configuration information

```
switch# show running-config
...
ficon vsan 2
portaddress 1
block
name SampleName
prohibit portaddress 3
portaddress 3
prohibit portaddress 1
file IPL
```

The following example displays the available port numbers:

```
switch# show ficon first-available port-number
Port number 129(0x81) is available
```

show file

To display the contents of a specified file in the file system, use the **show file** command.

show file *filename* [**cksum** | **md5sum**]

Syntax Description

filename	Specifies a filename.
cksum	Displays CRC checksum for a file.
md5sum	Displays MD5 checksum for a file.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the contents of the test file that resides in the slot0 directory.

```
switch# show file slot0:test
config t
Int fc1/1
no shut
end
show int
```

The following example displays the contents of a file residing in the current directory.

```
switch# show file myfile
```

The following example displays the CRC checksum for a file.

```
switch# show file bootflash:vboot-1 cksum
838096258
```

The following example displays the MD5 checksum for a file.

```
switch# show file bootflash:vboot-1 md5sum
3d8e05790155150734eb8639ce98a331
```

show flogi database

To list all the FLOGI sessions through all interfaces across all VSANs, use the **show flogi database** command.

show flogi database [**fcid** *fcid-id* | **interface** *interface* | **vsan** *vsan-id*]

Syntax Description

fcid *fcid-id*	Displays FLOGI database entries based on the FCID allocated.
interface *interface*	Displays FLOGI database entries based on the logged in interface.
vsan *vsan-id*	Displays FLOGI database entries based on the VSAN ID. The range is 1 to 4093.

Defaults

Displays the entire FLOGI database.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Output of this command is first sorted on interface and then on VSANs.

In a Fibre Channel fabric, each host or disk requires an FCID. Use the **show flogi database** command to verify if a storage device is displayed in the Fabric login (FLOGI) table as in the examples below. If the required device is displayed in the FLOGI table, the fabric login is successful. Examine the FLOGI database on a switch that is directly connected to the host HBA and connected ports.

Examples

The following example displays details on the FLOGI database.

```
switch# show flogi database
--------------------------------------------------------------------------------
INTERFACE  VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
sup-fc0    2     0xb30100  10:00:00:05:30:00:49:63  20:00:00:05:30:00:49:5e
fc9/13     1     0xb200e2  21:00:00:04:cf:27:25:2c  20:00:00:04:cf:27:25:2c
fc9/13     1     0xb200e1  21:00:00:04:cf:4c:18:61  20:00:00:04:cf:4c:18:61
fc9/13     1     0xb200d1  21:00:00:04:cf:4c:18:64  20:00:00:04:cf:4c:18:64
fc9/13     1     0xb200ce  21:00:00:04:cf:4c:16:fb  20:00:00:04:cf:4c:16:fb
fc9/13     1     0xb200cd  21:00:00:04:cf:4c:18:f7  20:00:00:04:cf:4c:18:f7

Total number of flogi = 6.
```

The following example displays the FLOGI interface.

```
switch# show flogi database interface fc 1/11
INTERFACE        VSAN    FCID           PORT NAME               NODE NAME
--------------------- ---- -------- ----------------------- ---------------------
fc9/13     1 0xa002ef 21:00:00:20:37:18:17:d2 20:00:00:20:37:18:17:d2
fc9/13     1 0xa002e8 21:00:00:20:37:38:a7:c1 20:00:00:20:37:38:a7:c1
fc9/13     1 0xa002e4 21:00:00:20:37:6b:d7:18 20:00:00:20:37:6b:d7:18
fc9/13     1 0xa002e2 21:00:00:20:37:18:d2:45 20:00:00:20:37:18:d2:45
fc9/13     1 0xa002e1 21:00:00:20:37:39:90:6a 20:00:00:20:37:39:90:6a
fc9/13     1 0xa002e0 21:00:00:20:37:36:0b:4d 20:00:00:20:37:36:0b:4d
fc9/13     1 0xa002dc 21:00:00:20:37:5a:5b:27 20:00:00:20:37:5a:5b:27
fc9/13     1 0xa002da 21:00:00:20:37:18:6f:90 20:00:00:20:37:18:6f:90
fc9/13     1 0xa002d9 21:00:00:20:37:5b:cf:b9 20:00:00:20:37:5b:cf:b9
fc9/13     1 0xa002d6 21:00:00:20:37:46:78:97 20:00:00:20:37:46:78:97

Total number of flogi = 10.
```

The following example displays the FLOGI VSAN.

```
switch# show flogi database vsan 1
--------------------------------------------------------------------------------
INTERFACE  VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
fc9/13       1     0xef02ef  22:00:00:20:37:18:17:d2  20:00:00:20:37:18:17:d2
fc9/13       1     0xef02e8  22:00:00:20:37:38:a7:c1  20:00:00:20:37:38:a7:c1
fc9/13       1     0xef02e4  22:00:00:20:37:6b:d7:18  20:00:00:20:37:6b:d7:18
fc9/13       1     0xef02e2  22:00:00:20:37:18:d2:45  20:00:00:20:37:18:d2:45
fc9/13       1     0xef02e1  22:00:00:20:37:39:90:6a  20:00:00:20:37:39:90:6a
fc9/13       1     0xef02e0  22:00:00:20:37:36:0b:4d  20:00:00:20:37:36:0b:4d
fc9/13       1     0xef02dc  22:00:00:20:37:5a:5b:27  20:00:00:20:37:5a:5b:27
fc9/13       1     0xef02da  22:00:00:20:37:18:6f:90  20:00:00:20:37:18:6f:90
fc9/13       1     0xef02d9  22:00:00:20:37:5b:cf:b9  20:00:00:20:37:5b:cf:b9
fc9/13       1     0xef02d6  22:00:00:20:37:46:78:97  20:00:00:20:37:46:78:97

Total number of flogi = 10.
```

The following example displays the FLOGI FCID.

```
switch# show flogi database fcid 0xef02e2
--------------------------------------------------------------------------------
INTERFACE  VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
fc9/13       1     0xef02e2  22:00:00:20:37:18:d2:45  20:00:00:20:37:18:d2:45

Total number of flogi = 1.
```

Related Commands

Command	Description
show fcns database	Displays all the local and remote name server entries

show fspf

To display global FSPF information, use the **show fspf** command. This information includes:

- the domain number of the switch
- the autonomous region for the switch
- Min_LS_arrival: the minimum time that must elapse before the switch accepts LSR updates
- Min_LS_interval: the minimum time that must elapse before the switch can transmit an LSR
- LS_refresh_time: the interval lapse between refresh LSR transmissions
- Max_age: the maximum time aa LSR can stay before being deleted

show fspf [**database** [**vsan** *vsan-id* [**domain** *domain-id*] [**detail**]] | **interface** | **vsan** *vsan-id* [**interface** [*interface-range*]]]

Syntax Description

database	To display information of fspf database for a VSAN. If no other parameters are given all the LSRs in the database are displayed. If more specific information is required then the domain number of the owner of the LSR may be given. Detail gives more detailed information on each LSR.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
domain *domain-id*	The domain of the database. The parameter *domain_num* is unsigned integers in the range 0-255.
detail	Displays detailed FSPF information for the VSAN.
interface *interface-range*	Display FSPF interface information for a given VSAN. If the interface number is specified information on the neighbor on that interface is displayed. If no interface is specified information on all interfaces are displayed. The parameter *interface-range* is of the format **fc***slot*/*port* **- fc***slot*/*port*.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays FSPF interface information.

```
switch# show fspf interface vsan 1 fc1/1
FSPF interface fc1/1 in VSAN 1
FSPF routing administrative state is active
Interface cost is 500
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is FULL
Neighbor Domain Id is 0x0c(12), Neighbor Interface index is 0x0f100000

Statistics counters :
   Number of packets received : LSU  8  LSA  8  Hello 118  Error packets 0
   Number of packets transmitted : LSU  8  LSA  8  Hello 119  Retransmitted LSU
 0
  Number of times inactivity timer expired for the interface = 0
```

The following example displays FSPF database information.

```
switch# show fspf database vsan 1

FSPF Link State Database for VSAN 1 Domain 0x0c(12)
LSR Type                = 1
Advertising domain ID   = 0x0c(12)
LSR Age                 = 1686
LSR Incarnation number  = 0x80000024
LSR Checksum            = 0x3caf
Number of links         = 2
 NbrDomainId      IfIndex   NbrIfIndex    Link Type         Cost
--------------------------------------------------------------------------------
   0x65(101) 0x0000100e     0x00001081               1          500
   0x65(101) 0x0000100f     0x00001080               1          500

FSPF Link State Database for VSAN 1 Domain 0x65(101)
LSR Type                = 1
Advertising domain ID   = 0x65(101)
LSR Age                 = 1685
LSR Incarnation number  = 0x80000028
LSR Checksum            = 0x8443
Number of links         = 6
 NbrDomainId      IfIndex   NbrIfIndex    Link Type         Cost
--------------------------------------------------------------------------------
   0xc3(195) 0x00001085     0x00001095               1          500
   0xc3(195) 0x00001086     0x00001096               1          500
   0xc3(195) 0x00001087     0x00001097               1          500
   0xc3(195) 0x00001084     0x00001094               1          500
    0x0c(12) 0x00001081     0x0000100e               1          500
    0x0c(12) 0x00001080     0x0000100f               1          500

FSPF Link State Database for VSAN 1 Domain 0xc3(195)
LSR Type                = 1
Advertising domain ID   = 0xc3(195)
LSR Age                 = 1686
LSR Incarnation number  = 0x80000033
LSR Checksum            = 0x6799
Number of links         = 4
 NbrDomainId      IfIndex   NbrIfIndex    Link Type         Cost
--------------------------------------------------------------------------------
   0x65(101) 0x00001095     0x00001085               1          500
   0x65(101) 0x00001096     0x00001086               1          500
   0x65(101) 0x00001097     0x00001087               1          500
   0x65(101) 0x00001094     0x00001084               1          500
```

This command displays FSPF information for a specified VSAN.

```
switch# show fspf vsan 1
FSPF routing for VSAN 1
FSPF routing administration status is enabled
FSPF routing operational status is UP
It is an intra-domain router
Autonomous region is 0
SPF hold time is 0 msec
MinLsArrival = 1000 msec , MinLsInterval = 5000 msec
Local Domain is 0x65(101)
Number of LSRs = 3, Total Checksum = 0x0001288b

Protocol constants :
   LS_REFRESH_TIME = 1800 sec
   MAX_AGE         = 3600 sec

Statistics counters :
   Number of LSR that reached MaxAge = 0
   Number of SPF computations        = 7
   Number of Checksum Errors         = 0
   Number of Transmitted packets :  LSU 65 LSA 55 Hello 474 Retranmsitted LSU 0
   Number of received packets :  LSU 55 LSA 60 Hello 464 Error packets 10
```

show hardware

To display switch hardware inventory details, use the **show hardware** command.

show hardware [**ipc-channel status**]

Syntax Description

ipc-channel status	Displays the status of the interprocess communication (IPC) channels.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the switch hardware inventory details.

```
switch# show hardware
Cisco Storage Area Networking Operating System (SAN-OS) Software
TAC support:http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc. All rights reserved.
The copyright for certain works contained herein are owned by
Andiamo Systems, Inc. and/or other third parties and are used and
distributed under license.

Software
  BIOS:     version 0.0.0
  loader:   version 1.0(0.259)
  kickstart:version 1.0(2) [build 1.0(0.280)]
  system:   version 1.0(2) [build 1.0(0.280)]

  BIOS compile time:      10/10/02
  kickstart image file is:bootflash:/boot-280
  kickstart compile time: 11/20/2002 6:00:00
  system image file is:   isan-280
  system compile time:    11/20/2002 6:00:00
```

```
Hardware
  RAM 963108 kB

  bootflash:503808 blocks (block size 512b)
  slot0:         0 blocks (block size 512b)

  172.22.92.28 uptime is 0 days 0 hour 31 minute(s) 23 second(s)

  Last reset
    Reason:Watchdog Timeout/External Reset
    System version:1.0(2)

This supervisor carries Pentium processor with 963108 kB of memory
Intel(R) Pentium(R) III CPU at 800MHz with 512 KB L2 Cache
Rev:Family  6, Model  11 stepping  1

512K bytes of non-volatile memory.
503808 blocks of internal bootflash (block size 512b)
```

Displays the status of the IPC channel:

```
switch# show hardware ipc-channel status
Active IPC-Channel:            A
```

show hosts

To display configured DNS host configuration details, use the **show hosts** command.

show hosts

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the configures hosts including the default domain, domain list, and name servers.

```
switch# show hosts
Default domain is cisco.com
Domain list: ucsc.edu harvard.edu yale.edu stanford.edu
Name/address lookup uses domain service
Name servers are 15.1.0.1 15.2.0.0
```

show incompatibility system

To display the HA compatibility status between the two supervisor modules, use the **show incompatibility system** command.

show incompatibility system [bootflash: | slot0: | volatile:]*image-filename*

Syntax Description

bootflash:	Source or destination location for internal bootflash memory
slot0:	Source or destination location for the CompactFlash memory or PCMCIA card.
volatile:	Source or destination location for the volatile directory.
image-filename	Specifies the name of the system or kickstart image.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.
3.0(1)	Provided an example to show that the command output provides the commands needed to disable incompatible features.

Usage Guidelines

If the HA compatibility is `strict` on an active supervisor module, the standby supervisor module synchronization may not succeed and may move into an inconsistent state.

If the HA compatibility is `loose`, the synchronization may happen without errors, but some resources may become unusable when a switchover happens.

Examples

The following examples display kernel core settings.

```
switch# show incompatibility system bootflash:old-image-y
The following configurations on active are incompatible with the system image
1) Feature Index : 67 , Capability : CAP_FEATURE_SPAN_FC_TUNNEL_CFG
Description : SPAN - Remote SPAN feature using fc-tunnels
Capability requirement : STRICT
2) Feature Index : 119 , Capability : CAP_FEATURE_FC_TUNNEL_CFG
Description : fc-tunnel is enabled
Capability requirement : STRICT
```

The following example shows commands needed to disable incompatible features.

```
switch# show incompatibility system bootflash:m9200-ek9-mz.1.3.4b.bin
The following configurations on active are incompatible with the system image
1) Service : cfs , Capability : CAP_FEATURE_CFS_ENABLED_DEVICE_ALIAS
Description : CFS - Distribution is enabled for DEVICE-ALIAS
Capability requirement : STRICT
Disable command : no device-alias distribute
```

show install all impact

To display the software compatibility matrix of a specific image, use the **show install all impact** command.

show install all impact [**asm-sfn** *image-filename*] [**kickstart** *image-filename*] [**ssi** *image-filename*] [**system** *image-filename*]

Syntax Description

asm-sfn	Specifies the ASM SFN boot variable.
kickstart	Specifies the kickstart boot variable.
ssi	Specifies the SSI boot variable.
system	Specifies the system boot variable.
image-filename	The name of an image.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

Use the **show install all impact** command to view the effect of updating the system from the running image to another specified image.

```
switch# show install all impact

Verifying image bootflash:/ilc1.bin
[####################] 100% -- SUCCESS

Verifying image bootflash:/vk73a
[####################] 100% -- SUCCESS

Verifying image bootflash:/vs73a
[####################] 100% -- SUCCESS

Extracting "slc" version from image bootflash:/vs73a.
[####################] 100% -- SUCCESS

Extracting "slc" version from image bootflash:/vs73a.
[####################] 100% -- SUCCESS

Extracting "system" version from image bootflash:/vs73a.
[####################] 100% -- SUCCESS
```

```
Extracting "kickstart" version from image bootflash:/vk73a.
[####################] 100% -- SUCCESS

Extracting "loader" version from image bootflash:/vk73a.
[####################] 100% -- SUCCESS

Extracting "slc" version from image bootflash:/vs73a.
[####################] 100% -- SUCCESS

Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     2       yes  non-disruptive          none
     4       yes  non-disruptive          none
     6       yes  non-disruptive          none
     9       yes  non-disruptive          none

Images will be upgraded according to following table:
Module       Image       Running-Version           New-Version  Upg-Required
------  ----------  --------------------  --------------------  ------------
     2         slc                1.2(1)                1.2(1)            no
     2        bios      v1.0.7(03/20/03)      v1.0.7(03/20/03)            no
     4         slc                1.2(1)                1.2(1)            no
     4        ilce                1.2(1)                1.2(1)            no
     4        bios      v1.0.7(03/20/03)      v1.0.7(03/20/03)            no
     6      system                1.2(1)                1.2(1)            no
     6   kickstart                1.2(1)                1.2(1)            no
     6        bios      v1.0.7(03/20/03)      v1.0.7(03/20/03)            no
     6      loader               1.0(3a)               1.0(3a)            no
     9         slc                1.2(1)                1.2(1)            no
     9        bios      v1.0.7(03/20/03)      v1.0.7(03/20/03)            no
```

The following command displays the error message that is displayed if a wrong image is provided.

```
switch# show install all impact system bootflash:
Compatibility check failed. Return code 0x40930003 (Invalid bootvar specified in
 the input).
```

show install all status

To display the on-going **install all** command status or the log of the last installed **install all** command from a Console, SSH, or Telnet session, use the **show install all status** command.

show install all status

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

This command only displays the status of an **install all** command that is issued form the CLI (not the Fabric Manager).

Examples

Use the **show install all status** command to view the output of a **install all** command process.

```
switch# show install all status
There is an on-going installation... <---------------------- in progress installation
Enter Ctrl-C to go back to the prompt.


Verifying image bootflash:/b-1.3.0.104
 -- SUCCESS


Verifying image bootflash:/i-1.3.0.104
 -- SUCCESS


Extracting "system" version from image bootflash:/i-1.3.0.104.
 -- SUCCESS


Extracting "kickstart" version from image bootflash:/b-1.3.0.104.
 -- SUCCESS


Extracting "loader" version from image bootflash:/b-1.3.0.104.
 -- SUCCESS


switch# show install all status
This is the log of last installation.          <<<<<< log of last install
```

```
Verifying image bootflash:/b-1.3.0.104
 -- SUCCESS


Verifying image bootflash:/i-1.3.0.104
 -- SUCCESS


Extracting "system" version from image bootflash:/i-1.3.0.104.
 -- SUCCESS


Extracting "kickstart" version from image bootflash:/b-1.3.0.104.
 -- SUCCESS


Extracting "loader" version from image bootflash:/b-1.3.0.104.
 -- SUCCESS
```

show in-order-guarantee

To display the present configured state of the in-order delivery feature, use the **show in-order-guarantee** command.

show in-order-guarantee

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the present configuration status of the in-order delivery feature.

```
switch# show in-order-guarantee
global inorder delivery configuration:guaranteed

VSAN specific settings
vsan 1 inorder delivery:guaranteed
vsan 101 inorder delivery:not guaranteed
vsan 1000 inorder delivery:guaranteed
vsan 1001 inorder delivery:guaranteed
vsan 1682 inorder delivery:guaranteed
vsan 2001 inorder delivery:guaranteed
vsan 2009 inorder delivery:guaranteed
vsan 2456 inorder delivery:guaranteed
vsan 3277 inorder delivery:guaranteed
vsan 3451 inorder delivery:guaranteed
vsan 3452 inorder delivery:guaranteed
vsan 3453 inorder delivery:guaranteed
```

show interface

You can check the status of an interface at any time by using the **show interface** command.

show interface [*interface-range*] [**bbcredit** | **brief** | **capabilities** | **counters** [**brief**] | **description** | **transceiver** [**calibrations** | **details**] | **trunk vsan** [*vsan-id*]]

Syntax Description

interface-range	Displays the type of interface.
bbcredit	Displays buffer-to-buffer credit information.
brief	Displays brief information.
capabilities	Displays hardware port capabilities for a specified interface.
counters	Displays the interface counter information.
description	Displays the interface description.
transceiver	Displays the transceiver information for a specified interface.
calibrations	Displays transceiver calibration information for the specified interface.
details	Displays detailed transceiver diagnostics information for the specified interface.
trunk vsan	Displays the trunking status of all VSANs.
vsan-id	Displays the trunking status of the specified VSANs. The range is 1 to 4093.

Defaults

Displays information for all interfaces on the switch.

Command Modes

EXEC

Command History

Release	Modification
1.0(2)	This command was introduced.
1.3(1)	Added the **bbcredit** keyword and support for cpp and fv interfaces.
3.0(1)	Added the **capabilities** option for Fibre Channel interfaces.

Usage Guidelines

You can specify a range of interfaces by issuing a command with the following example format:

interface fc1/1 - 5 , fc2/5 - 7

The spaces are required before and after the dash (-) and before and after the comma (,).

The **show interface** *interface-type slot/port* **transceiver** command can only be issued on a switch in the Cisco MDS 9100 Series if the SFP is present.

Table 22-4 lists the interface types supported by the **show interface** command.

Table 22-4 Interface Types for the show interface Command

Interface Type	Description
cpp *slot/port*	Displays information for a virtualization interface.
fc *slot/port*	Displays the Fibre Channel interface in the specified slot/port.
fc-tunnel *tunnel-id*	Displays description of the specified FC tunnel from 1 to 4095.
fcip *interface-number*	Specifies a FCIP interface. The range is 1 to 255.
fv *slot/dpp-number/fv-port*	Displays information for the virtual F port (FV port) interface in the specified slot along with the data path processor (DPP) number and the FV port number.
gigabitethernet *slot/port*	Displays information for a Gigabit Ethernet interface at the specified slot and port.
gigabitethernet *slot/port***.** *subinterface-number*	Displays information for a Gigabit Ethernet subinterface at the specified slot and port followed by a dot (.) indicator and the subinterface number. The subinterface range is 1 to 4093.
iscsi *slot/port*	Displays the description of the iSCSI interface in the specified slot and port.
mgmt 0	Displays the description of the management interface.
port-channel *port-channel-number*	Displays the PortChannel interface specified by the PortChannel number. The range is 1 to 128.
port-channel *port-channel-number* **.***subinterface-number*	Displays the PortChannel subinterface specified by the PortChannel number followed by a dot (.) indicator and the subinterface number. The port channel number range is 1 to 128. The subinterface range is 1 to 4093.
sup-fc 0	Displays the in-band interface details.
vsan *vsan-id*	Displays information for a VSAN. The range is 1 to 4093.

Examples

The following example shows how to display information about a Fibre Channel interface.

```
switch# show interface fc1/11
fc1/11 is up
    Hardware is Fibre Channel
    Port WWN is 20:0b:00:05:30:00:59:de
    Admin port mode is ST
    Port mode is ST
    Port vsan is 1
    Speed is 1 Gbps
    Rspan tunnel is fc-tunnel 100
    Beacon is turned off
    5 minutes input rate 248 bits/sec, 31 bytes/sec, 0 frames/sec
    5 minutes output rate 176 bits/sec, 22 bytes/sec, 0 frames/sec
      6862 frames input, 444232 bytes
        0 discards, 0 errors
        0 CRC, 0 unknown class
        0 too long, 0 too short
      6862 frames output, 307072 bytes
        0 discards, 0 errors
      0 input OLS, 0 LRR, 0 NOS, 0 loop inits
      0 output OLS, 0 LRR, 0 NOS, 0 loop inits
```

```
     16 receive B2B credit remaining
      3 transmit B2B credit remaining.
```

The following example shows how to display information about the in-band interface.

```
switch# show interface sup-fc0
sup-fc0 is up
    Hardware is FastEthernet, address is 0000.0000.0000
    MTU 2596 bytes, BW 1000000 Kbit
    66 packets input, 7316 bytes
    Received 0 multicast frames, 0 compressed
    0 input errors, 0 frame, 0 overrun 0 fifo
    64 packets output, 28068 bytes, 0 underruns
    0 output errors, 0 collisions, 0 fifo
    0 carrier errors
```

The following example shows how to display information about a VSAN interface.

```
switch# show interface vsan 2
vsan2 is up, line protocol is up
    WWPN is 10:00:00:05:30:00:59:1f, FCID is 0xb90100
    Internet address is 10.1.1.1/24
    MTU 1500 bytes, BW 1000000 Kbit
    0 packets input, 0 bytes, 0 errors, 0 multicast
    0 packets output, 0 bytes, 0 errors, 0 dropped
```

The following example shows how to display description information for all interfaces.

```
switch# show interface description
fc1/1
    no description
fc1/2
    no description
fc1/15
fcAnl

sup-fc0 is up

mgmt0 is up

vsan1 - IPFC interface

port-channel 15
no description

port-channel 98
no description
```

The following example shows how to display brief information for a range of interfaces.

```
switch# show interface fc2/1 - 5 brief
--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status           Oper  Oper   Port-channel
                  Mode   Trunk                    Mode  Speed
                         Mode                           (Gbps)
--------------------------------------------------------------------------------
fc1/1      1      auto   on      down             --    --     --
fc1/2      1      auto   on      fcotAbsent       --    --     --
fc1/3      1      F      --      notConnected     --    --     --
fc1/4      1      auto   on      fcotAbsent       --    --     --
fc1/5      1      F      --      up               F     2      --
fc1/6      1      auto   on      fcotAbsent       --    --     --
fc1/7      1      auto   on      down             --    --     --
fc1/8      1      auto   on      fcotAbsent       --    --     --
fc1/9      1      auto   on      fcotAbsent       --    --     --
```

```
fc1/10     1      auto   on      fcotAbsent       --    --     --
fc1/11     1      auto   on      down             --    --     --
fc1/12     1      auto   on      fcotAbsent       --    --     --
fc1/13     1      auto   on      down             --    --     --
fc1/14     1      auto   on      fcotAbsent       --    --     --
fc1/15     1      auto   on      down             --    --     --
fc1/16     1      auto   on      fcotAbsent       --    --     --
-------------------------------------------------------------------------------
Interface          Status   IP Address               Speed        MTU
-------------------------------------------------------------------------------
sup-fc0            up       --                       1 Gbps       2596
-------------------------------------------------------------------------------
Interface          Status   IP Address               Speed        MTU
-------------------------------------------------------------------------------
mgmt0              up       173.95.112/24         100 Mbps     1500
-------------------------------------------------------------------------------
Interface          Status   IP Address               Speed        MTU
-------------------------------------------------------------------------------
vsan1                 up    10.1.1.1/24              1 Gbps       1500
```

The following example shows how to display counter information for a FCIP interface.

```
switch# show interface fcip 3 counters
fcip3
    TCP Connection Information
      2 Active TCP connections
        Control connection: Local 43.1.1.2:3225, Remote 43.1.1.1:65532
        Data connection: Local 43.1.1.2:3225, Remote 43.1.1.1:65534
      30 Attempts for active connections, 0 close of connections
    TCP Parameters
      Path MTU 1500 bytes
      Current retransmission timeout is 300 ms
      Round trip time: Smoothed 10 ms, Variance: 5
      Advertised window: Current: 122 KB, Maximum: 122 KB, Scale: 1
      Peer receive window: Current: 114 KB, Maximum: 114 KB, Scale: 1
      Congestion window: Current: 2 KB, Slow start threshold: 1048560 KB
    5 minutes input rate 64 bits/sec, 8 bytes/sec, 0 frames/sec
    5 minutes output rate 64 bits/sec, 8 bytes/sec, 0 frames/sec
      910 frames input, 84652 bytes
         910 Class F frames input, 84652 bytes
         0 Class 2/3 frames input, 0 bytes
         0 Error frames timestamp error 0
      908 frames output, 84096 bytes
         908 Class F frames output, 84096 bytes
         0 Class 2/3 frames output, 0 bytes
         0 Error frames 0 reass frames
```

The following example shows how to display counter information for all interfaces.

```
switch# show interface counters brief

-------------------------------------------------------------------------------
Interface          Input (rate is 5 min avg)      Output (rate is 5 min avg)
                   ----------------------------- -----------------------------
                   Rate     Total                 Rate     Total
                   MB/s     Frames                MB/s     Frames
-------------------------------------------------------------------------------
fc9/1              0        0                     0        0
fc9/2              0        0                     0        0
fc9/3              0        0                     0        0
fc9/4              0        0                     0        0
...
-------------------------------------------------------------------------------
Interface          Input (rate is 5 min avg)      Output (rate is 5 min avg)
```

```
                  ----------------------------  ----------------------------
                  Rate     Total                Rate     Total
                  MB/s     Frames               MB/s     Frames
-------------------------------------------------------------------------------
iscsi4/1          0        0                    0        0
iscsi4/2          0        0                    0        0
iscsi4/3          0        0                    0        0
iscsi4/4          0        0                    0        0
...
vsan10 is up, line protocol is up
    WWPN is 10:00:00:05:30:00:07:23, FCID is 0xee0001
    Internet address is 10.1.1.5/24
    MTU 1500 bytes, BW 1000000 Kbit
    0 packets input, 0 bytes, 0 errors, 0 multicast
    0 packets output, 0 bytes, 0 errors, 0 dropped

-------------------------------------------------------------------------------
Interface          Input (rate is 5 min avg)      Output (rate is 5 min avg)
                   ----------------------------  ----------------------------
                   Rate     Total                Rate     Total
                   MB/s     Frames               MB/s     Frames
-------------------------------------------------------------------------------

port-channel 100   0        0                    0        0

-------------------------------------------------------------------------------
Interface          Input (rate is 5 min avg)      Output (rate is 5 min avg)
                   ----------------------------  ----------------------------
                   Rate     Total                Rate     Total
                   Mbits/s  Frames               Mbits/s  Frames
-------------------------------------------------------------------------------

fcip2              0        0                    0        0
fcip3              9        0                    9        0

fcip6              8        0                    8        0
fcip7              8        0                    8        0
```

The following example shows how to display information about a FCIP interface.

```
switch# show interface fcip 3
fcip3 is trunking
    Hardware is GigabitEthernet
    Port WWN is 20:ca:00:05:30:00:07:1e
    Peer port WWN is 20:ca:00:00:53:00:18:1e
    Admin port mode is auto, trunk mode is on
    Port mode is TE
    vsan is 1
    Trunk vsans (allowed active) (1,10)
    Trunk vsans (operational)    (1)
    Trunk vsans (up)             (1)
    Trunk vsans (isolated)       (10)
    Trunk vsans (initializing)   ()
    Using Profile id 3 (interface GigabitEthernet4/3)
    Peer Information
      Peer Internet address is 43.1.1.1 and port is 3225
      Special Frame is disabled
    Maximum number of TCP connections is 2
    Time Stamp is disabled
    B-port mode disabled
    TCP Connection Information
      2 Active TCP connections
        Control connection: Local 43.1.1.2:3225, Remote 43.1.1.1:65532
        Data connection: Local 43.1.1.2:3225, Remote 43.1.1.1:65534
```

```
    30 Attempts for active connections, 0 close of connections
  TCP Parameters
    Path MTU 1500 bytes
    Current retransmission timeout is 300 ms
    Round trip time: Smoothed 10 ms, Variance: 5
    Advertised window: Current: 122 KB, Maximum: 122 KB, Scale: 1
    Peer receive window: Current: 114 KB, Maximum: 114 KB, Scale: 1
    Congestion window: Current: 2 KB, Slow start threshold: 1048560 KB
  5 minutes input rate 64 bits/sec, 8 bytes/sec, 0 frames/sec
  5 minutes output rate 64 bits/sec, 8 bytes/sec, 0 frames/sec
    866 frames input, 80604 bytes
       866 Class F frames input, 80604 bytes
       0 Class 2/3 frames input, 0 bytes
       0 Error frames timestamp error 0
    864 frames output, 80048 bytes
       864 Class F frames output, 80048 bytes
       0 Class 2/3 frames output, 0 bytes
       0 Error frames 0 reass frames
    16 receive B2B credit remaining
     3 transmit B2B credit remaining.
```

The following example shows how to display information about a Gigabit Ethernet interface.

```
switch# show interface gigabitethernet 4/1
GigabitEthernet4/1 is up
    Hardware is GigabitEthernet, address is 0005.3000.2e12
    Internet address is 100.1.1.2/24
    MTU 1500 bytes, BW 1000000 Kbit
    Port mode is IPS
    Speed is 1 Gbps
    Beacon is turned off
    5 minutes input rate 32 bits/sec, 4 bytes/sec, 0 frames/sec
    5 minutes output rate 88 bits/sec, 11 bytes/sec, 0 frames/sec
    637 packets input, 49950 bytes
      0 multicast frames, 0 compressed
      0 input errors, 0 frame, 0 overrun 0 fifo
    659 packets output, 101474 bytes, 0 underruns
      0 output errors, 0 collisions, 0 fifo
      0 carrier errors
```

The following example shows how to display information about an iSCSI interface.

```
switch# show interface iscsi 2/1
iscsi2/1 is up
    Hardware is GigabitEthernet
    Port WWN is 20:41:00:05:30:00:50:de
    Admin port mode is ISCSI
    Port mode is ISCSI
    Speed is 1 Gbps
    iSCSI initiator is identified by name
    Number of iSCSI session: 7, Number of TCP connection: 7
    Configured TCP parameters
        Local Port is 3260
        PMTU discover is disabled
        Keepalive-timeout is 1 sec
        Minimum-retransmit-time is 300 ms
        Max-retransmissions 8
        Sack is disabled
        Minimum available bandwidth is 0 kbps
        Estimated round trip time is 0 usec
    5 minutes input rate 265184 bits/sec, 33148 bytes/sec, 690 frames/sec
    5 minutes output rate 375002168 bits/sec, 46875271 bytes/sec, 33833 frames/sec
    iSCSI statistics
      6202235 packets input, 299732864 bytes
```

```
    Command 6189718 pdus, Data-out 1937 pdus, 1983488 bytes, 0 fragments
  146738794 packets output, 196613551108 bytes
    Response 6184282 pdus (with sense 4), R2T 547 pdus
    Data-in 140543388 pdus, 189570075420 bytes
```

The following example shows how to display transceiver information for a Fibre Channel interface.

```
switch# show interface fc2/5 transceiver
fc2/5 fcot is present
    name is CISCO-INFINEON
    part number is V23848-M305-C56C
    revision is A3
    serial number is 30000474
    fc-transmitter type is short wave laser
    cisco extended id is unknown (0x0)
```

The following example shows how to display information about a Fibre Channel tunnel interface.

```
switch# show interface fc-tunnel 200
fc-tunnel 200 is up
Dest   IP Addr: 200.200.200.7   Tunnel ID: 200
Source IP Addr: 200.200.200.4   LSP ID: 1
Explicit Path Name:
```

The following example shows how to display hardware port information for a Fibre Channel interface.

```
switch(config-if)# show interface fc 3/9 capabilities
 Min Speed is 1 Gbps
 Max Speed is 2 Gbps
 FC-PH Version (high, low)                          (32,32)
 Receive data field size (max/min)                  (2112/256)  bytes
 Transmit data field size (max/min)                 (2112/128)  bytes
 Classes of Service supported are                   Class 2, Class 3, Class F
 Class 2 sequential delivery                        supported
 Class 3 sequential delivery                        supported
 Hold time (max/min)                                (100000/1) micro sec
 BB state change notification                       supported
 Maximum BB state change notifications              14
 Rate Mode change                                   not supported

 Rate Mode Capabilities                             Shared        Dedicated
  Receive BB Credit modification supported             no              yes
  FX mode Receive BB Credit (min/max/default)          --        (1/255/16)
  ISL mode Receive BB Credit (min/max/default)         --        (2/255/255)
  Performance buffer modification supported             no              yes
  FX mode Performance buffers (min/max/default)        --        (1/145/0)
  ISL mode Performance buffers (min/max/default)       --        (1/145/0)

 Out of Service capable                              no
 Beacon mode configurable                            yes
```

show inventory

To display the system hardware inventory, use the **show inventory** command.

show inventory

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

This command displays information about the field replaceable units (FRUs) in the switch, including product IDs, serial numbers, and version IDs.

Examples

The following example displays the system inventory information.

```
switch# show inventory
NAME: "Chassis",  DESCR: "MDS 9506 chassis"
PID: DS-C9506             ,  VID: 0.1,  SN: FOX0712S007

NAME: "Slot 1",  DESCR: "2x1GE IPS, 14x1/2Gbps FC Module"
PID: DS-X9302-14K9        ,  VID: 0.301,  SN: JAB083100JY

NAME: "Slot 5",  DESCR: "Supervisor/Fabric-1"
PID: DS-X9530-SF1-K9      ,  VID: 0.0,  SN: JAB0747080H

NAME: "Slot 6",  DESCR: "Supervisor/Fabric-1"
PID: DS-X9530-SF1-K9      ,  VID: 4.0,  SN: JAB074004VE

NAME: "Slot 17",  DESCR: "MDS 9506 Power Supply"
PID: DS-CAC-1900W         ,  VID: 1.0,  SN: DCA0702601V

NAME: "Slot 18",  DESCR: "MDS 9506 Power Supply"
PID: DS-CAC-1900W         ,  VID: 1.0,  SN: DCA0702601U

NAME: "Slot 19",  DESCR: "MDS 9506 Fan Module"
PID: DS-6SLOT-FAN         ,  VID: 0.1,  SN: FOX0638S150
```

show ip access-list

To display the IP access control lists (IP-ACLs) currently active, use the **show ip access-list** command.

show ip access-list [*list-number* | **usage**]

Syntax Description

ip access-list	Displays the information for all IP-ACLs.
list-number	Identifies the IP-ACL with an integer ranging from 1 to 256.
usage	Specifies the interface type.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays configured IP-ACLs.

```
switch# show ip access-list usage
Access List Name/Number          Filters IF   Status    Creation Time
-------------------------------- ------- ---- --------- -------------
abc                              3       7    active    Tue Jun 24 17:51:40 2003
x1                               3       1    active    Tue Jun 24 18:32:25 2003
x3                             0       1    not-ready Tue Jun 24 18:32:28 2003
```

The following example displays a summary of the specified IP-ACL

```
switch# show ip access-list abc
ip access-list abc permit tcp any any (0 matches)
ip access-list abc permit udp any any (0 matches)
ip access-list abc permit icmp any any (0 matches)
ip access-list abc permit ip 10.1.1.0 0.0.0.255 (2 matches)
ip access-list abc permit ip 10.3.70.0 0.0.0.255 (7 matches)
```

show ip arp

To display IP neighbors for the system, use the **show ip arp** command.

show ip arp [interface {cpp *module-number* **| gigabitethernet** *slot/port* **| mgmt | vsan** *vsan-id***}]**

Syntax Description

interface	Displays the IP neighbors for a specified interface.
cpp *module-number*	Specifies the virtualization IP over Fibre Channel (IPFC) interface by control plane processor (CPP) module number. The range is 1 to 6.
gigabitethernet *slot/port*	Specifies the Gigabit Ethernet interface by slot and port number. The range is 1 to 6.
mgmt	Specifies the management interface.
vsan *vsan-id*	Specifies the IPFC VSAN interface by VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays IP neighbor information.

```
switch# show ip arp
IP Address       Age(min)   Link-layer Addr         Type  Interface
10.10.10.100     0          0006.d623.4008          ARPA  GigabitEthernet1/1
10.10.10.9       5          0002.b3d9.ba6f          ARPA  GigabitEthernet1/1
10.10.10.16      11         0004.23bd.677b          ARPA  GigabitEthernet1/1
172.22.31.1      67         0000.0c07.ac01          ARPA  mgmt0
172.22.31.2      0          000e.d68f.c3fc          ARPA  mgmt0
172.22.31.3      0          000e.d68f.43fc          ARPA  mgmt0
172.22.31.250    1067       00e0.8152.7f8d          ARPA  mgmt0
```

Related Commands

Command	Description
show ip interface	Displays IP interface status and configuration information.
show ip traffic	Displays IP protocol statistics for the system.

show ip interface

To display IP interface status and configuration information, use the **show ip interface** command.

show ip interface [cpp *module-number* **| gigabitethernet** *slot/port* **| mgmt | port-channel** *number* **| vsan** *vsan-id***]**

Syntax Description

cpp *module-number*	Specifies the virtualization IP over Fibre Channel (IPFC) interface by CPP module number. The range is 1 to 6.
gigabitethernet *slot/port*	Specifies the Gigabit Ethernet interface by slot and port number. The range is 1 to 6.
mgmt	Specifies the management interface.
port-channel *number*	Specifies the PortChannel interface. The range is 1 to 256.
vsan *vsan-id*	Specifies the IPFC VSAN interface by VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays IP interface status and configuration information.

```
switch# show ip interface
GigabitEthernet1/1 is up
  Internet address is 10.10.10.1/24
  Broadcast address is 255.255.255.255

GigabitEthernet1/2 is up
  Internet address is 10.10.60.1/24
  Broadcast address is 255.255.255.255

GigabitEthernet2/2 is up
  Internet address is 10.10.20.1/24
  Broadcast address is 255.255.255.255

mgmt0 is up
  Internet address is 172.22.31.110/24
  Broadcast address is 255.255.255.255
```

Related Commands

Command	Description
show ip arp	Displays IP neighbors for the system.
show ip traffic	Displays IP protocol statistics for the system.

show ip route

To display the ip routes currently active, use the **show ip route** command.

show ip route [**configured**]

Syntax Description

configured	Displays configured IP routes.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays active IP routes.

```
switch# show ip route

Codes: C - connected, S - static

Default gateway is 172.22.95.1

C 10.0.0.0/24 is directly connected, vsan1
C 172.22.95.0/24 is directly connected, mgmt0
```

The following example displays configured IP routes.

```
switch# show ip route configured
         default      172.22.31.1          0.0.0.0      0            mgmt0
      10.10.11.0       10.10.11.1    255.255.255.0      0 GigabitEthernet1/1
      10.10.50.0       10.10.50.1    255.255.255.0      0 GigabitEthernet1/2.1
      10.10.51.0       10.10.51.1    255.255.255.0      0 GigabitEthernet1/2.2
      10.10.60.0       10.10.60.1    255.255.255.0      0 GigabitEthernet1/2
     172.22.31.0    172.22.31.110    255.255.255.0      0            mgmt0
```

show ip routing

To display the IP routing state, use the **show ip routing** command.

show ip routing

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example the IP routing state.

```
switch# show ip routing
ip routing is disabled
```

show ip traffic

To display IP protocol statistics for the system, use the **show ip traffic** command.

show ip traffic [interface gigabitethernet *slot/port***]**

Syntax Description

interface	Displays the IP neighbors for a specified interface.
gigabitethernet *slot/port*	Specifies the Gigabit Ethernet interface by slot and port number. The range is 1 to 6.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays IP protocol statistics for the Gigabit Ethernet interface.

```
switch# show ip traffic interface gigabitethernet 2/2
IP Statistics for GigabitEthernet2/2
  Rcvd:  0 total, 0 local destination
         0 errors, 0 unknown protocol, 0 dropped
  Sent:  30 total, 0 forwarded 0 dropped
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 fragments created, 0 couldn't fragment

ICMP Statistics:
  Rcvd:  0 total, 0 errors, 0 unreachables, 0 time exceeded
         0 echo, 0 echo reply, 0 mask requests, 0 mask replies
         0 redirects, 0 timestamp requests, 0 timestamp replies
  Sent:  0 total, 0 errors, 0 unreachables, 0 time exceeded
         0 echo, 0 echo reply, 0 mask requests, 0 mask replies
         0 redirects, 0 timestamp requests, 0 timestamp replies
```

Related Commands

Command	Description
show ip arp	Displays IP neighbors for the system.
show ip interface	Displays IP interface status and configuration information.

show ips arp

To display the IP storage ARP cache information, use the **show ips arp** command.

show ips arp interface gigabitethernet *slot/port*

Syntax Description

interface gigabitethernet *slot/port*	Specifies a Gigabit Ethernet interface by the slot and port.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Use the **show ips arp interface gigabitethernet** command to display the ARP cache on the Gigabit Ethernet interfaces. This command takes the main Ethernet interface and as a parameter and returns the ARP cache for that interface.

Examples

The following example displays ARP caches in the specified interface.

```
switch# show ips arp interface gigabitethernet 4/1
Protocol         Address   Age (min)   Hardware Addr  Type   Interface
Protocol         Address   Age (min)   Hardware Addr  Type   Interface
Internet     172.22.91.1    2    -  00:00:0c:07:ac:01  ARPA  GigabitEthernet4/4
Internet     172.22.91.2    0    -  00:02:7e:6b:a8:08  ARPA  GigabitEthernet4/4
Internet    172.22.91.17    0    -  00:e0:81:20:45:f5  ARPA  GigabitEthernet4/4
Internet    172.22.91.18    0    -  00:e0:81:05:f7:64  ARPA  GigabitEthernet4/4
Internet    172.22.91.30    0    -  00:e0:18:2e:9d:19  ARPA  GigabitEthernet4/4
...
```

show ips ip route

To show the IP storage route table information, use the **show ips ip route** command.

show ips ip route interface gigabitethernet *slot/port*

Syntax Description

interface gigabitethernet *slot/port*	Specifies a Gigabit Ethernet interface by the slot and port.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the IP route table information for a Gigabit Ethernet interface.

```
switch# show ips ip route interface gigabitethernet 8/1
Codes: C - connected, S - static

No default gateway

C 10.1.3.0/24 is directly connected, GigabitEthernet8/1
```

show ips ipv6

To display an IPv6 storage routing table, use the **show ips ipv6** command.

show ips ipv6 {**neighbors interface gigabitethernet** *slot/port* |
prefix-list interface gigabitethernet *slot/port* |
route interface gigabitethernet *slot/port* |
routers interface gigabitethernet *slot/port* |
traffic interface gigabitethernet *slot/port*}

Syntax Description

neighbors	Displays the IPv6 neighbors table.
interface	Displays the interface status and configuration.
gigabitethernet	Displays a Gigabit Ethernet interface.
slot/port	Specifies the slot and port number.
prefix-list	Displays theIPv6 prefix-list table.
route	Displays the IPv6 route table.
routers	Displays the IPv6 routers table.
traffic	Displays the IPv6 traffic table.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(0)	This command was introduced.

Usage Guidelines

You can use the **show ips ipv6** command to display information about IPv6 routing.

Examples

The following example displays IPv6 neighbors information.

```
switch# show ips ipv6 neighbours interface gigabitethernet 1/1
IPv6 Address                              Age (min)  Link-layer Addr  State  Inter
face
fe80::206:d6ff:fe23:4008                  0          0006.d623.4008      S
GigabitEthernet1/1
```

The following example displays the IPv6 prefix-list information.

```
switch# show ips ipv6 prefix-list interface gigabitethernet 1/1
Prefix                                 Prefix-len   Addr
     Valid   Preferred
2000::                                   64         2000::205:30ff:fe01:a6be
       1000     1000
```

The following example displays the IPv6 routing table.

```
switch# show ips ipv6 route interface gigabitethernet 4/2

IPv6 Routing Table - 4 entries
Codes: C - Connected, L - Local, S - Static, G - Gateway, M - Multicast
C 3000:8::/64 is directly connected, GigabitEthernet4/2.250
C 3000:7::/64 is directly connected, GigabitEthernet4/2
C fe80::/64 is directly connected, GigabitEthernet4/2
C fe80::/64 is directly connected, GigabitEthernet4/2.250
M ff02::/32 is multicast, GigabitEthernet4/2
M ff02::/32 is multicast, GigabitEthernet4/2.250
```

The following example displays IPv6 routers information.

```
switch# show ips ipv6 routers interface gigabitethernet 1/1
Addr                            Lifetime   Expire
fe80::206:d6ff:fe23:4008        3600       3600
```

The following example displays IPv6 traffic statistics.

```
switch#  show ips ipv6 traffic interface gigabitethernet 4/2
IPv6 statistics:
  Rcvd:  0 total
         0 bad header, 0 unknown option, 0 unknown protocol
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  20 generated
         0 fragmented into 0 fragments, 0 failed
         2 no route
ICMP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 too short
         0 unknown info type, 0 unknown error type
         unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
         parameter: 0 error, 0 header, 0 option
         0 hopcount expired, 0 reassembly timeout,0 too big
         0 echo request, 0 echo reply
         0 group query, 0 group report, 0 group reduce
         0 router solicit, 0 router advert, 0 redirects
         0 neighbor solicit, 0 neighbor advert
  Sent: 20 output, 0 rate-limited
         unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
         parameter: 0 error, 0 header, 0 option
         0 hopcount expired, 0 reassembly timeout,0 too big
         0 echo request, 0 echo reply
         0 group query, 6 group report, 0 group reduce
         2 router solicit, 0 router advert, 0 redirects
         0 neighbor solicit, 12 neighbor advert
```

Related Commands

Command	Description
ipv6 enable	Enables IPv6 processing.
show ipv6 route	Displays IPv6 routes configured on the system.

show ips stats

To display IP storage statistics, use the **show ips stats** command.

show ips stats {**buffer** | **dma-bridge** | **icmp** | **ip** | **mac**} **interface gigabitethernet** *slot*/*port*

show ips stats {**hw-comp** | **tcp**} {**all** | **interface gigabitethernet** *slot*/*port*}

Syntax Description

buffer	Displays IP storage buffer information.
dma-bridge	Displays the direct memory access (DMA) statistics.
icmp	Displays ICMP statistics.
ip	Displays IP statistics.
mac	Displays MAC statistics.
hw-comp	Displays hardware compression statistics.
tcp	Displays TCP statistics
all	Displays statistical information for all interfaces.
interface gigabitethernet *slot*/*port*	Specifies a Gigabit Ethernet interface by the slot and port.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Use the **show ips stats icmp interface gigabitethernet** command to obtain ICMP statistics for the selected interface.

Use the **show ips stats ip interface gigabitethernet 2/1** command to obtain IP statistics for the selected interface.

Use the **show ips stats mac interface gigabitethernet** command to obtain Ethernet statistics for the selected interface.

Use the **show ips stats tcp interface gigabitethernet** command to obtain TCP stats along with the connection list and TCP state or the selected interface.

Examples

The following example displays iSCSI buffer statistics.

```
switch# show ips stats buffer interface gigabitethernet 1/2
Buffer Statistics for port GigabitEthernet1/2
    Mbuf stats
      164248 total mbufs, 82119 free mbufs, 0 mbuf alloc failures
      123186 mbuf high watermark, 20531 mbuf low watermark
      0 free shared mbufs, 0 shared mbuf alloc failures
      82124 total clusters, 77005 free clusters, 0 cluster alloc failures
      86230 mbuf high watermark, 78017 mbuf low watermark
      0 free shared clusters, 0 shared cluster alloc failures
    Ether channel stats
      0 tcp segments sent, 0 tcp segments received
      0 xmit packets sent, 0 xmit packets received
      0 config packets sent, 0 config packets received
      0 MPQ packet send errors
```

The following example displays ICMP statistics.

```
switch# show ips stats icmp interface gigabitethernet 8/1
ICMP Statistics for port GigabitEthernet8/1
    2 ICMP messages received
    0 ICMP messages dropped due to errors
    ICMP input histogram
      2 echo request
    ICMP output histogram
      2 echo reply
```

The following example displays IP statistics.

```
switch# show ips stats ip interface gigabitethernet 8/1
Internet Protocol Statistics for port GigabitEthernet8/1
    22511807 total received, 22509468 good, 2459 error
    0 reassembly required, 0 reassembled ok, 0 dropped after timeout
    27935633 packets sent, 0 outgoing dropped, 0 dropped no route
    0 fragments created, 0 cannot fragment
```

The following example displays MAC statistics.

```
switch# show ips stats mac interface gigabitethernet 8/1
Ethernet MAC statistics for port GigabitEthernet8/1
    Hardware Transmit Counters
      28335543 frame 37251751286 bytes
      0 collisions, 0 late collisions, 0 excess collisions
      0 bad frames, 0 FCS error, 0 abort, 0 runt, 0 oversize
    Hardware Receive Counters
      18992406778 bytes, 22835370 frames, 0 multicasts, 2584 broadcasts
      0 bad, 0 runt, 0 CRC error, 0 length error
      0 code error, 0 align error, 0 oversize error
    Software Counters
      22835370 received frames, 28335543 transmit frames
      0 frames soft queued, 0 current queue, 0 max queue
      0 dropped, 0 low memory
```

The following example displays TCP statistics.

```
switch# show ips stats tcp interface gigabitethernet 8/1
TCP Statistics for port GigabitEthernet8/1
    Connection Stats
      0 active openings, 0 accepts
      0 failed attempts, 0 reset received, 0 established
    Segment stats
      23657893 received, 29361174 sent, 0 retransmitted
      0 bad segments received, 0 reset sent

    TCP Active Connections
      Local  Address        Remote Address        State      Send-Q   Recv-Q
      10.1.3.3:3260         10.1.3.106:51935      ESTABLISH  0        0
      10.1.3.3:3260         10.1.3.106:51936      ESTABLISH  0        0
      10.1.3.3:3260         10.1.3.106:51937      ESTABLISH  0        0
      10.1.3.3:3260         10.1.3.106:51938      ESTABLISH  0        0
      10.1.3.3:3260         10.1.3.106:51939      ESTABLISH  0        0
      10.1.3.3:3260         10.1.3.106:51940      ESTABLISH  0        0
      10.1.3.3:3260         10.1.3.106:51941      ESTABLISH  0        0
      10.1.3.3:3260         10.1.3.106:51942      ESTABLISH  0        0
      10.1.3.3:3260         10.1.3.106:51943      ESTABLISH  0        0
      10.1.3.3:3260         10.1.3.106:51944      ESTABLISH  0        0
      10.1.3.3:3260         10.1.3.115:1026       ESTABLISH  0        0
      10.1.3.3:3260         10.1.3.115:1027       ESTABLISH  0        0
      10.1.3.3:3260         10.1.3.115:1028       ESTABLISH  0        0
      10.1.3.3:3260         10.1.3.115:1029       ESTABLISH  0        0
      10.1.3.3:3260         10.1.3.115:1030       ESTABLISH  48       0
      10.1.3.3:3260         10.1.3.115:1031       ESTABLISH  48       0
      10.1.3.3:3260         10.1.3.115:1032       ESTABLISH  0        0
      10.1.3.3:3260         10.1.3.115:1033       ESTABLISH  0        0
      10.1.3.3:3260         10.1.3.115:1034       ESTABLISH  0        0
      0.0.0.0:3260          0.0.0.0:0             LISTEN     0        0
```

show ips status

To display the IP storage status, use the **show ips status** command.

show ips status [**module** *slot*]

Syntax Description

module *slot*	Identifies the module in the specified slot.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the IP storage status for all modules on the switch.

```
switch# show ips status
        Port 8/1 READY
        Port 8/2 READY
        Port 8/3 READY
        Port 8/4 READY
        Port 8/5 READY
        Port 8/6 READY
        Port 8/7 READY
        Port 8/8 READY
```

The following example displays the IP storage status for the module in slot 9.

```
switch# show ips status module 9
        Port 9/1 READY
        Port 9/2 READY
        Port 9/3 READY
        Port 9/4 READY
        Port 9/5 READY
        Port 9/6 READY
        Port 9/7 READY
        Port 9/8 READY
```

show ipv6 access-list

To display a summary of IPv6 access control lists (ACLs), use the **show ipv6 access-list** command.

show ipv6 access-list [*list-name*]

Syntax Description

list-name	Specifies the name of the ACL. The maximum size is 64.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(0)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays an IPv6 access control list.

```
switch# show ipv6 access-list
Access List Name/Number          Filters IF   Status    Creation Time
-------------------------------- ------- ---- --------- -------------
abc                              3       7    active    Tue Jun 24 17:51:40 2003
x1                               3       1    active    Tue Jun 24 18:32:25 2003
x3                               0       1    not-ready Tue Jun 24 18:32:28 2003
```

Related Commands

Command	Description
ipv6 access-list	Configures an IPv6-ACL.

show ipv6 interface

To display IPv6 interface status and configuration information, use the **show ipv6 interface** command.

show ipv6 interface [**gigabitethernet** *slot/port* | **mgmt 0** | **port-channel** *port-channel-number* | **vsan** *vsan-id*]

Syntax Description

gigabitethernet *slot/port*	Displays a Gigabit Ethernet interface.
mgmt 0	Displays the management interface.
port-channel	Displays a PortChannel interface.
port-channel-number	Specifies the PortChannel number. The range is 1 to 128.
vsan	Displays an IPFC VSAN interface.
vsan-id	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(0)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displaysIPv6 interface information.

```
switch# show ipv6 interface
GigabitEthernet1/2 is up
  IPv6 is enabled
  Global address(es):
    5000::1/64
  Link-local address(es):
    fe80::205:30ff:fe01:a6bf
  ND DAD is disabled
  ND reachable time is 30000 milliseconds
  ND retransmission time is 1000 milliseconds
  Stateless autoconfig for addresses disabled

GigabitEthernet2/2 is up
  IPv6 is enabled
  Global address(es):
    6000::1/64
  Link-local address(es):
    fe80::205:30ff:fe00:a413
  ND DAD is disabled
```

```
ND reachable time is 30000 milliseconds
ND retransmission time is 1000 milliseconds
Stateless autoconfig for addresses disabled
```

Related Commands

Command	Description
ipv6 address	Configures an IPv6 address.
ipv6 nd	Configures IPv6 neighbor discovery commands.
ipv6 route	Configures an IPv6 static route.
show ipv6 neighbors	Displays information about IPv6 neighbors for the system.
show ipv6 route	Displays the IPv6 routes configured on the system.

show ipv6 neighbours

To display IPv6 neighbors configuration information, use the **show ipv6 neighbours** command.

show ipv6 neighbours [**interface** {**gigabitethernet** *slot/port* | **mgmt 0** | **vsan** *vsan-id*}]

Syntax Description

interface	Displays the IP interface status and configuration.
gigabitethernet *slot/port*	Displays a Gigabit Ethernet interface slot and port number.
mgmt 0	Displays the management interface.
vsan *vsan-id*	Displays an IPFC VSAN interface and specifies the VSAN ID. The range is 1 to 4093

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(0)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays information about IPv6 neighbor discovery.

```
switch# show ipv6 neighbours gigabitethernet 2/1

IPv6 Address                                Age Link-layer Addr State Interface
2001:0DB8:0:4::2                              0 0003.a0d6.141e  REACH Ethernet2
FE80::XXXX:A0FF:FED6:141E                     0 0003.a0d6.141e  REACH Ethernet2
2001:0DB8:1::45a                              - 0002.7d1a.9472  REACH Ethernet2
```

Related Commands

Command	Description
ipv6 nd	Configures IPv6 neighbor discovery commands.

show ipv6 route

To display the IPv6 routes configured on the system, use the **show ipv6 route** command.

show ipv6 route

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(0)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays information about an IPv6 route.

```
switch# show ipv6 route
IPv6 Routing Table
Codes: C - Connected, L - Local, S - Static G - Gateway
C    5000::/64
     via fe80::205:30ff:fe01:a6bf, GigabitEthernet1/2
C    6000::/64
     via fe80::205:30ff:fe00:a413, GigabitEthernet2/2
L    fe80::/10
     via ::
L    ff00::/8
     via ::
```

Related Commandsl

Command	Description
ipv6 route	Configures an IPv6 route.

show ipv6 routing

To display IPv6 unicast routing information, use the **show ipv6 routing** command.

show ipv6 routing

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(0)	This command was introduced.

Usage Guidelines

None.

Examples

```
switch# show ipv6 routing
ipv6 routing is enabled
```

Related Commands

Command	Description
ipv6 routing	Enables IPv6 unicast routing.

show ipv6 traffic

To display IPv6 protocol statistics for the system, use the **show ipv6 traffic** command.

show ipv6 traffic [interface {**gigabitethernet** *slot/port* **| mgmt 0 | port-channel** *number* **| vsan** *vsan-id*}]

Syntax Description

interface	Displays the IP interface status and configuration.
gigabitethernet *slot/port*	Displays a Gigabit Ethernet interface slot and port number.
mgmt 0	Displays the management interface.
port-channel *number*	Dispalsy the PortChannel interface. The range is 1 to 256.
vsan *vsan-id*	Displays a IPFC VSAN interface and specifies the VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(0)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays IPv6 protocol statistics on the system.

```
switch# show ipv6 traffic
IPv6 Statistics:
  Rcvd:  1 total, 0 local destination
         0 errors, 0 truncated, 0 too big
         0 unknown protocol, 0 dropped
         0 fragments, 0 reassembled
         0 couldn't reassemble, 0 reassembly timeouts
  Sent:  0 generated, 0 forwarded 0 dropped
         0 fragmented, 0 fragments created, 0 couldn't fragment

ICMPv6 Statistics:
  Rcvd:  0 total, 0 errors, 0 unreachables, 0 time exceeded
         0 too big, 0 param probs, 0 admin prohibs
         0 echos, 0 echo reply, 0 redirects
         0 group query, 0 group report, 0 group reduce
         0 router solicit, 0 router advert
         0 neighbor solicit, 0 neighbor advert
  Sent:  74 total, 0 errors, 0 unreachables, 0 time exceeded
         0 too big, 0 param probs, 0 admin prohibs
         0 echos, 0 echo reply, 0 redirects
         0 group query, 53 group report, 0 group reduce
         0 router solicit, 0 router advert
         0 neighbor solicit, 21 neighbor advert
```

The following example displays IPv6 traffic on Gigabit Ethernet interface 2/2.

```
switch# show ipv6 traffic interface gigabitethernet 2/2
IPv6 Statistics for GigabitEthernet2/2
  Rcvd:  10 total, 0 local destination
         0 errors, 0 truncated, 0 too big
         0 unknown protocol, 0 dropped
         0 fragments, 0 reassembled
         0 couldn't reassemble, 0 reassembly timeouts
  Sent:  54 generated, 0 forwarded 0 dropped
         0 fragmented, 0 fragments created, 0 couldn't fragment

ICMPv6 Statistics for GigabitEthernet2/2
  Rcvd:  4 total, 0 errors, 0 unreachables, 0 time exceeded
         0 too big, 0 param probs, 0 admin prohibs
         0 echos, 0 echo reply, 0 redirects
         0 group query, 2 group report, 0 group reduce
         0 router solicit, 0 router advert
         0 neighbor solicit, 2 neighbor advert
  Sent:  21 total, 0 errors, 0 unreachables, 0 time exceeded
         0 too big, 0 param probs, 0 admin prohibs
         0 echos, 0 echo reply, 0 redirects
         0 group query, 6 group report, 3 group reduce
         2 router solicit, 0 router advert
         2 neighbor solicit, 8 neighbor advert
```

show iscsi global

To display global iSCSI configured information, use the **show iscsi global** command.

show iscsi global

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays all configured iSCSI initiators.

```
switch# show iscsi global
iSCSI Global information
Authentication: CHAP, NONE
Import FC Target: Enabled
Initiator idle timeout: 300 seconds
Dynamic Initiator: iSLB
Number of target node: 1
Number of portals: 2
Number of session: 0
Failed session: 0, Last failed initiator name:
```

show iscsi initiator

To display information about all the iSCSI nodes that are remote to the switch, use the **show iscsi initiator** command.

show iscsi initiator [**configured** [*initiator-name*] | **detail** | **fcp-session** [**detail**] | **iscsi-session** [**detail**] | **summary** [**name**]]

Syntax Description

configured	Displays the configured information for the iSCSI initiator.
initiator-name	Specifies the name of an initiator.
detail	Displays detailed iSCSI initiator information.
fcp-session	Displays the Fibre Channel session details.
iscsi-session	Displays iSCSI session details.
summary	Displays summary information.
name	Displays initiator name information.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

If no parameter is provided the command lists all the active iSCSI initiators. If the iSCSI node name is provided then the command lists the details of that iSCSI initiator.

Examples

The following example displays all iSCSI initiators.

```
switch# show iscsi initiator
iSCSI Node name is iqn.1987-05.com.cisco.01.15cee6e7925087abc82ed96377653c8
    iSCSI alias name: iscsi7-lnx
    Node WWN is 23:10:00:05:30:00:7e:a0 (dynamic)
    Member of vsans: 1
    Number of Virtual n_ports: 1
    Virtual Port WWN is 23:12:00:05:30:00:7e:a0 (dynamic)
      Interface iSCSI 8/3, Portal group tag: 0x382
        VSAN ID 1, FCID 0xdc0100

iSCSI Node name is iqn.1987-05.com.cisco:02.91b0ee2e8aa1.iscsi16-w2k
    iSCSI alias name: ISCSI16-W2K
    Node WWN is 23:1f:00:05:30:00:7e:a0 (dynamic)
    Member of vsans: 1
    Number of Virtual n_ports: 1
    Virtual Port WWN is 23:28:00:05:30:00:7e:a0 (dynamic)
      Interface iSCSI 8/3, Portal group tag: 0x382
```

```
        VSAN ID 1, FCID 0xdc0101

iSCSI Node name is iqn.1987-05.com.cisco.01.b6ca466f8b4d8e848ab17e92f24bf9cc
    iSCSI alias name: iscsi6-lnx
    Node WWN is 23:29:00:05:30:00:7e:a0 (dynamic)
    Member of vsans: 1, 2, 3, 4
    Number of Virtual n_ports: 1
    Virtual Port WWN is 23:2a:00:05:30:00:7e:a0 (dynamic)
      Interface iSCSI 8/3, Portal group tag: 0x382
        VSAN ID 4, FCID 0xee0000
        VSAN ID 3, FCID 0xee0100
        VSAN ID 2, FCID 0xee0000
        VSAN ID 1, FCID 0xdc0102
...
```

The following example displays detailed Information for all iSCSI initiators.

```
switch# show iscsi initiator detail
iSCSI Node name is iqn.1987-05.com.cisco.01.15cee6e7925087abc82ed96377653c8
    iSCSI alias name: iscsi7-lnx
    Node WWN is 23:10:00:05:30:00:7e:a0 (dynamic)
    Member of vsans: 1
    Number of Virtual n_ports: 1

    Virtual Port WWN is 23:10:00:05:30:00:7e:a0 (dynamic)
      Interface iSCSI 8/3, Portal group tag is 0x382
        VSAN ID 1, FCID 0xdc0100
        No. of FC sessions: 3
        No. of iSCSI sessions: 2

        iSCSI session details

          Target node: iqn.com.domainname.172.22.93.143.08-03.gw.22000020374b5247
          Statistics:
            PDU: Command: 0, Response: 0
            Bytes: TX: 0, RX: 0
            Number of connection: 1
          TCP parameters
            Connection Local 10.1.3.3:3260, Remote 10.1.3.107:34112
            Path MTU 1500 bytes
            Current retransmission timeout is 300 ms
            Round trip time: Smoothed 2 ms, Variance: 1
            Advertised window: Current: 6 KB, Maximum: 6 KB, Scale: 3
            Peer receive window: Current: 250 KB, Maximum: 250 KB, Scale: 2
            Congestion window: Current: 8 KB

          Target node: iqn.com.domainname.172.22.93.143.08-03.gw.22000020374b5247
          Statistics:
            PDU: Command: 0, Response: 0
            Bytes: TX: 0, RX: 0
            Number of connection: 1
          TCP parameters
            Connection Local 10.1.3.3:3260, Remote 10.1.3.107:34112
            Path MTU 1500 bytes
            Current retransmission timeout is 300 ms
            Round trip time: Smoothed 2 ms, Variance: 1
            Advertised window: Current: 6 KB, Maximum: 6 KB, Scale: 3
            Peer receive window: Current: 250 KB, Maximum: 250 KB, Scale: 2
            Congestion window: Current: 8 KB
...
```

show iscsi session

To display iSCSI session information, use the **show iscsi session** command.

show iscsi session [**incoming**] [**initiator** *name*] [**outgoing**] [**target** *name*] [**detail**]

Syntax Description

detail	Displays detailed iSCSI session information.
incoming	Displays incoming iSCSI sessions.
initiator *name*	Displays specific iSCSI initiator session information. Maximum length is 80 characters.
outgoing	Displays outgoing iSCSI sessions
target *name*	Displays specific iSCSI target session information. Maximum length is 80 characters.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

All the parameters are optional in the **show iscsi session** commands. If no parameter is provided the command lists all the active iSCSI initiator or target sessions. If the IP address or iSCSI node name is provided, then the command lists details of all sessions from that initiator or to that target.

Examples

The following command displays the iSCSI session information.

```
switch# show iscsi session
Initiator iqn.1987-05.com.cisco.01.15cee6e7925087abc82ed96377653c8
  Session #1
    Target iqn.com.domainname.172.22.93.143.08-03.gw.22000020374b5247
    VSAN 1, ISID 000000000000, Status active, no reservation

  Session #2
    Target iqn.com.domainname.172.22.93.143.08-03.gw.220000203738e77d
    VSAN 1, ISID 000000000000, Status active, no reservation

Initiator iqn.1987-05.com.cisco:02.91b0ee2e8aa1.iscsi16-w2k
  Session #1
    Discovery session, ISID 00023d00022f, Status active

  Session #2
    Target iqn.com.domainname.172.22.93.143.08-03.gw.2200002037388bc2
    VSAN 1, ISID 00023d000230, Status active, no reservation
...
```

The following command displays the specified iSCSI target.

```
switch# show iscsi session target
iqn.com.domainname.172.22.93.143.08-03.gw.220000203738e77d
Initiator iqn.1987-05.com.cisco.01.15cee6e7925087abc82ed96377653c8
  Session #1
    Target iqn.com.domainname.172.22.93.143.08-03.gw.220000203738e77d
    VSAN 1, ISID 000000000000, Status active, no reservation
```

Note On the IPS module, you can verify what iSCSI initiator IQN has been assigned which pWWN when it logs in by using the **show zone active vsan** *vsan-id* command.

```
switch# zone name iscsi_16_A vsan 16
* fcid 0x7700d4 [pwwn 21:00:00:20:37:c5:2d:6d]
* fcid 0x7700d5 [pwwn 21:00:00:20:37:c5:2e:2e]
* fcid 0x770100 [symbolic-nodename
iqn.1987-05.com.cisco.02.BC3FEEFC431B199F81F33E97E2809C14.NUYEAR]
```

The following command displays the specified iSCSI initiator.

```
switch# show iscsi session initiator iqn.1987-05.com.cisco:02.91b0ee2e8aa1.iscsi16-w2k
Initiator iqn.1987-05.com.cisco:02.91b0ee2e8aa1.iscsi16-w2k
  Session #1
    Discovery session, ISID 00023d00022f, Status active

  Session #2
    Target iqn.com.domainname.172.22.93.143.08-03.gw.2200002037388bc2
    VSAN 1, ISID 00023d000230, Status active, no reservation

  Session #3
    Target iqn.com.domainname.172.22.93.143.08-03.gw.210000203739ad7f
    VSAN 1, ISID 00023d000235, Status active, no reservation

  Session #4
    Target iqn.com.domainname.172.22.93.143.08-03.gw.210000203739aa3a
    VSAN 1, ISID 00023d000236, Status active, no reservation

  Session #5
    Target iqn.com.domainname.172.22.93.143.08-03.gw.210000203739ada7
    VSAN 1, ISID 00023d000237, Status active, no reservation

  Session #6
    Target iqn.com.domainname.172.22.93.143.08-03.gw.2200002037381ccb
    VSAN 1, ISID 00023d000370, Status active, no reservation

  Session #7
    Target iqn.com.domainname.172.22.93.143.08-03.gw.2200002037388b54
    VSAN 1, ISID 00023d000371, Status active, no reservation

  Session #8
    Target iqn.com.domainname.172.22.93.143.08-03.gw.220000203738a194
    VSAN 1, ISID 00023d000372, Status active, no reservation

  Session #9
    Target iqn.com.domainname.172.22.93.143.08-03.gw.2200002037360053
    VSAN 1, ISID 00023d000373, Status active, no reservation
```

show iscsi stats

To display the iSCSI statistics information, use the **show iscsi stats** command.

show iscsi stats [**iscsi** *slot*/*port*] [**clear** | **detail**]

Syntax Description

iscsi *slot*/*port*	Displays statistics for the specified iSCSI interface.
clear	Clears iSCSI statistics for the session or interface.
detail	Displays detailed iSCSI statistics for the session or interface.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following command displays brief iSCSI statistics.

```
switch# show iscsi stats
iscsi8/1
    5 minutes input rate 23334800 bits/sec, 2916850 bytes/sec, 2841 frames/sec
    5 minutes output rate 45318424 bits/sec, 5664803 bytes/sec, 4170 frames/sec
    iSCSI statistics
      86382665 packets input, 2689441036 bytes
        3916933 Command pdus, 82463404 Data-out pdus, 2837976576 Data-out bytes,
 0 fragments
      131109319 packets output, 2091677936 bytes
        3916876 Response pdus (with sense 0), 1289224 R2T pdus
        125900891 Data-in pdus, 93381152 Data-in bytes

iscsi8/2
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    iSCSI statistics
      0 packets input, 0 bytes
        0 Command pdus, 0 Data-out pdus, 0 Data-out bytes, 0 fragments
      0 packets output, 0 bytes
        0 Response pdus (with sense 0), 0 R2T pdus
        0 Data-in pdus, 0 Data-in bytes
```

```
iscsi8/3
    5 minutes input rate 272 bits/sec, 34 bytes/sec, 0 frames/sec
    5 minutes output rate 40 bits/sec, 5 bytes/sec, 0 frames/sec
    iSCSI statistics
      30 packets input, 10228 bytes
        0 Command pdus, 0 Data-out pdus, 0 Data-out bytes, 0 fragments
      30 packets output, 1744 bytes
        0 Response pdus (with sense 0), 0 R2T pdus
        0 Data-in pdus, 0 Data-in bytes

iscsi8/4
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    iSCSI statistics
      0 packets input, 0 bytes
        0 Command pdus, 0 Data-out pdus, 0 Data-out bytes, 0 fragments
      0 packets output, 0 bytes
        0 Response pdus (with sense 0), 0 R2T pdus
        0 Data-in pdus, 0 Data-in bytes

iscsi8/5
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    iSCSI statistics
      0 packets input, 0 bytes
        0 Command pdus, 0 Data-out pdus, 0 Data-out bytes, 0 fragments
      0 packets output, 0 bytes
        0 Response pdus (with sense 0), 0 R2T pdus
        0 Data-in pdus, 0 Data-in bytes

iscsi8/6
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    iSCSI statistics
      0 packets input, 0 bytes
        0 Command pdus, 0 Data-out pdus, 0 Data-out bytes, 0 fragments
      0 packets output, 0 bytes
        0 Response pdus (with sense 0), 0 R2T pdus
        0 Data-in pdus, 0 Data-in bytes

iscsi8/7
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    iSCSI statistics
      0 packets input, 0 bytes
        0 Command pdus, 0 Data-out pdus, 0 Data-out bytes, 0 fragments
      0 packets output, 0 bytes
        0 Response pdus (with sense 0), 0 R2T pdus
        0 Data-in pdus, 0 Data-in bytes

iscsi8/8
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    iSCSI statistics
      0 packets input, 0 bytes
        0 Command pdus, 0 Data-out pdus, 0 Data-out bytes, 0 fragments
      0 packets output, 0 bytes
        0 Response pdus (with sense 0), 0 R2T pdus
        0 Data-in pdus, 0 Data-in bytes
```

The following command displays detailed iSCSI statistics.

```
switch# show iscsi stats detail
iscsi8/1
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    iSCSI statistics
      0 packets input, 0 bytes
        0 Command pdus, 0 Data-out pdus, 0 Data-out bytes, 0 fragments
      0 packets output, 0 bytes
        0 Response pdus (with sense 0), 0 R2T pdus
        0 Data-in pdus, 0 Data-in bytes
  iSCSI Forward:
    Command: 0 PDUs (Received: 0)
    Data-Out (Write): 0 PDUs (Received 0), 0 fragments, 0 bytes
  FCP Forward:
    Xfer_rdy: 0 (Received: 0)
    Data-In: 0 (Received: 0), 0 bytes
    Response: 0 (Received: 0), with sense 0
    TMF Resp: 0

  iSCSI Stats:
    Login: attempt: 0, succeed: 0, fail: 0, authen fail: 0
    Rcvd: NOP-Out: 0, Sent: NOP-In: 0
          NOP-In: 0, Sent: NOP-Out: 0
          TMF-REQ: 0, Sent: TMF-RESP: 0
          Text-REQ: 0, Sent: Text-RESP: 0
          SNACK: 0
          Unrecognized Opcode: 0, Bad header digest: 0
          Command in window but not next: 0, exceed wait queue limit: 0
          Received PDU in wrong phase: 0
  FCP Stats:
    Total: Sent: 0
           Received: 0 (Error: 0, Unknown: 0)
    Sent: PLOGI: 0, Rcvd: PLOGI_ACC: 0, PLOGI_RJT: 0
          PRLI: 0, Rcvd: PRLI_ACC: 0, PRLI_RJT: 0, Error resp: 0
          LOGO: 0, Rcvd: LOGO_ACC: 0, LOGO_RJT: 0
          ABTS: 0, Rcvd: ABTS_ACC: 0
          TMF REQ: 0
          Self orig command: 0, Rcvd: data: 0, resp: 0
    Rcvd: PLOGI: 0, Sent: PLOGI_ACC: 0
          LOGO: 0, Sent: LOGO_ACC: 0
          PRLI: 0, Sent: PRLI_ACC: 0
          ABTS: 0

  iSCSI Drop:
    Command: Target down 0, Task in progress 0, LUN map fail 0
             CmdSeqNo not in window 0, No Exchange ID 0, Reject 0
             Persistent Resv 0    Data-Out: 0, TMF-Req: 0
  FCP Drop:
    Xfer_rdy: 0, Data-In: 0, Response: 0

  Buffer Stats:
    Buffer less than header size: 0, Partial: 0, Split: 0
    Pullup give new buf: 0, Out of contiguous buf: 0, Unaligned m_data: 0
```

```
iscsi8/2
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    iSCSI statistics
      0 packets input, 0 bytes
        0 Command pdus, 0 Data-out pdus, 0 Data-out bytes, 0 fragments
      0 packets output, 0 bytes
        0 Response pdus (with sense 0), 0 R2T pdus
        0 Data-in pdus, 0 Data-in bytes
  iSCSI Forward:
    Command: 0 PDUs (Received: 0)
    Data-Out (Write): 0 PDUs (Received 0), 0 fragments, 0 bytes
  FCP Forward:
    Xfer_rdy: 0 (Received: 0)
    Data-In: 0 (Received: 0), 0 bytes
    Response: 0 (Received: 0), with sense 0
...
```

The following command displays detailed statistics for the specified iSCSI interface.

```
switch# show iscsi stats iscsi 8/1
iscsi8/1
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    iSCSI statistics
      0 packets input, 0 bytes
        0 Command pdus, 0 Data-out pdus, 0 Data-out bytes, 0 fragments
      0 packets output, 0 bytes
        0 Response pdus (with sense 0), 0 R2T pdus
        0 Data-in pdus, 0 Data-in bytes
```

show iscsi virtual-target

To display all the iSCSI nodes that are local to the switch, use the **show iscsi virtual-target** command.

show iscsi virtual-target [**configured**] [*name*]

Syntax Description

configured	Show the information for all iSCSI ports.
name	Show iSCSI information for the specified virtual-target.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

If no parameter is provided the command lists all the active iSCSI virtual targets. If the iSCSI node name is provided then the command lists the details of that iSCSI virtual target.

Examples

The following example displays information on all the iSCSI virtual targets.

```
switch# show iscsi virtual-target
target: abc1
    Port WWN 21:00:00:20:37:a6:b0:bf
    Configured node
target: iqn.com.domainname.172.22.93.143.08-03.gw.22000020374b5247
    Port WWN 22:00:00:20:37:4b:52:47 , VSAN 1
    Auto-created node
...
target: iqn.com.domainname.172.22.93.143.08-03.gw.210000203739aa39
    Port WWN 21:00:00:20:37:39:aa:39 , VSAN 1
    Auto-created node
```

The following example displays a specified iSCSI virtual target.

```
switch# show iscsi virtual-target
iqn.com.domainname.172.22.93.143.08-03.gw.210000203739a95b
target: iqn.com.domainname.172.22.93.143.08-03.gw.210000203739a95b
    Port WWN 21:00:00:20:37:39:a9:5b , VSAN 1
    Auto-created node
```

The following example displays the trespass status for a virtual target.

```
switch# show iscsi virtual-target iqn.abc
target: abc
    Port WWN 00:00:00:00:00:00:00:00
    Configured node
    all initiator permit is disabled
    trespass support is  enabled S
```

show islb cfs-session status

To display iSCSI server load balancing (iSLB) Cisco Fabric Services information, use the **show islb** command.

show islb cfs-session status

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays iSLB session information.

```
ips-hac2# show islb cfs-session status
last action               : fabric distribute disable
last action result        : success
last action failure cause : success
```

Related Commands

Command	Description
show islb initiator	Displays iSLB initiator information.
show islb merge status	Displays iSLB merge status information.
show islb pending	Displays iSLB pending configurations.
show islb pending-diff	Displays iSLB pending configuration differences.
show islb session	Displays iSLB session information.
show islb status	Displays iSLB CFS status information.
show islb virtual-target	Displays iSLB virtual target information.
show islb vrrp	Display iSLB VRRP load balancing information.

show islb initiator

To display iSCSI server load balancing (iSLB) Cisco Fabric Services information, use the **show islb initiator** command.

show islb initiator [name *node-name* **[detail | fcp-session [detail] | iscsi-session [detail]] | configured [name** *initiator-name***] | detail | fcp-session [detail] | iscsi-session [detail] | summary [name]]**

Syntax Description

name *node-name*	Displays the initiator node name. The maximum size is 80.
detail	Displays more detailed information.
fcp-session	Displays Fbire Channel session details.
iscsi-session	Displays iSLB session details.
configured	Displays iSLB initiator configured information.
name *initiator-name*	Displays the configured initiator name. The maximum size is 223.
summary	Displays iSLB initiator summary information.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows iSLB initiator configuration information.

```
switch# show islb initiator configured
iSCSI Node name is 1.1.1.1

    No. of PWWN: 2
      Port WWN is 23:01:00:0c:85:90:3e:82
      Port WWN is 23:02:00:0c:85:90:3e:82
    Load Balance Metric: 1000
    Number of Initiator Targets: 0

iSCSI Node name is 2.2.2.2

    Load Balance Metric: 1000
    Number of Initiator Targets: 0
```

Related Commands

Command	Description
show islb cfs-session status	Displays iSLB session status and status information.
show islb merge status	Displays iSLB merge status information.
show islb pending	Displays iSLB pending configurations.
show islb pending-diff	Displays iSLB pending configuration differences.
show islb session	Displays iSLB session information.
show islb status	Displays iSLB CFS status information.
show islb virtual-target	Displays iSLB virtual target information.
show islb vrrp	Display iSLB VRRP load balancing information.

show islb merge status

To display iSCSI server load balancing (iSLB) merge status information, use the **show islb merge status** command.

show islb merge status

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows iSLB merge status information.

```
switch# show islb merge status
Merge Status: SUCCESS
```

Related Commands

Command	Description
show islb cfs-session status	Displays iSLB session information.
show islb initiator	Displays iSLB initiator information.
show islb pending	Displays iSLB pending configurations.
show islb pending-diff	Displays iSLB pending configuration differences.
show islb session	Displays iSLB session information.
show islb status	Displays iSLB CFS status information.
show islb virtual-target	Displays iSLB virtual target information.
show islb vrrp	Display iSLB VRRP load balancing information.

show islb pending

To display iSCSI server load balancing (iSLB) pending configurations, use the **show islb pending** command.

show islb pending

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows iSLB pending configuration information.

```
switch# show islb pending
iscsi initiator idle-timeout 10
islb initiator ip-address 10.1.1.1
static pWWN 23:01:00:0c:85:90:3e:82
static pWWN 23:06:00:0c:85:90:3e:82
username test1
islb initiator ip-address 10.1.1.2
static nWWN 23:02:00:0c:85:90:3e:82
```

Related Commands

Command	Description
show islb initiator	Displays iSLB initiator information.
show islb cfs-session status	Displays iSLB session information.
show islb merge status	Displays iSLB merge status information.
show islb pending-diff	Displays iSLB pending configuration differences.
show islb session	Displays iSLB session information.
show islb status	Displays iSLB CFS status information.
show islb virtual-target	Displays iSLB virtual target information.
show islb vrrp	Display iSLB VRRP load balancing information.

show islb pending-diff

To display iSCSI server load balancing (iSLB) pending configuration differences, use the **show islb pending-diff** command.

show islb pending-diff

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows iSLB pending configuration differences.

```
switch# show islb pending-diff
+iscsi initiator idle-timeout 10
islb initiator ip-address 10.1.1.1
+ static pWWN 23:06:00:0c:85:90:3e:82
+islb initiator ip-address 10.1.1.2
+ static nWWN 23:02:00:0c:85:90:3e:82
```

Related Commands

Command	Description
show islb cfs-session status	Displays iSLB session information.
show islb initiator	Displays iSLB initiator information.
show islb merge status	Displays iSLB merge status information.
show islb pending	Displays iSLB pending configurations.
show islb session	Displays iSLB session information.
show islb status	Displays iSLB CFS status information.
show islb virtual-target	Displays iSLB virtual target information.
show islb vrrp	Display iSLB VRRP load balancing information.

show islb session

To display iSLB session information, use the **show islb session** command.

show islb session [detail | incoming | initiator *initiator-node-name* **| iscsi** *slot-number* **| outgoing | target** *target-node-name*]

Syntax Description

detail	Displays detailed iSLB session information.
incoming	Displays incoming iSLB sessions.
initiator *initiator-node-name*	Displays session information for a specific iSLB initiator. The maximum size for the initiator node name is 80.
iscsi *slot-port*	Specifies the iSCSI interface.
outgoing	Displays outgoing iSLB sessions.
target	Displays session information for a specific iSLB target. The maximum size for the target node name is 80.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows iSLB session information.

```
switch# show islb session
Initiator iqn.1987-05.com.cisco.01.15cee6e7925087abc82ed96377653c8
  Session #1
      Target iqn.com.domainname.172.22.93.143.08-03.gw.22000020374b5247
      VSAN 1, ISID 000000000000, Status active, no reservation

  Session #2
      Target iqn.com.domainname.172.22.93.143.08-03.gw.220000203738e77d
      VSAN 1, ISID 000000000000, Status active, no reservation

Initiator iqn.1987-05.com.cisco:02.91b0ee2e8aa1.iscsi16-w2k
  Session #1
     Discovery session, ISID 00023d00022f, Status active

  Session #2
      Target iqn.com.domainname.172.22.93.143.08-03.gw.2200002037388bc2
     VSAN 1, ISID 00023d000230, Status active, no reservation
```

Related Commands

Command	Description
show islb cfs-session status	Displays iSLB session information.
show islb initiator	Displays iSLB initiator information.
show islb merge status	Displays iSLB merge status information.
show islb pending	Displays iSLB pending configurations.
show islb pending-diff	Displays iSLB CFS pending configuration differences.
show islb status	Displys iSLB CFS status information.
show islb virtual-target	Displays iSLB virtual target information.
show islb vrrp	Display iSLB VRRP load balancing information.

show islb status

To display iSCSI server load balancing (iSLB) Cisco Fabric Services status, use the **show islb status** command.

show islb status

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows iSLB CFS status.

```
switch# show islb status
iSLB Distribute is enabled
iSLB CFS Session does not exist
```

Related Commands

Command	Description
show islb cfs-session status	Displays iSLB session information.
show islb initiator	Displays iSLB initiator information.
show islb merge status	Displays iSLB merge status information.
show islb pending	Displays iSLB pending configurations.
show islb pending-diff	Displays iSLB CFS pending configuration differences.
show islb session	Displays iSLB session information.
show islb virtual-target	Displays iSLB virtual target information.
show islb vrrp	Display iSLB VRRP load balancing information.

show islb virtual-target

To display information about iSLB virtual targets, use the **show islb virtual-target** command.

show islb virtual-target [*name* | **configured** *name*]

Syntax Description

name	Specifies the iSLB virtual target name. The minimum length is 16 bytes and the maximum length is 223 bytes.
configured	Displays information about configured iSLB virtual targets.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows an iSLB target.

```
switch# show islb virtual-target newtarget0987654321
target: newtarget0987654321

    Configured node (iSLB)
    No. of initiators permitted: 1
      initiator fromtarget1234567890 is permitted
    All initiator permit is enabled
    Trespass support is  disabled
    Revert to primary support is  disabled
```

The following example shows all configured iSLB virtual targets.

```
switch# show islb virtual-target configured
target: testtarget1234567

    Configured node (iSLB)
    No. of initiators permitted: 1
      initiator trespass is permitted
    All initiator permit is disabled
    Trespass support is  disabled
    Revert to primary support is  disabled

target: testertarget987654321
    Port WWN 10:20:30:40:50:60:70:80
    Configured node (iSLB)
    No. of initiators permitted: 1
      initiator mytargetdevice is permitted
```

```
    All initiator permit is disabled
    Trespass support is  disabled
    Revert to primary support is  disabled

target: newtarget0987654321

    Configured node (iSLB)
    No. of initiators permitted: 1
      initiator fromtarget1234567890 is permitted
    All initiator permit is enabled
    Trespass support is  disabled
    Revert to primary support is  disabled

target: mytargetdevice123

    Configured node (iSLB)
    All initiator permit is disabled
    Trespass support is  enabled
    Revert to primary support is  disabled
```

Related Commands

Command	Description
show islb cfs-session status	Displays iSLB session information.
show islb initiator	Displays iSLB initiator information.
show islb merge status	Displays iSLB merge status information.
show islb pending	Displays iSLB pending configurations.
show islb pending-diff	Displays iSLB CFS pending configuration differences.
show islb session	Displays iSLB session information.
show islb status	Displays iSLB CFS status information.
show islb vrrp	Display iSLB VRRP load balancing information.

show islb vrrp

To display iSLB VRRP load balancing information, use the **show islb vrrp** command.

show islb vrrp [assignment [initiator *node-name* [**vr** *group-number*] **| vr** *group-number*] **|**
interface [switch *WWN* [**vr** *group-number*] **| vr** *group-number*] **| summary** [**vr** *group-number*]
| vr *group-number*]

Syntax Description

assignment	Displays iSLB VRRP initiator to interface assignment.
initiator *node-name*	Displays a specific iSLB initiator's interface assignment. The maximum size of the initiator node name is 80.
vr *group-number*	Displays information for a specific VR group. The range is 1 to 255.
interface	Displays iSLB VRRP interface information.
switch *WWN*	Displays a interface information for a specific switch. The format of the WWN is *hh:hh:hh:hh:hh:hh:hh:hh*.
summary	Displays iSLB VRRP load balancing summary information.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows iSLB VRRP interface information.

```
switch# show islb vrrp interface vr 41
-- Interfaces For Load Balance --

    Interface GigabitEthernet1/1.441
        Switch wwn: 20:00:00:0d:ec:02:cb:00
        VRRP group id: 41, VRRP IP address: 10.10.122.112
            Interface VRRP state: backup
            Interface load: 3000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 10.10.122.115
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None
```

```
    Interface GigabitEthernet1/2.441
        Switch wwn: 20:00:00:0d:ec:02:cb:00
        VRRP group id: 41, VRRP IP address: 10.10.122.112
            Interface VRRP state: backup
            Interface load: 2000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 10.10.122.114
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None

    Interface GigabitEthernet2/1.441
        Switch wwn: 20:00:00:0d:ec:0c:6b:c0
        VRRP group id: 41, VRRP IP address: 10.10.122.112
            Interface VRRP state: backup
            Interface load: 2000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 10.10.122.111
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None

    Interface GigabitEthernet2/2.441
        Switch wwn: 20:00:00:0d:ec:0c:6b:c0
        VRRP group id: 41, VRRP IP address: 10.10.122.112
            Interface VRRP state: master
            Interface load: 1000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 10.10.122.112
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None

    Interface GigabitEthernet2/3.441
        Switch wwn: 20:00:00:0d:ec:0c:6b:c0
        VRRP group id: 41, VRRP IP address: 10.10.122.112
            Interface VRRP state: backup
            Interface load: 2000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 10.10.122.113
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None
```

The following example shows iSLB VRRP summary information.

```
switch# show islb vrrp summary

                        -- Groups For Load Balance --
-------------------------------------------------------------------------------
               VR Id             VRRP Address Type             Configured Status
-------------------------------------------------------------------------------
```

```
                  41                          IPv4                        Enabled
                  42                          IPv4                        Enabled

                       -- Interfaces For Load Balance --
--------------------------------------------------------------------------------
 VR Id         VRRP IP              Switch WWN                 Ifindex      Load
--------------------------------------------------------------------------------
    41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/1.441      3000
    41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/2.441      2000
    41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/1.441      2000
M   41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/2.441      1000
    41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/3.441      2000
M   42   10.10.142.111 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/1.442      2000
    42   10.10.142.111 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/2.442      1000
    42   10.10.142.111 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/3.442      2000

                     -- Initiator To Interface Assignment --
--------------------------------------------------------------------------------
Initiator  VR Id         VRRP IP              Switch WWN                 Ifindex
--------------------------------------------------------------------------------
iqn.1987-05.com.cisco:01.09ea2e99c97
               41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/1.441
iqn.1987-05.com.cisco:01.5ef81885f8d
               41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/3.441
iqn.1987-05.com.cisco:01.8fbdb3fdf8
               41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/1.441
iqn.1987-05.com.cisco:01.99eddd9b134
               41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/1.441
iqn.1987-05.com.cisco:01.a1398a8c6bc6
               41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/3.441
iqn.1987-05.com.cisco:01.e15c63d09d18
               41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/2.441
iqn.1987-05.com.cisco:01.e9aab57a51e0
               41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/1.441
iqn.1987-05.com.cisco:01.ecc2b77b6086
               41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/2.441
iqn.1987-05.com.cisco:01.f047da798a44
               41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/2.441
iqn.1987-05.com.cisco:01.f686f5cd11f
               41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/1.441
```

The following example shows iSLB VRRP summary information for vr 41.

```
switch# show islb vrrp summary vr 41

                       -- Groups For Load Balance --
--------------------------------------------------------------------------------
               VR Id             VRRP Address Type             Configured Status
--------------------------------------------------------------------------------
                  41                          IPv4                        Enabled

                       -- Interfaces For Load Balance --
--------------------------------------------------------------------------------
 VR Id         VRRP IP              Switch WWN                 Ifindex      Load
--------------------------------------------------------------------------------
    41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/1.441      3000
    41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/2.441      2000
    41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/1.441      2000
M   41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/2.441      1000
    41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/3.441      2000

                     -- Initiator To Interface Assignment --
--------------------------------------------------------------------------------
Initiator  VR Id         VRRP IP              Switch WWN                 Ifindex
```

```
--------------------------------------------------------------------------------
iqn.1987-05.com.cisco:01.09ea2e99c97
              41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/1.441
iqn.1987-05.com.cisco:01.5ef81885f8d
              41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/3.441
iqn.1987-05.com.cisco:01.8fbdb3fdf8
              41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/1.441
iqn.1987-05.com.cisco:01.99eddd9b134
              41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/1.441
iqn.1987-05.com.cisco:01.a1398a8c6bc6
              41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/3.441
iqn.1987-05.com.cisco:01.e15c63d09d18
              41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/2.441
iqn.1987-05.com.cisco:01.e9aab57a51e0
              41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/1.441
iqn.1987-05.com.cisco:01.ecc2b77b6086
              41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/2.441
iqn.1987-05.com.cisco:01.f047da798a44
              41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/2.441
iqn.1987-05.com.cisco:01.f686f5cd11f
              41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/1.441
```

The following example shows complete iSLB VRRP load balancing information.

```
switch# show islb vrrp
-- Groups For Load Balance --

    VRRP group id 41
        Address type: IPv4
        Configured status: Enabled

    VRRP group id 42
        Address type: IPv4
        Configured status: Enabled

-- Interfaces For Load Balance --

    Interface GigabitEthernet1/1.441
        Switch wwn: 20:00:00:0d:ec:02:cb:00
        VRRP group id: 41, VRRP IP address: 10.10.122.112
            Interface VRRP state: backup
            Interface load: 3000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 10.10.122.115
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None

    Interface GigabitEthernet1/2.441
        Switch wwn: 20:00:00:0d:ec:02:cb:00
        VRRP group id: 41, VRRP IP address: 10.10.122.112
            Interface VRRP state: backup
            Interface load: 2000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 10.10.122.114
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None
```

```
Interface GigabitEthernet2/1.441
    Switch wwn: 20:00:00:0d:ec:0c:6b:c0
    VRRP group id: 41, VRRP IP address: 10.10.122.112
        Interface VRRP state: backup
        Interface load: 2000
        Interface redirection: enabled
        Group redirection: enabled
    Number of physical IP address: 1
        (1) 10.10.122.111
    Port vsan: 1
    Forwarding mode: store-and-forward
    Proxy initiator mode: disabled
    iSCSI authentication: CHAP or None

Interface GigabitEthernet2/2.441
    Switch wwn: 20:00:00:0d:ec:0c:6b:c0
    VRRP group id: 41, VRRP IP address: 10.10.122.112
        Interface VRRP state: master
        Interface load: 1000
        Interface redirection: enabled
        Group redirection: enabled
    Number of physical IP address: 1
        (1) 10.10.122.112
    Port vsan: 1
    Forwarding mode: store-and-forward
    Proxy initiator mode: disabled
    iSCSI authentication: CHAP or None

Interface GigabitEthernet2/3.441
    Switch wwn: 20:00:00:0d:ec:0c:6b:c0
    VRRP group id: 41, VRRP IP address: 10.10.122.112
        Interface VRRP state: backup
        Interface load: 2000
        Interface redirection: enabled
        Group redirection: enabled
    Number of physical IP address: 1
        (1) 10.10.122.113
    Port vsan: 1
    Forwarding mode: store-and-forward
    Proxy initiator mode: disabled
    iSCSI authentication: CHAP or None

Interface GigabitEthernet2/1.442
    Switch wwn: 20:00:00:0d:ec:0c:6b:c0
    VRRP group id: 42, VRRP IP address: 10.10.142.111
        Interface VRRP state: master
        Interface load: 2000
        Interface redirection: enabled
        Group redirection: enabled
    Number of physical IP address: 1
        (1) 10.10.142.111
    Port vsan: 1
    Forwarding mode: store-and-forward
    Proxy initiator mode: disabled
    iSCSI authentication: CHAP or None

Interface GigabitEthernet2/2.442
    Switch wwn: 20:00:00:0d:ec:0c:6b:c0
    VRRP group id: 42, VRRP IP address: 10.10.142.111
        Interface VRRP state: backup
        Interface load: 1000
        Interface redirection: enabled
        Group redirection: enabled
```

```
        Number of physical IP address: 1
            (1) 10.10.142.112
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None

    Interface GigabitEthernet2/3.442
        Switch wwn: 20:00:00:0d:ec:0c:6b:c0
        VRRP group id: 42, VRRP IP address: 10.10.142.111
            Interface VRRP state: backup
            Interface load: 2000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 10.10.142.113
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None

-- Initiator To Interface Assignment --

    Initiator iqn.1987-05.com.cisco:01.09ea2e99c97
        VRRP group id: 41, VRRP IP address: 10.10.122.112
        Assigned to switch wwn: 20:00:00:0d:ec:0c:6b:c0
            ifindex: GigabitEthernet2/1.441
        Waiting for the redirected session request: False
        Initiator weighted load: 1000

    Initiator iqn.1987-05.com.cisco:01.5ef81885f8d
        VRRP group id: 41, VRRP IP address: 10.10.122.112
        Assigned to switch wwn: 20:00:00:0d:ec:0c:6b:c0
            ifindex: GigabitEthernet2/3.441
        Waiting for the redirected session request: False
        Initiator weighted load: 1000

    Initiator iqn.1987-05.com.cisco:01.8fbdb3fdf8
        VRRP group id: 41, VRRP IP address: 10.10.122.112
        Assigned to switch wwn: 20:00:00:0d:ec:02:cb:00
            ifindex: GigabitEthernet1/1.441
        Waiting for the redirected session request: False
        Initiator weighted load: 1000

    Initiator iqn.1987-05.com.cisco:01.99eddd9b134
        VRRP group id: 41, VRRP IP address: 10.10.122.112
        Assigned to switch wwn: 20:00:00:0d:ec:02:cb:00
            ifindex: GigabitEthernet1/1.441
        Waiting for the redirected session request: False
        Initiator weighted load: 1000

    Initiator iqn.1987-05.com.cisco:01.a1398a8c6bc6
        VRRP group id: 41, VRRP IP address: 10.10.122.112
        Assigned to switch wwn: 20:00:00:0d:ec:0c:6b:c0
            ifindex: GigabitEthernet2/3.441
        Waiting for the redirected session request: False
        Initiator weighted load: 1000

    Initiator iqn.1987-05.com.cisco:01.e15c63d09d18
        VRRP group id: 41, VRRP IP address: 10.10.122.112
        Assigned to switch wwn: 20:00:00:0d:ec:02:cb:00
            ifindex: GigabitEthernet1/2.441
        Waiting for the redirected session request: False
        Initiator weighted load: 1000
```

```
Initiator iqn.1987-05.com.cisco:01.e9aab57a51e0
    VRRP group id: 41, VRRP IP address: 10.10.122.112
    Assigned to switch wwn: 20:00:00:0d:ec:02:cb:00
        ifindex: GigabitEthernet1/1.441
    Waiting for the redirected session request: False
    Initiator weighted load: 1000

Initiator iqn.1987-05.com.cisco:01.ecc2b77b6086
    VRRP group id: 41, VRRP IP address: 10.10.122.112
    Assigned to switch wwn: 20:00:00:0d:ec:0c:6b:c0
        ifindex: GigabitEthernet2/2.441
    Waiting for the redirected session request: False
    Initiator weighted load: 1000

Initiator iqn.1987-05.com.cisco:01.f047da798a44
    VRRP group id: 41, VRRP IP address: 10.10.122.112
    Assigned to switch wwn: 20:00:00:0d:ec:02:cb:00
        ifindex: GigabitEthernet1/2.441
    Waiting for the redirected session request: False
    Initiator weighted load: 1000

Initiator iqn.1987-05.com.cisco:01.f686f5cd11f
    VRRP group id: 41, VRRP IP address: 10.10.122.112
    Assigned to switch wwn: 20:00:00:0d:ec:0c:6b:c0
        ifindex: GigabitEthernet2/1.441
    Waiting for the redirected session request: False
    Initiator weighted load: 1000
```

Related Commands

Command	Description
show islb cfs-session status	Displays iSLB session information.
show islb initiator	Displays iSLB initiator information.
show islb merge status	Displays iSLB merge status information.
show islb pending	Displays iSLB pending configurations.
show islb pending-diff	Displays iSLB CFS pending configuration differences.
show islb session	Displays iSLB session information.
show islb status	Displays iSLB CFS status information.
show islb virtual-target	Displays iSLB virtual target information.

show isns

To display Internet Storage Name Service (iSNS) information, use the **show isns** command.

show isns {**config** |
database [**full** | **virtual-targets** [**local** | **switch** *switch-wwn*]] |
entity [**all** [**detail**] | **id** *entity-id*] |
iscsi global config [**all** | **switch** *switch-wwn*]] |
node [**all** [**detail**] | **configured** | **detail** | **name** *node-name* | **virtual** [**switch** *switch-wwn* [**detail**]]] |
portal [**all** [**detail**] | **detail** | **ipaddress** *ip-address* **port** *tcp-port* | **virtual** [**switch** *switch-wwn* [**detail**]]] |
profile [*profile-name* [**counters**] | **counters**] |
query *profile-name* {**gigabitethernet** *slot*/*port* | **port-channel** *port*} |
stats}

Syntax Description

config	Displays iSNS server configuration.
database	Displays the iSNS database contents.
full	Specifies all virtual targets or registered nodes in database.
virtual-targets	Specifies just virtual targets.
local	Specifies only local virtual targets.
switch *switch-wwn*	Specifies a specific switch WWN. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
entity	Displays entity attributes.
all	Specifies all information.
detail	Specifies detailed information.
id *entity-id*	Specifies an entity ID. Maximum length is 255.
iscsi global config	Displays iSCSI global configuration for import of Fibre Channel targets.
node	Displays node attributes.
configured	Specifies configured nodes with detailed information.
name *node-name*	Specifies the node name. Maximum length is 255.
virtual	Specifies virtual targets.
portal	Displays portal attributes.
ipaddress *ip-address*	Specifies the IP address for the portal.
port *tcp-port*	Specifies the TCP port for the portal. The range is 1 to 66535.
profile	Displays iSNS profile information.
profile-name	Specifies a profile name. Maximum length is 64 characters.
counters	Specifies statistics for the interfaces.
query *profile-name*	Specifies a query to send to the iSNS server.
gigabitethernet *slot*/*port*	Specifies a Gigabit Ethernet interface.
port-channel *port*	Specifies a PortChannel interface. The range is 1 to 128.
stats	Displays iSNS server statistics.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.0(1b)	Added **config**, **database**, **entity**, **iscsi**, **node**, **portal**, and **stats** options.

Usage Guidelines

To access all but the **profile** and **query** options for this command, you must perform the **isns-server enable** command.

Examples

The following example shows how to display the iSNS configuration.

```
switch# show isns config
Server Name: ips-hac1(Cisco Systems) Up since: Mon Apr 27 06:59:49 1981

    Index: 1    Version: 1     TCP Port: 3205
    fabric distribute (remote sync): ON
    ESI
       Non Response Threshold: 5 Interval(seconds): 60
   Database contents
       Number of Entities: 1
       Number of Portals: 0
       Number of ISCSI devices: 2
       Number of Portal Groups: 0
```

The following example displays a specified iSNS profile.

```
switch# show isns profile ABC

iSNS profile name ABC
tagged interface GigabitEthernet2/3
iSNS Server 10.10.100.204
```

The following example displays all iSNS profiles

```
switch# show isns profile

iSNS profile name ABC
tagged interface GigabitEthernet2/3
iSNS Server 10.10.100.204

iSNS profile name NBV
tagged interface GigabitEthernet2/5
iSNS Server 10.10.100.201
```

The following example displays iSNS PDU statistics for a specified iSNS profile.

```
switch# show isns profile ABC counters

iSNS profile name ABC
tagged interface GigabitEthernet2/3
iSNS statistics
  Input 54 pdus (registration/deregistration pdus only)
    Reg pdus 37,  Dereg pdus 17
  Output 54 pdus (registration/deregistration pdus only)
    Reg pdus  37,  Dereg pdus 17
iSNS Server  10.10.100.204
```

The following example displays iSNS PDU statistics for all iSNS profiles.

```
switch# show isns profile counters

iSNS profile name ABC
tagged interface GigabitEthernet2/3
iSNS statistics
  Input 54 pdus (registration/deregistration pdus only)
    Reg pdus 37,  Dereg pdus 17
  Output 54 pdus (registration/deregistration pdus only)
    Reg pdus  37,  Dereg pdus 17
iSNS Server  10.10.100.204


iSNS profile name NBV
tagged interface GigabitEthernet2/5
iSNS statistics
  Input 54 pdus (registration/deregistration pdus only)
    Reg pdus 37,  Dereg pdus 17
  Output 54 pdus (registration/deregistration pdus only)
    Reg pdus  37,  Dereg pdus 17
iSNS Server  10.10.100.201
```

Related Commands

Command	Description
isns-server enable	Enables the iSNS server.

show ivr

To display various Inter-VSAN Routing (IVR) configurations, use the **show ivr** command.

show ivr [**pending** | **pending-diff** | **session status** | **virtual-domains** [**vsan** *vsan-id*] | **virtual-fcdomain-add-status** | **vsan-topology** [**active** | **configured**] | **zone** [**active** | **name** *name* [**active**]] | **zoneset** [**active** | **brief** | **fabric** | **name** *name* | **status**]]

Syntax Description

merge	Displays the IVR merge status.
pending	Displays the IVR pending configuration.
pending-diff	Displays the IVR pending configuration differences with the active configuration.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
session	Displays the IVR session status.
status	Displays the status of the configured IVR session.
virtual-domains	Displays IVR virtual domains for all local VSANs.
virtual-fcdomain-add-status	Displays IVR virtual fcdomain status.
vsan-topology	Displays the IVR VSAN topology
active	Displays the active IVR facilities.
configured	Displays the configured IVR facilities
zone	Displays the Inter-VSA Zone (IVZ) configurations.
name *name*	Specifies the name as configured in the database.
zoneset	Displays the Inter-VSA Zone Set (IVZS) configurations.
brief	Displays configured information in brief format.
fabric	Displays the status of active zone set in the fabric.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.0(1b)	Added the **pending** and **pending-diff** keywords.

Usage Guidelines

To access this command, you must perform the **ivr enable** command.

Examples

The following example displays the status of the IVR virtual domain configuration.

```
switch# show ivr virtual-fcdomain-add-status
IVR virtual domains are added to fcdomain list in VSANS: 1
(As well as to VSANs in interoperability mode 2 or 3)
```

The following example displays IVR-enabled switches for a specified VSAN

```
switch# show ivr enabled-switches vsan 2
AFID    VSAN    DOMAIN      CAPABILITY  SWITCH WWN
-----------------------------------------------------------------------
   1      2     0x62( 98)    00000001    20:00:00:05:30:01:1b:c2 *

Total:   1 ivr-enabled VSAN-Domain pair>
```

The following example displays the status of the IVR session.

```
switch# show ivr session status
Last Action                : None
Last Action Result         : None
Last Action Failure Reason : None
```

The following example displays the configured IVR VSAN topology

```
switch# show ivr vsan-topology
AFID  SWITCH WWN                 Active   Cfg. VSANS
-------------------------------------------------------------
   1  20:00:00:05:30:00:3c:5e     yes     yes  3,2000
   1  20:00:00:05:30:00:58:de     yes     yes  2,2000
   1  20:00:00:05:30:01:1b:c2 *   yes     yes  1-2
   1  20:02:00:44:22:00:4a:05     yes     yes  1-2,6
   1  20:02:00:44:22:00:4a:07     yes     yes  2-5

Total:   5 entries in active and configured IVR VSAN-Topology

Current Status: Inter-VSAN topology is ACTIVE
Last activation time: Sat Mar 22 21:46:15 1980
```

The following example displays the active IVR VSAN topology

```
switch# show ivr vsan-topology active
AFID  SWITCH WWN                 Active   Cfg. VSANS
-------------------------------------------------------------
   1  20:00:00:05:30:00:3c:5e     yes     yes  3,2000
   1  20:00:00:05:30:00:58:de     yes     yes  2,2000
   1  20:00:00:05:30:01:1b:c2 *   yes     yes  1-2
   1  20:02:00:44:22:00:4a:05     yes     yes  1-2,6
   1  20:02:00:44:22:00:4a:07     yes     yes  2-5

Total:   5 entries in active IVR VSAN-Topology

Current Status: Inter-VSAN topology is ACTIVE
Last activation time: Sat Mar 22 21:46:15
```

The following example displays the configured IVR VSAN topology

```
switch# show ivr vsan-topology configured
AFID  SWITCH WWN                 Active   Cfg. VSANS
--------------------------------------------------------------
   1  20:00:00:05:30:00:3c:5e     yes     yes  3,2000
   1  20:00:00:05:30:00:58:de     yes     yes  2,2000
   1  20:00:00:05:30:01:1b:c2 *   yes     yes  1-2
   1  20:02:00:44:22:00:4a:05     yes     yes  1-2,6
   1  20:02:00:44:22:00:4a:07     yes     yes  2-5

Total:   5 entries in configured IVR VSAN-Topology
```

The following example displays the combined user-defined and the automatically discovered IVR VSAN topology database.

```
switch(config)# show ivr vsan-topology

AFID  SWITCH WWN                 Active   Cfg. VSANS
--------------------------------------------------------------
   1  20:00:00:0d:ec:04:99:00     yes      no  1-4
   1  20:00:00:0d:ec:0e:9c:80 *   yes      no  2,6-7,9
   1  20:00:00:0d:ec:0e:b0:40     yes      no  1-3,5,8
   1  20:00:00:0d:ec:04:99:00      no     yes  1-4
   1  20:00:00:0d:ec:0e:9c:80 *    no     yes  2,6-7,9
   1  20:00:00:0d:ec:0e:b0:40      no     yes  1-3,5,8


Total:   6 entries in active and configured IVR VSAN-Topology
```

Table 22-5 describes the significant fields shown in the **show ivr vsan-topology** display.

Table 22-5 show ivr vsan-topology Field Descriptions

Field	Description
AFID	Autonomous fabric ID (AFID)
Switch WWN	Switch world wide number
Active	Automatically discovered
Cfg.	Manually configured
VSANS	VSANs configured

The following example displays the IVZ configuration

```
switch# show ivr zone
zone name Ivz_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2

zone name ivr_qa_z_all
    pwwn 21:00:00:e0:8b:06:d9:1d vsan 1
    pwwn 21:01:00:e0:8b:2e:80:93 vsan 4
    pwwn 10:00:00:00:c9:2d:5a:dd vsan 1
    pwwn 10:00:00:00:c9:2d:5a:de vsan 2
    pwwn 21:00:00:20:37:5b:ce:af vsan 6
    pwwn 21:00:00:20:37:39:6b:dd vsan 6
    pwwn 22:00:00:20:37:39:6b:dd vsan 3
    pwwn 22:00:00:20:37:5b:ce:af vsan 3
    pwwn 50:06:04:82:bc:01:c3:84 vsan 5
```

The following example displays the active IVZS configuration

```
switch# show ivr zoneset active
zoneset name IVR_ZoneSet1
  zone name Ivz_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

The following example displays information for a specified IVZ

```
switch# show ivr zone name Ivz_vsan2-3
zone name Ivz_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

The following example displays the specified zone in the active IVZS

```
switch# show ivr zone name Ivz_vsan2-3 active
zone name Ivz_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

The following example displays the IVZS configuration

```
switch# show ivr zoneset
zoneset name ivr_qa_zs_all
  zone name ivr_qa_z_all
    pwwn 21:00:00:e0:8b:06:d9:1d vsan 1
    pwwn 21:01:00:e0:8b:2e:80:93 vsan 4
    pwwn 10:00:00:00:c9:2d:5a:dd vsan 1
    pwwn 10:00:00:00:c9:2d:5a:de vsan 2
    pwwn 21:00:00:20:37:5b:ce:af vsan 6
    pwwn 21:00:00:20:37:39:6b:dd vsan 6
    pwwn 22:00:00:20:37:39:6b:dd vsan 3
    pwwn 22:00:00:20:37:5b:ce:af vsan 3
    pwwn 50:06:04:82:bc:01:c3:84 vsan 5

zoneset name IVR_ZoneSet1
  zone name Ivz_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

The following example displays brief information for an IVR VSAN topology

```
switch# show ivr vsan-topology configured
AFID  SWITCH WWN                 Active   Cfg. VSANS
-----------------------------------------------------------
   1  20:00:00:05:30:00:3c:5e     yes     yes  3,2000
   1  20:00:00:05:30:00:58:de     yes     yes  2,2000
   1  20:00:00:05:30:01:1b:c2 *   yes     yes  1-2
   1  20:02:00:44:22:00:4a:05     yes     yes  1-2,6
   1  20:02:00:44:22:00:4a:07     yes     yes  2-5

Total:   5 entries in configured IVR VSAN-Topology
```

The following example displays brief information for the active IVZS

```
switch# show ivr zoneset brief Active
zoneset name IVR_ZoneSet1
  zone name Ivz_vsan2-3
```

The following example displays the status information for the IVZ

```
switch# show ivr zoneset brief status
Zoneset Status
_____________
    name               : IVR_ZoneSet1
    state              : activation success
    last activate time : Sat Mar 22 21:38:46 1980
    force option       : off

status per vsan:
_________________
     vsan     status
     ____     ______
     2        active
```

The following example displays the specified zone set

```
switch# show ivr zoneset name IVR_ZoneSet1
zoneset name IVR_ZoneSet1
  zone name Ivz_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

Related Commands

Command	Description
ivr distribute	Enables IVR CFS distribution.
ivr enable	Enables IVR.

show ivr fcdomain database

To display the IVR fcdomain database that contains the persistent FC ID mapping, use the **show ivr fcdomain database** command.

show ivr fcdomain database [**autonomous-fabric-num** *afid-num* **vsan** *vsan-id*]

Syntax Description

autonomous-fabric-num *afid-num*	Specifies the AFID. The range is 1 to 64.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.1(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays all IVR fcdomain database entries.

```
switch# show ivr fcdomain database
-------------------------------------------------
  AFID  Vsan  Native-AFID  Native-Vsan  Virtual-domain
-------------------------------------------------
    1     2        10          11         0xc(12)
   21    22        20          11         0xc(12)

Number of Virtual-domain entries: 2

-------------------------------------------------
  AFID  Vsan          Pwwn           Virtual-fcid
-------------------------------------------------
   21    22  11:22:33:44:55:66:77:88  0x114466
   21    22  21:22:33:44:55:66:77:88  0x0c4466
   21    22  21:22:33:44:55:66:78:88  0x0c4466

Number of Virtual-fcid entries: 3
```

The following example displays the IVR fcdomain database entries for a specific AFID and VSAN.

```
switch# show ivr fcdomain database autonomous-fabric-num 21 vsan 22
-------------------------------------------------
  AFID  Vsan  Native-AFID  Native-Vsan  Virtual-domain
-------------------------------------------------
   21    22        20          11         0xc(12)

Number of Virtual-domain entries: 1

-------------------------------------------------
  AFID  Vsan          Pwwn           Virtual-fcid
-------------------------------------------------
   21    22  11:22:33:44:55:66:77:88  0x114466
   21    22  21:22:33:44:55:66:77:88  0x0c4466
   21    22  21:22:33:44:55:66:78:88  0x0c4466

Number of Virtual-fcid entries: 3
```

Related Commands

Command	Description
ivr fcdomain database autonomous-fabric-num	Creates IVR persistent FC IDs.

show ivr service-group

To display an inter-VSAN routing (IVR) service groups, use the **show ivr service-group** command.

show ivr service-group [active | configured]

Syntax Description

active	Displays active IVR service groups.
configured	Displays configured IVR service groups.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can configure a maximum of 16 IVR service groups.

Examples

The following example displays IIVR service groups.

```
switch# show ivr service-group

IVR CONFIGURED Service Group
====================================
SG-ID SG-NAME AFID VSANS
--------------------------------------------------------------------------------
1 sg-100 1 200-201,250,270
2 sg-200 1 100-101,150,170
Total: 2 entries in configured service group table

IVR ACTIVE Service Group
====================================
SG-ID SG-NAME AFID VSANS
--------------------------------------------------------------------------------
1 sg-100 1 200-201,250,270
2 sg-200 1 100-101,150,170
Total: 2 entries in active service group table
```

Related Commands

Command	Description
clear ivr service-group database	Clears an IVR service group database.
ivr service-group name	Configures an IVR service group.

show ivr virtual-switch-wwn

To display an inter-VSAN routing (IVR) virtual switch WWN, use the **show ivr virtual-switch-wwn** command.

show ivr virtual-switch-wwn native-switch-wwn *switch-wwn* **native-vsan** *vsan-id*

Syntax Description

native-switch-wwn *switch-wwn*	Specifies the sWWN of the native switch. The format is in dotted hex.
native-vsan *vsan-id*	Specifies the ID of the native VSAN. The range is 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The sWWN of the virtual switch must be present in the fabric binding database of all the VSANs where the virtual switch is in use. If the sWWN is not in the database, you must add it before attempting to implement FICON over IVR.

Examples

The following example displays an IVR virtual sWNN.

```
switch# show ivr virtual-switch-wwn native-switch-wwn 20:00:00:0d:ec:00:8c:c0 native-vsan
1
virtual switch wwn : 20:01:00:0d:ec:00:8c:c1
```

Related Commands

Command	Description
show ivr	Displays IVR information.

show kernel core

To display kernel core configuration information, use the **show kernel core** command.

show kernel core {**limit** | **module** *slot* | **target**}

Syntax Description

limit	Displays the configured line card limit.
module *slot*	Displays the kernel core configuration for a module in the specified slot.
target	Displays the configured target IP address.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following examples display kernel core settings.

```
switch# show kernel core limit
2

switch# show kernel core target
10.50.5.5

switch# show kernel core module 5
module 5 core is enabled
         level is header
         dst_ip is 10.50.5.5
         src_port is 6671
         dst_port is 6666
         dump_dev_name is eth1
         dst_mac_addr is 00:00:0C:07:AC:01
```

show license

To display license information, use the **show license** command.

show license [**brief** | **file** *filename* | **host-id** *license-name* | **usage**]

Syntax Description

brief	Displays a list of license files installed on a switch.
file *filename*	Displays information for a specific license file.
host-id *license-name*	Displays host ID used to request node-locked license.
usage	Displays information about the current license usage.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays a specific license installed on a switch.

```
switch# show license file fcports.lic
fcports.lic:
SERVER this_host ANY
VENDOR cisco
FEATURE fcports cisco 1.000 permanent 30 HOSTID=VDH=4C0AF664 \
        SIGN=24B2B68AA676 <---------------------- fcport license
```

The following example displays a list of license files installed on a switch.

```
switch# show license brief
fcports.lic
ficon.lic
```

The following example displays all licenses installed on a switch.

```
switch# show license
fcports.lic:
SERVER this_host ANY
VENDOR cisco
FEATURE fcports cisco 1.000 permanent 30 HOSTID=VDH=4C0AF664 \
        SIGN=24B2B68AA676 <----------------------fcport license
ficon.lic:
FEATURE ficon cisco 1.000 permanent uncounted HOSTID=VDH=4C0AF664 \
        SIGN=CB7872B23700 <----------------------------ficon license
```

The following example displays the host IDs, required to request node locked license.

```
switch# show license host-id
License hostid:VDH=4C0AF664
```

The following example displays information about current license usage.

```
switch# show license usage
Feature                 Installed   License Status  ExpiryDate   Comments
                                    Count
--------------------------------------------------------------------------------
FM_SERVER_PKG           Yes         -       Unused   never        license missing
MAINFRAME_PKG           No          -       Unused                Grace Period 57days15hrs
ENTERPRISE_PKG          Yes         -       InUse    never        -
SAN_EXTN_OVER_IP        No          0       Unused                -
SAN_EXTN_OVER_IP_IPS4   No          0       Unused
--------------------------------------------------------------------------------
```

show line

To configure a virtual terminal line, use the **show line** command.

show line [**com1** [**user-input-string**] | **console** [**connected** | **user-input-string**]]

Syntax Description

com1	Displays aux line configuration.
user-input-string	Displays the user-input initial string.
console	Displays console line configuration.
connected	Displays the physical connection status.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.
3.0(1)	Modified examples for Supervisor-1 and Supervisor-2 modules.

Usage Guidelines

None.

Examples

The following example displays output from an MDS switch with a Supervisor-1 module.

```
switch# show line console
line Console:
Speed: 9600 bauds
Databits: 8 bits per byte
Stopbits: 1 bit(s)
Parity: none
Modem In: Enable
Modem Init-String -
default : ATE0Q1&D2&C1S0=1\015
Statistics: tx:12842 rx:366 Register Bits:RTS|CTS|DTR|DSR|CD|RI
```

The following example displays output from an MDS switch with a Supervisor-2 module.

```
switch# show line console
line Console:
Speed: 9600 bauds
Databits: 8 bits per byte
Stopbits: 1 bit(s)
Parity: none
Modem In: Enable
Modem Init-String -
default : ATE0Q0V1&D0&C0S0=1\015
Statistics: tx:12842 rx:366 Register Bits:RTS|CTS|DTR|DSR|CD|RI
```

The following example displays output from an MDS switch with a Supervisor-1 module.

```
switch# show line com1
line Aux:
Speed: 9600 bauds
Databits: 8 bits per byte
Stopbits: 1 bit(s)
Parity: none
Modem In: Enable
Modem Init-String -
default : ATE0Q1&D2&C1S0=1\015
Statistics: tx:17 rx:0 Register Bits:RTS|DTR
```

The following example displays output from an MDS switch with a Supervisor-2 module.

```
switch# show line com1
line Aux:
Speed: 9600 bauds
Databits: 8 bits per byte
Stopbits: 1 bit(s)
Parity: none
Modem In: Enable
Modem Init-String -
default : ATE0Q0V1&D0&C0S0=1\015
Statistics: tx:17 rx:0 Register Bits:RTS|DTR
```

Related Commands

Command	Description
line console	Configure primary terminal line.
line aux	Configures the auxiliary COM 1 port
clear line	Deleted configured line sessions.

show logging

To display the current message logging configuration, use the **show logging** command.

show logging [**console** | **info** | **last** *lines* | **level** *facility* | **logfile** | **module** | **monitor**| **nvram** [**last** *lines*] | **onboard** *information* | **pending** | **pending-diff** | **server** | **status**]

Syntax Description

console	Displays console logging configuration.
info	Displays logging configuration.
last *lines*	Displays last few lines of the log file. The range is 1 to 9999.
level *facility*	Displays facility logging configuration. Facility values include **aaa**, **acl**, **auth**, **authpriv**, **bootvar**, **callhome**, **cdp**, **cfs**, **cimserver**, **cron**, **daemon**, **device-alias**, **dstats**, **ethport**, **fc2d**, **fcc**, **fcd**, **fcdomain**, **fcns**, **fcsp-mgr**, **fdmi**, **ficon**, **flogi**, **fspf**, **ftp**, **ike**, **ipacl**, **ipconf**, **ipfc**, **ips**, **ipsec**, **isns**, **kernel**, **license**, **local***n*, **lpr**, **mail**, **mcast**, **module**, **news**, **platform**, **port**, **port-security**, **qos**, **radius**, **rdl**, **rib**, **rlir**, **rscn**, **scsi-target**, **security**, **syslog**, **sysmgr**, **systemhealth**, **tacacs**, **tlport**, **user**, **uucp**, **vni**, **vrrp-cfg**, **vsan**, **vshd**, **wwm**, **xbar**, **zone**.
logfile	Displays contents of the log file.
module	Displays module logging configuration.
monitor	Displays monitor logging configuration.
nvram	Displays NVRAM log.
onboard *information*	Displays onboard failure logging (OBFL) information. The types of information include **boot-uptime**, **cpu-hog**, **device-version**, **endtime**, **environmental-history**, **error-stats**, **exception-log**, **interrupt-stats**, **mem-leak**, **miscellaneous-error**, **module**, **obfl-history**, **obfl-logs**, **register-log**, **stack-trace**, **starttime**, **status**, **system-health**.
pending	Displays the server address pending configuration.
pending-diff	Displays the server address pending configuration differences with the active configuration.
server	Displays server logging configuration.
status	Displays the status of the last operation.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.0(1b)	Added the **pending**, **pending-diff**, and **status** keywords.
3.0(1)	Added the **onboard** keyword.

Usage Guidelines

None.

Examples

The following example displays current system message logging.

```
switch# show logging

Logging console:                enabled (Severity: notifications)
Logging monitor:                enabled (Severity: information)
Logging linecard:               enabled (Severity: debugging)
Logging server:                 enabled
{172.22.0.0}
        server severity:        debugging
        server facility:        local7
{172.22.0.0}
        server severity:        debugging
        server facility:        local7
Logging logfile:                enabled
        Name - external/sampleLogFile: Severity - notifications Size - 3000000

syslog_get_levels :: Error(-1) querying severity values for fcmpls at SAP 30
syslog_get_levels :: Error(-1) querying severity values for fcfwd at SAP 38
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
kern                    6                       4
user                    3                       3
mail                    3                       3
daemon                  7                       7
auth                    0                       0
syslog                  3                       3
lpr                     3                       3
news                    3                       3
uucp                    3                       3
cron                    3                       3
authpriv                3                       3
ftp                     3                       3
local0                  3                       3
local1                  3                       3
local2                  3                       3
local3                  3                       3
local4                  3                       3
local5                  3                       3
local6                  3                       3
local7                  3                       3
fspf                    3                       3
fcdomain                2                       2
module                  5                       5
zone                    2                       2
vni                     2                       2
ipconf                  2                       2
ipfc                    2                       2
xbar                    3                       3
fcns                    2                       2
fcs                     2                       2
acl                     2                       2
tlport                  2                       2
port                    5                       5
port_channel            5                       5
fcmpls                  0                       0
wwn                     3                       3
fcc                     2                       2
qos                     3                       3
```

```
vrrp_cfg                2                       2
fcfwd                   0                       0
ntp                     2                       2
platform                5                       5
vrrp_eng                2                       2
callhome                2                       2
mcast                   2                       2
rscn                    2                       2
securityd               2                       2
vhbad                   2                       2
rib                     2                       2
vshd                    5                       5

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)

Nov  8 16:48:04 excal-113 %LOG_VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console
from pts/1 (171.71.58.56)
Nov  8 17:44:09 excal-113 %LOG_VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console
from pts/0 (171.71.58.72)
```

The following example displays console logging status.

```
switch# show logging console
Logging console:                enabled (Severity: notifications)
```

The following example displays logging facility status.

```
switch# show logging facility
syslog_get_levels :: Error(-1) querying severity values for fcmpls at SAP 30
syslog_get_levels :: Error(-1) querying severity values for fcfwd at SAP 38
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
kern                    6                       4
user                    3                       3
mail                    3                       3
daemon                  7                       7
auth                    0                       0
syslog                  3                       3
lpr                     3                       3
news                    3                       3
uucp                    3                       3
cron                    3                       3
authpriv                3                       3
ftp                     3                       3
local0                  3                       3
local1                  3                       3
local2                  3                       3
local3                  3                       3
local4                  3                       3
local5                  3                       3
local6                  3                       3
local7                  3                       3
fspf                    3                       3
fcdomain                2                       2
module                  5                       5
zone                    2                       2
vni                     2                       2
ipconf                  2                       2
ipfc                    2                       2
xbar                    3                       3
fcns                    2                       2
fcs                     2                       2
```

```
acl                     2                       2
tlport                  2                       2
port                    5                       5
port_channel            5                       5
fcmpls                  0                       0
wwn                     3                       3
fcc                     2                       2
qos                     3                       3
vrrp_cfg                2                       2
fcfwd                   0                       0
ntp                     2                       2
platform                5                       5
vrrp_eng                2                       2
callhome                2                       2
mcast                   2                       2
rscn                    2                       2
securityd               2                       2
vhbad                   2                       2
rib                     2                       2
vshd                    5                       5

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
```

The following example displays logging information.

```
switch# show logging info

Logging console:                enabled (Severity: notifications)
Logging monitor:                enabled (Severity: information)
Logging linecard:               enabled (Severity: debugging)
Logging server:                 enabled
{172.22.95.167}
        server severity:        debugging
        server facility:        local7
{172.22.92.58}
        server severity:        debugging
        server facility:        local7
Logging logfile:                enabled
        Name - external/sampleLogFile: Severity - notifications Size - 3000000

syslog_get_levels :: Error(-1) querying severity values for fcmpls at SAP 30
syslog_get_levels :: Error(-1) querying severity values for fcfwd at SAP 38
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
kern                    6                       4
user                    3                       3
mail                    3                       3
daemon                  7                       7
auth                    0                       0
syslog                  3                       3
lpr                     3                       3
news                    3                       3
uucp                    3                       3
cron                    3                       3
authpriv                3                       3
ftp                     3                       3
local0                  3                       3
local1                  3                       3
local2                  3                       3
local3                  3                       3
local4                  3                       3
local5                  3                       3
```

```
local6                  3                       3
local7                  3                       3
fspf                    3                       3
fcdomain                2                       2
module                  5                       5
zone                    2                       2
vni                     2                       2
ipconf                  2                       2
ipfc                    2                       2
xbar                    3                       3
fcns                    2                       2
fcs                     2                       2
acl                     2                       2
tlport                  2                       2
port                    5                       5
port_channel            5                       5
fcmpls                  0                       0
wwn                     3                       3
fcc                     2                       2
qos                     3                       3
vrrp_cfg                2                       2
fcfwd                   0                       0
ntp                     2                       2
platform                5                       5
vrrp_eng                2                       2
callhome                2                       2
mcast                   2                       2
rscn                    2                       2
securityd               2                       2
vhbad                   2                       2
rib                     2                       2
vshd                    5                       5

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
```

The following example displays last few lines of a log file.

```
switch# show logging last 2
Nov  8 16:48:04 excal-113 %LOG_VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console
from pts/1 (171.71.58.56)
Nov  8 17:44:09 excal-113 %LOG_VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console
from pts/0 (171.71.58.72)
```

The following example displays switching module logging status.

```
switch# show logging module
Logging linecard:               enabled (Severity: debugging)
```

The following example displays monitor logging status.

```
switch# show logging monitor
Logging monitor:                enabled (Severity: information)
```

The following example displays server information.

```
switch# show logging server
Logging server:                 enabled
{172.22.95.167}
        server severity:        debugging
        server facility:        local7
{172.22.92.58}
        server severity:        debugging
        server facility:        local7
```

The following example shows onboard failure logging for boot-uptime for module 2.

```
switch# show logging onboard module 2 boot-uptime
----------------------------
    Module:  2
----------------------------


Wed Nov  9 12:05:56 2005:  Boot Record
-------------------------------------------------------------------------------
Boot Time..........:  Wed Nov  9 12:05:56 2005
Slot Number........:  2
Serial Number......:  JAB0912026U
Bios Version.......:    v0.0.8(08/18/05)
Alt Bios Version...:    v0.0.8(08/18/05)
Firmware Version...:  3.0(1) [build 3.0(0.276)]


Wed Nov  9 11:58:04 2005:  Card Uptime Record
-----------------------------------------------
Uptime: 273, 0 days 0 hour(s) 4 minute(s) 33 second(s)
Reset Reason: Reset Requested by CLI command reload (9)
Card Mode..........................:  Runtime




Wed Nov  9 12:05:56 2005:  Card Uptime Record
-----------------------------------------------
Uptime: 32, 0 days 0 hour(s) 0 minute(s) 32 second(s)
Reset Reason: Unknown (0)
Card Mode..........................:  Runtime
```

The following example shows onboard failure logging for boot-uptime.

```
switch# show logging onboard boot-uptime
----------------------------
    Module:  2
----------------------------


Wed Nov  9 12:05:56 2005:  Boot Record
-------------------------------------------------------------------------------
Boot Time..........:  Wed Nov  9 12:05:56 2005
Slot Number........:  2
Serial Number......:  JAB0912026U
Bios Version.......:    v0.0.8(08/18/05)
Alt Bios Version...:    v0.0.8(08/18/05)
Firmware Version...:  3.0(1) [build 3.0(0.276)]


Wed Nov  9 11:58:04 2005:  Card Uptime Record
-----------------------------------------------
Uptime: 273, 0 days 0 hour(s) 4 minute(s) 33 second(s)
Reset Reason: Reset Requested by CLI command reload (9)
Card Mode..........................:  Runtime




Wed Nov  9 12:05:56 2005:  Card Uptime Record
-----------------------------------------------
Uptime: 32, 0 days 0 hour(s) 0 minute(s) 32 second(s)
Reset Reason: Unknown (0)
```

```
Card Mode.......................:  Runtime


----------------------------
    Module:  5
----------------------------


Wed Nov  9 12:05:05 2005:  Boot Record
--------------------------------------------------------------------------------
Boot Time..........:  Wed Nov  9 12:05:05 2005
Slot Number........:  5
Serial Number......:  JAB091100TS
Bios Version.......:  00.01.01 (Oct 25 2005 - 15:48:45)
Alt Bios Version...:  00.01.01 (Oct 25 2005 - 15:48:45)
Firmware Version...:  3.0(1) [build 3.0(0.274)]


Wed Nov  9 11:58:04 2005:  Card Uptime Record
--------------------------------------------
Uptime: 503255, 5 days 19 hour(s) 47 minute(s) 35 second(s)
Reset Reason: Reset reason: Reset Requested by CLI command reload (9)
Card Mode.......................:  Runtime




Wed Nov  9 12:05:05 2005:  Card Uptime Record
--------------------------------------------
Uptime: 172, 0 days 0 hour(s) 2 minute(s) 52 second(s)
Reset Reason: Reset reason: Unknown (0)
Card Mode.......................:  Runtime
```

The following example shows onboard failure logging for device-version.

```
switch# show logging onboard device-version
----------------------------
    Module:  2
----------------------------

Device Version Record
-------------------------------------------------------------------------
Timestamp                 Device Name      Instance Hardware Software
                                                Num  Version  Version
-------------------------------------------------------------------------
Wed Nov  9 12:05:56 2005  Stratosphere            0        1        1
Wed Nov  9 12:05:56 2005  Stratosphere            1        1        1
Wed Nov  9 12:05:56 2005  Skyline-asic            0        1        1
Wed Nov  9 12:05:56 2005  Tuscany-asic            0        1        0
Wed Nov  9 12:05:56 2005  X-Bus IO                0        6        0
Wed Nov  9 12:05:56 2005  Power Mngmnt Epl        0        6        0
----------------------------
    Module:  5
----------------------------

Device Version Record
-------------------------------------------------------------------------
Timestamp                 Device Name      Instance Hardware Software
                                                Num  Version  Version
-------------------------------------------------------------------------
Wed Nov  9 12:05:05 2005  Power Mngmnt Epl        0        7        0
Wed Nov  9 12:05:05 2005  IO FPGA Molakini        0        8        0
Wed Nov  9 12:05:05 2005  bellagio2               0        1        0
```

```
Wed Nov  9 12:05:05 2005   BabyCaesar              0        1        0
```

The following example show onboard failure logging for system health.

```
switch# show logging onboard system-health

Feature supported only on active-sup
----------------------------
    Module:  5
----------------------------
Wed Nov  9 12:04:58 20050@345463 (5/31/0x0): System health started with pid 2607
Wed Nov  9 12:05:05 20050@943388 (5/31/0xb): Module Supervisor 5, swid 31 came online
Wed Nov  9 12:05:05 20050@944275 (5/31/0xb): LC config removed for module 7
Wed Nov  9 12:05:05 20050@944454 (5/31/0xb): LC config removed for module 8
Wed Nov  9 12:05:05 20050@944592 (5/31/0xb): LC config removed for module 9
Wed Nov  9 12:05:05 20050@944717 (5/31/0xb): LC config removed for module 10
Wed Nov  9 12:05:05 20050@944846 (5/31/0xb): LC config removed for module 11
Wed Nov  9 12:05:05 20050@944969 (5/31/0xb): LC config removed for module 12
Wed Nov  9 12:05:05 20050@945094 (5/31/0xb): LC config removed for module 13
Wed Nov  9 12:05:05 20050@945222 (5/31/0xb): LC config removed for module 14
Wed Nov  9 12:05:05 20050@945343 (5/31/0xb): LC config removed for module 15
Wed Nov  9 12:05:05 20050@945470 (5/31/0xb): LC config removed for module 16
Wed Nov  9 12:05:50 20050@814217 (2/29/0x0): System health started with pid 397
Wed Nov  9 12:05:56 20050@904068 (5/31/0xb): LC inserted for module 2
Wed Nov  9 12:05:59 20050@167373 (5/31/0xb): Module Linecard 2, swid 29 came online
switch# show logging onboard
boot-uptime            exception-log          obfl-logs
cpu-hog                interrupt-stats        register-log
device-version         mem-leak               stack-trace
endtime                miscellaneous-error    starttime
environmental-history  module                 status
error-stats            obfl-history           system-health
```

The following example show onboard failure logging for obfl-logs.

```
switch# show logging onboard obfl-logs
Module:  1 not online.


OBFL: Status:

    Module:  2 OBFL Log:                                    Enabled
    cpu-hog                                                 Enabled
    environmental-history                                   Enabled
    error-stats                                             Enabled
    exception-log                                           Enabled
    interrupt-stats                                         Enabled
    mem-leak                                                Enabled
    miscellaneous-error                                     Enabled
    obfl-log (boot-uptime/device-version/obfl-history)      Enabled
    register-log                                            Enabled
    stack-trace                                             Enabled


OBFL: Memory Leak:
----------------------------
    Module:  2
----------------------------


OBFL: Stack Trace:
----------------------------
    Module:  2
----------------------------
```

```
OBFL: Environment History:
----------------------------
    Module:  2
----------------------------

========== Sensor Temperature History Log ==========
--------------------------------------------------
Wed Nov  9 12:05:50 2005 sensor 0 temperature 31
Wed Nov  9 12:05:50 2005 sensor 1 temperature 31
Wed Nov  9 12:05:50 2005 sensor 2 temperature 29
Wed Nov  9 12:06:20 2005 sensor 0 temperature 33
Wed Nov  9 12:06:20 2005 sensor 1 temperature 34
Wed Nov  9 12:06:50 2005 sensor 0 temperature 35
Wed Nov  9 12:06:50 2005 sensor 1 temperature 36
Wed Nov  9 12:07:20 2005 sensor 1 temperature 38
Wed Nov  9 12:08:50 2005 sensor 0 temperature 37
Wed Nov  9 12:08:50 2005 sensor 1 temperature 40

========== Sensor Temperature Error Log ==========
--------------------------------------------------
Wed Nov  9 12:05:50 2005 Start of Service: sensor 0 initial temperature 31
Wed Nov  9 12:05:50 2005 Start of Service: sensor 1 initial temperature 31
Wed Nov  9 12:05:50 2005 Start of Service: sensor 2 initial temperature 29


OBFL: Interrupt Statistics:
----------------------------
    Module:  2
----------------------------


-------------------------------------------------------------------------------
 INTERRUPT COUNTS INFORMATION FOR DEVICE ID 63 DEVICE: Stratosphere
-------------------------------------------------------------------------------
                                  |       |       |   Time Stamp    |In|Port
   Interrupt Counter Name         | Count | Thresh |MM/DD/YY HH:MM:SS|st|Rang
                                  |       |       |                 |Id|e
-------------------------------------------------------------------------------
FCP_LAF_MISC_INT_DT_IN_OBUF       |7      |0      |11/09/05 12:06:00|00|1
FCP_MAC_SR1_LR_DETECTED           |1      |0      |11/09/05 12:06:00|00|1
FCP_MAC_SR1_LRR_DETECTED          |1      |0      |11/09/05 12:06:00|00|1
FCP_MAC_SR1_OLS_DETECTED          |1      |0      |11/09/05 12:06:00|00|1
FCP_MAC_SR2_LRR_IDLE_RECEIVED     |1      |0      |11/09/05 12:06:00|00|1
FCP_MAC_SR2_AL_NON_F8_LIP_RECEIVED|2      |0      |11/09/05 12:06:00|00|1
FCP_MAC_SR2_AL_LIP_RECEIVED       |1      |0      |11/09/05 12:06:00|00|1
FCP_MAC_SR2_AL_ARB_F0_RECEIVED    |1      |0      |11/09/05 12:06:00|00|1
FCP_LAF_MISC_INT_DT_IN_OBUF       |2      |0      |11/09/05 12:06:00|00|2
FCP_MAC_SR1_OLS_DETECTED          |1      |0      |11/09/05 12:06:00|00|2
FCP_MAC_SR2_AL_NON_F8_LIP_RECEIVED|2      |0      |11/09/05 12:06:00|00|2
FCP_MAC_SR2_AL_LIP_RECEIVED       |3      |0      |11/09/05 12:06:00|00|2
FCP_LAF_MISC_INT_DT_IN_OBUF       |b      |0      |11/09/05 12:06:00|00|3
FCP_MAC_SR1_LR_DETECTED           |3      |0      |11/09/05 12:06:00|00|3
FCP_MAC_SR1_LRR_DETECTED          |2      |0      |11/09/05 12:06:00|00|3
FCP_MAC_SR1_OLS_DETECTED          |2      |0      |11/09/05 12:06:00|00|3
FCP_MAC_SR2_LR_IDLE_RECEIVED      |1      |0      |11/09/05 12:06:00|00|3
FCP_MAC_SR2_LRR_IDLE_RECEIVED     |2      |0      |11/09/05 12:06:00|00|3
FCP_MAC_SR2_AL_NON_F8_LIP_RECEIVED|3      |0      |11/09/05 12:06:00|00|3
FCP_MAC_SR2_AL_LIP_RECEIVED       |1      |0      |11/09/05 12:06:00|00|3
FCP_MAC_SR2_AL_ARB_F0_RECEIVED    |2      |0      |11/09/05 12:06:00|00|3
FCP_LAF_MISC_INT_DT_IN_OBUF       |2      |0      |11/09/05 12:06:00|00|4
FCP_MAC_SR1_LRR_DETECTED          |1      |0      |11/09/05 12:06:00|00|4
FCP_MAC_SR1_OLS_DETECTED          |3      |0      |11/09/05 12:06:00|00|4
```

```
FCP_MAC_SR2_LRR_IDLE_RECEIVED       |1       |0       |11/09/05 12:06:00|00|4
FCP_MAC_SR2_AL_NON_F8_LIP_RECEIVED  |3       |0       |11/09/05 12:06:00|00|4
FCP_MAC_SR2_AL_LIP_RECEIVED         |3       |0       |11/09/05 12:06:00|00|4
FCP_LAF_MISC_INT_DT_IN_OBUF         |d       |0       |11/09/05 12:06:05|00|1
FCP_MAC_SR1_LRR_DETECTED            |2       |0       |11/09/05 12:06:05|00|1
FCP_MAC_SR1_OLS_DETECTED            |2       |0       |11/09/05 12:06:05|00|1
FCP_MAC_SR2_LRR_IDLE_RECEIVED       |2       |0       |11/09/05 12:06:05|00|1
FCP_MAC_SR2_AL_LIP_RECEIVED         |2       |0       |11/09/05 12:06:05|00|1
FCP_MAC_SR2_AL_ARB_F0_RECEIVED      |2       |0       |11/09/05 12:06:05|00|1
FCP_LAF_MISC_INT_DT_IN_OBUF         |3       |0       |11/09/05 12:06:05|00|2
FCP_MAC_SR1_LR_DETECTED             |1       |0       |11/09/05 12:06:05|00|2
FCP_MAC_SR1_OLS_DETECTED            |3       |0       |11/09/05 12:06:05|00|2
FCP_MAC_SR2_LR_IDLE_RECEIVED        |1       |0       |11/09/05 12:06:05|00|2
FCP_MAC_SR2_AL_NON_F8_LIP_RECEIVED  |4       |0       |11/09/05 12:06:05|00|2


OBFL: Error Statistics:
----------------------------
    Module:  2
----------------------------


OBFL: System Bootup Record:
----------------------------
    Module:  2
----------------------------


Wed Nov  9 12:05:56 2005:  Boot Record
-------------------------------------------------------------------------------
Boot Time..........:  Wed Nov  9 12:05:56 2005
Slot Number........:  2
Serial Number......:  JAB0912026U
Bios Version.......:    v0.0.8(08/18/05)
Alt Bios Version...:    v0.0.8(08/18/05)
Firmware Version...:  3.0(1) [build 3.0(0.276)]


Wed Nov  9 12:05:56 2005:  Card Uptime Record
----------------------------------------------
Uptime: 32, 0 days 0 hour(s) 0 minute(s) 32 second(s)
Reset Reason: Unknown (0)
Card Mode.........................:  Runtime



OBFL: Device Versions in Switch:
----------------------------
    Module:  2
----------------------------

Device Version Record
-------------------------------------------------------------------------
Timestamp                  Device Name      Instance Hardware Software
                                                Num  Version  Version
-------------------------------------------------------------------------
Wed Nov  9 12:05:56 2005   Stratosphere            0        1        1
Wed Nov  9 12:05:56 2005   Stratosphere            1        1        1
Wed Nov  9 12:05:56 2005   Skyline-asic            0        1        1
Wed Nov  9 12:05:56 2005   Tuscany-asic            0        1        0
Wed Nov  9 12:05:56 2005   X-Bus IO                0        6        0
Wed Nov  9 12:05:56 2005   Power Mngmnt Epl        0        6        0
```

```
OBFL: Exception Log:
------------------------------
    Module:  2
------------------------------


OBFL: Register Log:
------------------------------
    Module:  2
------------------------------


OBFL: Miscellaneous Error Logs:
------------------------------
    Module:  2
------------------------------

LC Config Record: Wed Nov  9 12:05:40 2005@471600
lc_copy_from_sup_to_lc() failure for sdwrap: 121


OBFL: Status:

    Module:  5 OBFL Log:                                    Enabled
    error-stats                                             Enabled
    exception-log                                           Enabled
    miscellaneous-error                                     Enabled
    obfl-log (boot-uptime/device-version/obfl-history)      Enabled
    system-health                                           Enabled
    stack-trace                                             Enabled


OBFL: Memory Leak:
------------------------------
    Module:  5
------------------------------
mem-leak: This option not supported on SUP.


OBFL: Stack Trace:
------------------------------
    Module:  5
------------------------------
stack-trace: This option not supported on SUP.


OBFL: Environment History:
------------------------------
    Module:  5
------------------------------

========== Sensor Temperature History Log ==========
----------------------------------------------------
Wed Nov  9 12:05:06 2005 sensor 0 temperature 36
Wed Nov  9 12:05:06 2005 sensor 1 temperature 35
Wed Nov  9 12:05:06 2005 sensor 2 temperature 31


OBFL: Interrupt Statistics:
------------------------------
    Module:  5
------------------------------
interrupt-stats: This option not supported on SUP.
```

```
OBFL: Error Statistics:
----------------------------
    Module:  5
----------------------------

------------------------------------------------------------------
Date (mm/dd/yy)=11/09/05  Time (hs:mn:sec): 12:10:05
Baby Ceaser data

------------------------------------------------------------------
Date (mm/dd/yy)=11/09/05  Time (hs:mn:sec): 12:10:05
Arbiter Bellagio2 data
GROUP:4
bkt_tx_perr_drop_cnt           0
bkr_rx_req_fifo_drop_cnt       0
bkr_rx_req_fifo_perr_drop_cnt  0
bkr_rx_di_lut_perr_drop_cnt    0
fil_drop_cnt                   0
crm_gid_drop_cnt               0
ser_rxs_perr_cnt               0
top_ddr_rx_perr_cnt            0
Bucket Counters
 Bkt Cos  Gresend            Grant          Request  Rresend
-------------------------------------------------------------
   0   0        0                0                0        0
   0   1        0                0                0        0
   0   2        0                0                0        0
   0   3        0             1127             1127        0
  64   0        0                0                0        0
  64   1        0                0                0        0
  64   2        0                0                0        0
  64   3        0                0                0        0
 128   0        0                0                0        0
 128   1        0                0                0        0
 128   2        0                0                0        0
 128   3        0                0                0        0
 192   0        0                0                0        0
 192   1        0                0                0        0
 192   2        0                0                0        0
 192   3        0               73               73        0
 256   0        0                0                0        0
 256   1        0                0                0        0
 256   2        0                0                0        0
 256   3        0                0                0        0
 320   0        0                0                0        0
 320   1        0                0                0        0
 320   2        0                0                0        0
 320   3        0                0                0        0
 384   0        0                0                0        0
 384   1        0                0                0        0
 384   2        0                0                0        0
 384   3        0                0                0        0
 448   0        0                0                0        0
 448   1        0                0                0        0
 448   2        0                0                0        0
 448   3        0                0                0        0
 512   0        0                0                0        0
 512   1        0                0                0        0
 512   2        0                0                0        0
 512   3        0                0                0        0
 576   0        0                0                0        0
 576   1        0                0                0        0
```

```
 576   2         0                0                0         0
 576   3         0                0                0         0
 640   0         0                0                0         0
 640   1         0                0                0         0
 640   2         0                0                0         0
 640   3         0                0                0         0
 704   0         0                0                0         0
 704   1         0                0                0         0
 704   2         0                0                0         0
 704   3         0                0                0         0
 768   0         0                0                0         0
 768   1         0                0                0         0
 768   2         0                0                0         0
 768   3         0                0                0         0
 832   0         0                0                0         0
 832   1         0                0                0         0
 832   2         0                0                0         0
 832   3         0                0                0         0
 896   0         0                0                0         0
 896   1         0                0                0         0
 896   2         0                0                0         0
 896   3         0                0                0         0
 960   0         0                0                0         0
 960   1         0                0                0         0
 960   2         0                0                0         0
 960   3         0                0                0         0
LDI Counters
LDI COS  OUT_REQ   CREDIT CREDITNA
---------------------------------
  0   0         0    14164       63
  0   1         0    41874       63
  0   2         0    41874       63
  0   3         0    41905       63
  1   0         0    14164       63
  1   1         0    41874       63
  1   2         0    41874       63
  1   3         0    41904       63
  2   0         0    14164       63
  2   1         0    41874       63
  2   2         0    41874       63
  2   3         0    41902       63
  3   0         0    14164       63
  3   1         0    41874       63
  3   2         0    41874       63
  3   3         0    41903       63
  4   0         0    14164       63
  4   1         0    41873       63
  4   2         0    41873       63
  4   3         0    41903       63
  5   0         0    14164       63
  5   1         0    41873       63
  5   2         0    41873       63
  5   3         0    41903       63
  6   0         0    14164       63
  6   1         0    41872       63
  6   2         0    41872       63
  6   3         0    41903       63
  7   0         0    14164       63
  7   1         0    41872       63
  7   2         0    41872       63
  7   3         0    41903       63
  8   0         0    14163       63
  8   1         0    41871       63
  8   2         0    41871       63
```

8	3	0	41902	63
9	0	0	14163	63
9	1	0	41871	63
9	2	0	41871	63
9	3	0	41902	63
10	0	0	14163	63
10	1	0	41871	63
10	2	0	41871	63
10	3	0	41901	63
11	0	0	14163	63
11	1	0	41871	63
11	2	0	41871	63
11	3	0	41901	63
12	0	0	14163	63
12	1	0	41870	63
12	2	0	41870	63
12	3	0	41901	63
13	0	0	14163	63
13	1	0	41870	63
13	2	0	41870	63
13	3	0	41900	63
14	0	0	14163	63
14	1	0	41869	63
14	2	0	41869	63
14	3	0	41900	63
15	0	0	14163	63
15	1	0	41869	63
15	2	0	41869	63
15	3	0	41900	63
16	0	0	14163	63
16	1	0	41869	63
16	2	0	41869	63
16	3	0	41900	63
17	0	0	14162	63
17	1	0	41868	63
17	2	0	41868	63
17	3	0	41899	63
18	0	0	14162	63
18	1	0	41868	63
18	2	0	41868	63
18	3	0	41898	63
19	0	0	14162	63
19	1	0	41868	63
19	2	0	41868	63
19	3	0	41898	63
20	0	0	14162	63
20	1	0	41868	63
20	2	0	41868	63
20	3	0	41898	63
21	0	0	14162	63
21	1	0	41867	63
21	2	0	41867	63
21	3	0	41898	63
22	0	0	14162	63
22	1	0	41867	63
22	2	0	41867	63
22	3	0	41897	63
23	0	0	14162	63
23	1	0	41866	63
23	2	0	41866	63
23	3	0	41897	63
24	0	0	0	0
24	1	0	0	0
24	2	0	0	0

24	3	0	0	0
25	0	0	0	0
25	1	0	0	0
25	2	0	0	0
25	3	0	0	0
26	0	0	0	0
26	1	0	0	0
26	2	0	0	0
26	3	0	0	0
27	0	0	0	0
27	1	0	0	0
27	2	0	0	0
27	3	0	0	0
28	0	0	0	0
28	1	0	0	0
28	2	0	0	0
28	3	0	0	0
29	0	0	0	0
29	1	0	0	0
29	2	0	0	0
29	3	0	0	0
30	0	0	0	0
30	1	0	0	0
30	2	0	0	0
30	3	0	0	0
31	0	0	0	0
31	1	0	0	0
31	2	0	0	0
31	3	0	0	0
32	0	0	0	0
32	1	0	0	0
32	2	0	0	0
32	3	0	0	0
33	0	0	0	0
33	1	0	0	0
33	2	0	0	0
33	3	0	0	0
34	0	0	0	0
34	1	0	0	0
34	2	0	0	0
34	3	0	0	0
35	0	0	0	0
35	1	0	0	0
35	2	0	0	0
35	3	0	0	0
36	0	0	0	0
36	1	0	0	0
36	2	0	0	0
36	3	0	0	0
37	0	0	0	0
37	1	0	0	0
37	2	0	0	0
37	3	0	0	0
38	0	0	0	0
38	1	0	0	0
38	2	0	0	0
38	3	0	0	0
39	0	0	0	0
39	1	0	0	0
39	2	0	0	0
39	3	0	0	0
40	0	0	0	0
40	1	0	0	0
40	2	0	0	0

40	3	0	0	0
41	0	0	0	0
41	1	0	0	0
41	2	0	0	0
41	3	0	0	0
42	0	0	0	0
42	1	0	0	0
42	2	0	0	0
42	3	0	0	0
43	0	0	0	0
43	1	0	0	0
43	2	0	0	0
43	3	0	0	0
44	0	0	0	0
44	1	0	0	0
44	2	0	0	0
44	3	0	0	0
45	0	0	0	0
45	1	0	0	0
45	2	0	0	0
45	3	0	0	0
46	0	0	0	0
46	1	0	0	0
46	2	0	0	0
46	3	0	0	0
47	0	0	0	0
47	1	0	0	0
47	2	0	0	0
47	3	0	0	0
48	0	0	0	0
48	1	0	0	0
48	2	0	0	0
48	3	0	0	0
49	0	0	0	0
49	1	0	0	0
49	2	0	0	0
49	3	0	0	0
50	0	0	0	0
50	1	0	0	0
50	2	0	0	0
50	3	0	0	0
51	0	0	0	0
51	1	0	0	0
51	2	0	0	0
51	3	0	0	0
52	0	0	0	0
52	1	0	0	0
52	2	0	0	0
52	3	0	0	0
53	0	0	0	0
53	1	0	0	0
53	2	0	0	0
53	3	0	0	0
54	0	0	0	0
54	1	0	0	0
54	2	0	0	0
54	3	0	0	0
55	0	0	0	0
55	1	0	0	0
55	2	0	0	0
55	3	0	0	0
56	0	0	0	0
56	1	0	0	0
56	2	0	0	0

```
 56   3         0         0         0
 57   0         0         0         0
 57   1         0         0         0
 57   2         0         0         0
 57   3         0         0         0
 58   0         0         0         0
 58   1         0         0         0
 58   2         0         0         0
 58   3         0         0         0
 59   0         0         0         0
 59   1         0         0         0
 59   2         0         0         0
 59   3         0         0         0
 60   0         0         0         0
 60   1         0         0         0
 60   2         0         0         0
 60   3         0         0         0
 61   0         0         0         0
 61   1         0         0         0
 61   2         0         0         0
 61   3         0         0         0
 62   0         0         0         0
 62   1         0         0         0
 62   2         0         0         0
 62   3         0         0         0
 63   0         0         0         0
 63   1         0         0         0
 63   2         0         0         0
 63   3         0         0         0

----------------------------------------------------------------
Date (mm/dd/yy)=11/09/05  Time (hs:mn:sec): 12:10:05
Arbiter Bellagio2 data
GROUP:10
bkt_tx_perr_drop_cnt           0
bkr_rx_req_fifo_drop_cnt       0
bkr_rx_req_fifo_perr_drop_cnt  0
bkr_rx_di_lut_perr_drop_cnt    0
fil_drop_cnt                   0
crm_gid_drop_cnt               0
ser_rxs_perr_cnt               0
top_ddr_rx_perr_cnt            0
Bucket Counters
 Bkt Cos  Gresend            Grant          Request  Rresend
-------------------------------------------------------------
   0   0         0                0                0         0
   0   1         0                0                0         0
   0   2         0                0                0         0
   0   3         0               73               73         0
  64   0         0                0                0         0
  64   1         0                0                0         0
  64   2         0                0                0         0
  64   3         0                0                0         0
 128   0         0                0                0         0
 128   1         0                0                0         0
 128   2         0                0                0         0
 128   3         0                0                0         0
 192   0         0                0                0         0
 192   1         0                0                0         0
 192   2         0                0                0         0
 192   3         0               59               59         0
 256   0         0                0                0         0
 256   1         0                0                0         0
 256   2         0                0                0         0
```

```
 256   3         0                 0                 0         0
 320   0         0                 0                 0         0
 320   1         0                 0                 0         0
 320   2         0                 0                 0         0
 320   3         0                 0                 0         0
 384   0         0                 0                 0         0
 384   1         0                 0                 0         0
 384   2         0                 0                 0         0
 384   3         0                 0                 0         0
 448   0         0                 0                 0         0
 448   1         0                 0                 0         0
 448   2         0                 0                 0         0
 448   3         0                 0                 0         0
 512   0         0                 0                 0         0
 512   1         0                 0                 0         0
 512   2         0                 0                 0         0
 512   3         0                 0                 0         0
 576   0         0                 0                 0         0
 576   1         0                 0                 0         0
 576   2         0                 0                 0         0
 576   3         0                 0                 0         0
 640   0         0                 0                 0         0
 640   1         0                 0                 0         0
 640   2         0                 0                 0         0
 640   3         0                 0                 0         0
 704   0         0                 0                 0         0
 704   1         0                 0                 0         0
 704   2         0                 0                 0         0
 704   3         0                 0                 0         0
 768   0         0                 0                 0         0
 768   1         0                 0                 0         0
 768   2         0                 0                 0         0
 768   3         0                 0                 0         0
 832   0         0                 0                 0         0
 832   1         0                 0                 0         0
 832   2         0                 0                 0         0
 832   3         0                 0                 0         0
 896   0         0                 0                 0         0
 896   1         0                 0                 0         0
 896   2         0                 0                 0         0
 896   3         0                 0                 0         0
 960   0         0                 0                 0         0
 960   1         0                 0                 0         0
 960   2         0                 0                 0         0
 960   3         0                 0                 0         0
LDI Counters
LDI COS  OUT_REQ   CREDIT CREDITNA
-----------------------------------
  0   0         0     9471        63
  0   1         0        0         0
  0   2         0        0         0
  0   3         0     9548        63
  1   0         0     9471        63
  1   1         0        0         0
  1   2         0        0         0
  1   3         0     9487        63
  2   0         0        0         0
  2   1         0        0         0
  2   2         0        0         0
  2   3         0        0         0
  3   0         0        0         0
  3   1         0        0         0
  3   2         0        0         0
  3   3         0        0         0
```

4	0	0	0	0
4	1	0	0	0
4	2	0	0	0
4	3	0	0	0
5	0	0	0	0
5	1	0	0	0
5	2	0	0	0
5	3	0	0	0
6	0	0	0	0
6	1	0	0	0
6	2	0	0	0
6	3	0	0	0
7	0	0	0	0
7	1	0	0	0
7	2	0	0	0
7	3	0	0	0
8	0	0	0	0
8	1	0	0	0
8	2	0	0	0
8	3	0	0	0
9	0	0	0	0
9	1	0	0	0
9	2	0	0	0
9	3	0	0	0
10	0	0	0	0
10	1	0	0	0
10	2	0	0	0
10	3	0	0	0
11	0	0	0	0
11	1	0	0	0
11	2	0	0	0
11	3	0	0	0
12	0	0	0	0
12	1	0	0	0
12	2	0	0	0
12	3	0	0	0
13	0	0	0	0
13	1	0	0	0
13	2	0	0	0
13	3	0	0	0
14	0	0	0	0
14	1	0	0	0
14	2	0	0	0
14	3	0	0	0
15	0	0	0	0
15	1	0	0	0
15	2	0	0	0
15	3	0	0	0
16	0	0	0	0
16	1	0	0	0
16	2	0	0	0
16	3	0	0	0
17	0	0	0	0
17	1	0	0	0
17	2	0	0	0
17	3	0	0	0
18	0	0	0	0
18	1	0	0	0
18	2	0	0	0
18	3	0	0	0
19	0	0	0	0
19	1	0	0	0
19	2	0	0	0
19	3	0	0	0

20	0	0	0	0
20	1	0	0	0
20	2	0	0	0
20	3	0	0	0
21	0	0	0	0
21	1	0	0	0
21	2	0	0	0
21	3	0	0	0
22	0	0	0	0
22	1	0	0	0
22	2	0	0	0
22	3	0	0	0
23	0	0	0	0
23	1	0	0	0
23	2	0	0	0
23	3	0	0	0
24	0	0	0	0
24	1	0	0	0
24	2	0	0	0
24	3	0	0	0
25	0	0	0	0
25	1	0	0	0
25	2	0	0	0
25	3	0	0	0
26	0	0	0	0
26	1	0	0	0
26	2	0	0	0
26	3	0	0	0
27	0	0	0	0
27	1	0	0	0
27	2	0	0	0
27	3	0	0	0
28	0	0	0	0
28	1	0	0	0
28	2	0	0	0
28	3	0	0	0
29	0	0	0	0
29	1	0	0	0
29	2	0	0	0
29	3	0	0	0
30	0	0	0	0
30	1	0	0	0
30	2	0	0	0
30	3	0	0	0
31	0	0	0	0
31	1	0	0	0
31	2	0	0	0
31	3	0	0	0
32	0	0	0	0
32	1	0	0	0
32	2	0	0	0
32	3	0	0	0
33	0	0	0	0
33	1	0	0	0
33	2	0	0	0
33	3	0	0	0
34	0	0	0	0
34	1	0	0	0
34	2	0	0	0
34	3	0	0	0
35	0	0	0	0
35	1	0	0	0
35	2	0	0	0
35	3	0	0	0

```
36   0          0          0          0
36   1          0          0          0
36   2          0          0          0
36   3          0          0          0
37   0          0          0          0
37   1          0          0          0
37   2          0          0          0
37   3          0          0          0
38   0          0          0          0
38   1          0          0          0
38   2          0          0          0
38   3          0          0          0
39   0          0          0          0
39   1          0          0          0
39   2          0          0          0
39   3          0          0          0
40   0          0          0          0
40   1          0          0          0
40   2          0          0          0
40   3          0          0          0
41   0          0          0          0
41   1          0          0          0
41   2          0          0          0
41   3          0          0          0
42   0          0          0          0
42   1          0          0          0
42   2          0          0          0
42   3          0          0          0
43   0          0          0          0
43   1          0          0          0
43   2          0          0          0
43   3          0          0          0
44   0          0          0          0
44   1          0          0          0
44   2          0          0          0
44   3          0          0          0
45   0          0          0          0
45   1          0          0          0
45   2          0          0          0
45   3          0          0          0
46   0          0          0          0
46   1          0          0          0
46   2          0          0          0
46   3          0          0          0
47   0          0          0          0
47   1          0          0          0
47   2          0          0          0
47   3          0          0          0
48   0          0          0          0
48   1          0          0          0
48   2          0          0          0
48   3          0          0          0
49   0          0          0          0
49   1          0          0          0
49   2          0          0          0
49   3          0          0          0
50   0          0          0          0
50   1          0          0          0
50   2          0          0          0
50   3          0          0          0
51   0          0          0          0
51   1          0          0          0
51   2          0          0          0
51   3          0          0          0
```

```
 52   0         0         0         0
 52   1         0         0         0
 52   2         0         0         0
 52   3         0         0         0
 53   0         0         0         0
 53   1         0         0         0
 53   2         0         0         0
 53   3         0         0         0
 54   0         0         0         0
 54   1         0         0         0
 54   2         0         0         0
 54   3         0         0         0
 55   0         0         0         0
 55   1         0         0         0
 55   2         0         0         0
 55   3         0         0         0
 56   0         0         0         0
 56   1         0         0         0
 56   2         0         0         0
 56   3         0         0         0
 57   0         0         0         0
 57   1         0         0         0
 57   2         0         0         0
 57   3         0         0         0
 58   0         0         0         0
 58   1         0         0         0
 58   2         0         0         0
 58   3         0         0         0
 59   0         0         0         0
 59   1         0         0         0
 59   2         0         0         0
 59   3         0         0         0
 60   0         0         0         0
 60   1         0         0         0
 60   2         0         0         0
 60   3         0         0         0
 61   0         0         0         0
 61   1         0         0         0
 61   2         0         0         0
 61   3         0         0         0
 62   0         0         0         0
 62   1         0         0         0
 62   2         0         0         0
 62   3         0         0         0
 63   0         0         0         0
 63   1         0         0         0
 63   2         0         0         0
 63   3         0         0         0


OBFL: System Bootup Record:
----------------------------
    Module:  5
----------------------------


OBFL: Device Versions in Switch:
----------------------------
    Module:  5
----------------------------


OBFL: Exception Log:
----------------------------
```

```
    Module:  5
----------------------------


OBFL: Register Log:
----------------------------
    Module:  5
----------------------------
register-log: This option not supported on SUP.


OBFL: Miscellaneous Error Logs:
----------------------------
    Module:  5
----------------------------.
```

Related Commands

Command	Description
logging	Configures logging parameters.

show mcast

To display multicast information, use the **show mcast** command.

show mcast [**vsan** *vsan-id*]

Syntax Description

vsan *vsan-id*	Displays information for a VSAN. The range is 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays multicast information.

```
switch# show mcast
Multicast root for VSAN 1
        Configured root mode : Principal switch
        Operational root mode : Principal switch
        Root Domain ID : 0x15(21)


Multicast root for VSAN 73
        Configured root mode : Principal switch
        Operational root mode : Principal switch
        Root Domain ID : 0x65(101)


Multicast root for VSAN 99
        Configured root mode : Principal switch
        Operational root mode : Principal switch
        Root Domain ID : 0xe4(228)


Multicast root for VSAN 4001
        Configured root mode : Principal switch
        Operational root mode : Principal switch
        Root Domain ID : 0xe9(233)


Multicast root for VSAN 4002
        Configured root mode : Principal switch
        Operational root mode : Principal switch
        Root Domain ID : 0x78(120)
```

```
Multicast root for VSAN 4003
        Configured root mode : Principal switch
        Operational root mode : Principal switch
        Root Domain ID : 0xe0(224)


Multicast root for VSAN 4004
        Configured root mode : Principal switch
        Operational root mode : Lowest domain switch
        Root Domain ID : 0x01(1)
```

Related Commands

Command	Description
mcast root	Configures the multicast root VSAN.

show module

To verify the status of a module, use the **show module** command.

show module [*slot* [**recovery-steps**] | **diag** | **uptime** | **xbar** *number*]

Syntax Description

slot	Specifies the slot number for the module.
recovery-steps	Displays information about modules and the steps to recover a module.
diag	Displays module-related information.
uptime	Displays the length of time that the modules have been functional in the switch.
xbar *number*	Displays information about the specified crossbar, either 1 or 2.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.
3.0(1)	Added the **recovery-steps** and **xbar** options.

Usage Guidelines

If your chassis has more than one switching module, you will see the progress check if you issue the show module command several times and view the status column each time.

The switching module goes through a testing and an initializing stage before displaying an `ok` status.

The following table describes the possible states in which a module can exist.

Use the **uptime** option to display the time that a specified supervisor module, switching module, or services module is functional in the switch. This time is computed from the time a module goes online after a disruptive upgrade or reset.

You can use the **recovery-steps** option only for modules that are powered down because of problems with index allocation.

Before using the **recovery-steps** option, make sure that **debug module no-power-down** is not on.

Note You cannot use the **recovery-steps** option to recover a Supervisor module.

For additional information about port indices, refer to the *Cisco MDS 9000 Family CLI Configuration Guide* and to the *Cisco MDS 9000 Family Troubleshooting Guide*.

Examples

The following example displays information about the modules on the switch.

```
switch# show module
Mod  Ports  Module-Type                      Model              Status
---  -----  -------------------------------- ------------------ ------------
2    32     Advanced Services Module         DS-X9032-SMV       powered-dn
4    32     Advanced Services Module         DS-X9032-SMV       powered-dn
5    0      Supervisor/Fabric-1              DS-X9530-SF1-K9    active *
6    0      Supervisor/Fabric-1              DS-X9530-SF1-K9    ha-standby
8    32     1/2 Gbps FC Module               DS-X9032           ok

Mod  Sw           Hw      World-Wide-Name(s) (WWN)
---  -----------  ------  --------------------------------------------------
5    1.2(2)       0.610   --
6    1.2(2)       0.610   --
8    1.2(2)       0.3     21:c1:00:0b:46:79:f1:40 to 21:e0:00:0b:46:79:f1:40


Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
5    00-d0-97-38-b4-01 to 00-d0-97-38-b4-05  JAB06350B0H
6    00-d0-97-38-b3-f9 to 00-d0-97-38-b3-fd  JAB06350B1R
8    00-05-30-00-2b-e2 to 00-05-30-00-2b-e6  jab062407x4

* this terminal session
```

The following example displays diagnostic information about the modules on the switch.

```
switch# show module diag

Diag status for module 2 (. = PASS, F = FAIL, N = N/A)
CPU           .
SPROM         .
ASICS         .

Diag status for module 4 (. = PASS, F = FAIL, N = N/A)
CPU           .
SPROM         .
ASICS         .
```

The following example displays uptime information about the modules on the switch.

```
switch#  show module uptime
------ Module 1 -----
Module Start Time:   Wed Apr 14 18:12:48 2004
Up Time:             16 days, 5 hours, 59 minutes, 41 seconds

------ Module 6 -----
Module Start Time:   Wed Apr 14 18:11:57 2004
Up Time:             16 days, 6 hours, 0 minutes, 32 second
```

The following example displays information about the crossbar.

```
switch# show module xbar 1
Xbar Ports  Module-Type                      Model              Status
---  -----  -------------------------------- ------------------ ------------
1    0      Xbar                             DS-13SLT-FAB1      ok

Xbar Sw           Hw      World-Wide-Name(s) (WWN)
---  -----------  ------  --------------------------------------------------
1    NA           0.306   --


Xbar MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    NA                                      JAB094102RQ
```

The following example uses the **show module**, **show port index-allocation**, and **show module recovery-steps** commands to display a Generation 1 module that is powered down due to a lack of indices.

```
switch# show module
Mod  Ports  Module-Type                       Model          Status
---  -----  -------------------------------- ------------------ --
1    48     1/2/4 Gbps FC Module             DS-X9148           ok
2    48     1/2/4 Gbps FC Module             DS-X9148           ok
3    48     1/2/4 Gbps FC Module             DS-X9148           ok
4    48     1/2/4 Gbps FC Module             DS-X9148           ok
6    0      Supervisor/Fabric-1              DS-X9530-SF1-K9    active *
7    48     1/2/4 Gbps FC Module             DS-X9148           ok
9    16     1/2 Gbps FC Module               DS-X9016   powered-dn

Mod  Power-Status  Power Down Reason
---  ------------  --------------------------
9    powered-dn    Insufficient resources (dest Index)

switch# show port index-allocation
Module index distribution:
-----------------------------------------------------+
Slot | Allowed |      Alloted indices info            |
     |  range* | Total |          Index values        |
-----|---------|-------|------------------------------|
 1   |   0-  31|   48  | 160-187,192-207,220-223      | (Slot 2 shares 28-31)
     |         |       |(Slot 3 shares 16-27) (Slot 7 shares 0-15)|
 2   |  32-  63|   48  | 28-63,240-251                |
 3   |  64-  95|   48  | 16-27,64-95,188-191          |
 4   |  96- 127|   48  | 96-127,224-239               |
 7   | 128- 159|   48  | 0-15,128-159                 |
 8   | 160- 191|   -   | (None)                       | (Slot 1 shares 160-187
     |         |       |) (Slot 3 shares 188-191)     |
 9   | 192- 223|   -   | (None)                       | (Slot 1 shares 192-207
     |         |       |,220-223)                     |
SUP  | 253-255 |   3   | 253-255                      |

*Allowed range applicable only for Generation-1 modules

switch# show module 9 recovery-steps
Failure Reason:
Insufficient indices in range 0-255. Module cannot be powered up
```

The following example uses the **show module**, **show port index-allocation**, and **show module recovery-steps** commands to display a Generation 1 module that is powered down because indices are not available in its slot. Specifically, indices 28 through 31 are taken by a 48-port card in slot 2.

```
switch# show module
Mod  Ports  Module-Type                       Model
Status
---  -----  -------------------------------- ------------------ --
1    32     1/2 Gbps FC Module                          powered-dn
2    48     1/2/4 Gbps FC Module             DS-X9148           ok
4    48     1/2/4 Gbps FC Module             DS-X9148           ok
6    0      Supervisor/Fabric-1              DS-X9530-SF1-K9    active *

Mod  Power-Status  Power Down Reason
---  ------------  --------------------------
1    powered-dn    Insufficient resources (dest Index)

switch# show port index-allocation

Module index distribution:
```

```
-----------------------------------------------------+
Slot | Allowed |      Alloted indices info            |
     |  range* | Total |          Index values        |
-----|---------|-------|------------------------------|
 1   |   0-  31|   -   | (None)                       | (Slot 2 shares 28-31)
 2   |  32-  63|   48  | 28-63,240-251                |
 3   |  64-  95|   -   | (None)                       |
 4   |  96- 127|   48  | 96-127,224-239               |
 7   | 128- 159|   -   | (None)                       |
 8   | 160- 191|   -   | (None)                       |
 9   | 192- 223|   -   | (None)                       |
SUP  | 253-255 |   3   | 253-255                      |

*Allowed range applicable only for Generation-1 modules

switch# show module 1 recovery-steps
Failure Reason:
Indices in allowed range 0 - 31 unavailable
Check "show port index-allocation" for more details

Recovery Steps:
Insert failed module in any one of the slots: 3, 7, 8, 9
```

The following example uses the **show module**, **show port index-allocation**, and **show module recovery-steps** commands to display a Generation 1 module that is powered down because of a lack of indices between 0 and 255.

```
switch# show module
Mod  Ports  Module-Type                       Model           Status
---  -----  -------------------------------- ------------------ ------------
1    48     1/2/4 Gbps FC Module             DS-X9148           ok
2    48     1/2/4 Gbps FC Module             DS-X9148           ok
3    48     1/2/4 Gbps FC Module             DS-X9148           ok
4    48     1/2/4 Gbps FC Module             DS-X9148           ok
5    0      Supervisor/Fabric-2              DS-X9530-SF2-K9    active *
6    0      Supervisor/Fabric-2              DS-X9530-SF2-K9    ha-standby
7    48     1/2/4 Gbps FC Module             DS-X9148           ok
8    24     1/2/4 Gbps FC Module             DS-X9124           ok
9    32     1/2 Gbps FC Module                            powered-dn

Mod  Power-Status  Power Down Reason
---  ------------  --------------------------
9    powered-dn    Insufficient resources (dest Index)

switch# show port index-allocation

Module index distribution:
-----------------------------------------------------+
Slot | Allowed |      Alloted indices info            |
     |  range  | Total |          Index values        |
-----|---------|-------|------------------------------|
 1   |   0-1023|   48  | 160-207                      |
 2   |   0-1023|   48  | 3-50                         |
 3   |   0-1023|   48  | 0-2,208-252                  |
 4   |   0-1023|   48  | 51-98                        |
 7   |   0-1023|   48  | 99-146                       |
 8   |   0-1023|   24  | 147-159,256-266              |
 9   |  -----  |   -   | (None)                       |
SUP  | 253-255 |   3   | 253-255                      |

switch# show module 9 recovery-steps
Failure Reason:
Insufficient indices in range 0-255. Module cannot be powered up
```

The following example uses the **show module**, **show port index-allocation**, and **show module recovery-steps** commands to display a Generation 1 module that is powered down due to non-availability of contiguous indices.

```
switch# show module
Mod  Ports  Module-Type                       Model          Status
---  -----  -------------------------------- ------------------ --
1    48     1/2/4 Gbps FC Module                          powered-dn
3    12     1/2/4 Gbps FC Module             DS-X9112           ok
4    8      IP Storage Services Module                    powered-dn
5    48     1/2/4 Gbps FC Module             DS-X9148           ok
6    48     1/2/4 Gbps FC Module             DS-X9148           ok
7    0      Supervisor/Fabric-2              DS-X9530-SF2-K9    active *
8    0      Supervisor/Fabric-2              DS-X9530-SF2-K9    ha-standby
9    24     1/2/4 Gbps FC Module             DS-X9124           ok
11   4      10 Gbps FC Module                DS-X9704           ok
12   48     1/2/4 Gbps FC Module             DS-X9148           ok
13   16     1/2 Gbps FC Module               DS-X9016           ok

Mod  Power-Status  Power Down Reason
---  ------------  --------------------------
1    powered-dn    Config down
4    powered-dn    Insufficient resources (dest Index)

Mod  Sw           Hw      World-Wide-Name(s) (WWN)
---  -----------  ------  --------------------------------------------------
3    3.0(0.322)   0.222   20:81:00:05:30:01:9c:02 to 20:8c:00:05:30:01:9c:02

switch# show port index-allocation

Module index distribution:
-------------------------------------------------------+
Slot | Allowed |      Alloted indices info             |
     |  range  | Total |          Index values         |
-----|---------|-------|-------------------------------|
 1   |  -----  |   -   | (None)                        |
 2   |  -----  |   -   | (None)                        |
 3   |   0- 255|   12  | 219-230                       |
 4   |  -----  |   -   | (None)                        |
 5   |   0- 255|   48  | 0-13,74-79,96-123             |
 6   |   0- 255|   48  | 124-150,232-252               |
 9   |   0- 255|   24  | 154-177                       |
10   |  -----  |   -   | (None)                        |
11   |   0- 255|    4  | 151-153,231                   |
12   |   0- 255|   48  | 32-73,178-183                 |
13   |   0- 255|   16  | 80-95                         |
SUP  | 253-255 |   3   | 253-255                       |

switch# show module 4 recovery-steps
Failure Reason:
Contiguous and aligned indices unavailable for Generation-1 modules
Check "show port index-allocation" for more details
Please follow the steps below:
1. Power-off module in one of the following slots: 12
2. Power-on module in slot 4 and wait till it comes online
3. Power-on the module powered-off in step 1
4. Do "copy running-config startup-config" to save this setting
```

The following example uses the **show module**, **show port index-allocation**, and **show module recovery-steps** commands to display a Generation 1 module that is powered down because of alignment, even though contiguous indices 208 through 252 are available.

```
switch# show module
```

```
Mod  Ports  Module-Type                       Model          Status
---  -----  --------------------------------- -------------- ------------
1    48     1/2/4 Gbps FC Module              DS-X9148       ok
2    48     1/2/4 Gbps FC Module              DS-X9148       ok
4    48     1/2/4 Gbps FC Module              DS-X9148       ok
5    0      Supervisor/Fabric-2               DS-X9530-SF2-K9  active *
6    0      Supervisor/Fabric-2               DS-X9530-SF2-K9  ha-standby
7    48     1/2/4 Gbps FC Module              DS-X9148       ok
9    32     1/2 Gbps FC Module                DS-X9032   powered-dn

Mod  Power-Status  Power Down Reason
---  ------------  --------------------------
9    powered-dn    Insufficient resources (dest Index)

switch# show port index-allocation

Module index distribution:
-----------------------------------------------------+
Slot | Allowed |      Alloted indices info            |
     |  range  | Total |          Index values        |
-----|---------|-------|------------------------------|
 1   |   0-1023|   48  | 160-207                      |
 2   |   0-1023|   48  | 3-50                         |
 3   |  -----  |   -   | (None)                       |
 4   |   0-1023|   48  | 51-98                        |
 7   |   0-1023|   48  | 99-146                       |
 8   |  -----  |   -   | (None)                       |
 9   |  -----  |   -   | (None)                       |
SUP  | 253-255 |   3   | 253-255                      |

switch# show module 9 recovery-steps
Failure Reason:
Contiguous and aligned indices unavailable for Generation-1 modules
Check "show port index-allocation" for more details
Recovery Steps:
Please follow the steps below:
1. Power off module in ANY ONE of the slots: 1, 4
2. Power on failed module in slot 9 and wait till it comes online
3. Power on the module that was powered off in step 1 and wait till it comes
   online
4. Do "copy running-config startup-config" to save this setting
```

show nasb

To display the Network-Accelerated Serverless Backup (NASB) configuration on the Storage Services Module (SSM), use the **show nasb** command in EXEC mode.

show nasb [**module** *slot*] [**vsan** *vsan-id*]

Syntax Description

module *slot*	Specifies the slot number with the SSM where NASB is configured.
vsan *vsan-id*	Displays information for the specified VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the NASB configuration on all SSM modules in the switch.

```
switch# show nasb
NASB: module 4 vsan 1:DPP-1, VT-nWWN=2700000530002926, pWWN=2701000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-2, VT-nWWN=2702000530002926, pWWN=2703000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-3, VT-nWWN=2704000530002926, pWWN=2705000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-4, VT-nWWN=2706000530002926, pWWN=2707000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-5, VT-nWWN=2708000530002926, pWWN=2709000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-6, VT-nWWN=270a000530002926, pWWN=270b000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-7, VT-nWWN=270c000530002926, pWWN=270d000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-8, VT-nWWN=270e000530002926, pWWN=270f000530002926 (provisioned)
NASB: module 4 vsan 3:DPP-1, VT-nWWN=26f0000530002926, pWWN=26f1000530002926 (provisioned)
NASB: module 4 vsan 3:DPP-2, VT-nWWN=26f2000530002926, pWWN=26f3000530002926 (provisioned)
NASB: module 4 vsan 3:DPP-3, VT-nWWN=26f4000530002926, pWWN=26f5000530002926 (provisioned)
NASB: module 4 vsan 3:DPP-4, VT-nWWN=26f6000530002926, pWWN=26f7000530002926 (provisioned)
NASB: module 4 vsan 3:DPP-5, VT-nWWN=26f8000530002926, pWWN=26f9000530002926 (provisioned)
NASB: module 4 vsan 3:DPP-6, VT-nWWN=26fa000530002926, pWWN=26fb000530002926 (provisioned)
NASB: module 4 vsan 3:DPP-7, VT-nWWN=26fc000530002926, pWWN=26fd000530002926 (provisioned)
NASB: module 4 vsan 3:DPP-8, VT-nWWN=26fe000530002926, pWWN=26ff000530002926 (provisioned)
NASB: module 8 vsan 3:DPP-1, VT-nWWN=2500000530002926, pWWN=2501000530002926 (not
provisioned)
NASB: module 8 vsan 3:DPP-2, VT-nWWN=2502000530002926, pWWN=2503000530002926 (not
provisioned)
NASB: module 8 vsan 3:DPP-3, VT-nWWN=2504000530002926, pWWN=2505000530002926 (not
provisioned)
NASB: module 8 vsan 3:DPP-4, VT-nWWN=2506000530002926, pWWN=2507000530002926 (not
provisioned)
NASB: module 8 vsan 3:DPP-5, VT-nWWN=2508000530002926, pWWN=2509000530002926 (not
provisioned)
```

```
NASB: module 8 vsan 3:DPP-6, VT-nWWN=250a000530002926, pWWN=250b000530002926 (not
provisioned)
NASB: module 8 vsan 3:DPP-7, VT-nWWN=250c000530002926, pWWN=250d000530002926 (not
provisioned)
NASB: module 8 vsan 3:DPP-8, VT-nWWN=250e000530002926, pWWN=250f000530002926 (not
provisioned)
```

The following example displays the NASB configuration on the SSM in slot 4.

```
switch# show nasb module 4
NASB: module 4 vsan 1:DPP-1, VT-nWWN=2700000530002926, pWWN=2701000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-2, VT-nWWN=2702000530002926, pWWN=2703000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-3, VT-nWWN=2704000530002926, pWWN=2705000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-4, VT-nWWN=2706000530002926, pWWN=2707000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-5, VT-nWWN=2708000530002926, pWWN=2709000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-6, VT-nWWN=270a000530002926, pWWN=270b000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-7, VT-nWWN=270c000530002926, pWWN=270d000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-8, VT-nWWN=270e000530002926, pWWN=270f000530002926 (provisioned)
NASB: module 4 vsan 3:DPP-1, VT-nWWN=26f0000530002926, pWWN=26f1000530002926 (provisioned)
NASB: module 4 vsan 3:DPP-2, VT-nWWN=26f2000530002926, pWWN=26f3000530002926 (provisioned)
NASB: module 4 vsan 3:DPP-3, VT-nWWN=26f4000530002926, pWWN=26f5000530002926 (provisioned)
NASB: module 4 vsan 3:DPP-4, VT-nWWN=26f6000530002926, pWWN=26f7000530002926 (provisioned)
NASB: module 4 vsan 3:DPP-5, VT-nWWN=26f8000530002926, pWWN=26f9000530002926 (provisioned)
NASB: module 4 vsan 3:DPP-6, VT-nWWN=26fa000530002926, pWWN=26fb000530002926 (provisioned)
NASB: module 4 vsan 3:DPP-7, VT-nWWN=26fc000530002926, pWWN=26fd000530002926 (provisioned)
NASB: module 4 vsan 3:DPP-8, VT-nWWN=26fe000530002926, pWWN=26ff000530002926 (provisioned)
```

The following example displays the NASB configuration on the SSM in slot 4 and VSAN 1.

```
switch# show nasb module 4 vsan 1
NASB: module 4 vsan 1:DPP-1, VT-nWWN=2700000530002926, pWWN=2701000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-2, VT-nWWN=2702000530002926, pWWN=2703000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-3, VT-nWWN=2704000530002926, pWWN=2705000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-4, VT-nWWN=2706000530002926, pWWN=2707000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-5, VT-nWWN=2708000530002926, pWWN=2709000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-6, VT-nWWN=270a000530002926, pWWN=270b000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-7, VT-nWWN=270c000530002926, pWWN=270d000530002926 (provisioned)
NASB: module 4 vsan 1:DPP-8, VT-nWWN=270e000530002926, pWWN=270f000530002926 (provisioned)
```

Table 22-6 describes the significant fields shown in the display.

Table 22-6 show nasb Field Descriptions

Field	Description
tpc module	Displays the slot number of the SSM.
vsan	Displays the VSAN number in the database associated to the NASB process.
DPP-	Displays which of the eight data path processors (DPP) is forwarding the data.
VT-nWWN=	Displays the virtual target (VT) node WWN associated with this XCopy LUN.
pWWN=	Displays the port WWN associated with this XCopy LUN.
provisioned	Implies the range of FC *slot*/*port-port* interfaces has been enabled using the **ssm enable feature nasb** command.
not provisioned	Implies the range of FC *slot*/*port-port* interfaces has not been enabled using the **ssm enable feature nasb** command.

Related Commands

Command	Description
nasb module	Enables TPC on a VSAN and maps it to the SSM where the feature has been enabled.

show ntp

To display the configured Network Time Protocol (NTP) server and peer associations, use the **show ntp** command.

show ntp {**peers** | **pending peers** | **pending-diff** | **session-status** | **statistics** [**io** | **local** | **memory** | **peer** {**ipaddr** *ip-address* | **name** *peer-name*}] | **timestamp-status**}

Syntax Description

peers	Displays all the peers.
pending peers	Displays pending NTP configuration changes on all peers.
pending-diff	Displays the differences between the pending NTP configuration changes and the active NTP configuration.
session-status	Displays the Cisco Fabric Services (CFS) session status.
statistics	Displays the NTP statistics
io	Displays the input/output statistics.
local	Displays the counters maintained by the local NTP.
memory	Displays the statistics counters related to memory code.
peer	Displays the per-peer statistics counter of a peer.
ipaddr *ip-address*	Displays the peer statistics for the specified IP address.
name *peer-name*	Displays the peer statistics for the specified peer name.
timestamp-status	Displays if the timestamp check is enabled.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
2.0(1b)	Added the **pending**, **pending-diff**, and **session-status** keywords.

Usage Guidelines

None.

Examples

The following example displays the NTP peer information.

```
switch# show ntp peers
-----------------------------------------
  Peer IP Address               Serv/Peer
-----------------------------------------
  10.20.10.2                    Server
  10.20.10.0                    Peer
```

The following example displays the NTP IO statistics.

```
switch# show ntp statistics io
time since reset:     11152
receive buffers:      9
free receive buffers: 9
used receive buffers: 9
low water refills:    0
dropped packets:      0
ignored packets:      0
received packets:     3
packets sent:         2
packets not sent:     0
interrupts handled:   3
received by int:      3
```

The following example displays the NTP local statistics.

```
switch# show ntp statistics local
system uptime:          11166
time since reset:       11166
bad stratum in packet:  0
old version packets:    4
new version packets:    0
unknown version number: 0
bad packet format:      0
packets processed:      0
bad authentication:     0
```

The following example displays the NTP memory statistics information.

```
switch# show ntp statistics memory
time since reset:     11475
total peer memory:    15
free peer memory:     15
calls to findpeer:    0
new peer allocations: 0
peer demobilizations: 0
hash table counts:      0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
```

The following example displays the NTP peer statistics information using the IP address of the peer.

```
switch# show ntp statistics peer ipaddr 10.1.1.1
```

The following example displays the NTP peer statistics information using the name of the peer.

```
switch# show ntp statistics peer name Peer1
```

The following example displays the NTP timestamp status information.

```
switch# show ntp timestamp-status
Linecard 9 does not support Timestamp check.
```

Related Commands

Command	Description
ntp	Configures NTP parameters.

show port index-allocation

To display port index allocation information, use the **show port index-allocation** command.

show port index-allocation [startup]

Syntax Description

startup	Displays port index allocation information at startup.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

All software releases prior to Cisco SAN-OS Release 3.0(1) support Generation 1 hardware. Cisco SAN-OS Release 3.0(1) and later support Generation 2 hardware. You can combine Generation 1 and Generation 2 switching modules, with either Supervisor-1 modules or Supervisor-2 modules. However, combining switching modules and supervisor modules has the following limitations:

- Supervisor-1 modules only support a maximum of 256 port indexes, regardless of type of switching modules.
- Supervisor-2 modules support a maximum of 1024 port indexes when all switching modules in the chassis are Generation 2.
- Supervisor-2 modules only support a maximum of 256 port indexes when both Generation 1 and Generation 2 switching modules are installed in the chassis.

Note On a switch where the maximum number of port indexes is 256, any module that exceeds that limit does not power up.

Examples

The following example displays port index allocation information at startup on a Cisco MDS switch with only Generation 1 switching modules installed.

```
ips-hac1# show port index-allocation startup

Startup module index distribution:
-------------------------------------------------------+
Slot | Allowed |      Alloted indices info             |
     |  range  | Total |          Index values         |
-----|---------|-------|-------------------------------|
 1   |   0-  31|   32  | 0-31                          |
 2   |  32-  63|   32  | 32-63                         |
 3   |  64-  95|   32  | 64-95                         |
SUP  |  -----  |    3  | 253-255                       |
```

The following example displays current port index allocation on a Cisco MDS switch with only Generation 1 switching modules installed.

```
switch# show port index-allocation

Module index distribution:
-------------------------------------------------------+
Slot | Allowed |      Alloted indices info             |
     |  range  | Total |          Index values         |
-----|---------|-------|-------------------------------|
 1   |   0-  31|   32  | 0-31                          |
 2   |  32-  63|   32  | 32-63                         |
 3   |  64-  95|   32  | 64-95                         |
 4   |  96- 127|   -   | (None)                        |
SUP  |  -----  |    3  | 253-255                       |
```

The following example displays port index allocation information at startup on a Cisco MDS switch with Generation 1 and Generation 2 switching modules installed.

```
switch# show port index-allocation startup
Startup module index distribution:
-------------------------------------------------------+
Slot | Allowed |      Alloted indices info             |
     |  range  | Total |          Index values         |
-----|---------|-------|-------------------------------|
 4   |   0- 255|   32  | 0-31                          |
 5   |   0- 255|   32  | 32-63                         |
 6   |   0- 255|   32  | 96-127                        |
 9   |   0- 255|   24  | 64-87                         |
SUP  |  -----  |    3  | 253-255                       |
```

The following example shows the current port index allocation on a Cisco MDS switch with Generation 1 and Generation 2 switching modules installed.

```
switch# show port index-allocation

Module index distribution:
-------------------------------------------------------+
Slot | Allowed |      Alloted indices info             |
     |  range  | Total |          Index values         |
-----|---------|-------|-------------------------------|
 1   |   0- 255|   -   | (None)                        |
 2   |   0- 255|   -   | (None)                        |
 3   |   0- 255|   -   | (None)                        |
 4   |   0- 255|   32  | 0-31                          |
 5   |   0- 255|   32  | 32-63                         |
 6   |   0- 255|   32  | 96-127                        |
 9   |   0- 255|   24  | 64-87                         |
10   |   0- 255|   -   | (None)                        |
11   |   0- 255|   -   | (None)                        |
12   |   0- 255|   -   | (None)                        |
13   |   0- 255|   -   | (None)                        |
SUP  |  -----  |    3  | 253-255                       |
```

show port-channel

Use the **show port-channel** command to view information about existing PortChannel configurations.

show port-channel {**compatibility-parameters** | **consistency** [**detail**] | **database** [**interface port-channel** *port-channel-number*] | **summary** | **usage**}

Syntax Description

compatibility-parameters	Displays compatibility parameters.
consistency	Displays the database consistency information of all modules.
detail	Displays detailed database consistency information.
database	Displays PortChannel database information.
interface port-channel *port-channel-number*	Specifies the PortChannel number. The range is 1 to 256.
summary	Displays PortChannel summary.
usage	Displays PortChannel number usage.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	• Increased the **interface port-channel** range to 256. • Modified the output of the **compatibility-parameters** option.

Usage Guidelines

None.

Examples

The following example displays the PortChannel summary.

```
switch# show port-channel summary
NEW
```

The following example displays the PortChannel compatibility parameters.

```
switch# show port-channel compatibility-parameters
Parameters that have to be consistent across all members in a port-channel.

1. physical port layer

Members must have the same interface type, such as fibre channel, ethernet
or fcip.

2. port mode
```

Members must have the same port mode configured, either E or AUTO. If they are configured in AUTO port mode, they have to negotiate E mode when they come up. If a member negotiates a different mode, it will be suspended.

3. trunk mode

Members must have the same trunk mode configured. If they are configured in AUTO trunking mode, they have to negotiate the same trunking mode when they come up. If a member negotiates a different mode, it will be suspended.

4. speed

Members must have the same speed configured. If they are configured in AUTO speed, they have to negotiate the same speed when they come up. If a member negotiates a different speed, it will be suspended.

5. MTU

Members have to have the same MTU configured. This only applies to ethernet port-channel.

6. ethernet port index

This only applies to ethernet port-channel. Each ethernet port-channel could only have two ethernet ports. They must be in the same slot, their port indices must be adjacent and the lower number must be odd. Example: Gigabitethernet 8/5 - 6.

7. rate mode

Members must have the same rate mode configured. Rate Mode applies only to isola FC ports

8. Maximum Speed Mismatch

Members must be configured to auto-negotiate to the same maximum speed.

9. Resources Unavailable

Members must be able to acquire resources required to maintain compatibility. Check shared resources like speed, rate-mode and port mode.

10. Out of Service

Members must be in-service.

11. port VSAN

Members must have the same port VSAN.

12. port allowed VSAN list

Members must have the same port allowed VSAN list.

13. IP address

Members must not have IP address configured. This only applies to ethernet port-channel.

14. IPv6 configuration

Members must not have any IPv6 configuration. This only applies to ethernet port-channel.

```
15. port-security active bindings

Members must all be permitted by the activated port-security bindings and
fabric-bindings in all the allowed VSANs.

16. FC receive buffer size

Members must have the same fc receive buffer size. If the configured
receive buffer size is not compatible with the port capability then the
port will be error disabled

17. IP ACLs

Members must not have IP ACLs configured individually on them. This only
applies to ethernet port-channel.

18. sub interfaces

Members must not have sub-interfaces.

19. Access VLAN

Members must have same Access VLAN configured.

20. Native VLAN

Members must have same Native VLAN configured.

21. Duplex Mode

Members must have same Duplex Mode configured.

22. Ethernet Layer

Members must have same Ethernet Layer (switchport/no-switchport) configured.


23. Span Port

Members cannot be SPAN ports.
```

The following example displays the PortChannel database.

```
switch# show port-channel database
port-channel 2
    Administrative channel mode is on
    Operational channel mode is on
    Last membership update succeeded
    First operational port is fc2/2
    1 port in total, 1 port up
    Ports:   fc2/2    [up]
```

The **show port-channel consistency** command has two options—without detail **and detail**.

Command Without Details

```
switch# show port-channel consistency
Database is consistent
switch#
```

Command With Details

```
switch# show port-channel consistency detail
Authoritative port-channel database:
================================================
```

```
totally 1 port-channels
port-channel 2:
    1 ports, first operational port is fc2/2
    fc2/2    [up]
================================================
database 1: from module 5
================================================
totally 1 port-channels

port-channel 2:
    1 ports, first operational port is fc2/2
    fc2/2    [up]
================================================
database 2: from module 2
================================================
totally 1 port-channels
port-channel 2:
    1 ports, first operational port is fc2/2
    fc2/2    [up]
================================================
```

The **show port-channel usage** command displays details of the used and unused PortChannel numbers.

PortChannel Usage

```
switch# show port-channel usage
Totally 2 port-channel numbers used
====================================
Used  :   3, 9
Unused:   1-2, 4-8, 10-256
```

show port-resources module

To display information about port resources in a Generation 2 module, use the **show port-resources** command.

show port-resources module *slot*

Syntax Description

slot	Specifies the module number. The range is 1 to 6.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the Generation 2 module shared resources configuration.

```
switch# show port-resources module 2
Module 2
Available dedicated buffers are 5164

Port-Group 1
 Total bandwidth is 12.8 Gbps
 Total shared bandwidth is 4.8 Gbps
 Allocated dedicated bandwidth is 8.0 Gbps
--------------------------------------------------------------------------
Interfaces in the Port-Group B2B Credit Bandwidth Rate Mode
                               Buffers (Gbps)
--------------------------------------------------------------------------
fc2/1                                16       4.0 shared
fc2/2                                16       4.0 shared
fc2/3                                16       4.0 shared
fc2/4                                16       4.0 shared
fc2/5                                16       4.0 dedicated
fc2/6                                16       4.0 dedicated

Port-Group 2
 Total bandwidth is 12.8 Gbps
 Total shared bandwidth is 4.8 Gbps
 Allocated dedicated bandwidth is 8.0 Gbps
--------------------------------------------------------------------------
Interfaces in the Port-Group B2B Credit Bandwidth Rate Mode
                               Buffers (Gbps)
--------------------------------------------------------------------------
fc2/7                                16       4.0 shared
```

```
fc2/8                                 16       4.0 shared
fc2/9                                 16       4.0 shared
fc2/10                                16       4.0 shared
fc2/11                                16       4.0 dedicated
fc2/12                                16       4.0 dedicated

Port-Group 3
 Total bandwidth is 12.8 Gbps
 Total shared bandwidth is 4.8 Gbps
 Allocated dedicated bandwidth is 8.0 Gbps
--------------------------------------------------------------------
Interfaces in the Port-Group B2B Credit Bandwidth Rate Mode
                                  Buffers (Gbps)
--------------------------------------------------------------------
fc2/13                                16       4.0 shared
fc2/14                                16       4.0 shared
fc2/15                                16       4.0 shared
fc2/16                               250       4.0 dedicated
fc2/17                                16       2.0 dedicated
fc2/18                                16       2.0 dedicated

Port-Group 4
 Total bandwidth is 12.8 Gbps
 Total shared bandwidth is 0.8 Gbps
 Allocated dedicated bandwidth is 12.0 Gbps
--------------------------------------------------------------------
Interfaces in the Port-Group B2B Credit Bandwidth Rate Mode
                                  Buffers (Gbps)
--------------------------------------------------------------------
fc2/19                                16       1.0 shared
fc2/20                                16       1.0 shared
fc2/21                                16       1.0 shared
fc2/22                                16       4.0 dedicated
fc2/23                                16       4.0 dedicated
fc2/24                                16       4.0 dedicated
```

Related Commands

Command	Description
show module	Verifies the status of a module.

show port-security

To display configured port security feature information, use the **show port-security database** command.

show port-security
{**database** [**active** [**vsan** *vsan-id*]] | **fwwn** *fwwn-id* **vsan** *vsan-id* | **interface** {**fc** *slot/port* | **port-channel** *port*} **vsan** *vsan-id* | **vsan** *vsan-id*] |
pending [**vsan** *vsan-id*] |
pending-diff [**vsan** *vsan-id*] |
statistics [**vsan** *vsan-id*] |
status [**vsan** *vsan-id*] |
violations [**last** *count* | **vsan** *vsan-id*]}

Syntax Description

database	Displays database-related port security information.
active	Displays the activated database information.
vsan *vsan-id*	Displays information for the specified database.
fwwn *fwwn-id*	Displays information for the specified fabric WWN.
interface	Displays information for an interface.
fc *slot/port*	Displays information for the specified Fibre Channel interface.
port-channel *port*	Displays information for the specified PortChannel interface. The range is 1 to 128.
pending	Displays the server address pending configuration.
pending-diff	Displays the server address pending configuration differences with the active configuration.
statistics	Displays port security statistics.
status	Displays the port security status on a per VSAN basis.
violations	Displays violations in the port security database.
last *count*	Displays the last number of lines in the database. The range is 1 to 100.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.
2.0(1b)	Added the **pending** and **pending-diff** keywords.

Usage Guidelines

The access information for each port can be individually displayed. If you specify the fwwn or interface options, all devices that are paired in the active database (at that point) with the given fWWN or the interface are displayed.

The **show port-security** command issued with the **last** *number* option displays only the specified number of entries that appear first.

Examples

The following example displays the contents of the port security database.

```
switch# show port-security database
-------------------------------------------------------------------------------------
VSAN    Logging-in Entity             Logging-in Point(     Interface)
-------------------------------------------------------------------------------------
1       21:00:00:e0:8b:06:d9:1d(pwwn) 20:0d:00:05:30:00:95:de(fc1/13)
1       50:06:04:82:bc:01:c3:84(pwwn) 20:0c:00:05:30:00:95:de(fc1/12)
2       20:00:00:05:30:00:95:df(swwn) 20:0c:00:05:30:00:95:de(port-channel 128)
3       20:00:00:05:30:00:95:de(swwn) 20:01:00:05:30:00:95:de(fc1/1)
[Total 4 entries]
```

The following example displays the output of the active port security database in VSAN 1.

```
switch# show port-security database vsan 1
-------------------------------------------------------------------------------
Vsan   Logging-in Entity              Logging-in Point        (Interface)
-------------------------------------------------------------------------------
1                  *                  20:85:00:44:22:00:4a:9e (fc3/5)
1      20:11:00:33:11:00:2a:4a(pwwn)  20:81:00:44:22:00:4a:9e (fc3/1)
[Total 2 entries]
```

The following example displays the active database.

```
switch# show port-security database active
-------------------------------------------------------------------------------------
VSAN    Logging-in Entity             Logging-in Point(     Interface)     Learnt
-------------------------------------------------------------------------------------
1       21:00:00:e0:8b:06:d9:1d(pwwn) 20:0d:00:05:30:00:95:de(fc1/13)          Yes
1       50:06:04:82:bc:01:c3:84(pwwn) 20:0c:00:05:30:00:95:de(fc1/12)          Yes
2       20:00:00:05:30:00:95:df(swwn) 20:0c:00:05:30:00:95:de(port-channel 128)Yes
3       20:00:00:05:30:00:95:de(swwn) 20:01:00:05:30:00:95:de(fc1/1)
[Total 4 entries]
```

The following example displays the wildcard fwwn port security in VSAN 1.

```
switch# show port-security database fwwn 20:85:00:44:22:00:4a:9e vsan 1
Any port can login thru' this fwwn
```

The following example displays the configured fWWN port security in VSAN 1.

```
switch# show port-security database fwwn 20:01:00:05:30:00:95:de vsan 1
20:00:00:0c:88:00:4a:e2(swwn)
```

The following example displays the interface port information in VSAN 2.

```
switch# show port-security database interface fc 1/1 vsan 2
20:00:00:0c:88:00:4a:e2(swwn)
```

The following example displays the port security statistics.

```
switch# show port-security statistics
Statistics For VSAN: 1
-----------------------
Number of pWWN permit: 2
Number of nWWN permit: 2
Number of sWWN permit: 2
Number of pWWN deny  : 0
Number of nWWN deny  : 0
Number of sWWN deny  : 0
```

```
Total Logins permitted  : 4
Total Logins denied     : 0
Statistics For VSAN: 2
------------------------
Number of pWWN permit: 0
Number of nWWN permit: 0
Number of sWWN permit: 2
Number of pWWN deny  : 0
Number of nWWN deny  : 0
Number of sWWN deny  : 0
...
```

The following example displays the status of the active database and the autolearn configuration.

```
switch# show port-security status
VSAN 1 :Activated database, auto-learning is enabled
VSAN 2 :No Active database, auto-learning is disabled
...
```

The following example displays the previous 100 violations.

```
switch# show port-security violations

-------------------------------------------------------------------------------------------
VSAN    Interface      Logging-in Entity             Last-Time              [Repeat count]
-------------------------------------------------------------------------------------------
1       fc1/13         21:00:00:e0:8b:06:d9:1d(pwwn) Jul  9 08:32:20 2003   [20]
                       20:00:00:e0:8b:06:d9:1d(nwwn)
1       fc1/12         50:06:04:82:bc:01:c3:84(pwwn) Jul  9 08:32:20 2003   [1]
                       50:06:04:82:bc:01:c3:84(nwwn)
2       port-channel 1 20:00:00:05:30:00:95:de(swwn) Jul  9 08:32:40 2003   [1]
[Total 2 entries]
```

Related Commands

Command	Description
port-security	Configures port security parameters.

show processes

To display general information about all the processes, use the **show processes** command.

show processes [**cpu** | **log** [**details** | **pid** *process-id*] | **memory**]

Syntax Description

cpu	Displays processes CPU information.
log	Displays information about process logs.
details	Displays detailed process log information.
pid *process-id*	Displays process information about a specific process ID. The range is 0 to 2147483647.
memory	Displays processes memory information.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following examples display general information about system processes.

```
switch# show process
PID    State  PC        Start_cnt    TTY   Process
-----  -----  --------  -----------  ----  -------------
  868      S  2ae4f33e            1     -  snmpd
  869      S  2acee33e            1     -  rscn
  870      S  2ac36c24            1     -  qos
  871      S  2ac44c24            1     -  port-channel
  872      S  2ac7a33e            1     -  ntp
    -     ER         -            1     -  mdog
    -     NR         -            0     -  vbuilder

PID: process ID.

State: process state

       D   uninterruptible sleep (usually IO)
       R   runnable (on run queue)
       S   sleeping
       T   traced or stopped
       Z   a defunct ("zombie") process

    NR  not-running
```

```
    ER  should be running but currently not-running

PC: Current program counter in hex format

Start_cnt: how many times a process has been started.

TTY: Terminal that controls the process. A "-" usually means a daemon not
     running on any particular tty.

Process: name of the process.

=====================================================

2. show processes cpu (new output)
Description: show cpu utilization information about the processes.

switch# show processes cpu

PID    Runtime(ms)  Invoked   uSecs  1Sec   Process
-----  -----------  --------  -----  -----  -----------
  842         3807    137001     27    0.0  sysmgr
 1112         1220     67974     17    0.0  syslogd
 1269          220     13568     16    0.0  fcfwd
 1276         2901     15419    188    0.0  zone
 1277          738     21010     35    0.0  xbar_client
 1278         1159      6789    170    0.0  wwn
 1279          515     67617      7    0.0  vsan

Runtime(ms): cpu time the process has used, expressed in milliseconds
Invoked: Number of times the process has been invoked.
uSecs:  Microseconds of CPU time in average for each process invocation.
1Sec:    CPU utilization in percentage for the last 1 second.

=====================================================
3. show processes mem
Description: show memory information about the processes.

PID    MemAlloc  StackBase/Ptr      Process
-----  --------  -----------------  ----------------
 1277    120632  7ffffcd0/7fffefe4  xbar_client
 1278     56800  7ffffce0/7ffffb5c  wwn
 1279   1210220  7ffffce0/7ffffbac  vsan
 1293    386144  7ffffcf0/7fffebd4  span
 1294   1396892  7ffffce0/7fffdff4  snmpd
 1295    214528  7ffffcf0/7ffff904  rscn
 1296     42064  7ffffce0/7ffffb5c  qos

MemAlloc: total memory allocated by the process.
StackBase/Ptr: process stack base and current stack pointer in hex format

=====================================================
3. show processes log
Description: list all the process logs

switch# show processes log
Process           PID     Normal-exit  Stack-trace  Core     Log-create-time
----------------  ------  -----------  -----------  -------  ---------------
fspf              1339             N            Y        N  Jan  5 04:25
lichen               1559             N            Y        N  Jan  2 04:49
rib               1741             N            Y        N  Jan  1 06:05

Normal-exit: whether or not the process exited normally.
Stack-trace: whether or not there is a stack trace in the log.
Core: whether or not there exists a core file.
```

```
Log-create-time: when the log file got generated.
```

The following example displays the detail log information about a particular process.

```
switch# show processes log pid 1339
Service: fspf
Description: FSPF Routing Protocol Application

Started at Sat Jan  5 03:23:44 1980 (545631 us)
Stopped at Sat Jan  5 04:25:57 1980 (819598 us)
Uptime: 1 hours 2 minutes 2 seconds

Start type: SRV_OPTION_RESTART_STATELESS (23)
Death reason: SYSMGR_DEATH_REASON_FAILURE_SIGNAL (2)
Exit code: signal 9 (no core)
CWD: /var/sysmgr/work

Virtual Memory:

    CODE      08048000 - 0809A100
    DATA      0809B100 - 0809B65C
    BRK       0809D988 - 080CD000
    STACK     7FFFFD20
    TOTAL     23764 KB

Register Set:

    EBX 00000005         ECX 7FFFF8CC         EDX 00000000
    ESI 00000000         EDI 7FFFF6CC         EBP 7FFFF95C
    EAX FFFFFDFE         XDS 8010002B         XES 0000002B
    EAX 0000008E (orig)  EIP 2ACE133E         XCS 00000023
    EFL 00000207         ESP 7FFFF654         XSS 0000002B

Stack: 1740 bytes. ESP 7FFFF654, TOP 7FFFFD20

0x7FFFF654: 00000000 00000008 00000003 08051E95 ................
0x7FFFF664: 00000005 7FFFF8CC 00000000 00000000 ................
0x7FFFF674: 7FFFF6CC 00000001 7FFFF95C 080522CD ........\....".."
0x7FFFF684: 7FFFF9A4 00000008 7FFFFC34 2AC1F18C ........4......*
```

show qos

To display the current QoS settings along with a the number of frames marked high priority, use the **show qos** command.

show qos {**class-map [name** *class-name*] | **dwrr** | **policy-map [name** *policy-name*] | **service policy** [**interface fc** *slot*/*port* | **vsan** *vsan-id*] | **statistics**}

Syntax Description

class-map	Displays QoS class maps.
name *class-name*	Specifies a class map name. Maximum length is 63 alpha-numeric characters.
dwrr	Displays deficit weighted round robin queue weights.
policy-map	Displays QoS policy-maps.
name *policy-name*	Specifies a policy map name. Maximum length is 63 alpha-numeric characters.
service policy	Displays QoS service policy associations.
interface fc *slot*/*port*	Specifies a Fibre Channel interface.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
statistics	Displays QoS related statistics.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

To access all but the **statistics** option for this command, you must perform the **qos enable** command.

Examples

The following example displays the contents of all class maps.

```
switch# show qos class-map
qos class-map MyClass match-any
    match dest-wwn 20:01:00:05:30:00:28:df
    match src-wwn 23:15:00:05:30:00:2a:1f
    match src-intf fc2/1
qos class-map Class2 match-all
    match src-intf fc2/14
qos class-map Class3 match-all
    match src-wwn 20:01:00:05:30:00:2a:1f
```

The following example displays the contents of a specified class map.

```
switch# show qos class-map name MyClass
qos class-map MyClass match-any
    match dest-wwn 20:01:00:05:30:00:28:df
    match src-wwn 23:15:00:05:30:00:2a:1f
    match src-intf fc2/1
```

The following example displays all configured policy maps.

```
switch# show qos policy-map
qos policy-map MyPolicy
    class MyClass
    priority medium

qos policy-map Policy1
    class Class2
    priority low
```

The following example displays a specified policy map.

```
switch# show qos policy-map name MyPolicy
qos policy-map MyPolicy
    class MyClass
        priority medium
```

The following example displays scheduled DWRR configurations

```
switch# show qos dwrr
qos dwrr-q high weight 50
qos dwrr-q medium weight 30
qos dwrr-q low weight 20
```

The following example displays all applied policy maps.

```
switch# show qos service policy
qos service policy MyPolicy vsan 1
qos service policy Policy1 vsan 4
```

The following example displays QoS statistics.

```
switch# show qos statistics
Total number of FC frames transmitted from the Supervisor= 301431
Number of highest-priority FC frames transmitted         = 137679
Current priority of FC control frames = 7    (0 = lowest; 7 = highest)
```

show radius

To display the RADIUS Cisco Fabric Services (CFS) distribution status and other details, use the **show radius** command.

show radius {**distribution status** | **pending** | **pending-diff**}

Syntax Description

distribution status	Displays the status of the RADIUS CFS distribution.
pending	Displays the pending configuration that is not yet applied.
pending-diff	Displays the difference between the active configuration and the pending configuration.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the RADIUS distribution status.

```
switch# show radius distribution status
session ongoing: no
session db: does not exist
merge protocol status: merge activation done

last operation: none
last operation status: none
```

Related Commands

Command	Description
radius distribute	Enables RADIUS CFS distribution.

show radius-server

To display all configured RADIUS server parameters, use the **show radius-server** command.

show radius-server [*server-name* | *ipv4-address* | *ipv6-address*]
[**directed-request** | **groups** | **sorted** | **statistics**]

Syntax Description

server-name	Specifies the RADIUS server DNS name. The maximum character size is 256.
ipv4-address	Specifies the RADIUS server IP address in the format *A.B.C.D*.
ipv6-address	Specifies the RADIUS server IP address in the format *X:X::X*.
directed-request	Displays an enabled directed request RADIUS server configuration.
groups	Displays configured RADIUS server group information.
sorted	Displays RADIUS server information sorted by name.
statistics	Displays RADIUS statistics for the specified RADIUS server.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	• Added the *server-name*, *ipv4-address*, and *ipv6-address* arguments. • Added the **directed-request** and **statistics** options.

Usage Guidelines

Only administrators can view the RADIUS preshared key.

Examples

The following example shows the output of the **show radius-server** command.

```
switch# show radius-server
Global RADIUS shared secret:Myxgqc
retransmission count:5
timeout value:10

following RADIUS servers are configured:
        myradius.cisco.users.com:
                available for authentication on port:1812
                available for accounting on port:1813
        172.22.91.37:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:23MHcUnD
        10.10.0.0:
                available for authentication on port:1812
                available for accounting on port:1813
               RADIUS shared secret:hostkey----> for administrators only
```

show rlir

To display the information about Registered Link Incident Report (RLIR), Link Incident Record Registration (LIRR), and Distribute Registered Link Incident Record (DRLIR) frames, use the **show rlir** command.

show rilr {**erl** [**vsan** *vsan-id*] | **history** | **recent** [**interface fc** *slot/port* | **portnumber** *port-number*] | **statistics** [**vsan** *vsan-id*]}

Syntax Description

erl *vsan-id*	Displays Established Registration List (ERL) information.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
history	Displays link incident history.
recent	Displays recent link incident.
interface fc *slot/port*	Specifies a Fibre Channel interface at a slot and port.
portnumber *port-number*	Specifies a port number for the link incidents. The range is 1 to 224.
statistics	Displays RLIR statistics.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(2)	This command was introduced.

Usage Guidelines

If available, the host timestamp (marked by the *) is printed along with the switch timestamp. If the host timestamp is not available, only the switch timestamp is printed.

Examples

The following example displays the RLIR statistics for all VSANs.

```
switch# show rlir statistics

Statistics for VSAN: 1
------------------------

Number of LIRR received      = 0
Number of LIRR ACC sent      = 0
Number of LIRR RJT sent      = 0
Number of RLIR sent          = 0
Number of RLIR ACC received  = 0
Number of RLIR RJT received  = 0
Number of DRLIR received     = 0
Number of DRLIR ACC sent     = 0
Number of DRLIR RJT sent     = 0
Number of DRLIR sent         = 0
```

```
Number of DRLIR ACC received = 0
Number of DRLIR RJT received = 0


Statistics for VSAN: 4
-------------------------

Number of LIRR received      = 0
Number of LIRR ACC sent      = 0
Number of LIRR RJT sent      = 0
Number of RLIR sent          = 0
Number of RLIR ACC received  = 0
Number of RLIR RJT received  = 0
Number of DRLIR received     = 0
Number of DRLIR ACC sent     = 0
Number of DRLIR RJT sent     = 0
Number of DRLIR sent         = 0
Number of DRLIR ACC received = 0
Number of DRLIR RJT received = 0


Statistics for VSAN: 61
-------------------------

Number of LIRR received      = 0
Number of LIRR ACC sent      = 0
Number of LIRR RJT sent      = 0
Number of RLIR sent          = 0
Number of RLIR ACC received  = 0
Number of RLIR RJT received  = 0
Number of DRLIR received     = 0
Number of DRLIR ACC sent     = 0
Number of DRLIR RJT sent     = 0
Number of DRLIR sent         = 0
Number of DRLIR ACC received = 0
Number of DRLIR RJT received = 0
```

The following example displays the RLIR statistics for a specified VSAN.

```
switch# show rlir statistics vsan 4

Statistics for VSAN: 4
-------------------------

Number of LIRR received      = 0
Number of LIRR ACC sent      = 0
Number of LIRR RJT sent      = 0
Number of RLIR sent          = 0
Number of RLIR ACC received  = 0
Number of RLIR RJT received  = 0
Number of DRLIR received     = 0
Number of DRLIR ACC sent     = 0
Number of DRLIR RJT sent     = 0
Number of DRLIR sent         = 0
Number of DRLIR ACC received = 0
Number of DRLIR RJT received = 0
```

The following example displays the RLIR statistics for all ERLs.

```
switch# show rlir erl

Established Registration List for VSAN: 2
-------------------------------------------
FC-ID       LIRR FORMAT    REGISTERED FOR
```

```
---------------------------------------------
0x0b0200    0x18           always receive
Total number of entries = 1

Established Registration List for VSAN: 100
---------------------------------------------
FC-ID       LIRR FORMAT    REGISTERED FOR
---------------------------------------------
0x0b0500    0x18           conditional receive
0x0b0600    0x18           conditional receive
Total number of entries = 2
```

The following example displays the ERLs for the specified VSAN.

```
switch# show rlir erl vsan 100
Established Registration List for VSAN: 100
---------------------------------------------
FC-ID       LIRR FORMAT    REGISTERED FOR
---------------------------------------------
0x0b0500    0x18           conditional receive
0x0b0600    0x18           conditional receive

Total number of entries = 2
```

The following example displays the RLIR history.

```
switch# show rlir history
Link incident history
-------------------------------------------------------------------------------
*Host Time Stamp
 Switch Time Stamp          Port   Interface   Link Incident
-------------------------------------------------------------------------------
*Sun Nov 30 21:47:28 2003
 Sun Nov 30 13:47:55 2003     2        fc1/2   Implicit Incident
*Sun Nov 30 22:00:47 2003
 Sun Nov 30 14:01:14 2003     2        fc1/2   NOS Received
*Sun Nov 30 22:00:55 2003
 Sun Nov 30 14:01:22 2003     2        fc1/2   Implicit Incident
*Mon Dec 1 20:14:26 2003
 Mon Dec  1 12:14:53 2003     4        fc1/4   Implicit Incident
*Mon Dec 1 20:14:26 2003
 Mon Dec  1 12:14:53 2003     4        fc1/4   Implicit Incident
*Thu Dec 4 04:43:32 2003
 Wed Dec  3 20:43:59 2003     2        fc1/2   NOS Received
*Thu Dec 4 04:43:41 2003
 Wed Dec  3 20:44:08 2003     2        fc1/2   Implicit Incident
*Thu Dec 4 04:46:53 2003
 Wed Dec  3 20:47:20 2003     2        fc1/2   NOS Received
*Thu Dec 4 04:47:05 2003
 Wed Dec  3 20:47:32 2003     2        fc1/2   Implicit Incident
*Thu Dec 4 04:48:07 2003
 Wed Dec  3 20:48:34 2003     2        fc1/2   NOS Received
*Thu Dec 4 04:48:39 2003
 Wed Dec  3 20:49:06 2003     2        fc1/2   Implicit Incident
*Thu Dec 4 05:02:20 2003
 Wed Dec  3 21:02:47 2003     2        fc1/2   NOS Received
*Thu Dec 4 05:02:29 2003
 Wed Dec  3 21:02:56 2003     2        fc1/2   Implicit Incident
*Thu Dec 4 05:02:47 2003
 Wed Dec  3 21:03:14 2003     4        fc1/4   NOS Received
*Thu Dec 4 05:02:54 2003
 Wed Dec  3 21:03:21 2003     4        fc1/4   Implicit Incident
*Thu Dec 4 05:02:54 2003
 Wed Dec  3 21:03:21 2003     4        fc1/4   Implicit Incident
```

...

The following example displays recent RLIRs for a specified interface.

```
switch# show rlir recent interface fc1/1
Recent link incident records
-------------------------------------------------------------------------------
*Host Time Stamp
 Switch Time Stamp          Port   Interface   Link Incident
-------------------------------------------------------------------------------


*Thu Dec 4 05:02:29 2003
 Wed Dec  3 21:02:56 2003     2        fc1/2   Implicit Incident
*Thu Dec 4 05:02:54 2003
 Wed Dec  3 21:03:21 2003     4        fc1/4   Implicit Incident
switch#
```

The following example displays the recent RLIRs for a specified port number.

```
switch# show rlir recent portnumber 1
Recent link incident records
-------------------------------------------------------------------------------
*Host Time Stamp
 Switch Time Stamp          Port   Interface   Link Incident
-------------------------------------------------------------------------------


*Thu Dec 4 05:02:29 2003
 Wed Dec  3 21:02:56 2003     2        fc1/2   Implicit Incident
*Thu Dec 4 05:02:54 2003
 Wed Dec  3 21:03:21 2003     4        fc1/4   Implicit Incident
```

show rmon

To display the remote monitoring (RMON) configuration, use the **show rmon** command.

show rmon {**alarms** | **events** | **hcalarms** | **logs**}

Syntax Description

alarms	Displays the configured RMON alarms.
events	Displays the configured RMON events.
hcalarms	Displays the high capacity (HC) RMON alarms.
logs	Displays the RMON event logs.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.
2.1(2)	Addedthe **logs** option.
3.0(1)	Added the **hcalarms** option.

Usage Guidelines

To configure a high capacity RMON alarm, use the CISCO-HC-ALARM-MIB.

Examples

The following example displays the configured RMON alarms.

```
switch# show rmon alarms
Alarm 20 is active, owned by test
 Monitors 1.3.6.1.2.1.2.2.1.16.16777216 every 256000 second(s)
 Taking delta samples, last value was 17
 Rising threshold is 15, assigned to event 1
 Falling threshold is 0, assigned to event 0
 On startup enable rising or falling alarm
```

The following example displays the configured RMON events.

```
switch# show rmon events
Event 2 is active, owned by Test2
 Description is CriticalErrors
 Event firing causes log and trap to community eventtrap, last fired 1
```

The following example displays the high capacity RMON alarms.

```
switch# show rmon hcalarms
High Capacity Alarm 10 is active, owned by Testuser
 Monitors 1.3.6.1.2.1.31.1.1.1.6.16785408 every 300 second(s)
 Taking absolute samples, last value was 0 (valuePositive)
 Rising threshold low is 4294967295 & high is 15 (valuePositive)
```

```
Rising threshold assigned to event 1
Falling threshold low is 0 & high is 0 (valueNotAvailable)
Falling threshold assigned to event 0
On startup enable rising alarm
Number of Failed Attempts is 0
```

Related Commands

Command	Description
rmon alarm	Configures RMON alarms.
rmon event	Configures RMON events.

show role

To display roles (and their associated rules) configured on the switch, including those roles that have not yet been committed to persistent storage, use the **show role** command.

show role [name *string* **| pending | pending-diff | session status | status]**

Syntax Description

name *string*	Specifies a name of the role.
pending	Displays uncommitted role configuration for fabric distribution.
pending-diff	Displays the differences between the pending configuration and the active configuration.
session status	Displays the session status for a role.
status	Displays the status of the latest Cisco Fabric Services (CFS) operation.

Defaults

Displays information for all roles.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
2.0(1b)	Added the **pending**, **pending-diff**, **session**, and **status** options.

Usage Guidelines

The rules are displayed by rule number and are based on each role. All roles are displayed even if role name is not specified.

Only network-admin role can access this command.

Examples

The following example shows how to display information for all roles.

```
switch# show role
Role: network-admin
Description: Predefined Network Admin group. This role cannot be modified
Access to all the switch commands

Role: network-operator
Description: Predefined Network Operator group. This role cannot be modified
Access to Show commands and selected Exec commands

Role: sangroup
Description: SAN management group
----------------------------------------
Rule   Type   Command-type   Feature
----------------------------------------
  1.   permit    config           *
  2.     deny    config        fspf
```

```
  3.   permit     debug        zone
  4.   permit      exec      fcping
```

The following examples displays the role session status.

```
switch# show role session status
Last Action                : None
Last Action Result         : None
Last Action Failure Reason : None
```

Related Commands

Command	Description
role abort	Enables authorization role CFS distribution.
role commit	Enables authorization role CFS distribution.
role distribute	Enables authorization role CFS distribution.
role name	Configures authorization roles.

show rscn

To display Registered State Change Notification (RSCN) information, use the **show rscn** command.

show rscn {**event-tov vsan** *vsan-id* | **pending vsan** *vsan-id* | **pending-diff vsan** *vsan-id* | **scr-table** [**vsan** *vsan-id*] | **statistics** [**vsan** *vsan-id*]}

Syntax Description

event-tov	Displays the event timeout value.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
pending	Displays the pending configuration.
pending-diff	Displays the difference between the active and the pending configuration.
scr-table	Displays the State Change Registration table.
statistics	Displays RSCN statistics.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the **event-tov**, **pending**, and **pending-diff** options.

Usage Guidelines

The SCR table cannot be configured. It is only populated if one or more Nx ports send SCR frames to register for RSCN information. If the **show rscn scr-table** command does not return any entries, no Nx port is interested in receiving RSCN information.

Examples

The following example displays RSCN information.

```
switch# show rscn scr-table vsan 1
SCR table for VSAN: 1
---------------------------------------------
FC-ID         REGISTERED FOR
---------------------------------------------
0x1b0300      fabric detected rscns

Total number of entries = 1
```

The following example displays RSCN statistics.

```
switch# show rscn statistics vsan 1

Statistics for VSAN: 1
-------------------------

Number of SCR received         = 0
```

```
Number of SCR ACC sent         = 0
Number of SCR RJT sent         = 0
Number of RSCN received        = 0
Number of RSCN sent            = 0
Number of RSCN ACC received    = 0
Number of RSCN ACC sent        = 0
Number of RSCN RJT received    = 0
Number of RSCN RJT sent        = 0
Number of SW-RSCN received     = 0
Number of SW-RSCN sent         = 0
Number of SW-RSCN ACC received = 0
Number of SW-RSCN ACC sent     = 0
Number of SW-RSCN RJT received = 0
Number of SW-RSCN RJT sent     = 0
```

The following example shows the RSCN event timeout value configured on VSAN 1.

```
switch# show rscn event-tov vsan 1
Event TOV : 2000 ms
switch#
```

The following example shows the difference between the active RSCN configuration and the pending RSCN configuration on VSAN 1.

```
switch# show rscn pending-diff vsan 1
-  rscn event-tov 2000
+  rscn event-tov 20
switch#
```

show running-config

To display the running configuration file, use the **show running-config** command

show running-config
[**diff** |
interface [cpp | **fc** | **fc** *slot/port* | **fc-tunnel** *tunnel-id* | **fcip** *fcip-number* | **gigabitethernet** *slot/port* | **iscsi** *slot/port* | **mgmt 0** | **port-channel** | **svc** | **vsan** *vsan-id*] |
vsan *vsan-id*]

Syntax Description

diff	Displays the difference between the running and startup configurations.
interface	Displays running configuration information for a range of interfaces.
cpp	Displays the virtualization interface.
fc *slot/port*	Displays the Fibre Channel interface in the specified slot and port.
fc-tunnel *tunnel-id*	Displays description of the specified FC tunnel from 1 to 4095.
fcip *fcip-number*	Displays the description of the specified FCIP interface from 1 to 255.
gigabitethernet *slot/port*	Displays the description of the Gigabit Ethernet interface in the specified slot and port.
iscsi *slot/port*	Displays the description of the iSCSI interface in the specified slot and port.
mgmt 0	Displays the description of the management interface.
port-channel	Displays the description of the PortChannel interface.
sup-fc	Displays the inband interface details.
svc	Displays the virtualization interface specific to the CSM module.
vsan *vsan-id*	Displays VSAN-specific information. The ID ranges from 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

If the running configuration is different from the startup configuration, issue the **show startup-config diff** command to view the differences.

Examples

The following example displays the configuration currently running on the switch.

```
switch# show running-config
Building Configuration ...
 interface fc1/1
 interface fc1/2
 interface fc1/3
 interface fc1/4
 interface mgmt0
ip address 172.22.95.112 255.255.255.0
no shutdown
vsan database
boot system bootflash:isan-237; sup-1
boot kickstart bootflash:boot-237 sup-1
callhome
ip default-gateway 172.22.95.1
switchname switch
trunk protocol enable
username admin password 5 /AFDAMD4B2xK2  role network-admin
```

The following example displays the difference between the running configuration and the startup configuration.

```
switch# show running-config diff
Building Configuration ...
*** Startup-config
--- Running-config
****************** 1,16 ****
  fcip enable

  ip default-gateway 172.22.91.1

  iscsi authentication none
  iscsi enable

! iscsi import target fc

  iscsi virtual-target name vt
    pWWN 21:00:00:04:cf:4c:52:c1
  all-initiator-permit

--- 1,20 ----
  fcip enable

+ aaa accounting logsize 500
+
+
+

  ip default-gateway 172.22.91.1

  iscsi authentication none
  iscsi enable

! iscsi initiator name junk

  iscsi virtual-target name vt
    pWWN 21:00:00:04:cf:4c:52:c1
  all-initiator-permit
```

The following example displays running configuration information for a specified interface—in this case, the management interface.

```
switch# show running-config interface mgmt0

interface mgmt0

  ip address 255.255.255.0 255.255.255.0
```

The following example displays running configuration information for a specified feature—in this case, VSANS.

```
switch# show running-config feature vsan
vsan database
vsan 2 suspend
vsan 3
vsan 4

vsan database
vsan 3 interface fc1/1
```

show san-ext-tuner

To display SAN extension tuner information, use the **show san-ext-tuner** command.

show san-ext-tuner {**interface gigabitethernet** *slot*/*port* [**nport pwwn** *pwwn-id* **vsan** *vsan-id* **counters**] | **nports**}

Syntax Description

interface	Displays SAN extension tuner information for a specific Gigabit Ethernet interface.
gigabitethernet *slot*/*port*	Specifies a Gigabit Ethernet interface.
nport	Specifies an N port.
pwwn *pwwn-id*	Specifies a pWWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
counters	Specifies SAN extension tuner counters.
nports	Displays SAN extension tuner information for all nports.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display SAN extension tuner N port information.

```
switch# show san-ext-tuner nports
```

Related Commands

Command	Description
san-ext-tuner	Enters SAN extension tuner configuration mode.

show santap module

To display the SANTap configuration on the Storage Services Module (SSM), use the **show santap module** command in EXEC mode.

show santap module *slot* {**avt** [*name* | **brief**] | **avtlun** | **cvt** [*cvt-id* | **brief**] | **dvt** [*name* | **brief**] | **dvtlun** | **rvt** [*name* | **brief**] | **rvtlun** | **session** [*session-id* | **brief**]}

Syntax Description

slot	Displays SANTap configuration for a module in the specified slot.
avt	Displays the appliance virtual target (AVT) configuration.
avtlun	Displays the appliance AVT LUN configuration.
cvt	Displays the control virtual target (CVT) configuration.
cvt-id	Specifies a user configured CVT ID. The range is 1 to 65536.
dvt	Displays the data virtual target (DVT) configuration.
dvtlun	Displays the DVT LUN configuration.
rvt	Displays the remote virtual target (AVT) configuration.
rvtlun	Displays the RVT LUN configuration.
session	Displays the SANTap session information.
session-id	Specifies a user configured session ID. The range is 1 to 65536.
name	User specified name.
brief	Displays a brief format version of the display.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the SANTap AVT configuration.

```
switch# show santap module 2 avt

 AVT Information :
        avt pwwn     = 2a:4b:00:05:30:00:22:25
        avt nwwn     = 2a:60:00:05:30:00:22:25
        avt id       = 12
        avt vsan     = 4
        avt if_index = 0x1080000
        hi pwwn      = 21:00:00:e0:8b:07:61:aa
        tgt pwwn     = 22:00:00:20:37:88:20:ef
        tgt vsan     = 1
```

The following example displays the SANTap configuration AVT LUN.

```
switch# show santap module 2 avtlun

 AVT LUN Information :
        avt pwwn     = 2a:4b:00:05:30:00:22:25
        avt lun      = 0x0
        xmap id      = 16
        avt id       = 12
        tgt lun      = 0x0
```

The following example displays the SANTap configuration CVT.

```
switch# show santap module 2 cvt

 CVT Information :
        cvt pwwn     = 25:3c:00:05:30:00:22:25
        cvt nwwn     = 25:3d:00:05:30:00:22:25
        cvt id       = 1
        cvt xmap_id  = 2
        cvt vsan     = 10
```

The following example displays the SANTap configuration DVT.

```
switch# show santap module 2 dvt

 DVT Information :
        dvt pwwn     = 22:00:00:20:37:88:20:ef
        dvt nwwn     = 20:00:00:20:37:88:20:ef
        dvt id       = 3
        dvt mode     = 3
        dvt vsan     = 3
        dvt fp_port  = 0
        dvt if_index = 0x1080000
        dvt name     = MYDVT
```

The following example displays the SANTap configuration DVTLUN.

```
switch# show santap module 2 dvtlun

 DVT LUN Information :
        dvt pwwn     = 22:00:00:20:37:88:20:ef
        dvt lun      = 0x0
        xmap id      = 8
        dvt id       = 3
        dvt mode     = 0
        dvt vsan     = 3
        tgt pwwn     = 22:00:00:20:37:88:20:ef
        tgt lun      = 0x0
        tgt vsan     = 1
```

The following example displays the SANTap configuration session.

```
switch# show santap module 2 session

 Session Information :
        session id    = 1
        host pwwn     = 21:00:00:e0:8b:07:61:aa
        dvt pwwn      = 22:00:00:20:37:88:20:ef
        dvt lun       = 0x0
        tgt pwwn      = 00:00:00:00:00:00:00:00
        tgt lun       = 0x0
        adt pwwn      = 77:77:77:77:77:77:77:77
        adt lun       = 0x0
        num ranges    = 0
        dvt id        = 0
        vdisk id      = 0
        session state = 0
        mrl requested = 1
        pwl requested = 1
        iol requested = 0
```

The following example displays the SANTap configuration RVT.

```
switch# show santap module 2 rvt

 RVT Information :
        rvt pwwn     = 2a:61:00:05:30:00:22:25
        rvt nwwn     = 2a:62:00:05:30:00:22:25
        rvt id       = 17
        rvt vsan     = 4
        rvt if_index = 0x1080000
```

The following example displays the SANTap configuration RVTLUN.

```
switch# show santap module 2 rvtlun

 RVT LUN Information :
        rvt pwwn     = 2a:61:00:05:30:00:22:25
        rvt lun      = 0x0
        xmap id      = 22
        rvt id       = 17
        app pwwn     = 22:00:00:20:37:39:b1:00
        app lun      = 0x0
        app vsan     = 1
```

Table 22-7 describes the significant fields shown in the previous displays.

Table 22-7 show santap Field Descriptions

Field	Description
app lun	Displays the appliance LUN.
app pwwn	Displays the appliance port world wide name.
app vsan	Displays the appliance VSAn number.
avt id	Displays the AVT ID number.
avt if_index	Displays the AVT interface index number.
avt lun	Displays the AVT LUN.
avt nwwn	Displays the AVT Node port world wide name.
avt pwwn	Displays the AVT port world wide name

Table 22-7 show santap Field Descriptions (continued)

Field	Description
avt vsan	Displays the AVT VSAN number.
cvt id	Displays the CVT ID number.
cvt nwwn	Displays the CVT Node port world wide name.
cvt pwwn	Displays the CVT port world wide name
cvt vsan	Displays the CVT VSAN number.
cvt xmap_id	Displays the CVT Xmap ID number.
dvt fp_port	Displays the DVT fabric port number.
dvt id	Displays the DVT
dvt if_index	Displays the DVT interface index number.
dvt lun	Displays the DVT LUN.
dvt mode	Displays the DVT mode.
dvt name	Displays the DVT name.
dvt nwwn	Displays the DVT Node port world wide name.
dvt pwwn	Displays the DVT port world wide name.
dvt vsan	Displays the DVT VSAN number.
host pwwn	Displays the host port world wide name.
num ranges	Displays the number ranges.
rvt id	Displays the RVT ID number.
rvt if_index	Displays the RVT interface index.
rvt lun	Displays the RVT LUN.
rvt nwwn	Displays the RVT Node port world wide name.
rvt pwwn	Displays the RVT port world wide name.
rvt vsan	Displays the RVT VSAN number.
session id	Displays the session ID number.
session state	Displays the session state.
tgt lun	Displays the target LUN.
tgt pwwn	Displays the target port world wide name.
tgt vsan	Displays the target VSAN number.
vdisk id	Displays the virtual disk ID number.
xmap id	Displays the Xmap ID number.

Related Commands

Command	Description
santap module	Configures the mapping between the SSM and the VSAN where the appliance is configured

show scheduler

To display command scheduler information, use the **show scheduler** command.

show scheduler {**config** | **job** [**name** *jobname*] | **logfile** | **schedule** [**name** *schedulename*]}

Syntax Description

config	Displays command scheduler configuration information.
job	Displays job information.
name *jobname*	Restricts the output to a specific job name. Maximum length is 31 characters.
logfile	Displays the log file.
schedule	Displays schedule information.
name *schedulename*	Restricts the output to a specific schedule name. Maximum length is 31 characters.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, the command scheduler must be enabled using the **scheduler enable** command.

Examples

The following example displays the command scheduler configuration information.

```
switch# show scheduler config
config terminal
  scheduler enable
end
```

The following example displays the command scheduler schedule information.

```
switch# show scheduler schedule configureVsan99
Schedule Name : configureVsan99
-----------------------------------
User Name : admin
Schedule Type : Run once on Tue Aug 10 09:48:00 2004
Last Execution Time: Tue Aug 10 09:48:00 2004
-----------------------------------------------
Job Name       Status
-----------------------------------------------
addMemVsan99   Success (0)
```

The following example displays the command scheduler logfile information.

```
switch# show scheduler logfile
Job Name : addMemVsan99 Job Status: Success (0)
Schedule Name : configureVsan99 User Name : admin
Completion time: Tue Aug 10 09:48:00 2004
-------------------------- Job Output --------------------------
'config terminal'
'vsan database'
'vsan 99 interface fc1/1'
'vsan 99 interface fc1/2'
'vsan 99 interface fc1/3'
'vsan 99 interface fc1/4'
```

The following example displays the command scheduler configuration information.

```
switch# show scheduler config
config terminal
  scheduler enable
  scheduler logfile size 512
end
config terminal
  scheduler job name addMemVsan99
    config terminal
      vsan database
        vsan 99 interface fc1/1
        vsan 99 interface fc1/2
        vsan 99 interface fc1/3
        vsan 99 interface fc1/4
end
config terminal
  scheduler schedule name configureVsan99
    time start 2004:8:10:9:52
    job name addMemVsan99
end
```

Related Commands

Command	Description
scheduler enable	Enables the command scheduler.
scheduler job name	Configures command scheduler jobs.
scheduler schedule name	Configures command schedules.

show scsi-flow

To display SCSI flow information, use the **show scsi-flow** command.

show scsi-flow [**flow-id** *flow-id*]|
statistics [**flow-id** *flow-id* {**lun** *lun-number*}]]

Syntax Description

flow-id *flow-id*	Displays a specific SCSI flow index.
statistics	Displays the statistics for the SCSI flow.
lun *lun-number*	Displays statics for a specific LUN number.

Defaults

None

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(2)	This command was introduced.

Examples

The following example displays SCSI flow services configuration for all SCSI flow identifiers.

```
switch# show scsi-flow
Flow Id: 3
        Initiator VSAN: 101
        Initiator WWN: 21:00:00:e0:8b:05:76:28
        Target VSAN: 102
        Target WWN: 21:00:00:20:37:38:7f:7d
        Target LUN: ALL LUNs
        Flow Verification Status:
        -------------------------
           Initiator Verification Status:   success
           Target Verification Status:      success
           Initiator Linecard Status:       success
           Target Linecard Status:          success
        Feature Status:
        ---------------
          Write-Acceleration enabled
            Write-Acceleration Buffers: 1024
            Configuration Status:  success
          Statistics enabled
            Configuration Status:  success

Flow Id: 4
        Initiator VSAN: 101
        Initiator WWN: 21:00:00:e0:8b:05:76:28
        Target VSAN: 102
        Target WWN: 21:00:00:20:37:38:a7:89
        Target LUN: ALL LUNs
        Flow Verification Status:
        -------------------------
```

```
    Initiator Verification Status:   success
    Target Verification Status:      success
    Initiator Linecard Status:       success
    Target Linecard Status:          success
Feature Status:
---------------
  Write-Acceleration enabled
    Write-Acceleration Buffers: 1024
    Configuration Status:  success
```

Table 22-8 describes the significant fields shown in the **show scsi-flow** command output.

Table 22-8 show scsi-flow Field Descriptions

Field	Description
Initiator Verification Status	Verifies that the name server, FLOGI server, and zone server information for the initiator on the local switch are correct.
Target Verification Status	Verifies that the names sever and zone server information for the target on the local switch are correct.
Initiator Linecard Status	Verifies that the initiator is connected to an SSM and if DPP provisioning is enabled for the module.
Target Linecard Status	Verifies in the following order: 1. The target switch sees the proper name server and zone server information for the initiator. 2. The target switch sees the proper name server, FLOGI server and zone server information for the target. 3. The target is connected to an SSM and if DPP provisioning is enabled for that module.

The following example displays SCSI flow services configuration for a specific SCSI flow identifier.

```
switch# show scsi-flow flow-id 3
Flow Id: 3
        Initiator VSAN: 101
        Initiator WWN: 21:00:00:e0:8b:05:76:28
        Target VSAN: 102
        Target WWN: 21:00:00:20:37:38:7f:7d
        Target LUN: ALL LUNs
        Flow Verification Status:
        -------------------------
           Initiator Verification Status:   success
           Target Verification Status:      success
           Initiator Linecard Status:       success
           Target Linecard Status:          success
        Feature Status:
        ---------------
          Write-Acceleration enabled
            Write-Acceleration Buffers: 1024
            Configuration Status:  success
          Statistics enabled
            Configuration Status:  success
```

The following example displays SCSI flow services statistics for all SCSI flow identifiers.

```
switch# show scsi-flow statistics

Stats for flow-id 4 LUN=0x0000
------------------------------
 Read Stats
  I/O Total count=2
  I/O Timeout count=0
  I/O Total block count=4
  I/O Max block count=2
  I/O Min response time=5247 usec
  I/O Max response time=10160 usec
  I/O Active Count=0

 Write Stats
  I/O Total count=199935
  I/O Timeout count=0
  I/O Total block count=12795840
  I/O Max block count=64
  I/O Min response time=492 usec
  I/O Max response time=10056529 usec
  I/O Active Count=16

 Non Read-Write Stats
  Test Unit Ready=4
  Report LUN=38
  Inquiry=50
  Read Capacity=3
  Mode Sense=0
  Request Sense=0

 Total Stats
  Rx Frame Count=3792063
  Rx Frame Byte Count=6549984752
  Tx Frame Count=3792063
  Tx Frame Byte Count=6549984752

 Error Stats
  SCSI Status Busy=0
  SCSI Status Reservation Conflict=0
  SCSI Status Task Set Full=0
  SCSI Status ACA Active=0
  Sense Key Not Ready=0
  Sense Key Medium Error=0
  Sense Key Hardware Error=0
  Sense Key Illegal Request=0
  Sense Key Unit Attention=28
  Sense Key Data Protect=0
  Sense Key Blank Check=0
  Sense Key Copy Aborted=0
  Sense Key Aborted Command=0
  Sense Key Volume Overflow=0
  Sense Key Miscompare=0
```

The following example displays SCSI flow services statistics for a specific SCSI flow identifier.

```
switch# show scsi-flow statistics flow-id 4

Stats for flow-id 4 LUN=0x0000
------------------------------
 Read Stats
  I/O Total count=2
  I/O Timeout count=0
  I/O Total block count=4
  I/O Max block count=2
  I/O Min response time=5247 usec
  I/O Max response time=10160 usec
  I/O Active Count=0

 Write Stats
  I/O Total count=199935
  I/O Timeout count=0
  I/O Total block count=12795840
  I/O Max block count=64
  I/O Min response time=492 usec
  I/O Max response time=10056529 usec
  I/O Active Count=16
```

show scsi-target

To display information about existing SCSI target configurations, use the **show scsi-target** command.

show scsi-target {**auto-poll** | **custom-list** | **devices** [**vsan** *vsan-id*] [**fcid** *fcid-id*] | **disk** [**vsan** *vsan-id*] [**fcid** *fcid-id*] | **lun [vsan** *vsan-id*] [**fcid** *fcid-id*] [**os** [**aix** | **all** | **hpux** | **linux** | **solaris** | **windows**] | **pwwn** | **status** | **tape** [**vsan** *vsan-id*] [**fcid** *fcid-id*]}

Syntax Description

auto-poll	Displays SCSI target auto polling information.
custom-list	Displays customized discovered targets.
devices	Displays discovered scsi-target devices information
disk	Displays discovered disk information.
lun	Displays discovered SCSI target LUN information.
os	Discovers the specified operating system.
aix	Specifies the AIX operating system.
all	Specifies all operating systems.
hpux	Specifies the HPUX operating system.
linux	Specifies the Linux operating system.
solaris	Specifies the Solaris operating system.
windows	Specifies the Windows operating system.
vsan *vsan-range*	Specifies the VSAN ID or VSAN range. The ID range is 1 to 4093.
fcid *fcid-id*	Specifies the FCID of the SCSI target to display.
status	Displays SCSI target discovery status.
tape	Displays discovered tape information.
pwwn	Displays discover pWWN information for each OS.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

Use the **show scsi-target auto-poll** command to verify automatic discovery of scsi-targets which come online.

Examples

The following example displays the status of a SCSI discovery.

```
switch# show scsi-target status
discovery completed
```

The following example displays a customized discovered targets:

```
switch# show scsi-target custom-list
---------------
VSAN DOMAIN
---------------
1       56
```

The following example displays discovered disk information.

```
switch# show scsi-target disk
-------------------------------------------------------------------------------
VSAN    FCID        PWWN                      VENDOR    MODEL              REV
-------------------------------------------------------------------------------
1       0x9c03d6    21:00:00:20:37:46:78:97   Company 4 ST318203FC         0004
1       0x9c03d9    21:00:00:20:37:5b:cf:b9   Company 4 ST318203FC         0004
1       0x9c03da    21:00:00:20:37:18:6f:90   Company 4 ST318203FC         0004
1       0x9c03dc    21:00:00:20:37:5a:5b:27   Company 4 ST318203FC         0004
1       0x9c03e0    21:00:00:20:37:36:0b:4d   Company 4 ST318203FC         0004
1       0x9c03e1    21:00:00:20:37:39:90:6a   Company 4 ST318203 CLAR18    3844
1       0x9c03e2    21:00:00:20:37:18:d2:45   Company 4 ST318203 CLAR18    3844
1       0x9c03e4    21:00:00:20:37:6b:d7:18   Company 4 ST318203 CLAR18    3844
1       0x9c03e8    21:00:00:20:37:38:a7:c1   Company 4 ST318203FC         0004
1       0x9c03ef    21:00:00:20:37:18:17:d2   Company 4 ST318203FC         0004
```

The following example displays the discovered LUNs for all OSs.

```
switch# show scsi-target lun os all

ST336607FC from SEAGATE (Rev 0006)
FCID is 0xed0001 in VSAN 7, PWWN is 21:00:00:04:cf:fb:42:f8
-------------------------------------------------------------------------------
OS  LUN    Capacity Status  Serial Number    Device-Id
           (MB)
-------------------------------------------------------------------------------
WIN 0x0    36704    Online  3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
AIX 0x0    36704    Online  3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
SOL 0x0    36704    Online  3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
LIN 0x0    36704    Online  3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
HP  0x0    36704    Online  3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
```

The following example displays the discovered LUNs. for the Solaris OS.

```
switch# show scsi-target lun os solaris

ST336607FC from SEAGATE (Rev 0006)
FCID is 0xed0001 in VSAN 7, PWWN is 21:00:00:04:cf:fb:42:f8
-------------------------------------------------------------------------------
OS  LUN    Capacity Status  Serial Number    Device-Id
           (MB)
-------------------------------------------------------------------------------
SOL 0x0    36704    Online  3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
```

The following example displays auto-polling information. Each user is indicated by the internal UUID number, which indicates that a CSM or an IPS module is in the chassis.

```
switch# show scsi-target auto-poll
auto-polling is enabled, poll_start:0 poll_count:1 poll_type:0
USERS OF AUTO POLLING
---------------------
uuid:54
```

The following example displays the port WWN that is assigned to each OS (Windows, AIX, Solaris, Linux, or HPUX).

```
switch# show scsi-target pwwn
------------------------------
OS     PWWN
------------------------------
WIN    24:91:00:05:30:00:2a:1e
AIX    24:92:00:05:30:00:2a:1e
SOL    24:93:00:05:30:00:2a:1e
LIN    24:94:00:05:30:00:2a:1e
HP     24:95:00:05:30:00:2a:1e
```

show snmp

To display SNMP status and setting information, use the **show snmp** command.

show snmp [**community** | **engineid** | **group** | **host** | **sessions** | **user**]

Syntax Description

community	Displays SNMP community strings.
engineid	Displays SNMP engine ID information.
group	Displays SNMP group information.
host	Displays SNMP host information.
sessions	Displays SNMP session information.
user	Displays SNMPv3 user information.

Defaults

Displays the system contact, the system location, packet traffic information, community strings, and user information.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
2.0(1b)	Added the **engineid**, **group**, and **sessions** keywords.

Usage Guidelines

None.

Examples

The following example displays SNMP information.

```
switch# show snmp
sys contact:
sys location:

1631 SNMP packets input
        0 Bad SNMP versions
        0 Unknown community name
        0 Illegal operation for community name supplied
        0 Encoding errors
        64294 Number of requested variables
        1 Number of altered variables
        1628 Get-request PDUs
        0 Get-next PDUs
        1 Set-request PDUs
152725 SNMP packets output
        0 Too big errors
        1 No such name errors
        0 Bad values errors
        0 General errors
```

```
Community                      Access
---------                      ------
public                          rw

User                           Group                          Auth  Priv
____                           _____                          ____  ____
admin                          network-admin                  md5   no
```

The following example displays SNMP user details.

```
switch# show snmp user
User                           Group                          Auth  Priv
____                           _____                          ____  ____
steve                          network-admin                  md5   des
sadmin                         network-admin                  md5   des
stever                         network-operator               md5   des
```

The following example displays SNMP community information.

```
switch# show snmp community
Community                      Access
---------                      ------
private                         rw
public                          ro
v93RACqPNH                      ro
```

The following example displays SNMP host information.

```
switch# show snmp host
Host                            Port Version  Level  Type   SecName
____                            ____ _______  ______ ____   _______
171.16.126.34                   2162 v2c      noauth trap   public
171.16.75.106                   2162 v2c      noauth trap   public
171.31.124.81                   2162 v2c      noauth trap   public
171.31.157.193                  2162 v2c      noauth trap   public
171.31.157.98                   2162 v2c      noauth trap   public
171.31.49.25                    2162 v2c      noauth trap   public
171.31.49.32                    2188 v2c      noauth trap   public
171.31.49.49                    2162 v2c      noauth trap   public
171.31.49.49                    3514 v2c      noauth trap   public
171.31.49.54                    2162 v2c      noauth trap   public
171.31.58.54                    2162 v2c      noauth trap   public
171.31.58.81                    2162 v2c      noauth trap   public
171.31.58.97                    1635 v2c      noauth trap   public
171.31.58.97                    2162 v2c      auth   trap   public
171.31.58.97                    3545 v2c      auth   trap   public
172.22.00.43                    2162 v2c      noauth trap   public
172.22.00.65                    2162 v2c      noauth trap   public
172.22.05.234                   2162 v2c      noauth trap   public
172.22.05.98                    1050 v2c      noauth trap   public
```

The following example displays SNMP engine ID information.

```
switch# show snmp engineID
Local SNMP engineID: 800000090300053000A79E
```

The following example displays SNMP group information.

```
switch# show snmp group
groupname: network-admin
security model: any
security level: noAuthNoPriv
readview: network-admin-rd
writeview: network-admin-wr
notifyview: network-admin-rd
storage-type: permanent
row status: active

groupname: network-admin
security model: any
security level: authNoPriv
readview: network-admin-rd
writeview: network-admin-wr
notifyview: network-admin-rd
storage-type: permanent
row status: active

groupname: network-operator
security model: any
security level: noAuthNoPriv
readview: network-operator-rd
writeview: network-operator-wr
notifyview: network-operator-rd
storage-type: permanent
row status: active

groupname: network-operator
security model: any
security level: authNoPriv
readview: network-operator-rd
writeview: network-operator-wr
notifyview: network-operator-rd
storage-type: permanent
row status: active
```

show span session

To display specific information about a Switched Port Analyzer (SPAN) session, use the **show span session** command.

show span session [*session-id* [**brief**] | **brief**]

Syntax Description

session-id	SPAN session ID (1-16).
brief	Displays SPAN session configuration in brief format.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays SPAN sessions in a brief format.

```
switch# show span session brief
-------------------------------------------------------
 Session  Admin          Oper           Destination
          State          State          Interface
-------------------------------------------------------
 7        no suspend     active         fc2/7
```

The following example displays a specific SPAN session details.

```
switch# show span session 7
Session 7 (active)
   Destination is fc2/7
   No session filters configured
   No ingress (rx) sources
   Egress (tx) sources are
     port-channel 7,
```

The following example displays all SPAN sessions.

```
switch# show span session
Session 1 (inactive as no destination)
Destination is not specified
   Session filter vsans are 1
   No ingress (rx) sources
   No egress (tx) sources

Session 2 (active)
   Destination is fc9/5
   No session filters configured
   Ingress (rx) sources are
      vsans 1
     sup-fc0,
   Egress (tx) sources are
     sup-fc0,
```

The following example displays a SPAN session mapped to a FC tunnel interface.

```
switch# show span session
Session 2 (active)
   Destination is fc-tunnel 100
   No session filters configured
   Ingress (rx) sources are
     fc2/16,
   Egress (tx) sources are
     fc2/16,
```

show sprom

To display vendor ID, product component attributes, serial number information that can be used to track field replacable units, use the **show sprom** command.

show sprom {**backplane** *backplane-index* |
clock *clock-module-index* |
fan |
mgmt-module |
module *module-number sprom-index* |
powersupply *powersupply-index* |
sup}

Syntax Description

backplane *backplane-index*	Display attributes that can be used to uniquely identify a switch. The range is 1 to 2.
clock *clock-module-index*	Display attributes of the clock module. There are two clock modules in a switch. This module is absent in MDS9216 type switch. The range is 1 to 2.
fan	Display attributes that uniquely identified fan.
mgmt-module	Display attributes of management module. This module is only present in MDS9216 type switch.
module *module-number sprom-index*	Display Vendor ID, product's component attributes for the given switching module. There can be up to 4 sub-components in a module. Each of them will have a SPROM associated with it.
powersupply *powersupply-index*	Displays attributes of the first or the second power-supply. This contains information about the powersupply capacity in watts when it is used in 110Volts and 220Volts respectively. This information is used for power-budget allocation. The range is 1 to 2.
sup	Display Vendor ID, product's component attributes for the current supervisor module

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use the **show sprom** command to get unique information about a specific module, supervisor module, switch, power-supply module, or a fan module. If the customer needs to report a problem with a module, supervisor module, switch, power-supply module, or a fan module and does not have access to management station, then he can extract serial number information from **show sprom**.

Examples

The following example displays management module information. This module and command are specific to the Cisco MDS 9216 switch.

```
switch# show sprom mgmt-module
DISPLAY SAM sprom contents:
Common block:
 Block Signature :0xabab
 Block Version   :2
 Block Length    :156
 Block Checksum  :0x1295
 EEPROM Size     :0
 Block Count     :2
 FRU Major Type  :0x0
 FRU Minor Type  :0x0
 OEM String      :Cisco Systems Inc
 Product Number  :SAM SMITH
 Serial Number   :12345678901
 Part Number     :SAM-SMITH-06
 Part Revision   :A0
 Mfg Deviation   :
 H/W Version     :1.0
 Mfg Bits        :1
 Engineer Use    :0
 snmpOID         :0.0.0.0.0.0.0.0
 Power Consump   :-200
 RMA Code        :0-0-0-0
Linecard Module specific block:
 Block Signature :0x6003
 Block Version   :2
 Block Length    :103
 Block Checksum  :0x3c7
 Feature Bits    :0x0
 HW Changes Bits :0x0
 Card Index      :9009
 MAC Addresses   :00-12-34-56-78-90
 Number of MACs  :4
 Number of EOBC links :4
 Number of EPLD  :0
 Port Type-Num   :200-16
 SRAM size       :0
 Sensor #1       :0,0
 Sensor #2       :0,0
 Sensor #3       :0,0
 Sensor #4       :0,0
 Sensor #5       :0,0
 Sensor #6       :0,0
 Sensor #7       :0,0
 Sensor #8       :0,0
```

The following command displays supervisor module information.

```
switch# show sprom sup
DISPLAY supervisor sprom contents:
Common block:
 Block Signature : 0xabab
 Block Version   : 2
 Block Length    : 156
 Block Checksum  : 0x10a8
 EEPROM Size     : 512
 Block Count     : 2
 FRU Major Type  : 0x6002
 FRU Minor Type  : 0x7d0
 OEM String      : Cisco Systems
 Product Number  : DS-X9530-SF1-K9
```

```
 Serial Number   : abcdefgh
 Part Number     : 73-7523-06
 Part Revision   : 0.0
 Mfg Deviation   : 0.0
 H/W Version     : 0.0
 Mfg Bits        : 0
 Engineer Use    : 0
 snmpOID         : 9.5.1.3.1.1.2.2000
 Power Consump   : -524
 RMA Code        : 0-0-0-0
Supervisor Module specific block:
 Block Signature : 0x6002
 Block Version   : 2
 Block Length    : 103
 Block Checksum  : 0x927
 Feature Bits    : 0x0
 HW Changes Bits : 0x0
 Card Index      : 9003
 MAC Addresses   : 00-05-30-00-18-be
 Number of MACs  : 4
 Number of EPLD  : 1
 EPLD A          : 0x0
 Sensor #1       : 75,60
 Sensor #2       : 60,55
 Sensor #3       : -127,-127
 Sensor #4       : -127,-127
 Sensor #5       : -128,-128
 Sensor #6       : -128,-128
 Sensor #7       : -128,-128
 Sensor #8       : -128,-128
```

Related Commands

Command	Description
show hardware	Displays brief information about the list of field replacable units in the switch.

show ssh

To display Secure Shell information (SSH), use the **show ssh** command.

show ssh {**key** [**dsa** | **rsa** | **rsa1**] | **server**}

Syntax Description

key	Displays SSH keys.
server	Displays the SSH server status.
dsa	Displays DSA SSH keys.
rsa	Displays RSA SSH keys.
rsa1	Displays RSA1 SSH keys.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

To display the host key pair details for the specified key or for all keys, if no key is specified, use the **show ssh key** command. To display the status of the SSH protocol (enabled or disabled) and the versions that are enabled for that switch, use the **show ssh server** command.

Examples

The following example displays SSH server status.

```
switch# show ssh server
ssh is enabled
version 1 enabled
version 2 enabled
```

The following example displays Host Key Pair details.

```
switch# show ssh key
rsa1 Keys generated:Sun Jan 13 07:16:26 1980

1024 35

fingerprint:
1024 67:76:02:bd:3e:8d:f5:ad:59:5a:1e:c4:5e:44:03:07

could not retrieve rsa key information

dsa Keys generated:Sun Jan 13 07:40:08 1980

ssh-dss AAAAB3NzaC1kc3MAAABBAJTCRQOydNRel2v7uiO6Fix+OTn8eGdnnDVxw5eJs5OcOEXOyjaW
cMMYsEgxc9ada1NElp8Wy7GPMWGOQYj9CU0AAAAVAMCcWhNN18zFNOIPo7cU3t7d0iEbAAAAQBdQ8UAO
i/Cti84qFb3kTqXlS9mEhdQUo0lHcH5bw5PKfj2Y/dLR437zCBKXetPj4p7mhQ6Fq5os8RZtJEyOsNsA
AABAA0oxZbPyWeR5NHATXiyXdPI7j9i8fgyn9FNipMkOF2Mn75Mi/lqQ4NIq0gQNvQOx27uCeQlRts/Q
wI4q68/eaw==

fingerprint:
512 f7:cc:90:3d:f5:8a:a9:ca:48:76:9f:f8:6e:71:d4:ae
```

show ssm provisioning

To display the attributes of the Storage Services Module (SSM) installed, use the **show ssm provisioning** command.

show ssm provisioning

Command History

Release	Modification
2.0(2)	This command was introduced.
2.1(1a)	Added Provisioning Status column to the display.

Examples

The following example provisions the SSM installed in the switch.

```
switch# show ssm provisioning
Module   Ports       Application        Provisioning Status
----------------------------------------------------------
   4      1-32       scsi-flow                   success
```

Table 22-9 describes the significant fields shown in the **show ssm provisioning** command output.

Table 22-9 show ssm provisioning Field Descriptions

Field	Description
Module	Slot where SSM is installed.
Ports	Ports available on the SSM.
Application	Feature configured on the SSM.
Provisioning Status	Displays the status of the SSM attributes.

Related Commands

Command	Description
ssm enable feature	Enables the SCSI flow feature on the SSM.

show startup-config

To display the startup configuration file, use the **show startup-config** command

show startup-config [**log**]

Syntax Description

log	Displays execution log of last used ASCII startup configuration.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the switch configuration at startup.

```
switch# show startup-config
vsan database
vsan 2
vsan 3
vsan 4
vsan 5
vsan 31
vsan 32 suspend
vsan 100
vsan 300

 interface port-channel 1
switchport mode E
switchport trunk mode off

 interface port-channel 2
fspf cost 100 vsan 2
switchport mode E
no switchport trunk allowed vsan all
switchport trunk allowed vsan add 1-99
switchport trunk allowed vsan add 101-4093

 interface port-channel 3
switchport mode E
switchport trunk mode off

 interface port-channel 4
switchport mode E
no switchport trunk allowed vsan all
```

```
switchport trunk allowed vsan add 1-99
switchport trunk allowed vsan add 101-4093

 interface port-channel 5
switchport mode E
no switchport trunk allowed vsan all
switchport trunk allowed vsan add 1-10interface port-channel 5
switchport mode E
no switchport trunk allowed vsan all
switchport trunk allowed vsan add 1-10

interface port-channel 8
switchport mode E

 interface vsan1

no shutdown

snmp-server community public rw
snmp-server user admin network-admin auth md5 0xe84b06201ae3bfb726a2eab9f485eb57
 localizedkey
snmp-server host 171.69.126.34 traps version 2c public udp-port 2162
snmp-server host 171.69.75.106 traps version 2c public udp-port 2162
vsan database
vsan 3 interface fc2/9
vsan 3 interface fc2/14
vsan 5 interface fc9/11
vsan 2 interface fc9/12
vsan 3 interface port-channel 3
vsan 3 interface port-channel 4
vsan 100 interface port-channel 8

boot system bootflash:/isan-8b-u sup-1
boot kickstart bootflash:/boot-3b sup-1
boot system bootflash:/isan-8b-u sup-2
boot kickstart bootflash:/boot-3b sup-2

ip default-gateway 172.22.90.1
power redundancy-mode combined force

username admin password 5 HyLyYqb4.q74Y  role network-admin
zone name Z1 vsan 1
  member pwwn 10:00:00:00:77:99:60:2c
  member pwwn 21:00:00:20:37:a6:be:14

zone default-zone permit vsan 1
zoneset distribute full vsan 51-58

zoneset name ZS1 vsan 1
  member Z1

zoneset  activate name ZS1 vsan 1

 interface fc2/1
switchport mode E
switchport trunk mode off
no shutdown

 interface fc2/2

 interface fc2/3
channel-group 1 force
no shutdown
```

```
interface fc2/6
channel-group 2 force
no shutdown

 interface fc2/7
switchport mode E
no shutdown
no switchport trunk allowed vsan all
switchport trunk allowed vsan add 1-25

interface fc2/9
switchport mode E
switchport trunk mode off
no shutdown

 interface fc2/10
channel-group 3 force
no shutdown

 interface fc2/12
channel-group 4 force
no shutdown

 interface fc2/14
switchport mode E
no shutdown
no switchport trunk allowed vsan all
switchport trunk allowed vsan add 1-99
switchport trunk allowed vsan add 101-4093

 interface fc2/15
channel-group 6 force
no shutdown

 interface fc2/16
channel-group 6 force
no shutdown
.
.
.
interface fc9/10
switchport mode F
no shutdown

 interface fc9/11
switchport trunk mode off
no shutdown

 interface fc9/12
switchport mode E
switchport speed 1000
switchport trunk mode off
no shutdown

 interface fc9/15
no shutdown
no switchport trunk allowed vsan all
switchport trunk allowed vsan add 1-99
switchport trunk allowed vsan add 101-4093
```

```
 interface fc9/16
switchport mode FL
no shutdown

 interface mgmt0
ip address 172.22.90.38 255.255.255.0
no shutdown
```

show switchname

To display the switch network name, use the **show switchname** command.

show switchname [**serialnum**]

Syntax Description

serialnum	Displays switch serial number.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the name of the switch.

```
switch# show switchname
switch-123
```

The following example displays the switch name and serial number.

```
switch# show switchname
switch-123
Serial Number #1   : FOX0712S007
Serial Number #2   :
```

show system

To display the system information, use the **show system** command.

show system {**cores** | **default** {**switchport** | **zone**} | **directory information** | **error-id** {*hex-id* | **list**} | **exception-info** | **pss shrink status** [**details**] | **redundancy status** | **reset-reason** [**module** *slot*] | **resources** | **uptime**}

Syntax Description

cores	Displays core transfer option.
default	Displays system default values.
switchport	Displays default values for switchport attributes.
zone	Displays default values for a zone.
directory information	Directory information of System Manager.
error-id	Displays description about errors.
hex-id	Specifies the error ID in hexadecimal format. The range is 0x0 to 0xffffffff.
list	Specifies all error IDs.
exception-info	Displays last exception log information.
pss shrink status	Displays the last PSS shrink status.
details	Displays detailed information on the last PSS shrink status.
redundancy status	Redundancy status.
reset-reason	Displays the last four reset reason codes.
module *slot*	Specifies the module number to display the reset-reason codes.
resources	Show the CPU and memory statistics.
uptime	Displays how long the system has been up and running.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the **zone** option.

Usage Guidelines

Use the **show system redundancy status** command to ensure that the system is ready to accept a switchover.

Examples

The following example displays the system redundancy status.

```
switch# show system redundancy status
Redundancy mode
---------------
      administrative:   HA
         operational:   None

This supervisor (sup-2)
-----------------------
    Redundancy state:   Active
    Supervisor state:   Active
      Internal state:   Active with no standby

Other supervisor (sup-1)
------------------------
    Redundancy state:   Not present
```

The following example displays the default switch port states.

```
switch# show system default switchport
System default port state is down
System default trunk mode is on
```

The following example displays error information for a specified ID.

```
switch# show system error-id 0x401D0019
Error Facility: module
Error Description: Failed to stop Linecard Async Notification.
```

The following example displays the system health information.

```
switch# show system health
System Health Services iteration frequency 5 seconds
Active SUP arbiter is Working
Active SUP bootflash is Working
```

The following example displays the system reset information.

```
switch# show system reset reason
----- reset reason for module 6 -----
1) At 520267 usecs after Tue Aug  5 16:06:24 1980
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 1.2(0.73a)
2) At 653268 usecs after Tue Aug  5 15:35:24 1980
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 1.2(0.45c)
3) No time
    Reason: Unknown
    Service:
    Version: 1.2(0.45c)
4) At 415855 usecs after Sat Aug  2 22:42:43 1980
    Reason: Power down triggered due to major temperature alarm
    Service:
    Version: 1.2(0.45c)
```

The following example displays system-related CPU and memory statistics.

```
switch# show system resources
Load average:   1 minute: 0.43   5 minutes: 0.17   15 minutes: 0.11
Processes   :   100 total, 2 running
CPU states  :   0.0% user,   0.0% kernel,   100.0% idle
Memory usage:   1027628K total,    313424K used,    714204K free
                   3620K buffers,   22278K cache
```

The following example displays the system uptime.

```
switch# show system uptime
Start Time: Sun Oct 13 18:09:23 2030
Up Time:    0 days, 9 hours, 46 minutes, 26 seconds
```

Use the **show system cores** command to display the currently configured scheme for copying cores.

```
switch# show system cores
Transfer of cores is enabled
```

Use the **show system default zone** command to display the default values for a zone.

```
switch# show system default zone
system default zone default-zone permit
system default zone distribute active only
```

show system health

To display configured Online System Health Management (OSHM) information, use the **show system health** command.

show system health [module *slot* **| statistics** [**loopback** [**interface** {**fc** *slot*/*port*| **iscsi** *slot*/*port*} | **module** *slot* [**timelog**] | **timelog**] | **module** *slot*]

Syntax Description

module *slot*	Displays information for a module in the switch,
statistics	Displays OHMS statistics.
interface	Specifies the required interface.
fc *slot*/*port*	Specifies the Fiber Channel interface at the specified slot and port.
iscsi *slot*/*port*	Specifies the iSCSI interface at the specified slot and port.
loopback	Displays the OHMS loopback test statistics.
timelog	Displays the loopback round trip times.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the current health of all modules in the switch.

```
switch# show system health

Current health information for module 2.

Test                       Frequency    Status          Action
------------------------------------------------------------------
Bootflash                  5 Sec        Running         Enabled
EOBC                       5 Sec        Running         Enabled
Loopback                   5 Sec        Running         Enabled
------------------------------------------------------------------

Current health information for module 6.

Test                       Frequency    Status          Action
------------------------------------------------------------------
InBand                     5 Sec        Running         Enabled
Bootflash                  5 Sec        Running         Enabled
EOBC                       5 Sec        Running         Enabled
```

```
Management Port           5 Sec         Running         Enabled
-----------------------------------------------------------------
```

The following example displays the current health of a specified module.

```
switch# show system health module 8

Current health information for module 8.

Test                       Frequency    Status          Action
-----------------------------------------------------------------
Bootflash                  5 Sec        Running         Enabled
EOBC                       5 Sec        Running         Enabled
Loopback                   5 Sec        Running         Enabled
-----------------------------------------------------------------
```

The following example displays the health statistics for all modules.

```
switch# show system health statistics

Test statistics for module # 1
-------------------------------------------------------------------------------
Test Name           State            Freq(s)    Run    Pass    Fail CFail Errs
-------------------------------------------------------------------------------
Bootflash           Running             5s    12900   12900       0     0    0
EOBC                Running             5s    12900   12900       0     0    0
Loopback            Running             5s    12900   12900       0     0    0
-------------------------------------------------------------------------------

Test statistics for module # 3
-------------------------------------------------------------------------------
Test Name           State            Freq(s)    Run    Pass    Fail CFail Errs
-------------------------------------------------------------------------------
Bootflash           Running             5s    12890   12890       0     0    0
EOBC                Running             5s    12890   12890       0     0    0
Loopback            Running             5s    12892   12892       0     0    0
-------------------------------------------------------------------------------

Test statistics for module # 5
-------------------------------------------------------------------------------
Test Name           State            Freq(s)    Run    Pass    Fail CFail Errs
-------------------------------------------------------------------------------
InBand              Running             5s    12911   12911       0     0    0
Bootflash           Running             5s    12911   12911       0     0    0
EOBC                Running             5s    12911   12911       0     0    0
Management Port     Running             5s    12911   12911       0     0    0
-------------------------------------------------------------------------------

Test statistics for module # 6
-------------------------------------------------------------------------------
Test Name           State            Freq(s)    Run    Pass    Fail CFail Errs
-------------------------------------------------------------------------------
InBand              Running             5s    12907   12907       0     0    0
Bootflash           Running             5s    12907   12907       0     0    0
EOBC                Running             5s    12907   12907       0     0    0
-------------------------------------------------------------------------------

Test statistics for module # 8
-------------------------------------------------------------------------------
Test Name           State            Freq(s)    Run    Pass    Fail CFail Errs
-------------------------------------------------------------------------------
Bootflash           Running             5s    12895   12895       0     0    0
EOBC                Running             5s    12895   12895       0     0    0
Loopback            Running             5s    12896   12896       0     0    0
```

```
--------------------------------------------------------------------------------
```

The following example displays the statistics for a specified module.

```
switch# show system health statistics module 3

Test statistics for module # 3
--------------------------------------------------------------------------------
Test Name           State            Freq(s)    Run     Pass    Fail CFail Errs
--------------------------------------------------------------------------------
Bootflash           Running              5s    12932   12932       0     0    0
EOBC                Running              5s    12932   12932       0     0    0
Loopback            Running              5s    12934   12934       0     0    0
--------------------------------------------------------------------------------
```

The following example displays the loopback test statistics for the entire switch.

```
switch# show system health statistics loopback
----------------------------------------------------------------
Mod Port Status                Run      Pass      Fail   CFail Errs
  1   16 Running              12953     12953         0       0    0
  3   32 Running              12945     12945         0       0    0
  8    8 Running              12949     12949         0       0    0
----------------------------------------------------------------
```

The following example displays the loopback test statistics for a specified interface.

```
switch# show system health statistics loopback interface fc 3/1
----------------------------------------------------------------
Mod Port Status                Run      Pass      Fail   CFail Errs
  3    1 Running                  0         0         0       0    0
----------------------------------------------------------------
```

Note Interface-specific counters will remain at zero unless the module-specific loopback test reports errors or failures.

The following example displays the loopback test time log for all modules.

```
switch# show system health statistics loopback timelog
----------------------------------------------------------------
Mod         Samples     Min(usecs)     Max(usecs)     Ave(usecs)
  1            1872            149            364            222
  3            1862            415            743            549
  8            1865            134            455            349
----------------------------------------------------------------
```

The following example displays the loopback test statistics for a specified module.

```
switch# show system health statistics loopback module 8 timelog
----------------------------------------------------------------
Mod         Samples     Min(usecs)     Max(usecs)     Ave(usecs)
  8            1867            134            455            349
----------------------------------------------------------------
```

show tacacs+

To display the TACACS+ Cisco Fabric Services (CFS) distribution status and other details, use the **show tacacs+** command.

show tacacs+ {**distribution status** | **pending** | **pending-diff**}

Syntax Description

distribution status	Displays the status of the TACACS+ CFS distribution.
pending	Displays the pending configuration that is not yet applied.
pending-diff	Displays the difference between the active configuration and the pending configuration.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, TACACS+ must be enabled using the **tacacs+ enable** command.

Examples

The following example shows how to display the TACACS+ distribution status.

```
switch# show tacacs+ distribution status
session ongoing: no
session db: does not exist
merge protocol status: merge activation done

last operation: none
last operation status: none
```

Related Commands

Command	Description
tacacs+ enable	Enables TACACS+.
tacacs+ distribute	Initiates TACACS+ configuration distribution.

show tacacs-server

To display all configured TACACS+ server parameters, use the **show tacacs-server** command.

show tacacs-server [*server-name* | *ipv4-address* | *ipv6-address*]
[**directed-request** | **groups** | **sorted** | **statistics**]

Syntax Description

server-name	Specifies the TACACS+ server DNS name. The maximum character size is 256.
ipv4-address	Specifies the TACACS+ server IP address in the format *A.B.C.D*.
ipv6-address	Specifies the TACACS+ server IP address in the format *X:X::X*.
directed-request	Displays an enabled directed request TACACS+ server configuration.
groups	Displays configured TACACS+ server group information.
sorted	Displays TACACS+ server information sorted by name.
statistics	Displays TACACS+ statistics for the specified TACACS+ server.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	• Added the *server-name*, *ipv4-address*, and *ipv6-address* arguments. • Added the **directed-request** and **statistics** options.

Usage Guidelines

None.

Examples

The following command displays the configured TACACS+ server information.

```
switch# show tacacs-server
Global TACACS+ shared secret:tacacsPword
timeout value:30
total number of servers:3

following TACACS+ servers are configured:
        171.71.58.91:
                available on port:2
        cisco.com:
                available on port:49
        171.71.22.95:
                available on port:49
                TACACS+ shared secret:MyKey
```

The following command displays the configured TACACS+ server groups.

```
switch# show tacacs-server groups
total number of groups:1

following TACACS+ server groups are configured:
        group TacServer:
                server 171.71.58.91 on port 2
```

show tech-support

To display information useful to technical support when reporting a problem, use the **show tech-support** command.

show tech-support [**brief** | **details** | **fcdomain** | **interface** {**fc** *slot*/*port* | **gigabitethernet** *slot*/*port*} **vsan** *vsan-id* | **module** *slot* | **vsan** *vsan-id* | **zone** *vsan-id*]

Syntax Description

brief	Provides a summary of the current running state of the switch.
details	Provides detailed information for each **show** command.
fcdomain	Displays detailed fcdomain information.
interface	Displays interface status and configuration information
fc *slot*/*port*	Specifies the Fiber Channel interface at the specified slot and port.
gigabitethernet *slot*/*port*	Specifies the Gigabit Ethernet interface at the specified slot and port.
module	Displays module status information.
port-channel	Displays detailed PortChannel information.
vsan *vsan-id*	Display VSAN status and configuration information. The range is 1 to 4093.
zone *vsan-id*	Displays zone server information for the specified VSAN ID. The range is 1 to 4093.

Defaults

The default displays output on a per-command basis, with each command being the title of the output that follows. A line separates the output from the next command. The software removes passwords and other security information.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.
3.0(1)	Added the **fcdomain**, **port-channel** and **zone** options.

Usage Guidelines

The **show tech-support** command is a compilation of several **show** commands and can be quite lengthy. For a sample display of the output of the **show tech-support** command, see the individual command explanation for the following commands.

If you enter the **show tech-support** command without arguments, the output displays the equivalent of all the following **show** commands.

- **show version**
- **show environment**
- **show module**
- **show hardware**

- **show running-config**
- **show interface**
- **show accounting log**
- **show process**
- **show process log**
- **show processes log details**

Examples

The following example displays technical support information for a specific module.

```
switch# show tech-support module 1

'terminal length 0'

'show module '
Mod  Ports  Module-Type                       Model              Status
---  -----  --------------------------------- ------------------ ------------
1    16     1/2 Gbps FC/Supervisor            DS-X9216-K9-SUP    active *
2    32     1/2 Gbps FC Module                DS-X9032           ok

Mod  Sw           Hw      World-Wide-Name(s) (WWN)
---  -----------  ------  --------------------------------------------------
1    1.0(0.271)   0.0     20:01:00:05:30:00:21:9e to 20:10:00:05:30:00:21:9e
2    1.0(0.271)   0.0     20:41:00:05:30:00:21:9e to 20:60:00:05:30:00:21:9e

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    00-05-30-00-40-b6 to 00-05-30-00-40-ba
2    00-05-30-00-11-22 to 00-05-30-00-11-26

* this terminal session

'show environment'
Clock:
----------------------------------------------------------
Clock           Model                Hw         Status
----------------------------------------------------------
A               Clock Module         --         ok/active
B               Clock Module         --         ok/standby

Fan:
-----------------------------------------------------
Fan             Model                Hw         Status
-----------------------------------------------------
Chassis         DS-2SLOT-FAN         0.0        ok
PS-1            --                   --         ok
PS-2            --                   --         absent

Temperature:
-------------------------------------------------------------------
Module   Sensor   MajorThresh   MinorThres   CurTemp     Status
                  (Celsius)    (Celsius)    (Celsius)
-------------------------------------------------------------------
1        1        75           60           30          ok
1        2        65           50           28          ok
1        3        -127         -127         40          ok
1        4        -127         -127         36          ok

2        1        75           60           32          ok
```

```
2        2        65            50           26          ok
2        3        -127          -127         41          ok
2        4        -127          -127         31          ok
```

The **show tech-support brief** command provides a summary of the current running state of the switch.

```
vegas01# show tech-support brief
Switch Name           : vegas01
Switch Type           : DS-X9216-K9-SUP
Kickstart Image       : 1.3(2a) bootflash:///m9200-ek9-kickstart-mz.1.3.1.10.bin
System Image          : 1.3(2a) bootflash:///m9200-ek9-mz.1.3.1.10.bin
IP Address/Mask       : 10.76.100.164/24
Switch WWN            : 20:00:00:05:30:00:84:9e
No of VSANs           : 9
Configured VSANs      : 1-6,4091-4093

VSAN    1:    name:VSAN0001, state:active, interop mode:default
              domain id:0x6d(109), WWN:20:01:00:05:30:00:84:9f [Principal]
              active-zone:VR, default-zone:deny

VSAN    2:    name:VSAN0002, state:active, interop mode:default
              domain id:0x7d(125), WWN:20:02:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny

VSAN    3:    name:VSAN0003, state:active, interop mode:default
              domain id:0xbe(190), WWN:20:03:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny

VSAN    4:    name:VSAN0004, state:active, interop mode:default
              domain id:0x5a(90), WWN:20:04:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny

VSAN    5:    name:VSAN0005, state:active, interop mode:default
              domain id:0x13(19), WWN:20:05:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny

VSAN    6:    name:VSAN0006, state:active, interop mode:default
              domain id:0x1f(31), WWN:20:06:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny

VSAN 4091:    name:VSAN4091, state:active, interop mode:default
              domain id:0x08(8), WWN:2f:fb:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny

VSAN 4092:    name:VSAN4092, state:active, interop mode:default
              domain id:0x78(120), WWN:2f:fc:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny

VSAN 4093:    name:VSAN4093, state:active, interop mode:default
              domain id:0x77(119), WWN:2f:fd:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny


--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          FCOT   Oper  Oper    Port
                  Mode   Trunk                         Mode  Speed   Channel
                         Mode                                 (Gbps)
--------------------------------------------------------------------------------
fc1/1      1      auto   on      fcotAbsent       --     --           --
fc1/2      1      auto   on      fcotAbsent       --     --           --
fc1/3      1      auto   on      fcotAbsent       --     --           --
fc1/4      1      auto   on      fcotAbsent       --     --           --
fc1/5      1      auto   on      notConnected     swl    --           --
fc1/6      1      auto   on      fcotAbsent       --     --           --
```

```
fc1/7      1      auto   on      fcotAbsent       --     --           --
fc1/8      1      auto   on      fcotAbsent       --     --           --
fc1/9      1      auto   on      fcotAbsent       --     --           --
fc1/10     1      auto   on      fcotAbsent       --     --           --
fc1/11     1      auto   on      fcotAbsent       --     --           --
fc1/12     1      auto   on      fcotAbsent       --     --           --
fc1/13     1      auto   on      fcotAbsent       --     --           --
fc1/14     1      auto   on      fcotAbsent       --     --           --
fc1/15     1      auto   on      fcotAbsent       --     --           --
fc1/16     1      auto   on      fcotAbsent       --     --           --

--------------------------------------------------------------------------------
Interface          Status                            Speed
                                                     (Gbps)
--------------------------------------------------------------------------------
sup-fc0            up                                1

--------------------------------------------------------------------------------
Interface               Status     IP Address         Speed        MTU
--------------------------------------------------------------------------------
mgmt0                   up         10.76.100.164/24   100 Mbps     1500


Power Supply:
------------------------------------------------------
PS  Model                Power     Power       Status
                         (Watts)   (Amp @42V)
------------------------------------------------------
1   WS-CAC-950W          919.38    21.89       ok
2                        --        --          absent

Mod Model                Power     Power       Power     Power       Status
                         Requested Requested   Allocated Allocated
                         (Watts)   (Amp @42V)  (Watts)   (Amp @42V)
--- -------------------  -------   ----------  --------- ----------  ----------
1    DS-X9216-K9-SUP     220.08    5.24        220.08    5.24        powered-up
2    DS-X9032            199.92    4.76        199.92    4.76        powered-up

Power Usage Summary:
--------------------
Power Supply redundancy mode:                  redundant

Total Power Capacity                           919.38   W

Power reserved for Supervisor(s)[-]            220.08   W
Power reserved for Fan Module(s)[-]            47.88    W
Power currently used by Modules[-]             199.92   W

                                               -------
Total Power Available                          451.50
```

The following example displays zone server information for VSAN 1.

```
switch# show tech-support zone vsan 1
`show zone status vsan 1`
VSAN: 1 default-zone: permit distribute: active only Interop: default
    mode: basic merge-control: allow session: none
    hard-zoning: enabled
Default zone:
    qos: disabled broadcast: disabled ronly: disabled
Full Zoning Database :
    Zonesets:0  Zones:0 Aliases: 0
Active Zoning Database :
    Name: vhost-zone  Zonesets:1  Zones:9
```

```
Status: Activation failed [Error: Unknown error Dom 21]:
        at 23:36:44 UTC Dec 19 2005
```

show telnet server

To display the state of the Telnet access configuration, use the **show telnet server** command.

show telnet server

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the status of the Telnet server.

```
switch# show telnet server
telnet service enabled
```

show terminal

To display the terminal information, use the **show terminal** command

show terminal

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays terminal information.

```
switch# show terminal
TTY:  Type: "vt100"
Length: 25 lines, Width: 80 columns
Session Timeout: 30 minutes
```

show tlport

To display configured TL port information, use the **show tlport** command

show tlport {**alpa-cache** | **discapp fcid** *fcid-id* [**vsan** *vsan-id*] [**verbose**] | **interface fc** *slot*/*port* {**all** | **private** | **proxied** | **topology** | **unsupported**} | **list** [**vsan** *vsan-id*]}

Syntax Description

alpa-cache	Displays the contents of the ALPA cache.
discapp	Displays private N port parameters.
fcid *fcid-id*	Specifies the FCID of the N port.
verbose	Specifies the verbose mode.
vsan *vsan-id*	Specifies the N port VSAN ID. The range is 1 to 4093.
interface	Displays TL ports in the selected interface.
fc *slot*/*port*	Specifies the Fiber Channel interface at the specified slot and port.
all	Displays all proxied & private devices on this TL Port.
private	Displays all private devices on this TL Port.
proxied	Displays all proxied devices on this TL Port.
topology	Displays loop topology for this TL Port.
unsupported	Displays all unsupported devices on this TL Port.
list	Displays TL ports in all VSANs.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The **show tlport** command displays the TL port interface configurations. This command provides a list of all TL ports configured on a box and displays the associated VSAN, the FCID for the port (only domain and area are valid), and the current operational state of the TL port (up or initializing).

Examples

The following example displays the TL ports in all VSANs.

```
switch# show tlport list
-------------------------------
Interface Vsan FC-ID    State
------------------------ ------
fc1/16    1    0x420000 Init
fc2/26    1    0x150000 Up
```

The following example displays the detailed information for a specific TL port.

```
switch# show tlport interface fc1/16 all
fc1/16 is up, vsan 1, FCID 0x420000
--------------------------------------------------------------------------------
alpa pWWN                   nWWN                   SCSI Type Device  FC-ID
--------------------------------------------------------------------------------
0x01 20:10:00:05:30:00:4a:de 20:00:00:05:30:00:4a:de Initiator Proxied 0xfffc42
0x73 22:00:00:20:37:39:ae:54 20:00:00:20:37:39:ae:54 Target    Private 0x420073
0xef 20:10:00:05:30:00:4a:de 20:00:00:05:30:00:4a:de Initiator Switch  0x0000ef
```

The following example displays TL port information for private devices.

```
switch# show tlport int fc1/16 pri
fc1/16 is up, vsan 1, FCID 0x420000
------------------------------------------------------------------------
alpa pWWN                   nWWN                   SCSI Type FC-ID
------------------------------------------------------------------------
0x73 22:00:00:20:37:39:ae:54 20:00:00:20:37:39:ae:54 Target    0x420073
0x74 22:00:00:20:37:38:d3:de 20:00:00:20:37:38:d3:de Target    0x420074
```

The following example displays TL port information for proxied devices.

```
switch# show tlport int fc1/16 prox
fc1/16 is up, vsan 1, FCID 0x420000
------------------------------------------------------------------------
alpa pWWN                   nWWN                   SCSI Type FC-ID
------------------------------------------------------------------------
0x01 20:10:00:05:30:00:4a:de 20:00:00:05:30:00:4a:de Initiator 0xfffc42
0x02 21:00:00:e0:8b:01:95:e7 20:00:00:e0:8b:01:95:e7 Initiator 0x420100
```

The following example displays the contents of the alpa-cache.

```
switch# show tlport alpa-cache
-----------------------------------------------------
alpa              pWWN               Interface
-----------------------------------------------------
0x02  22:00:00:20:37:46:09:bd     fc1/2
0x04  23:00:00:20:37:46:09:bd     fc1/2
```

show topology

To display topology information for connected switches, use the **show topology** command.

show topology [**vsan** *vsan-id*]

Syntax Description

vsan *vsan-id*	Displays information for a VSAN. The range is 1 to 4093.

Defaults

Displays information for all VSANs.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays topology information.

```
switch# show topology

FC Topology for VSAN 1 :
--------------------------------------------------------------------------------
           Interface         Peer Domain      Peer Interface     Peer IP Address
--------------------------------------------------------------------------------
               fc1/1           0xef(239)              fc2/15       172.22.46.220
               fc1/5           0xe6(230)               fc1/5       172.22.46.222
               fc1/6           0xe6(230)               fc1/6       172.22.46.222
               fc1/7           0xe6(230)               fc1/7       172.22.46.222
               fc1/8           0xe3(227)               fc1/1       172.22.46.233
              fc1/10           0xe6(230)              fc1/10       172.22.46.222
              fc1/11           0xe6(230)              fc1/11       172.22.46.222
              fc1/12           0xe6(230)              fc1/12       172.22.46.222
              fc1/13           0xe6(230)              fc1/13       172.22.46.222
              fc1/14           0xe6(230)              fc1/14       172.22.46.222
              fc1/15           0xe6(230)              fc1/15       172.22.46.222
              fc1/16           0xe6(230)              fc1/16       172.22.46.222
               fcip2           0xef(239)               fcip2       172.22.46.220

FC Topology for VSAN 73 :
--------------------------------------------------------------------------------
           Interface         Peer Domain      Peer Interface     Peer IP Address
--------------------------------------------------------------------------------
               fc1/1           0x65(101)              fc2/15       172.22.46.220
               fcip2           0x65(101)               fcip2       172.22.46.220
```

```
FC Topology for VSAN 4001 :
-------------------------------------------------------------------------------
           Interface         Peer Domain      Peer Interface     Peer IP Address
-------------------------------------------------------------------------------
               fc1/1           0xef(239)              fc2/15       172.22.46.220
               fc1/5           0xeb(235)               fc1/5       172.22.46.222
               fc1/6           0xeb(235)               fc1/6       172.22.46.222
               fc1/7           0xeb(235)               fc1/7       172.22.46.222
               fc1/8           0xed(237)               fc1/1       172.22.46.233
              fc1/10           0xeb(235)              fc1/10       172.22.46.222
              fc1/11           0xeb(235)              fc1/11       172.22.46.222
              fc1/12           0xeb(235)              fc1/12       172.22.46.222
              fc1/13           0xeb(235)              fc1/13       172.22.46.222
              fc1/14           0xeb(235)              fc1/14       172.22.46.222
              fc1/15           0xeb(235)              fc1/15       172.22.46.222
              fc1/16           0xeb(235)              fc1/16       172.22.46.222
               fcip2           0xef(239)               fcip2       172.22.46.220

FC Topology for VSAN 4002 :
-------------------------------------------------------------------------------
           Interface         Peer Domain      Peer Interface     Peer IP Address
-------------------------------------------------------------------------------
               fc1/1           0xeb(235)              fc2/15       172.22.46.220
               fc1/5           0xe9(233)               fc1/5       172.22.46.222
               fc1/6           0xe9(233)               fc1/6       172.22.46.222
               fc1/7           0xe9(233)               fc1/7       172.22.46.222
               fc1/8            0x1c(28)               fc1/1       172.22.46.233
              fc1/10           0xe9(233)              fc1/10       172.22.46.222
              fc1/11           0xe9(233)              fc1/11       172.22.46.222
              fc1/12           0xe9(233)              fc1/12       172.22.46.222
              fc1/13           0xe9(233)              fc1/13       172.22.46.222
              fc1/14           0xe9(233)              fc1/14       172.22.46.222
              fc1/15           0xe9(233)              fc1/15       172.22.46.222
              fc1/16           0xe9(233)              fc1/16       172.22.46.222
               fcip2           0xeb(235)               fcip2       172.22.46.220

FC Topology for VSAN 4003 :
-------------------------------------------------------------------------------
           Interface         Peer Domain      Peer Interface     Peer IP Address
-------------------------------------------------------------------------------
               fc1/1           0xdd(221)              fc2/15       172.22.46.220
               fc1/5           0xdb(219)               fc1/5       172.22.46.222
               fc1/6           0xdb(219)               fc1/6       172.22.46.222
               fc1/7           0xdb(219)               fc1/7       172.22.46.222
               fc1/8            0x60(96)               fc1/1       172.22.46.233
              fc1/10           0xdb(219)              fc1/10       172.22.46.222
              fc1/11           0xdb(219)              fc1/11       172.22.46.222
              fc1/12           0xdb(219)              fc1/12       172.22.46.222
              fc1/13           0xdb(219)              fc1/13       172.22.46.222
              fc1/14           0xdb(219)              fc1/14       172.22.46.222
              fc1/15           0xdb(219)              fc1/15       172.22.46.222
              fc1/16           0xdb(219)              fc1/16       172.22.46.222
               fcip2           0xdd(221)               fcip2       172.22.46.220

FC Topology for VSAN 4004 :
-------------------------------------------------------------------------------
           Interface         Peer Domain      Peer Interface     Peer IP Address
-------------------------------------------------------------------------------
               fc1/9             0x01(1)              Port 1       172.22.46.226
```

show trunk protocol

To display trunk protocol status, use the **show trunk protocol** command.

show trunk protocol

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays trunk protocol status.

```
switch# show trunk protocol
Trunk protocol is enabled
```

show user-account

To display configured information about user accounts, use the **show user-account** command.

show user-account [*user-name* | **iscsi**]

Syntax Description

user-name	Displays the user account information for the specified user name.
iscsi	Displays the iSCSI user account information.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays information for a specified user.

```
switch# show user-account user1
user:user1
        this user account has no expiry date
        roles:network-operator
no password set. Local login not allowed
Remote login through RADIUS is possible
```

The following example displays information for all users.

```
switch# show user-account
show user-account
user:admin
        this user account has no expiry date
        roles:network-admin

user:usam
        expires on Sat May 31 00:00:00 2003
        roles:network-admin network-operator

user:msam
        this user account has no expiry date
        roles:network-operator

user:user1
        this user account has no expiry date
        roles:network-operator
no password set. local login not allowed
Remote login through RADIUS is possible
```

show users

To display all users currently accessing the switch, use the **show users** command.

show users

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays all users.

```
switch# show users
admin    pts/7        Jan 12 20:56 (10.77.202.149)
admin    pts/9        Jan 12 23:29 (modena.cisco.com)
admin    pts/10       Jan 13 03:05 (dhcp-171-71-58-120.cisco.com)
admin    pts/11       Jan 13 01:53 (dhcp-171-71-49-49.cisco.com)
```

show version

To display the version of system software that is currently running on the switch, use the **show version** command.

show version [**clock-module epld** | **epld** *url* | **image** {**bootflash:** | **slot0:** | **volatile:**}*image-filename* | **module** *slot* [**epld**]]

Syntax Description

clock-module	Displays all current EPLD versions on the clock module.
epld	Displays all current versions of EPLDs on a specified module.
epld *url*	Displays all EPLD versions that are available at the specified URL (bootflash:, ftp:, scp:, sftp:, slot0:, tftp:, or volatile:)
image	Displays the software version of a given image.
bootflash:	Specifies internal bootflash memory.
slot0:	Specifies CompactFlash memory or PCMCIA card.
volatile:	Specifies the volatile directory.
image-filename	Specifies the name of the system or kickstart image.
module *slot*	Displays the software version of a module in the specified slot.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
1.0(3)	Command was modified.
3.0(1)	Added the **clock-module** option.

Usage Guidelines

Use the **show version image** command to verify the integrity of the image before loading the images. This command can be used for both the system and kickstart images.

Use the **show version** command to verify the version on the active and standby supervisor modules before and after an upgrade.

Examples

The following examples display the versions of the system, kickstart, and failed images.

```
switch(boot)# show version image bootflash:system_image <------------system image
 image name: m9500-sf1ek9-mz.1.0.3.bin
 system:     version 1.0(3)
 compiled:   10/25/2010 12:00:00
```

```
switch(boot)# show version image bootflash:kickstart_image <-------------kickstart image
  image name: m9500-sf1ek9-kickstart-mz.1.0.3.upg.bin
  kickstart:  version 1.0(3)
  loader:     version 1.0(3)
  compiled:   10/25/2010 12:00:00

switch# show version image bootflash:bad_image <--------------failure case
Md5 Verification Failed
Image integrity check failed
```

The following example displays current EPLD versions for a specified module.

```
switch# show version module 2 epld
Module Number                       2
EPLD Device                   Version
------------------------------------
Power Manager                    0x06
XBUS IO                          0x07
UD chip Fix                      0x05
Sahara                           0x05
```

The following example displays available EPLD versions.

```
switch# show version epld bootflash:m9000-epld-2.0.1b.img
MDS series EPLD image, built on Mon Sep 20 16:39:36 2004
Module Type                          EPLD Device         Version
------------------------------------------------------------------
MDS 9500 Supervisor 1                XBUS 1 IO              0x09
                                     XBUS 2 IO              0x0c
                                     UD Flow Control        0x05
                                     PCI ASIC I/F           0x04
1/2 Gbps FC Module (16 Port)         XBUS IO                0x07
                                     UD Flow Control        0x05
                                     PCI ASIC I/F           0x05
1/2 Gbps FC Module (32 Port)         XBUS IO                0x07
                                     UD Flow Control        0x05
                                     PCI ASIC I/F           0x05
Advanced Services Module             XBUS IO                0x07
                                     UD Flow Control        0x05
                                     PCI ASIC I/F           0x05
                                     PCI Bridge             0x05
IP Storage Services Module (8 Port)  Power Manager          0x07
                                     XBUS IO                0x03
                                     UD Flow Control        0x05
                                     PCI ASIC I/F           0x05
                                     Service Module I/F     0x0a
                                     IPS DB I/F             0x1a
IP Storage Services Module (4 Port)  Power Manager          0x07
                                     XBUS IO                0x03
                                     UD Flow Control        0x05
                                     PCI ASIC I/F           0x05
                                     Service Module I/F     0x1a
Caching Services Module Power        Manager                0x08
                                     XBUS IO                0x03
                                     UD Flow Control        0x05
                                     PCI ASIC I/F           0x05
                                     Service Module I/F     0x72
                                     Memory Decoder 0       0x02
                                     Memory Decoder 1       0x02
MDS 9100 Series Fabric Switch        XBUS IO                0x03
                                     PCI ASIC I/F           0x40000003
2x1GE IPS, 14x1/2Gbps FC Module      Power Manager          0x07
                                     XBUS IO                0x05
                                     UD Flow Control        0x05
                                     PCI ASIC I/F           0x07
                                     IPS DB I/F             0x1a
```

The following example displays the entire output for the show version command.

```
switch# show version
Cisco Storage Area Networking Operating System (SAN-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2003, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
Andiamo Systems, Inc. and/or other third parties and are used and
distributed under license. Some parts of this software are covered
under the GNU Public License. A copy of the license is available
at http://www.gnu.org/licenses/gpl.html.

Software
  BIOS:      version 1.0.8
  loader:    version 1.1(2)
  kickstart: version 2.0(1b) [build 2.0(0.6)] [gdb]
  system:    version 2.0(1b) [build 2.0(0.6)] [gdb]
```

```
  BIOS compile time:       08/07/03
  kickstart image file is: bootflash:///m9500-sf1ek9-kickstart-mzg.2.0.0.6.bin
  kickstart compile time:  10/25/2010 12:00:00
  system image file is:    bootflash:///m9500-sf1ek9-mzg.2.0.0.6.bin
  system compile time:     10/25/2020 12:00:00


Hardware
  RAM 1024584 kB

  bootflash: 1000944 blocks (block size 512b)
  slot0:           0 blocks (block size 512b)

  172.22.92.181 uptime is 0 days 2 hours 18 minute(s) 1 second(s)

  Last reset at 970069 usecs after Tue Sep 16 22:31:25 1980
    Reason: Reset Requested by CLI command reload
    System version: 2.0(0.6)
    Service:
```

The following examples displays a before and after comparison scenario after the loader version is updated.

```
switch# show version
Cisco Storage Area Networking Operating System (SAN-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2003 by Cisco Systems, Inc. All rights reserved.
The copyright for certain works contained herein are owned by
Andiamo Systems, Inc. and/or other third parties and are used and
distributed under license.
Software
  BIOS:      version 1.0(3)
  loader:    version 1.0(2) <----------existing version
  kickstart: version 1.0(3)
  system:    version 1.0(3)
  BIOS compile time:       11/18/02
  kickstart image file is: bootflash:/kickstart_image
  kickstart compile time:  1/20/2003 12:00:00
  system image file is:    bootflash:/system_image
  system compile time:     1/20/2003 12:00:00

switch# show version
Cisco Storage Area Networking Operating System (SAN-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2003 by Cisco Systems, Inc. All rights reserved.
The copyright for certain works contained herein are owned by
Andiamo Systems, Inc. and/or other third parties and are used and
distributed under license.
Software
  BIOS:      version 1.0(3)
  loader:    version 1.0(3) <----------new version
.....
```

The following example displays the version details for a specified module.

```
switch# show ver mod 4
Mod No   Mod Type       SW Version           SW Interim Version
4        LC             1.0(3)               1.0(3)
```

show vrrp

To display the VRRP configuration information, use the **show vrrp** command.

show vrrp [**ipv6**] [**statistics** | **vr** *group* [**interface** *type*]]

Syntax Description

ipv6	Displays IPv6 virtual router information.
statistics	Displays cumulative VRRP statistics for this device.
vr *group*	Displays the virtual router information. The range is 1 to 255.
interface *type*	Displays the interface type, which can be **mgmt 0** for the management interface, Gigabit Ethernet, PortChannel, or VSAN for the IPFC VSAN interface.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the **IPv6** option.

Usage Guidelines

None.

Examples

The following example displays VRRP configured information.

```
switch# show vrrp vr 7 interface vsan 2 configuration
vr id 7 configuration
admin state down
priority 100
no authentication
advertisement-Interval 1
preempt yes
tracking interface vsan1 priority 2
protocol IP
```

The following example displays VRRP status information.

```
switch# show vrrp vr 7 interface vsan 2 status
vr id 7 status
MAC address 00:00:5e:00:01:07
Operational state: init
```

The following example displays VRRP statistics.

```
switch# show vrrp vr 7 interface vsan 2 statistics
vr id 7 statistics
Become master 0
Advertisement 0
Advertisement Interval Error 0
Authentication Failure 0
TTL Error 0
Priority 0 Received 0
Priority 0 Sent 0
Invalid Type 0
Mismatch Address List 0
Invalid Authentication Type 0
Mismatch Authentication 0
Invalid Packet Length 0
```

The following example displays VRRP cumulative statistics.

```
switch# show vrrp statistics
Invalid checksum 0
Invalid version 0
Invalid VR ID 0
```

The following example displays VRRP IPv6 configuration information.

```
switch# show vrrp ipv6 vr 1 interface gigabitethernet 4/8 configuration
IPv6 vr id 1 configuration
admin state up
priority 100
associated ip: 2550:1::3:408:1 accept
advertisement-interval 100
preempt no
protocol IPv6
```

The following example displays VRRP IPv6 statistics information.

```
switch# show vrrp ipv6 vr 1 interface gigabitethernet 4/8 statistics
IPv6 vr id 1 statistics
Become master 1
Advertisement 0
Advertisement Interval Error 0
TTL Error 0
Priority 0 Received 0
Priority 0 Sent 0
Invalid Type 0
Mismatch Address List 0
Invalid Packet Length 0
```

The following example displays VRRP IPv6 status information.

```
switch# show vrrp ipv6 vr 1 interface gigabitethernet 4/8 status
IPv6 vr id 1 status
MAC address 00:00:5e:00:02:01
Operational state: master
Up time 17 hour(s),  21 min,  43 sec
Master IP address: fe80::20c:30ff:fe0c:f6c7
```

show vsan

To display information about configured VSAN, use the **show vsan** command.

show vsan [*vsan-id* [**membership**] | **membership interface** {**fc** *slot/port* | **fcip** *fcip-id* | **fv** *slot/dpp-number/fv-port* | **iscsi** *slot/port* | **portchannel** *portchannel-number.subinterface-number*}] | **usage**]

Syntax Description

vsan *vsan-id*	Displays information for the specified VSAN ID. The range is 1 to 4093.
membership	Displays membership information.
interface	Specifies the interface type.
fc *slot/port*	Specifies a Fibre Channel interface by the slot and port.
fcip *fcip-id*	Specifies a FC IP interface ID. The range is 1 to 255.
fv *slot/dpp-number/fv-port*	Specifies a virtual F port (FV port) interface in the specified slot along with the data path processor (DPP) number and the FV port number.
port-channel *portchannel-number.subinterface-number*	Specifies a PortChannel interface specified by the PortChannel number followed by a dot (.) indicator and the subinterface number.
usage	Displays VSAN usage in the system.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(2)	This command was modified.

Usage Guidelines

For the **show vsan membership interface** command, interface information is not displayed if interfaces are not configured on this VSAN.

The interface range must be in ascending order and non-overlapping. You can specify a range using a hyphen and several interfaces using commas:

- The interface range format for an FC interface range is **fc***slot/port - port* **, fc***slot/port* **, fc***slot/port*
  (For example, `show int fc1/1 - 3 , fc1/5 , fc2/5`)
- The interface range format for an FV interface range is **fv***slot/dpp/fvport* **-** *fvport* , **fv***slot/dpp/port* , **fv***slot/dpp/port*
  (For example, `show int fv2/1/1 - 3 , fv2/1/5 , fv2/2/5`)
- The format for a PortChannel is **port-channel** *portchannel-number.subinterface-number*
  (For example, **show int port-channel 5.1***)*

Examples

The following examples displays configured VSAN information.

```
switch# show vsan 1
vsan 1 information
         name:VSAN0001  state:active
         interoperability mode:yes ß verify mode
         loadbalancing:src-id/dst-id/oxid
         operational state:up

switch# show vsan usage
4 vsan configured
configured vsans:1-4
vsans available for configuration:5-4093

switch # show vsan 1 membership
vsan 1 interfaces:
        fc1/1   fc1/2   fc1/3   fc1/4   fc1/5   fc1/6   fc1/7   fc1/9
        fc1/10  fc1/11  fc1/12  fc1/13  fc1/14  fc1/15  fc1/16  port-channel 99
```

The following example displays membership information for all VSANs.

```
switch # show vsan membership
vsan 1 interfaces:
        fc2/16  fc2/15  fc2/14  fc2/13  fc2/12  fc2/11  fc2/10  fc2/9
        fc2/8   fc2/7   fc2/6   fc2/5   fc2/4   fc2/3   fc2/2   fc2/1
        fc1/16  fc1/15  fc1/14  fc1/13  fc1/12  fc1/11  fc1/10  fc1/9
        fc1/7   fc1/6   fc1/5   fc1/4   fc1/3   fc1/2   fc1/1
vsan 2 interfaces:
vsan 7 interfaces:
        fc1/8
vsan 100 interfaces:
vsan 4094(isolated vsan) interfaces:
```

The following example displays membership information for a specified interface.

```
switch # show vsan membership interface fc1/1
fc1/1
        vsan:1
        allowed list:1-4093

switch# show vsan
vsan 1 information
         name:VSAN0001  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 2 information
         name:VmVSAN  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 3 information
         name:Disk_A  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 4 information
         name:Host_B  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up
```

```
vsan 4094:isolated_vsan

switch# show vsan membership interface fv 2/1/3 , fv2/1/5 - 7
fv2/1/3
        vsan:2
        allowed list:1-4093
fv2/1/5
        vsan:3
        allowed list:1-4093
fv2/1/6
        vsan:4
        allowed list:1-4093
fv2/1/7
        vsan:4
        allowed list:1-409
```

show wwn

To display the status of the WWN configuration, use the **show wwn** command.

show wwn {**status block-id** *number* | **switch** | **vsan-wwn**}

Syntax Description

status block-id *number*	Displays WWN usage and alarm status for a block ID. The range is 34 to 1793.
switch	Displays switch WWN.
vsan-wwn	Displays all user-configured VSAN WWNs.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the **vsan-wwn** keyword.

Usage Guidelines

None.

Examples

The following example displays the WWN of the switch.

```
switch# show wwn switch
Switch WWN is 20:01:ac:16:5e:52:00:01
```

The following example displays a user-configured VSAN WWN.

```
switch# show wwn vsan-wwn
vsan wwn configured by user
---- ----------------------
100 20:64:08:00:88:0d:5f:81
```

show zone

To display zone information, use the **show zone** command.

show zone
[**active** [**vsan** *vsan-id*] |
ess [**vsan** *vsan-id*] |
member {**fcalias** *alias-name* | **fcid** *fcid-id* [**lun** *lun-id*] | **pwwn** *wwn* [**lun** *lun-id*]} [**active** | **vsan** *vsan-id*] |
name *string* [**active**] [**vsan** *vsan-id*] |
statistics [**lun-zoning** [**vsan** *vsan-id*] | **read-only-zoning** [**vsan** *vsan-id*] | **vsan** *vsan-id*] |
status [**vsan** *vsan-range*]
vsan [**vsan** *vsan-id*]]

Syntax Description

active	Displays zones which are part of active zone set.
ess	Displays ESS information.
member	Displays all zones in which the given member is part of.
name	Displays members of a specified zone.
statistics	Displays zone server statistics.
status	Displays zone server current status.
vsan *vsan-id*	Displays zones belonging to the specified VSAN ID. The range is 1 to 4093.
lun *lun-id*	Specifies a LUN ID.
lun-zoning	Displays LUN zoning related statistics
read-only-zoning	Displays read-only zoning related statistics

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.
2.1(1a)	Modified the **show zone status** display.

Usage Guidelines

None.

Examples

The following example displays configured zone information.

```
switch# show zone
zone name Zone3 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:9c:48:e5
zone name Zone2 vsan 2
```

```
  fwwn 20:41:00:05:30:00:2a:1e
  fwwn 20:42:00:05:30:00:2a:1e
  fwwn 20:43:00:05:30:00:2a:1e
zone name Zone1 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:a6:be:2f
  pwwn 21:00:00:20:37:9c:48:e5
  fcalias Alias1
zone name Techdocs vsan 3
  ip-address 10.15.0.0 255.255.255.0
```

The following example displays zone information for a specific VSAN.

```
switch# show zone vsan 1
zone name Zone3 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:9c:48:e5
zone name Zone2 vsan 1
  fwwn 20:41:00:05:30:00:2a:1e
  fwwn 20:42:00:05:30:00:2a:1e
  fwwn 20:43:00:05:30:00:2a:1e
  fwwn 20:44:00:05:30:00:2a:1e
  fwwn 20:45:00:05:30:00:2a:1e
  fwwn 20:46:00:05:30:00:2a:1e
  fwwn 20:47:00:05:30:00:2a:1e
  fwwn 20:48:00:05:30:00:2a:1e
  fwwn 20:49:00:05:30:00:2a:1e
  fwwn 20:4a:00:05:30:00:2a:1e
  fwwn 20:4b:00:05:30:00:2a:1e
  fwwn 20:4c:00:05:30:00:2a:1e
  fwwn 20:4d:00:05:30:00:2a:1e
  fwwn 20:4e:00:05:30:00:2a:1e
  fwwn 20:4f:00:05:30:00:2a:1e
  fwwn 20:50:00:05:30:00:2a:1e
  fwwn 20:51:00:05:30:00:2a:1e
  fwwn 20:52:00:05:30:00:2a:1e
  fwwn 20:53:00:05:30:00:2a:1e
  fwwn 20:54:00:05:30:00:2a:1e
  fwwn 20:55:00:05:30:00:2a:1e
  fwwn 20:56:00:05:30:00:2a:1e
  fwwn 20:57:00:05:30:00:2a:1e
  fwwn 20:58:00:05:30:00:2a:1e
  fwwn 20:59:00:05:30:00:2a:1e
  fwwn 20:5a:00:05:30:00:2a:1e
  fwwn 20:5b:00:05:30:00:2a:1e
  fwwn 20:5c:00:05:30:00:2a:1e
  fwwn 20:5d:00:05:30:00:2a:1e
  fwwn 20:5e:00:05:30:00:2a:1e
  fwwn 20:5f:00:05:30:00:2a:1e
  fwwn 20:60:00:05:30:00:2a:1e
zone name Zone1 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:a6:be:2f
  pwwn 21:00:00:20:37:9c:48:e5
  fcalias Alias1
```

The following example displays members of a specific zone.

```
switch# show zone name Zone1
zone name Zone1 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:a6:be:2f
  pwwn 21:00:00:20:37:9c:48:e5
  fcalias Alias1
```

The following example displays all zones to which a member belongs using the FCID.

```
switch# show zone member pwwn 21:00:00:20:37:9c:48:e5
          VSAN: 1
zone Zone3
zone Zone1
fcalias Alias1
```

The following example displays the number of control frames exchanged with other switches.

```
switch# show zone statistics
Statistics For VSAN: 1
**********************************
Number of Merge Requests Sent: 24
Number of Merge Requests Recvd: 25
Number of Merge Accepts Sent: 25
Number of Merge Accepts Recvd: 25
Number of Merge Rejects Sent: 0
Number of Merge Rejects Recvd: 0
Number of Change Requests Sent: 0
Number of Change Requests Recvd: 0
Number of Change Rejects Sent: 0
Number of Change Rejects Recvd: 0
Number of GS Requests Recvd: 0
Number of GS Requests Rejected: 0
Statistics For VSAN: 2
**********************************
Number of Merge Requests Sent: 4
...
Number of GS Requests Rejected: 0
```

The following example displays LUN-zoning details.

```
switch# show zone statistics lun-zoning
LUN zoning statistics for VSAN: 1
************************************************************
S-ID: 0x123456, D-ID: 0x22222, LUN: 00:00:00:00:00:00:00:00
------------------------------------------------------------
Number of Inquiry commands received:         10
Number of Inquiry data No LU sent:            5
Number of Report LUNs commands received:     10
Number of Request Sense commands received:    1
Number of Other commands received:            0
Number of Illegal Request Check Condition sent: 0

S-ID: 0x123456, D-ID: 0x22222, LUN: 00:00:00:00:00:00:00:01
------------------------------------------------------------
Number of Inquiry commands received:          1
Number of Inquiry data No LU sent:            1
Number of Request Sense commands received:    1
Number of Other commands received:            0
Number of Illegal Request Check Condition sent:  0
```

The following example displays read-only zone details.

```
switch# show zone statistics read-only-zoning
Read-only zoning statistics for VSAN: 2
************************************************************
S-ID: 0x33333, D-ID: 0x11111, LUN: 00:00:00:00:00:00:00:64
------------------------------------------------------------
Number of Data Protect Check Condition Sent:  12
```

The following example displays the status of the configured zones.

```
switch# show zone status
VSAN: 1 default-zone: deny distribute: active only Interop: default
    mode: basic merge-control: allow session: none
    hard-zoning: enabled
Default zone:
    qos: low broadcast: disabled ronly: disabled
Full Zoning Database :
    Zonesets:0  Zones:0 Aliases: 0
Active Zoning Database :
    Database Not Available
Status:
.............
VSAN: 3 default-zone: deny distribute: active only Interop: default
    mode: basic merge-control: allow session: none
    hard-zoning: enabled
Default zone:
    qos: low broadcast: disabled ronly: disabled
Full Zoning Database :
    Zonesets:0  Zones:0 Aliases: 0
Active Zoning Database :
    Database Not Available
Status:
```

The following example checks the status of the **zoneset distribute vsan** command and displays the default zone attributes of a specific VSAN or all active VSANs.

```
switch# show zone status vsan 1
VSAN:1 default-zone:deny distribute:active only Interop:default
    mode:basic merge-control:allow session:none
    hard-zoning:enabled
Default zone:
    qos:low broadcast:disabled ronly:disabled
Full Zoning Database :
    Zonesets:0  Zones:0 Aliases:0
Active Zoning Database :
    Database Not Available
Status:
```

Table 22-10 describes the significant fields shown in the **show zone status vsan** display.

Table 22-10 show zone status Field Descriptions

Field	Description
VSAN:	VSAN number displayed
default-zone:	Default-zone policy either permit or deny.
Default zone:	The Default zone field displays the attributes for the specified VSAN. The attributes include: Qos level, broadcast zoning enabled/disabled, and read-only zoning enabled/disabled.
distribute:	Distribute full-zone set (full) or active-zone set (active only).
Interop:	Displays interop mode. 100 = default, 1 = standard, 2 and 3 = Non-Cisco Vendors.
mode:	Displays zoning mode either basic or enhanced.
merge control:	Displays merge policy either allow or restrict.
Hard zoning is enabled	If hardware resources (TCAM) becomes full, hard zoning is automatically disabled.

Table 22-10 show zone status Field Descriptions (continued)

Field	Description
Full Zoning Database:	Displays values of zone database.
Active Zoning Database:	Displays values of active zone database.
Status:	Displays status of last zone distribution.

show zone analysis

To display detailed analysis and statistical information about the zoning database, use the **show zone analysis** command.

show zone analysis {active vsan *vsan-id* **| vsan** *vsan-id* **| zoneset** *name* **vsan** *vsan-id*} **|**

Syntax Description

active	Displays analysis information for the active zone set.
vsan *vsan-id*	Displays analysis information for the specified VSAN ID. The range is 1 to 4093.
zoneset *name*	Displays zone set analysis information for the specified zone set.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays detailed statistics and analysis of the active zoning database.

```
switch# show zone analysis active vsan 1
   Zoning database analysis vsan 1
     Active zoneset : zs1 [* | -]
       Activated at: 14:36:56 UTC Oct 04 2005
       Activated From: Local [CLI / SNMP / GS / CIM / INTERNAL] or
                       Merge [interface] or
                       Remote [Domain, IP-Address]
                              [Switch name]
       Default zone policy: permit/deny
       Number of devices zoned in vsan: 8/10 (Unzoned: 2 | Default-zone: #)
       Number of zone members resolved: 11/16 (Unresolved: 5)
       Num zones: 1
       Number of IVR zones: 2
       Number of IPS zones: 3
       Formatted database size: < 1 Kb / 2000 kb ( < 1% usage)
```

Table 22-11 describes the fields displayed in the output of a **show zone analysis** command for the active zoning database.

Table 22-11 show zone analysis Field Descriptions for the Active Zoning Database

Field	Description
Active zoneset	Displays the active zone set name. If a zone set has changed in the full zoning database, an asterisk (*) appears after the zone set name. If the active zone set is not present in the full zoning database, a minus sign (-) appears after the zone set name.
Activated at	Displays the time the zone set was activated.
Activated from	Displays the agent that most recently modified the active zoning database. The agent can be one of the following three types: • Local: indicates that the active database was last modified locally through a configuration change from one of the following applications: – CLI: The active zoning database was modified by the user from the Command Line Interface. – SNMP: The active zoning database was modified by the user through the Simple Network Management Protocol (SNMP). – GS: The active zoning database was modified from the Generic Services (GS) client. – CIM: The active zoning database was modified by the applications using the Common Information Model (CIM). – INTERNAL: The active zoning database was modified as a result of an internal activation either from Inter-VSAN Routing (IVR) or from the IP Storage services manager. • Merge: indicates that the active database was last modified by the Merge protocol. The interface on which the merge occurred is also displayed. • Remote: indicates that the active database was last modified by the Change protocol, initiated by a remote switch. The domain, IP address, and switch name of the switch initiating the change are also displayed. **Note** The switch name is displayed on the next line, aligned with the domain, only if the switch name is set. The default switch name *switch* and the *ip-address* are not displayed.
Default zoning policy: permit/deny	Displays the status of the default zoning policy for this VSAN.

Table 22-11 show zone analysis Field Descriptions for the Active Zoning Database

Field	Description
Number of devices zoned in vsan: a/b (Unzoned: c | Default-zone: d)	Displays the number of devices that are present in the zoning configuration. • a = The number of unique resolved members in the active database. • b = The number of devices logged in, which is the same as the number of entries in the Fibre Channel name server (FCNS) database. • c = The number of devices logged in, but not zoned in the zoning configuration. • d = The number of devices in the default zone. d is displayed only if the default zoning policy is permit.
Number of zone members resolved: a/b (Unresolved: c)	Displays the number of members that are resolved in this VSAN in the form: a out of b members in the zone set are resolved. The number of resolved members is not necessarily unique. For example, if a pWWN member and a fWWN member resolve to the same FC ID, then that member is counted as two resolved members out of two members present. • a = The number of members resolved. • b = The total number of members present. • c = The total number of members unresolved.
Num zones	Displays the total number of zones that are present in the active zone set.
Number of IVR zones	Displays the number of zones added and activated by IVR.
Number of IPS zones	Displays the number of zones added and activated by the IP Storage services manager (IPS-MGR).
Formatted database size	Displays the total size of the active database when formatted to be sent over the wire. The formatted database size is displayed in kilobytes (KB) in this format: < *X* KB / *Y* KB, as in the following example. Formatted database size: < 1 KB/2000 KB In this example, the formatted database size is less than 1 KB out of the maximum size of 2000 KB.

The following example displays detailed statistics and analysis of the full zoning database.

```
switch# sh zone analysis vsan 1
   Zoning database analysis vsan 1
     Full zoning database
       Last updated at: 14:36:56 UTC Oct 04 2005
       Last updated by: Local [CLI / SNMP / GS / CIM / INTERNAL] or
                        Merge [interface] or
                        Remote [Domain, IP-Address]
                               [Switch name]
       Num zonesets: 1
       Num zones: 1
       Num aliases: 0
       Num attribute groups: 0
       Formatted database size: < 1 Kb / 2000 kb ( < 1% usage)

     Unassigned zones:
       zone name z1 vsan 1
```

Table 22-12 describes the fields displayed in the output of a **show zone analysis** command for the full zoning database.

Table 22-12 show zone analysis Field Descriptions for the Full Zoning Database

Field	Description
Last updated at	Displays a time stamp showing when the full zoning database was last updated.
Last Updated by	Displays the agent that most recently modified the full zoning database. The agent can be one of the following three types: • Local: indicates that the full database was last modified locally through a configuration change from one of the following applications: – CLI: The full zoning database was modified by the user from the Command Line Interface. – SNMP: The full zoning database was modified by the user through the Simple Network Management Protocol (SNMP). – GS: The full zoning database was modified from the Generic Services (GS) client. – CIM: The full zoning database was modified by the applications using the Common Information Model (CIM). – INTERNAL: The full zoning database was modified as a result of an internal activation either from Inter-VSAN Routing (IVR) or from the IP Storage services manager. • Merge: indicates that the full database was last modified by the Merge protocol. In this case, the interface on which the merge occurred is also displayed. • Remote: indicates that the full database was last modified by the Change protocol, initiated by a remote switch, when the full zone set distribution was enabled. The domain, IP address, and switch name of the switch initiating the change are also displayed. **Note** The switch name is displayed on the next line, aligned with the domain, only if the switch name is set. The default switch name *switch* and the *ip-address* are not displayed.
Num zonesets	Displays the total number of zone sets in the database.
Num zones	Displays the total number of zones in the database, including unassigned zones.
Num aliases	Displays the total number of aliases in the database, including unassigned FC aliases.
Num attribute groups	Displays the total number of attribute groups in the database. This field applies only when enhanced zoning is used.

Table 22-12 show zone analysis Field Descriptions (continued)for the Full Zoning Database

Field	Description
Formatted database size	Displays the total size of the full database when formatted to be sent over the wire. The formatted database size is displayed in kilobytes in this format: < *X* KB / *Y* KB, as in the following example. Formatted database size: < 1 KB/2000 KB In this example, the formatted database size is less than 1 KB out of the maximum size of 2000 KB.
Unassigned zones	Displays all the unassigned zones in the VSAN. Only the names of the zones are displayed. The details about the members of the zone are not displayed in this section.

The followng example displays zone set analysis information. See Table 22-12 for a description of the fields in this example.

```
switch# show zone analysis zoneset zs1 vsan 1
Zoning database analysis vsan 1
  Zoneset analysis: zs1
    Num zonesets: 1
    Num zones: 0
    Num aliases: 0
    Num attribute groups: 0
    Formattted size: 20 bytes / 2048 Kb
```

Related Commands

Command	Description
zone compact database	Compacts a zone database in a VSAN.

show zone-attribute-group

To display the device name information, use the **show zone-attribute-group** command.

show zone-attribute-group [**name** *group-name*] [**pending**] [**vsan** *vsan-id*]

Syntax Description

name *group-name*	Displays the entire device name database.
pending	Displays the pending device name database information.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Defaults

Displays information for default zone attribute groups.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the contents of pending zone attribute groups.

```
switch# show zone-autoboot-group pending
zone-attribute-group name $default_zone_attr_group$ vsan 4061
zone-attribute-group name admin-group vsan 4061
  broadcast
```

Related Commands

Command	Description
zone-attribute-group name	Configures zone attribute groups.

show zoneset

To display the configured zone sets, use the **show zoneset** command.

show zoneset [**name** *zoneset-name*] [**brief**] [**active**] [**vsan** *vsan-id*]

Syntax Description

name *zoneset-name*	Displays members of a specified zone set. Maximum length is 64 characters.
brief	Displays members in brief mode.
active	Displays only active zone sets.
vsan *vsan-id*	Displays zone sets belonging to the specified VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

EXEC mode

Command History

Release	Modification
1.2(2)	This command was modified.

Usage Guidelines

None.

Examples

The following example displays configured zone set information.

```
switch# show zoneset vsan 1
zoneset name ZoneSet2 vsan 1
  zone name Zone2 vsan 1
    fwwn 20:4e:00:05:30:00:2a:1e
    fwwn 20:4f:00:05:30:00:2a:1e
    fwwn 20:50:00:05:30:00:2a:1e
    fwwn 20:51:00:05:30:00:2a:1e
    fwwn 20:52:00:05:30:00:2a:1e
  zone name Zone1 vsan 1
    pwwn 21:00:00:20:37:6f:db:dd
    pwwn 21:00:00:20:37:a6:be:2f
    pwwn 21:00:00:20:37:9c:48:e5
    fcalias Alias1
zoneset name ZoneSet1 vsan 1
  zone name Zone1 vsan 1
    pwwn 21:00:00:20:37:6f:db:dd
    pwwn 21:00:00:20:37:a6:be:2f
    pwwn 21:00:00:20:37:9c:48:e5
    fcalias Alias1
```

The following example displays configured zone set information for a specific VSAN.

```
switch# show zoneset vsan 2-3
zoneset name ZoneSet2 vsan 1
  zone name Zone2 vsan 1
    fwwn 20:52:00:05:30:00:2a:1e
    fwwn 20:53:00:05:30:00:2a:1e
    fwwn 20:54:00:05:30:00:2a:1e
    fwwn 20:55:00:05:30:00:2a:1e
    fwwn 20:56:00:05:30:00:2a:1e
  zone name Zone1 vsan 1
    pwwn 21:00:00:20:37:6f:db:dd
    pwwn 21:00:00:20:37:a6:be:2f
    pwwn 21:00:00:20:37:9c:48:e5
    fcalias Alias1
zoneset name ZoneSet1 vsan 1
  zone name Zone1 vsan 1
    pwwn 21:00:00:20:37:6f:db:dd
    pwwn 21:00:00:20:37:a6:be:2f
    pwwn 21:00:00:20:37:9c:48:e5
    fcalias Alias1
```

CHAPTER 23

T Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "Command Modes" section to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

tacacs+ abort

To discard a TACACS+ Cisco Fabric Services (CFS) distribution session in progress, use the **tacacs+ abort** command in configuration mode.

tacacs+ abort

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, TACACS+ must be enabled using the **tacacs+ enable** command.

Examples

The following example shows how to discard a TACACS+ CFS distribution session in progress.

```
switch# config terminal
switch(config)# tacacs+ abort
```

Related Commands

Command	Description
show tacacs+	Displays TACACS+ CFS distribution status and other details.
tacacs+ distribute	Enables CFS distribution for TACACS+.
tacacs+ enable	Enables TACACS+.

tacacs+ commit

To apply the pending configuration pertaining to the TACACS+ Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **tacacs+ commit** command in configuration mode.

tacacs+ commit

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, TACACS+ must be enabled using the **tacacs+ enable** command.

Examples

The following example shows how to apply a TACACS+ configuration to the switches in the fabric.

```
switch# config terminal
switch(config)# tacacs+ commit
```

Related Commands

Command	Description
show tacacs+	Displays TACACS+ CFS distribution status and other details.
tacacs+ enable	Enables TACACS+.
tacacs+ distribute	Enables CFS distribution for TACACS+.

tacacs+ distribute

To enable Cisco Fabric Services (CFS) distribution for TACACS+, use the **tacacs+ distribute** command. To disable this feature, use the **no** form of the command.

tacacs+ distribute

no tacacs+ distribute

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, TACACS+ must be enabled using the **tacacs+ enable** command.

Examples

The following example shows how to enable TACACS+ fabric distribution.

```
switch# config terminal
switch(config)# tacacs+ distribute
```

Related Commands

Command	Description
show tacacs+	Displays TACACS+ CFS distribution status and other details.
tacacs+ commit	Commits TACACS+ database changes to the fabric.
tacacs+ enable	Enables TACACS+.

tacacs+ enable

To enable TACACS+ in a switch, use the **tacacs+ enable** command in configuration mode. The disable this feature, use the **no** form of the command.

tacacs+ enable

no tacacs+ enable

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Further TACACS+ commands are only available when the TACACS+ feature is enabled.

Using SHA-1 as the hash algorithm may prevent RADIUS or TACACS+ usage.

Examples

```
switch# config terminal
switch(config)# tacacs+ enable
```

Related Commands

Command	Description
show	Displays TACACS+ server information.

tacacs-server deadtime

To set a periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness, use the **tacacs-server deadtime** command. To disable the monitoring of the nonresponsive TACACS+ server, use the **no** form of the command.

tacacs-server deadtime *time*

no tacacs-server deadtime *time*

Syntax Description

time	Specifies the time interval in minutes. The range is 1 to 1440.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Setting the time interval to zero disables the timer. If the dead time interval for an individual TACACS+ server is greater than zero (0), that value takes precedence over the value set for the server group.

When the dead time interval is 0 minutes, TACACS+ server monitoring is not performed unless the TACACS+ server is part of a server group and the dead time interval for the group is greater than 0 minutes.

Examples

The following example shows how to set a duration of 10 minutes.

```
switch# config terminal
switch(config)# tacacs-server deadtime 10
```

Related Commands

Command	Description
deadtime	Sets a time interval for monitoring a nonresponsive TACACS+ server.
show tacacs-server	Displays all configured TACACS+ server parameters.

tacacs-server directed-request

To specify a TACACS+ server to send authentication requests to when logging in, use the **tacacs-server directed-request** command. To revert to sending the authentication request to the configured group, use the **no** form of the command.

tacacs-server directed-request

no tacacs-server directed-request

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The user can specify the *username@servername* during login. The user name is sent to the server name for authentication.

Examples

The following example shows how to specify a TACACS+ server to send authentication requests when logging in.

```
switch# config terminal
switch(config)# tacacs-server directed-request
```

Related Commands

Command	Description
show tacacs-server	Displays all configured TACACS+ server parameters.
show tacacs-server directed request	Displays a directed request TACACS+ server configuration.

tacacs-server host

To configure TACACS+ server options on a switch, use the **tacacs-server host** command in configuration mode. Use the **no** form of the command to revert to factory defaults.

tacacs-server host {*server-name* | *ipv4-address* | *ipv6-address*}
[**key** [**0**|**7**] *shared-secret*] [**port** *port-number*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds*]

no tacacs-server host {*server-name* | *ipv4-address* | *ipv6-address*}
[**key** [**0**|**7**] *shared-secret*] [**port** *port-number*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds*]

Syntax Description

server-name	Specifies the TACACS+ server DNS name. The maximum character size is 256.
ipv4-address	Specifies the TACACS+ server IP address. in the format *A.B.C.D*.
ipv6-address	Specifies the TACACS+ server IP address in the format *X:X::X*.
key	Configures the TACACS+ server's shared secret key.
0	Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the TACACS+ client and server. This is the default.
7	Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the TACACS+ client and server.
shared secret	Configures a preshared key to authenticate communication between the TACACS+ client and server.
port *port-number*	Configures a TACACS+ server port for authentication. The range is 1 to 65535.
test	Configures parameters to send test packets to the TACACS+ server.
idle-time *time*	Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.
password *password*	Specifies a user password in the test packets. The maximum size is 32.
username *name*	Specifies a user name in the test packets. The maximum size is 32.
timeout	Configures a TACACS+ server timeout period.
seconds	Specifies the timeout (in seconds) between retransmissions to the TACACS+ server. The range is 1 to 60 seconds.

Defaults

Idle-time is not set. Server monitoring is turned off.
Timeout is 1 second.
Username is test.
Password is test.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Added the *ipv6-address* argument and the **test** option.

Usage Guidelines

This command is only available when the TACACS+ feature is enabled using the **tacacs+ enable** command.

When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not performed.

Examples

The following example configures TACACS+ authentication.

```
switch# config terminal
switch(config)# tacacs-server host 10.10.2.3 key HostKey
switch(config)# tacacs-server host tacacs2 key 0 abcd
switch(config)# tacacs-server host tacacs3 key 7 1234
switch(config)# tacacs-server host 10.10.2.3 test idle-time 10
switch(config)# tacacs-server host 10.10.2.3 test username tester
switch(config)# tacacs-server host 10.10.2.3 test password 2B9ka5
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.
tacacs+ enable	Enables TACACS+.

tacacs-server key

To configure a global TACACS+ shared secret, use the **tacacs-server key** command. Use the **no** form of this command to removed a configured shared secret.

tacacs-server key [**0** | **7**] *shared-secret*

no tacacs-server key [**0** | **7**] *shared-secret*

Syntax Description

key	Global TACACS+ shared secret.
0	Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the TACACS+ client and server. This is the default.
7	Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the TACACS+ client and server.
shared-secret	Configures a preshared key to authenticate communication between the TACACS+ client and server.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You need to configure the TACACS+ preshared key to authenticate the switch to the TACACS+ server. The length of the key is restricted to 65 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all TACACS+ server configurations on the switch. You can override this global key assignment by explicitly using the **key** option in the **tacacs-server host** command.

This command is only available when the TACACS+ feature is enabled using the **tacacs+ enable** command.

Examples

The following example configures TACACS+ server shared keys.

```
switch# config terminal
switch(config)# tacacs-server key AnyWord
switch(config)# tacacs-server key 0 AnyWord
switch(config)# tacacs-server key 7 public
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.
tacacs+ enable	Enable TACACS+.

tacacs-server timeout

To specify the time between retransmissions to the TACACS+ servers, use the **tacacs-server timeout** command. You can revert the retransmission time to its default by issuing the **no** form of the command.

tacacs-server timeout *seconds*

notacacs-server timeout *seconds*

Syntax Description

seconds	Specifies the time (in seconds) between retransmissions to the RADIUS server. The default is one (1) second and the valid range is 1 to 60 seconds.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(2)	This command was introduced.

Usage Guidelines

This command is only available when the TACACS+ feature is enabled using the **tacacs+ enable** command.

Examples

The following example configures the TACACS+ server timeout value.

```
switch# config terminal
switch(config)# tacacs-server timeout 30
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.
tacacs+ enable	Enable TACACS+.

tail

To display the last lines (tail end) of a specified file, use the **tail** command in EXEC mode.

tail *filename* [*number-of-lines*]

Syntax Description

filename	The name of the file for which you want to view the last lines.
number-of-lines	(Optional) The number of lines you want to view. The range is 0 to 80 lines.

Defaults

Displays the last 10 lines.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You need two separate CLI terminals to use this command. In one terminal, execute the run-script or any other desired command. In the other, issue the **tail** command for the mylog file. On the second terminal session, you will see the last lines of the mylog file (as it grows) that is being saved in response to the command issued in the first terminal.

If you specify a long file and would like to exit in the middle, enter **Ctrl-c** to exit this command.

Examples

The following example displays the last lines (tail end) of a specified file.

```
switch# run-script slot0:test mylog
```

In another terminal, issue the **tail** command for the mylog file.

```
switch# tail mylog
config terminal
```

In the second CLI terminal, you see the last lines of the mylog file (as it grows) that is being saved in response to the command issued in the first terminal.

tape-read command-id

To configure a SCSI tape read command for a SAN tuner extension N port, use the **tape-read command-id** command.

tape-read command-id *cmd-id* **target** *pwwn* **transfer-size** *bytes* [**continuous [filemark-frequency** *frequency*] | **num-transactions** *number* [**filemark-frequency** *frequency*]]

Syntax Description

cmd-id	Specifies the command identifier. The range is 0 to 2147483647.
target *pwwn*	Specifies the target port WWN. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
transfer-size *bytes*	Specifies the transfer size in multiples of 512 bytes. The range is 512 to 8388608.
continuous	Specifies that the command is performed continuously.
filemark-frequency *frequency*	Specifies the filemark frequency. The range is 1 to 2147483647.
num-transactions *number*	Specifies a number of transactions. The range is 1 to 2147483647.

Defaults

Filemark frequency: 0.

Command Modes

SAN extension N port configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

To stop a continuous SCSI tape read command in progress, use the **stop command-id** command.

Note There can be just one outstanding I/O at a time to the virtual N port that emulates the tape behavior.

Examples

The following example configures a single SCSI tape read command.

```
switch# san-ext-tuner
switch(san-ext)# nWWN 10:00:00:00:00:00:00:00
switch(san-ext)# nport pwwn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2
switch(san-ext-nport)# tape-read command-id 100 target 22:22:22:22:22:22:22:22
transfer-size 512000 num-transactions 5000000 filemark-frequency 32
```

The following example configures a continuous SCSI tape read command.

```
switch# san-ext-tuner
switch(san-ext)# nWWN 10:00:00:00:00:00:00:00
switch(san-ext)# nport pwwn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2
switch(san-ext-nport)# tape-read command-id 100 target 22:22:22:22:22:22:22:22
transfer-size 512000 continuous filemark-frequency 32
```

Related Commands

Command	Description
nport pwwn	Configures a SAN extension tuner N port.
san-ext-tuner	Enables the SAN extension tuner feature.
show san-ext-tuner	Displays SAN extension tuner information.
stop	Cancels a SCSI command in progress on a SAN extension tuner N port.

tape-write command-id

To configure a SCSI tape write command for a SAN tuner extension N port, use the **tape-write command-id** command.

tape-write command-id *cmd-id* **target** *pwwn* **transfer-size** *bytes* [**continuous** [**filemark-frequency** *frequency*] | **num-transactions** *number* [**filemark-frequency** *frequency*]]

Syntax Description

cmd-id	Specifies the command identifier. The range is 0 to 2147483647.
target *pwwn*	Specifies the target port WWN. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
transfer-size *bytes*	Specifies the transfer size in multiples of 512 bytes. The range is 512 to 8388608.
continuous	Specifies that the command is performed continuously.
filemark-frequency *frequency*	Specifies the filemark frequency. The range is 1 to 2147483647.
num-transactions *number*	Specifies a number of transactions. The range is 1 to 2147483647.

Defaults

Filemark frequency: 0.

Command Modes

SAN extension N port configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

To stop a continuous SCSI tape write command in progress, use the **stop command-id** command.

Note There can be just one outstanding I/O at a time to the virtual N port that emulates the tape behavior.

Examples

The following example configures a single SCSI tape write command.

```
switch# san-ext-tuner
switch(san-ext)# nWWN 10:00:00:00:00:00:00:00
switch(san-ext)# nport pwwn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2
switch(san-ext-nport)# tape-write command-id 100 target 22:22:22:22:22:22:22:22
transfer-size 512000 num-transactions 5000000 filemark-frequency 32
```

The following example configures a continuous SCSI tape write command.

```
switch# san-ext-tuner
switch(san-ext)# nWWN 10:00:00:00:00:00:00:00
switch(san-ext)# nport pwwn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2
switch(san-ext-nport)# tape-write command-id 100 target 22:22:22:22:22:22:22:22
transfer-size 512000 continuous filemark-frequency 32
```

Related Commands

Command	Description
nport pwwn	Configures a SAN extension tuner N port.
san-ext-tuner	Enables the SAN extension tuner feature.
show san-ext-tuner	Displays SAN extension tuner information.
stop	Cancels a SCSI command in progress on a SAN extension tuner N port.

target (iSLB initiator configuration)

To configure an iSLB initiator target, use the **target** command in iSLB initiator configuration submode. To remove the target configuration, use the **no** form of the command.

target {device-alias *device-alias* **| pwwn** *pWWN***}**
[vsan *vsan-id***]**
[no-zone]
[trespass]
[revert-primary-port]
[fc-lun *LUN* **iscsi-lun** *LUN***]**
[sec-device-alias *device-alias* **| sec-pwwn** *pWWN*]
[**sec-vsan** *sec-vsan-id*]
[**sec-lun** *LUN*]
[iqn-name *target-name***]**

no target {device-alias *device-alias* **| pwwn** *pWWN***}**
[vsan *vsan-id***]**
[no-zone]
[trespass]
[revert-primary-port]
[fc-lun *LUN* **iscsi-lun** *LUN***]**
[sec-device-alias *device-alias* **| sec-pwwn** *pWWN*]
[**sec-vsan** *sec-vsan-id*]
[**sec-lun** *LUN*]
[iqn-name *target-name***]**

Syntax Description

device-alias *device-alias*	Specifies the device alias of the Fibre Channel target.
pwwn *pWWN*	Specifies the pWWN of the Fibre Channel target. The format is *hh:hh:hh:hh:hh:hh:hh:hh*.
vsan	Assigns VSAN membership to the initiator target.
vsan-id	Specifies the VSAN ID. The range is 1 to 4093.
no-zone	Indicates no automatic zoning.
trespass	Enables trespass support.
revert-primary-port	Reverts to the primary port when it comes back up.
fc-lun *LUN*	Specifies the Fibre Channel LUN of the Fibre Channel target. The format is 0xhhhh[:hhhh[:hhhh[:hhhh]]]
iscsi-lun *LUN*	Specifies the iSCSI LUN. The format is 0xhhhh[:hhhh[:hhhh[:hhhh]]].
sec-device-alias	Specifies the device alias of the secondary Fibre Channel target.
target-device-alias	Specifies the initiator's target device alias. The maximum size is 64.
sec-pwwn *pWWN*	Specifies the pWWN of the secondary Fibre Channel target. The format is *hh:hh:hh:hh:hh:hh:hh:hh*.
sec-vsan	Assigns VSAN membership to the initiator.
sec-vsan-id	Specifies the VSAN ID. The range is 1 to 4093.
sec-lun *LUN*	Specifies the FC LUN of the secondary Fibre Channel target. The format is 0xhhhh[:hhhh[:hhhh[:hhhh]]].

iqn-name	Specifies the name of the target.
target-name	Specifies the initiator's target name. The maximum size is 223.

Defaults

None.

Command Modes

iSLB initiator configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can configure an iSLB initiator target using the device alias or the pWWN. You have the option of specifying one or more of the following optional parameters:

- Secondary pWWN
- Secondary device alias
- LUN mapping
- IQN
- VSAN identifier

Note The VSAN identifier is optional if the target is online. If the target is not online, the VSAN identifier is required.

If you configure an IQN for an initiator target, then that name is used to identify the initiator target. Otherwise, a unique IQN is generated for the initiator target.

Examples

The following example configures an iSLB initiator using an IP address and then enters iSLB initiator configuration submode.

```
switch# config t
switch(config)# islb initiator ip-address 100.10.10.10
```

The following example grants iSLB initiator access to the target using a pWWN with auto zoning enabled (default).

```
switch (config-islb-init)# target pwwn 26:00:01:02:03:04:05:06
```

The following example grants iSLB initiator access to the target using a pWWN with auto zoning disabled.

```
switch (config-islb-init)# target pwwn 26:00:01:02:03:04:05:06 no-zone
```

The following example grants iSLB initiator access to the target using a device alias and optional LUN mapping.

```
switch(config-islb-init)# target device-alias SampleAlias fc-lun 0x1234 iscsi-lun 0x2345
```

The following example grants iSLB initiator access to the target using a device alias and an optional IQN.

```
switch(config-islb-init)# target device-alias SampleAlias iqn-name
iqn.1987-01.com.cisco.initiator
```

The following example grants iSLB initiator access to the target using a device alias and a VSAN identifier.

```
switch(config-islb-init)# target device-alias SampleAlias vsan 10
```

Note The VSAN identifier is optional if the target is online. If the target is not online, the VSAN identifier is required.

The following example disables the configured iSLB initiator target.

```
switch (config-islb-init)# no target pwwn 26:00:01:02:03:04:05:06
```

Related Commands

Command	Description
islb initiator	Assigns an iSLB name and IP address to the iSLB initiator and enters iSLB initiator configuration submode.
show islb initiator	Displays iSLB CFS information.
show islb initiator detail	Displays detailed iSLB initiator information.
show islb initiator summary	Displays iSLB initiator summary information.

tcp cwm

To configure congestion window monitoring (CWM) TCP parameters, use the **tcp cwm** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp cwm [**burstsize** *size*]

no tcp cwm [**burstsize** *size*]

Syntax Description

burstsize *size*	Specifies the burstsize ranging from 10 to 100 KB.

Defaults

Enabled.

The default FCIP burst size is 10 KB.

The default iSCSI burst size is 50 KB

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

Use these TCP parameters to control TCP retransmission behavior in a switch.

Examples

The following example configures a FCIP profile and enables congestion monitoring.

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)# tcp cwm
```

The following example assigns the burstsize value at 20 KB:

```
switch(config-profile)# tcp cwm burstsize 20
```

The following example disables congestion monitoring.

```
switch(config-profile)# no tcp cwm
```

The following example leaves the CWM feature in an enabled state but changes the burstsize to the default of 10 KB.

```
switch(config-profile)# no tcp cwm burstsize 25
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp keepalive-timeout

To configure the interval between which the TCP connection verifies if the FCIP link is functioning, use the **tcp keepalive-timeout** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp keepalive-timeout *seconds*

no tcp keepalive-timeout *seconds*

Syntax Description

seconds	Specifies the time in seconds. The range is 1 to 7200.

Defaults

60 seconds.

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command can be used to detect FCIP link failures.

Examples

The following example configures a FCIP profile:

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)#
```

The following example specifies the keepalive timeout interval for the TCP connection:

```
switch(config-profile)# tcp keepalive-timeout 120
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp maximum-bandwidth-kbps

To manage the TCP window size in Kbps, use the **tcp maximum-bandwidth-kbps** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp max-bandwidth-kbps *bandwidth* **min-available-bandwidth-kbps** *threshold* {**round-trip-time-ms** *milliseconds* | **round-trip-time-us** *microseconds*}

no tcp max-bandwidth-kbps *bandwidth* **min-available-bandwidth-kbps** *threshold* {**round-trip-time-ms** *milliseconds* | **round-trip-time-us** *microseconds*}

Syntax Description

bandwidth	Specifies the Kbps bandwidth. The range is 1000 to 1000000.
min-available-bandwidth-kbps	Configures the minimum slow start threshold.
threshold	Specifies the Kbps threshold. The range is 1000 to 1000000.
round-trip-time-ms *milliseconds*	Configures the estimated round trip time across the IP network to reach the FCIP peer end point in milliseconds. The range is 0 to 300.
round-trip-time-us *microeconds*	Configures the estimated round trip time across the IP network to reach the FCIP peer end point in microseconds. The range is 0 to 300000.

Defaults

Enabled.

The FCIP defaults are **max-bandwidth** = 1G, **min-available-bandwidth** = 500 Kbps, and **round-trip-time** =1 ms.

The iSCSI defaults are **max-bandwidth** = 1G, **min-available-bandwidth** = 70 Kbps, and **round-trip-time** =1 ms.

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **maximum-bandwidth** option and the **round-trip-time** option together determine the window size.

The **minimum-available-bandwidth** option and the **round-trip-time** option together determine the threshold below which TCP aggressively increases its size. After it reaches the threshold the software uses standard TCP rules to reach the maximum available bandwidth.

Examples

The following example configures a FCIP profile:

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)#
```

The following example configures the maximum available bandwidth at 900 Kbps, the minimum slow start threshold as 300 Kbps, and the round trip time as 10 milliseconds:

```
switch(config-profile)# tcp max-bandwidth-kbps 900 min-available-bandwidth-kbps 300
round-trip-time-ms 10
```

The following example reverts to the factory defaults:

```
switch(config-profile)# no tcp max-bandwidth-kbps 900 min-available-bandwidth-kbps 300
round-trip-time-ms 10
```

The following example configures the maximum available bandwidth at 2000 Kbps, the minimum slow start threshold as 2000 Kbps, and the round trip time as 200 microseconds:

```
switch(config-profile)# tcp max-bandwidth-kbps 2000 min-available-bandwidth-kbps 2000
round-trip-time-us 200
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp maximum-bandwidth-mbps

To manage the TCP window size in Mbps, use the **tcp maximum-bandwidth-mbps** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp max-bandwidth-mbps *bandwidth* **min-available-bandwidth-mbps** *threshold* {**round-trip-time-ms** *milliseconds* | **round-trip-time-us** *microseconds*}

no tcp max-bandwidth-mbps *bandwidth* **min-available-bandwidth-mbps** *threshold* {**round-trip-time-ms** *milliseconds* | **round-trip-time-us** *microseconds*}

Syntax Description

bandwidth	Specifies the Mbps bandwidth. The range is 1 to 1000.
min-available-bandwidth-mbps	Configures the minimum slow start threshold.
threshold	Specifies the Mbps threshold. The range is 1 to 1000.
round-trip-time-ms *milliseconds*	Configures the estimated round trip time across the IP network to reach the FCIP peer end point in milliseconds. The range is 0 to 300.
round-trip-time-us *microeconds*	Configures the estimated round trip time across the IP network to reach the FCIP peer end point in microseconds. The range is 0 to 300000.

Defaults

Enabled.

The FCIP defaults are **max-bandwidth** = 1G, **min-available-bandwidth** = 500 Kbps, and **round-trip-time** =1 ms.

The iSCSI defaults are **max-bandwidth** = 1G, **min-available-bandwidth** = 70 Kbps, and **round-trip-time** =1 ms.

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **maximum-bandwidth** option and the **round-trip-time** option together determine the window size.

The **minimum-available-bandwidth** option and the **round-trip-time** option together determine the threshold below which TCP aggressively increases its size. After it reaches the threshold the software uses standard TCP rules to reach the maximum available bandwidth.

Examples

The following example configures a FCIP profile:

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)#
```

The following example configures the maximum available bandwidth at 900 Mbps, the minimum slow start threshold as 300 Mbps, and the round trip time as 10 milliseconds:

```
switch(config-profile)# tcp max-bandwidth-mbps 900 min-available-bandwidth-mbps 300
round-trip-time-ms 10
```

The following example reverts to the factory defaults:

```
switch(config-profile)# no tcp max-bandwidth-mbps 900 min-available-bandwidth-mbps 300
round-trip-time-ms 10
```

The following example configures the maximum available bandwidth at 2000 Mbps, the minimum slow start threshold as 2000 Mbps, and the round trip time as 200 microseconds:

```
switch(config-profile)# tcp max-bandwidth-mbps 2000 min-available-bandwidth-mbps 2000
round-trip-time-us 200
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp max-jitter

To estimate the maximum delay jitter experienced by the sender in microseconds, use the **tcp max-jitter** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp max-jitter *microseconds*

no tcp max-jitter *microseconds*

Syntax Description

microseconds	Specifies the delay time in microseconds ranging from 0 to 10000.

Defaults

Enabled.

The default value is 100 microseconds for FCIP and 500 microseconds for iSCSI interfaces.

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures delay jitter time:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# fcip profile 3
switch(config-profile)# tcp max-jitter 600
switch(config-profile)# do show fcip profile 3
FCIP Profile 3
    Internet Address is 10.3.3.3  (interface GigabitEthernet2/3)
    Tunnels Using this Profile: fcip3
    Listen Port is 3225
    TCP parameters
        SACK is enabled
        PMTU discovery is enabled, reset timeout is 3600 sec
        Keep alive is 60 sec
        Minimum retransmission timeout is 200 ms
        Maximum number of re-transmissions is 4
        Send buffer size is 0 KB
        Maximum allowed bandwidth is 1000000 kbps
        Minimum available bandwidth is 500000 kbps
        Estimated round trip time is 1000 usec
        Congestion window monitoring is enabled, burst size is 10 KB
        Configured maximum jitter is 600 us
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp max-retransmissions

To specify the maximum number of times a packet is retransmitted before TCP decides to close the connection, use the **tcp max-retransmissions** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp max-retransmissions *number*

no tcp max-retransmissions *number*

Syntax Description

number	Specifies the maximum number. The range is 1 to 8.

Defaults

Enabled.

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The default is 4 and the range is from 1 to 8 retransmissions.

Examples

The following example configures a FCIP profile:

```
switch# config terminal
switch(config)# fcip profile 5
```

The following example specifies the maximum number of retransmissions :

```
switch(config-profile)# tcp max-retransmissions 6
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp min-retransmit-time

To control the minimum amount of time TCP waits before retransmitting, use the **tcp min-retransmit-time** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp min-retransmit-time *milliseconds*

no tcp min-retransmit-time *milliseconds*

Syntax Description

milliseconds	Specifies the time in milliseconds. The range is 200 to 5000.

Defaults

300 milliseconds.

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures a FCIP profile:

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)#
```

The following example specifies the minimum TCP retransmit time for the TCP connection:

```
switch(config-profile)# tcp min-retransmit-time 500
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp pmtu-enable

To configure path MTU (PMTU) discovery, use the **tcp pmtu-enable** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp pmtu-enable [**reset-timeout** *seconds*]

no tcp pmtu-enable [**reset-timeout** *seconds*]

Syntax Description

reset-timeout *seconds*	Specifies the PMTU reset timeout. The range is 60 to 3600 seconds.

Defaults

Enabled.

3600 seconds.

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures a FCIP profile:

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)#
```

The following example disables PMTU discovery:

```
switch(config-profile)# no tcp pmtu-enable
```

The following example enables PMTU discovery with a default of 3600 seconds:

```
switch(config-profile)# tcp pmtu-enable
```

The following example specifies the PMTU reset timeout to 90 seconds:

```
switch(config-profile)# tcp pmtu-enable reset-timeout 90
```

The following example leaves the PMTU in an enabled state but changes the timeout to the default of 3600 seconds:

```
switch(config-profile)# no tcp pmtu-enable reset-timeout 600
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp qos

To specify the differentiated services code point (DSCP) value to mark all IP packets (type of service—TOS field in the IP header) on an ISCSI interface, use the **tcp qos** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp qos *value*

no tcp qos *value*

Syntax Description

value	Applies the control DSCP value to all outgoing frames in the control TCP connection.

Defaults

0

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Use these TCP parameters to control TCP retransmission behavior in a switch.

Examples

The following example configures the TCP QoS value on an iSCSI interface.

```
switch# config terminal
switch(config)# interface iscsi 1/2
switch(config-if)# tcp qos 5
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp qos control

To specify the differentiated services code point (DSCP) value to mark all IP packets (type of service—TOS field in the IP header), use the **tcp qos control** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp qos control *value* **data** *value*

no tcp qos control *value* **data** *value*

Syntax Description

value	Applies the control DSCP value to all FCIP frames in the control TCP connection.
data *value*	Applies the data DSCP value applies to all FCIP frames in the data connection.

Defaults

Enabled.

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Use these TCP parameters to control TCP retransmission behavior in a switch.

Examples

The following example configures a FCIP profile:

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)#
```

The following example configures the control TCP connection and data connection to mark all packets on that DSCP value:

```
switch(config-profile)# tcp qos control 3 data 5
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp sack-enable

To enable selective acknowledgment (SACK) to overcome the limitations of multiple lost packets during a TCP transmission, use the **tcp sack-enable** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp sack-enable

no tcp sack-enable

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The receiving TCP sends back SACK advertisements to the sender. The sender can then retransmit only the missing data segments.

Examples

The following example configures a FCIP profile:

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)#
```

The following example enables the SACK mechanism on the switch:

```
switch(config-profile)# tcp sack-enable
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp send-buffer-size

To define the required additional buffering—beyond the normal send window size —that TCP allows before flow controlling the switch's egress path for the FCIP interface, use the **tcp send-buffer-size** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp send-buffer-size s*ize*

no tcp send-buffer-size *size*

Syntax Description

size	Specifies the buffer size in KB. The range is 0 to 8192.

Defaults

Enabled.

The default FCIP buffer size is 0 KB.

The default iSCSI buffer size is 4096 KB

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures a FCIP profile:

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)#
```

The following example configure the advertised buffer size to 5000 KB :

```
switch(config-profile)# tcp send-buffer-size 5000
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp-connection

To configure the number of TCP connections for the FCIP interface, use the **tcp-connection** command. To revert to the default, use the **no** form of the command.

tcp-connection *number*

no tcp-connection *number*

Syntax Description

number	Enters the number of attempts (1 or 2).

Defaults

Two attempts.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Access this command from the `switch(config-if)#` submode.

Use the **tcp-connection** option to specify the number of TCP connections from a FCIP link. By default, the switch tries two (2) TCP connections for each FCIP link.

Examples

The following example configures the TCP connections.

```
switch# config terminal
switch(config)# interface fcip 50
switch(config-if)# tcp-connection 1
switch(config-if)# no tcp-connection 1
```

Related Commands

Command	Description
show interface fcip	Displays an interface configuration for a specified FCIP interface.

telnet

To log in to a host that supports Telnet, use the **telnet** command in EXEC mode.

telnet {*hostname* | *ip-address*} [*port*]

Syntax Description

hostname	Specifies a host name. Maximum length is 64 characters.
ip-address	Specifies an IP address.
port	(Optional) Specifies a port number. The range is 0 to 2147483647.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example establishes a Telnet session to the specified IP address.

```
switch# telnet 172.22.91.153
Trying 172.22.91.153...
Connected to 172.22.91.153.
Login:xxxxxxxx
Password:xxxxxxxxx
switch#
```

Related Commands

Command	Description
telnet server enable	Enables the Telnet server.

telnet server enable

To enable the Telnet server if you wish to return to a Telnet connection from a secure SSH connection, use the **telnet server enable** command. To disable the Telnet server, use the **no** form of this command

telnet server enable

no telnet server enable

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example enables the Telnet server.

```
switch(config)# telnet server enable
updated
```

The following example disables the Telnet server.

```
switch(config)# no telnet server enable
updated
```

Related Commands

Command	Description
telnet	Logs in to a host that supports Telnet.

terminal

To configure terminal attributes, use the **terminal** command in EXEC mode. To revert to the defaults, use the **no** form of the command.

terminal {**length** *lines* | **monitor** | **session-timeout** | **terminal-type** *type* | **tree-update** | **width** *integer*}

terminal no {**length** | **monitor** | **session-timeout** | **terminal-type** | **width**}

Syntax Description

length *lines*	Specifies the number of lines on the screen. The range is 0 to 512. Enter 0 to scroll continuously.
monitor	Copies Syslog output to the current terminal line.
session-timeout	Specifies the session timeout value in minutes. The range is 0 to 525600. Enter 0 to disable.
terminal-type *type*	Sets the terminal type. Maximum length is 80 characters.
tree-update	Updates the main parse tree.
width *integer*	Sets the width of the display terminal, from 0 to 80.

Defaults

The default number of lines for the length is 24. The default width is 80 lines.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Remember that all terminal parameter-setting commands are set locally and do not remain in effect after a session is ended. You must perform this task at the EXEC prompt at each session to see the debugging messages.

If the length is not 24 and the width is not 80, then you need to set a length and width.

Examples

The following example displays debug command output and error messages during the current terminal session.

```
switch# terminal monitor
Aug  8 10:32:42 sup48 % LOG_PLATFORM-5-PLATFORM_MOD_CFG_PWRDN: Module 1 powered down
Aug  8 10:32:42 sup48 % LOG_PLATFORM-5-PLATFORM_MOD_PWRDN: Module 1 powered down
Aug  8 10:32:42 sup48 % LOG_PLATFORM-5-PLATFORM_MOD_INSERT: Module 1 has been inserted
Aug  8 10:33:12 sup48 % LOG_PLATFORM-5-PLATFORM_MOD_PWRON: Module 1 powered up
Aug  8 10:33:13 sup48 % LOG_MODULE-5-MOD_REG_OK: LCM - Registration succeeded for module 1
Aug  8 10:38:15 sup48 % LOG_PLATFORM-5-PLATFORM_MOD_CFG_PWRDN: Module 1 powered down
Aug  8 10:38:15 sup48 % LOG_PLATFORM-5-PLATFORM_MOD_INSERT: Module 1 has been inserted
......
```

The following example stops the current terminal monitoring session.

```
switch# terminal no monitor
```

Related Commands

Command	Description
show terminal	Displays terminal configuration information.

time

To configure the time for the command schedule, use the **time** command. To disable this feature, use the **no** form of the command.

time {**daily** *daily-schedule* | **monthly** *monthly-schedule* | **start** {*start-time* | **now**} | **weekly** *weekly-schedule*}

no time

Syntax Description

daily *daily-schedule*	Configures a daily command schedule. The format is *HH*:*MM*, where *HH* is hours (0 to 23) and *MM* is minutes (0 to 59). Maximum length is 5 characters.
monthly *monthly-schedule*	Configures a monthly command schedule. The format is *dm*:*HH*:*MM*, where *dow* is the day of the month (1 to 31), *HH* is hours (0 to 23) and *MM* is minutes (0 to 59). Maximum length is 8 characters.
start	Schedules a job to run at a future time.
start-time	Specifies the future time to run the job. The format is *yyyy*:*mmm*:*dd*:*HH*:*MM*, where *yyyy* is the year, *mmm* is the month (jan to dec), *dd* is the day of the month (1 to 31), *HH* is hours (0 to 23) and *MM* is minutes (0 to 59). Maximum length is 18 characters.
now	Starts the job two minutes after the command is entered.
weekly *weekly-schedule*	Configures a weekly command schedule. The format is *dow*:*HH*:*MM*, where *dow* is the day of the week (1 to 7, Sun to Sat), *HH* is hours (0 to 23) and *MM* is minutes (0 to 59). Maximum length is 10 characters.

Defaults

Disabled.

Command Modes

Scheduler job configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, the command scheduler must be enabled using the **scheduler enable** command.

Examples

The following example shows how to configure a command schedule job to run every Friday at 2200.

```
switch# config terminal
switch(config)# scheduler schedule name MySchedule
switch(config-schedule)# time weekly 6:22:00
```

The following example starts a command schedule job in two minutes and repeats every 24 hours.

```
switch(config-schedule)# time start now repeat 24:00
```

Related Commands

Command	Description
scheduler enable	Enables the command scheduler.
scheduler schedule name	Configures a schedule for the command scheduler.
show scheduler	Displays schedule information.

time-stamp

To enable FCIP time stamps on a frame, use the **time-stamp** command. To disable this command for the selected interface, use the **no** form of the command.

time-stamp [**acceptable-diff** *number*]

no time-stamp [**acceptable-diff** *number*]

Syntax Description

acceptable-diff *number*	Configures the acceptable time difference for timestamps in milliseconds. The range is 500 to 10000.

Defaults

Disabled.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Access this command from the `switch(config-if)#` submode.

The **time-stamp** option instructs the switch to discard frames that are older than a specified time.

Examples

The following example enables the timestamp for an FCIP interface.

```
switch# config terminal
switch(config)# interface fcip 50
switch(config-if)# time-stamp
switch(config-if)# time-stamp acceptable-diff 4000
```

Related Commands

Command	Description
show interface fcip	Displays the configuration for a specified FCIP interface.

tlport alpa-cache

To manually configure entries in an ALPA cache, use the **tlport alpa-cache** command

tlport alpa-cache interface *interface* **pwwn** *pwwn* **alpa** *alpa*

no tlport alpa-cache interface *interface* **pwwn** *pwwn*

Syntax Description

interface *interface*	Specifies a Fibre Channel interface.
pwwn *pwwn*	Specifies the peer WWN ID for the ALPA cache entry.
alpa *alpa*	Specifies the ALPA cache to which this entry is to be added.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(5)	This command was introduced.

Usage Guidelines

Generally, ALPA cache entries are automatically populated when an ALPA is assigned to a device. Use this command only if you wish to manually add further entries.

Examples

The following example configures the specified pWWN as a new entry in this cache

```
switch# config terminal
switch(config)# tlport alpa-cache interface fc1/2 pwwn 22:00:00:20:37:46:09:bd alpa 0x02
```

Related Commands

Command	Description
show tlport	Displays TL port information.

traceroute

To print the route an IP packet takes to a network host, use the **traceroute** command in EXEC mode.

traceroute [ipv6] [*hostname* [**size** *packet-size*] | *ip-address*] | *hostname* | *ip-address*]

Syntax Description

ipv6	Traces a route to an IPv6 destination.
hostname	Specifies a host name. Maximum length is 64 characters.
size *packet-size*	Specifies a packet size. The range is 0 to 64.
ip-address	Specifies an IP address.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the **ipv6** argument.

Usage Guidelines

This command traces the route an IP packet follows to an Internet host by launching UDP probe packets with a small TTL (time to live) and then listening for an ICMP (Internet Control Message Protocol) "time exceeded" reply from a gateway.

Note Probes start with a TTL of one and increase by one until encountering an ICMP "port unreachable." This means that the host was accessed or a maximum flag was found. A line is printed showing the TTL, address of the gateway, and round-trip time of each probe. If the probe answers come from different gateways, the address of each responding system is printed.

Examples

The following example prints the route IP packets take to the network host www.cisco.com.

```
switch# traceroute www.cisco.com
traceroute to www.cisco.com (171.71.181.19), 30 hops max, 38 byte packets
 1  kingfisher1-92.cisco.com (172.22.92.2)  0.598 ms  0.470 ms  0.484 ms
 2  nubulab-gw1-bldg6.cisco.com (171.71.20.130)  0.698 ms  0.452 ms  0.481 ms
 3  172.24.109.185 (172.24.109.185)  0.478 ms  0.459 ms  0.484 ms
 4  sjc12-lab4-gw2.cisco.com (172.24.111.213)  0.529 ms  0.577 ms  0.480 ms
 5  sjc5-sbb4-gw1.cisco.com (171.71.241.174)  0.521 ms  0.495 ms  0.604 ms
 6  sjc12-dc2-gw2.cisco.com (171.71.241.230)  0.521 ms  0.614 ms  0.479 ms
 7  sjc12-dc2-cec-css1.cisco.com (171.71.181.5)  2.612 ms  2.093 ms  2.118 ms
 8  www.cisco.com (171.71.181.19)  2.496 ms *  2.135 ms
```

transfer-ready-size

To configure the target transfer ready size for SCSI write commands on a SAN tuner extension N port, use the **transfer-ready-size** command.

transfer-ready-size *bytes*

Syntax Description

bytes	Specifies the transfer ready size in bytes. The range is 0 to 2147483647.

Defaults

None.

Command Modes

SAN extension N port configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

For a SCSI **write command-id** command with a larger transfer size, the target performs multiple transfers based on the specified transfer size.

Examples

The following example configures the transfer ready size on a SAN extension tuner N port.

```
switch# san-ext-tuner
switch(san-ext)# nWWN 10:00:00:00:00:00:00:00
switch(san-ext)# nport pwwn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2
switch(san-ext-nport)# transfer-ready-size 512000
```

Related Commands

Command	Description
nport pwwn	Configures a SAN extension tuner N port.
san-ext-tuner	Enables the SAN extension tuner feature.
show san-ext-tuner	Displays SAN extension tuner information.
write command-id	Configures a SCSI write command for a SAN extension tuner N port.

transport email

To configure the customer ID with the Call Home function, use the **transport email** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

transport email {**from** *email-address* | **reply-to** *email-address* | **smtp-server** *ip-address* [**port** *port-number*]

no transport email {**from** *email-address* | **reply-to** *email-address* | **smtp-server** *ip-address* [**port** *port-number*]

Syntax Description

from *email-address*	Specifies the from email address. For example: SJ-9500-1@xyz.com. The maximum length is 255 characters.
reply-to *email-address*	Specifies the reply-to email address. For address, example: admin@xyz.com. The maximum length is 255 characters.
smtp-server *ip-address*	Specifies the SMTP server address, either DNS name or IP address. The maximum length is 255 characters.
port *port-number*	(Optional) Changes depending on the server location. The port usage defaults to 25 if no port number is specified.

Defaults

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures the from and reply-to e-mail addresses.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# transport email from user@company1.com
switch(config-callhome)# transport email reply-to person@place.com
```

The following example configures the SMTP server and ports.

```
switch(config-callhome)# transport email smtp-server 192.168.1.1
switch(config-callhome)# transport email smtp-server 192.168.1.1 port 30
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

trunk protocol enable

To configure the trunking protocol, use the **trunk protocol enable** command in configuration mode. To disable this feature, use the **no** form of the command.

trunk protocol enable

no trunk protocol enable

Syntax Description

This command has no other arguments or keywords.

Defaults

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

If the trunking protocol is disabled on a switch, no port on that switch can apply new trunk configurations. Existing trunk configurations are not affected—the TE port continues to function in trunking mode, but only supports traffic in VSANs that it negotiated previously (when the trunking protocol was enabled). Also, other switches that are directly connected to this switch are similarly affected on the connected interfaces. In some cases, you may need to merge traffic from different port VSANs across a non-trunking ISL. If so, you need to disable the trunking protocol.

Examples

The following example shows how to disable the trunk protocol feature.

```
switch# config terminal
switch(config)# no trunk protocol enable
```

The following example shows how to enable the trunk protocol feature.

```
switch(config)# trunk protocol enable
```

Related Commands

Command	Description
show trunk protocol	Displays the trunk protocol status.

CHAPTER 24

U Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "Command Modes" section to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

undebug all

To disable all debugging, use the **undebug all** command.

undebug all

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use this command to turn off all debugging.

Examples

The following example shows how to disable all debugging on the switch.

```
switch# undebug all
```

Related Commands

Command	Description
no debug all	Also disables all **debug** commands configured on the switch.
show debug	Displays all debug commands configured on the switch.

update license

To update an existing license, use the **update license** command in EXEC mode.

update license {*url* | **bootflash:** | **slot0:** | **volatile:**} *filename*

Syntax Description

update license	Updates an installed, expiring license.
url	Specifies the URL for the license file to be uninstalled.
bootflash:	Specifies the license file location in internal bootflash memory.
slot0:	Specifies the license file in the CompactFlash memory or PCMCIA card.
volatile:	Specifies the license file in the volatile file system.
filename	Specifies the name of the license file to update.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(2)	This command was introduced.

Examples

The following example updates a specific license.

```
switch# update license bootflash:sanextn2.lic sanextn1.lic
Updating sanextn1.lic:
SERVER this_host ANY
VENDOR cisco
# An example fcports license
INCREMENT SAN_EXTN_OVER_IP cisco 1.000 permanent 1 HOSTID=VDH=ABCD \
        NOTICE=<LicFileID>san_extn1.lic</LicFileID><LicLineID>0</LicLineID> \
        SIGN=33088E76F668

with bootflash:/sanextn2.lic:
SERVER this_host ANY
VENDOR cisco
# An example fcports license
INCREMENT SAN_EXTN_OVER_IP cisco 1.000 permanent 1 HOSTID=VDH=ABCD \
        NOTICE=<LicFileID>san_extn2.lic</LicFileID><LicLineID>1</LicLineID> \
        SIGN=67CB2A8CCAC2

Do you want to continue? (y/n) y
Updating license ..done
```

use-profile

To bind a profile to the FCIP interface, use the **use-profile** option. To disable a configured profile, use the **no** form of the option.

use-profile *profile-id*

no use-profile *profile-id*

Syntax Description

use-profile *profile-id*	Specifies the profile ID to be used. The range is 1 to 255.

Defaults

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Access this command from the `switch(config-if)#` submode.

This command binds the profile with the FCIP interface.

Examples

```
switch# config terminal
switch(config)# interface fcip 50
switch(config-if)# use-profile 100
switch(config-if)# no use-profile 100
```

Related Commands

Command	Description
show interface fcip	Displays an interface configuration for a specified FCIP interface.
show fcip	Displays information about the FCIP profile.

username

To define a user, use the **username** command in configuration mode. Use the **no** form of a command to undo the configuration or revert to factory defaults.

username *name* [**expire** *date* | **iscsi** | **password [0 | 5 | 7]** *user-password* [**expire** *date*] **[role** *rolename*] | **role** *rolename* | **ssh-cert-dn** *distinguished-name* **{dsa | rsa}** | **sshkey** {*key-content* | **file** *filename*}]

no username *name* [**expire** *date* | **iscsi** | **password [0 | 5 | 7]** *user-password* [**expire** *date*] **[role** *rolename*] | **role** *rolename* | **ssh-cert-dn** *distinguished-name* **{dsa | rsa}** | **sshkey** {*key-content* | **file** *filename*}]

Syntax Description

name	Specifies the name of the user. Maximum length is 32 characters.
expire *date*	Specifies the date when this user account expires (in YYYY-MM-DD format).
iscsi	Identifies an iSCSI user.
password	Configures a password for the user. The password is limited to 64 characters. The minimum length is 8 characters.
user-password	Enters the password. Maximum length is 32 characters.
0	Specifies a clear text password for the user.
5	Specifies a strongly encrypted password for the user.
7	Specifies an encrypted password for the user.
role *rolename*	Specifies the role name of the user. Maximum length is 32 characters.
ssh-cert-dn *distinguished-name*	Specifies the SSH X.509 certificate distinguished name. The maximum size is 512.
dsa	Specifies the DSA algorithm.
rsa	Specifies the RSA algorithm.
sshkey *key_content*	Specifies the actual contents of the SSH public key in OPENSSH format.
file *filename*	Specifies a file containing the SSH public key either in OPENSSH or IETF SECH or Public Key Certificate in PEM format.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
2.0(1b)	• Removed the **update_snmpv3** option. • Added level **7** for passwords.
3.0(1)	Added the **ssh-cert-dn**, **dsa**, and **rsa** options.

Usage Guidelines

To change the SNMP password, a clear text CLI password is required. You must know the SNMPv3 password to change the password using the CLI.

The password specified in the **username** command is synchronized as the `auth` and `priv` passphrases for the SNMP user.

Deleting a user using either command results in the user being deleted for both SNMP and CLI.

User-role mapping changes are synchronized in SNMP and CLI.

The SSH X.509 certificate distinguished name (DN) is in fact the subject name in the certificate. You need to extract the subject name from the certificate and specify the subject name as the argument to the **username** command.

Examples

The following example shows how to define a user.

```
switch(config)# username knuckles password testpw role bodega
switch(config)# do show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:knuckles
        this user account has no expiry date
        roles:bodega
```

The following example configures the name for a user to log in using iSCSI authentication.

```
switch(config)# username iscsi
```

The following example places you in the mode for the specified role (techdocs). The prompt indicates that you are now in the role configuration submode. This submode is now specific to the techdocs group.

```
switch(config)# role name techdocs
switch(config-role)#
```

The following example deletes the role called techdocs.

```
switch(config)# no role name techdocs
```

The following example assigns a description to the new role. The description is limited to one line and can contain spaces.

```
switch(config-role)# description Entire Tech. Docs. group
```

The following example resets the description for the Tech. Docs. group.

```
switch(config-role)# no description
```

The following example creates or updates the user account (usam) along with a password (abcd) that is set to expire on 2003-05-31.

```
switch(config)# username usam password abcd expire 2003-05-31
```

The following example creates or updates the user account (msam) along with a password (abcd) specified in clear text (indicated by 0).

```
switch(config)# username msam password 0 abcd role network-operator
```

The following example specifies an encrypted (specified by 5) password (!@*asdsfsdfjh!@df) for the user account (user1).

```
switch(config)# username user1 password 5!@*asdsfsdfjh!@df
```

The following example adds the specified user (usam) to the network-admin role.

```
switch(config)# username usam role network-admin
```

The following example deletes the specified user (usam) from the vsan-admin role.

```
switch(config)# no username usam role vsan-admin
```

The following example shows how to define a distinguished name on a switch for SSH certificate authentication.

```
switch# config t
switch(config)# username knuckles ssh-cert-dn /CN=excal-1.cisco.com rsa
switch(config)# do show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:knuckles
        this user account has no expiry date
        roles:network-operator
        ssh cert DN : /CN=excal-1.cisco.com; Algo: x509v3-sign-rsa
```

The following example specifies the SSH X.509 certificate distinguished name and DSA algorithm for an existing user account (usam).

```
switch(config)# username usam ssh-cert-dn usam-dn dsa
```

The following example specifies the SSH X.509 certificate distinguished name and RSA algorithm for an existing user account.

```
switch(config)# username user1 ssh-cert-dn user1-dn rsa
```

The following example deletes the SSH X.509 certificate distinguished name for the user account.

```
switch(config)# no username admin ssh-cert-dnadmin-dn dsa
```

The following example identifies the contents of the SSH key for the specified user (usam).

```
switch(config)# username usam sshkey fsafsd2344234234ffgsdfg
```

The following example deletes the SSH key content identification for the user (usam).

```
switch(config)# no username usam sshkey fsafsd2344234234ffgsdfgffsdfsfsfssf
```

The following example updates the SNMPv3 password for the specified user (joe). The local CLI password and the SNMP password are updated. If user Joe does not exist, the command fails.

```
switch(config)# username joe password wxyz6789 update-snmpv3 abcd1234
```

Related Commands

Command	Description
role	Configures user roles.
show username	Displays user name information.

username (iSCSI initiator configuration and iSLB initiator configuration)

To assign a username for iSCSI login authentication, use the **username** command in iSCSI initiator configuration submode. To assign a username for iSLB login authentication, use the **username** command in iSLB initiator configuration submode.To disable this feature, use the **no** form of the command.

username *username*

no username *username*

Syntax Description

username	Specifies the username for iSCSI or iSLB login authentication.

Defaults

None.

Command Modes

iSCSI initiator configuration submode.
iSLB initiator configuration submode.

Command History

Release	Modification
1.3(2)	This command was introduced.
3.0(1)	Added iSLB initiator configuration submode.

Usage Guidelines

None.

Examples

The following example assigns the username for iSCSI login authentication of an iSCSI initiator.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# iscsi initiator name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-init)# username iSCSIloginUsername
switch(config-iscsi-init)#
```

The following example assigns the username tester for iSLB login authentication of an iSLB initiator.

```
switch# config t
switch(config)# islb initiator ip-address 100.10.10.10
switch(config-iscsi-islb-init)# username ?
  <WORD>  Enter username <Max Size - 32>
switch(config-iscsi-islb-init)# username tester
```

The following example removes the username tester for an iSLB initiator.

```
switch (config-iscsi-islb-init)# no username tester
```

Related Commands

Command	Description
iscsi initiator name	Assigns an iSCSI name and changes to iSCSI initiator configuration submode.
show iscsi initiator	Displays information about a configured iSCSI initiator.
show iscsi initiator configured	Displays iSCSI initiator information for the configured iSCSI initiator.
show iscsi initiator detail	Displays detailed iSCSI initiator information.
show iscsi initiator summary	Displays iSCSI initiator summary information.
islb initiator	Assigns an iSLB name and IP address to the iSLB initiator and enters iSLB initiator configuration submode.
show islb initiator	Displays iSLB initiator information.
show islb initiator configured	Displays iSLB initiator information for the configured iSLB initiator.
show islb initiator detail	Displays detailed iSLB initiator information.
show islb initiator summary	Displays iSLB initiator summary information.

CHAPTER 25

V Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "Command Modes" section to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

vrrp

To enable VRRP, use the **vrrp** command in configuration mode. Use the **no** form of the command to revert to the factory defaults or to negate a command.

vrrp *ipv4-vr-group-number*
{address *ip-address* [**secondary**] |
advertisement-interval *seconds* |
authentication {**md5** *keyname* **spi** *index* | **text** *password*} |
preempt |
priority *value* |
shutdown |
track interface {**mgmt 0** | **vsan** *vsan-id*}

ipv6 *ipv6-vr-group-number*
{address *ipv6-address* |
advertisement-interval *centiseconds* |
preempt |
priority *value* |
shutdown |
track interface {**mgmt 0** | **vsan** *vsan-id*}}
}

vrrp *ipv4-vr-group-number*
no address *ip-address* [**secondary**] |
no advertisement-interval |
no authentication |
no preempt |
no priority |
no shutdown |
no track}

vrrp *ipv6-vr-group-number*
no address *ipv6-address* |
no advertisement-interval |
no preempt |
no priority |
no shutdown |
no track}

no vrrp *ipv4-vr-group-number*

no vrrp *ipv6-vr-group-number*

Syntax Description

ipv4-vr-group-number	Specifies an IPv4 virtual router group number. The range is 1 to 255.
address *ip-address*	Adds or removes an IP address to the virtual router.
secondary	Configures a virtual IP address without an owner.
advertisement-interval *seconds*	Sets the time interval between advertisements. For IPv4, the range is 1 to 255 seconds.
authentication	Configures the authentication method.

md5 *keyname*	Sets the MD5 authentication key. Maximum length is 16 characters.
spi *index*	Sets the security parameter index. The range is 0x0 to 0xffffff.
text *password*	Sets an authentication password. Maximum length is 8 characters.
preempt	Enables preemption of lower priority master.
priority *value*	Configures the virtual router priority. The range is 1 to 254.
shutdown	Disables the VRRP configuration.
track	Tracks the availability of another interface.
interface	Configures an interface to track.
mgmt 0	Specifies the management interface.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
ipv6 *ipv6-vr-group-number*	Specifies VRRP IPv6 on the interface. The range is 1 to 255.
address *ipv6-address*	Adds or removes an IPv6 address to the virtual router.
advertisement-interval *centiseconds*	Sets the time interval between advertisements. For IPv6, the range is 100 to 4095 centiseconds.

Defaults

Disabled.

Command Modes

Interface configuration mode.

Command History

Release	Modified
1.0(2)	This command was introduced.
3.0(1)	• Added the **IPv6** option. • Added the **address** and **advertisement-interval** options that are specific to IPv6.

Usage Guidelines

You enter the Virtual Router configuration submode to access the options for this command. From the VSAN or mgmt0 (management) interface configuration submode, enter **vrrp** *number* to enter the `switch(config-if-vrrp)#` prompt. By default, a virtual router is always disabled (**shutdown**). VRRP can be configured only if this state is disabled. Be sure to configure at least one IP address before attempting to enable a virtual router.

The total number of of VRRP groups that can be configured on a Gigabit Ethernet port, including main interfaces and subinterfaces, cannot exceed seven. This limitation applies to both IPv4 and IPv6 groups.

Note If you configure secondary VRRP IPv6 addresses on an IPFC VSAN interface, you must remove the secondary VRRP IPv6 addresses before downgrading to a release prior to Cisco Release 3.0(1). This is required only when you configure IPv6 addresses.

For additional information about VRRP, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

Examples

The following example enables VRRP configuration.

```
switch(config-if-vrrp)# no shutdown
```

The following example disables VRRP configuration.

```
switch(config-if-vrrp)# shutdown
```

The following example configures an IPv4 address for the selected VRRP.

```
switch# config terminal
switch(config)# interface vsan 1
switch(config-if)# vrrp 250
switch(config-if-vrrp)# address 10.0.0.10
```

Related Commands

Command	Description
show vrrp	Displays VRRP configuration information.
clear vrrp	Clears all the software counters for the specified virtual router.

vsan (iSCSI initiator configuration and iSLB initiator configuration)

To assign an iSCSI or iSLB initiator to a VSAN other than the default VSAN, use the **vsan** command in iSCSI initiator configuration submode or iSLB initiator configuration submode. To disable this feature, use the **no** form of the command.

vsan *vsan-id*

no vsan *vsan-id*

Syntax Description

vsan-id	Specifies a VSAN ID. The range 1 to 4093.

Defaults

None.

Command Modes

iSCSI initiator configuration submode.
iSLB initiator configuration submode.

Command History

Release	Modification
1.3(2)	This command was introduced.
3.0(1)	Added iSLB initiator configuration submode.

Usage Guidelines

When you configure an iSLB initiator in a VSAN other than VSAN 1(the default VSAN), the initiator is automatically removed from VSAN 1. For example, if you configure an iSLB initiator in VSAN 2 and you also want it to be present in VSAN 1, you must explicitly configure the initiator in VSAN 1.

Examples

The following example assigns an iSCSI initiator to a VSAN other than the default VSAN.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# iscsi initiator name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-init)# vsan 40
switch(config-iscsi-init)#
```

The following example assigns an iSLB initiator to a VSAN other than the default VSAN.

```
switch# config t
switch(config)# islb initiator ip-address 100.10.10.10
ips-hac2(config-islb-init)# vsan ?
  <1-4093>  Enter VSAN
ips-hac2(config-islb-init)# vsan 10
```

The following example removes the iSLB initiator.

```
switch (config-islb-init)# no vsan 10
```

Related Commands

Command	Description
iscsi initiator name	Assigns an iSCSI name and changes to iSCSI initiator configuration submode.
show iscsi initiator	Displays information about a configured iSCSI initiator.
show iscsi initiator configured	Displays iSCSI initiator information for the configured iSCSI initiator.
show iscsi initiator detail	Displays detailed iSCSI initiator information.
show iscsi initiator summary	Displays iSCSI initiator summary information.
islb initiator	Assigns an iSLB name and IP address to the iSLB initiator and enters iSLB initiator configuration submode.
show islb initiator	Displays iSLB initiator information.
show islb initiator configured	Displays iSLB initiator information for the configured iSLB initiator.
show islb initiator detail	Displays detailed iSLB initiator information.
show islb initiator summary	Displays iSLB initiator summary information.

vsan database

To create multiple fabrics sharing the same physical infrastructure, assign ports to VSANs, turn on or off interop mode, load balance either per originator exchange or by source-destination ID, and enter VSAN database submode, use the **vsan database** command. To remove a configuration, use the **no** command in VSAN database submode.

vsan database
vsan *vsan-id* [**interface fc** *slot/port* | **fcip** *fcip-id* | **fv** *slot/dpp-number/fv-port* | **iscsi** *slot/port* | **port-channel** *portchannel-number.subinterface-number*} | **interop** [*mode*] [**loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] | **loadbalancing** {**src-dst-id** | **src-dst-ox-id**} | **name** *name* **[interop** [*mode*] [**loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] | **loadbalancing** {**src-dst-id** | **src-dst-ox-id**} | **suspend [interop** [*mode*] [**loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] | **loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] | **suspend [interop** [*mode*] [**loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] | **loadbalancing** {**src-dst-id** | **src-dst-ox-id**}]]

vsan database
no vsan *vsan-id* [**interface** {**fc** *slot/port* | **fcip** *fcip-id* | **fv** *slot/dpp-number/fv-port* | **iscsi** *slot/port* | **port-channel** *portchannel-number.subinterface-number*} | **interop** [*mode*] [**loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] | **loadbalancing** {**src-dst-id** | **src-dst-ox-id**} | **name** *name* **[interop** [*mode*] [**loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] | **loadbalancing** {**src-dst-id** | **src-dst-ox-id**} | **suspend [interop** [*mode*] [**loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] | **loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] | **suspend [interop** [*mode*] [**loadbalancing** {**src-dst-id** | **src-dst-ox-id**}] | **loadbalancing** {**src-dst-id** | **src-dst-ox-id**}]]

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
interface	Adds interfaces to a VSAN.
fc *slot/port*	Specifies the Fibre Channel interface by slot and port number.
fcip *fcip-id*	Specifies the FCIP interface.
fv *slot/dpp-number/fv-port*	Configures the virtual F port (FV port) interface in the specified slot along with the data path processor (DPP) number and the FV port number.
iscsi *slot/port*	Configures the iSCSI interface in the specified slot/port.
port-channel *portchannel-number.subinterface-number*	Configures the PortChannel interface specified by the PortChannel number followed by a dot (.) indicator and the subinterface number.
interop	Turns on interoperability mode.
mode	Specifies the interop mode. The range is 1 to 4.
loadbalancing	Configures load-balancing scheme.
src-dst-id	Sets src-id/dst-id for load-balancing.
src-dst-ox-id	Sets ox-id/src-id/dst-id for load-balancing (default).
name *name*	Assigns a name to the VSAN. Maximum length is 32 characters.
suspend	Suspends the VSAN.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.2(2)	This command was introduced.
3.0(1)	Increased the interop mode range to 4.

Usage Guidelines

Change to VSAN database submode to issue this command.

The interface range must be in ascending order and non-overlapping. You can specify a range using a hyphen and several interfaces using commas:

- The interface range format for a FC interface range is
  fcslot/port - port , fcslot/port , fcslot/port
  (For example, **`show int fc1/1 - 3 , fc1/5 , fc2/5`**)
- The interface range format for a FV interface range is
  fvslot/dpp/fvport - fvport , fvslot/dpp/port , fvslot/dpp/port
  (For example, **`show int fv2/1/1 - 3 , fv2/1/5 , fv2/2/5`**)
- The format for a PortChannel is
  port-channel portchannel-number.subinterface-number
  (For example, **`show int port-channel 5.1`**)

There are four interop modes:

- Interop mode 1 - Standards based interop mode that requires all other vendors in the fabric to be in interop mode.
- Interop mode 2 - Brocade native mode (Core PID 0).
- Interop mode 3 - Brocade native mode (Core PID 1).
- Interop mode 4 - McData native mode.

Note Before you configure Interop mode 4 (or remove the configuration), you must suspend the VSAN. You should unsuspend the VSAN only after you configure a VSAN-dependent switch WWN with the McData OUI [08:00:88].

Examples

The following examples show how to create multiple fabrics sharing the same physical infrastructure and how to assign ports to VSANs.

```
switch# config terminal
switch(config)# vsan database
switch(config-db)#
switch-config-db# vsan 2
switch(config-vsan-db)# vsan 2 name TechDoc
updated vsan 2
switch(config-vsan-db)# vsan 2 loadbalancing src-dst-id
switch(config-vsan-db)# vsan 2 loadbalancing src-dst-ox-id
switch(config-vsan-db)# vsan 2 suspend
```

```
switch(config-vsan-db)# no vsan 2 suspend
switch(config-vsan-db)# vsan 2 interface fv2/8/2
switch(config-vsan-db)# vsan 2 interface iscsi 2/1
switch(config-vsan-db)# end
switch#
```

The following example shows how to suspend a VSAN and enable interop mode 4.

```
switch# config t
switch(config)# vsan database
switch(config-vsan-db)# vsan 100 suspend
switch(config-vsan-db)# vsan 100 interop 4
switch(config-vsan-db)# exit
```

Related Commands

Command	Description
vsan wwn	Configures a WWN for a suspended VSAN that has interop mode 4 enabled.

vsan policy deny

To configure a vsan-based role, use the **vsan policy deny** command in configuration mode. Use the **no** form of this command to delete a configured role.

vsan policy deny
permit vsan *vsan-id*

vsan policy deny
no permit vsan *vsan-id*

no vsan policy deny

Syntax Description

permit	Remove commands from the role.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

Permit.

Command Modes

Configuration mode—role name submode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

You can configure a role so that it only allows commands to be performed for a selected set of VSANs. By default, the VSAN policy of a role is **permit**. In other words, the role can perform commands configured by the **rule** command in all VSANs. In order to selectively allow VSANs for a role, the VSAN policy needs to be set to **deny** and then the appropriate VSANs need to be permitted.

Examples

The following example places you in sangroup role submode.

```
switch# config t
switch(config)# role name sangroup
switch(config-role)#
```

The following example changes the VSAN policy of this role to deny and places you in a submode where VSANs can be selectively permitted.

```
switch(config)# vsan policy deny
switch(config-role-vsan)
```

The following example deletes the configured VSAN role policy and reverts to the factory default (permit).

```
switch(config-role)# no vsan policy deny
```

The following example permits this role to perform the allowed commands for VSANs 10 through 30.

```
switch(config-role)# permit vsan 10-30
```

The following example removes the permission for this role to perform commands for vsan 15 to 20.

```
switch(config-role-vsan)# no permit vsan 15-20
```

CHAPTER 26

W Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. Please see the Command Mode section to determine the appropriate mode for each command. For more information, see the *Cisco MDS 9000 Family CLI Configuration Guide*.

write command-id

To configure a SCSI write command for a SAN tuner extension N port, use the **write command-id** command.

write command-id *cmd-id* **target** *pwwn* **transfer-size** *bytes* [**outstanding-ios** *value* [**continuous** | **num-transactions** *number*]]

Syntax Description

cmd-id	Specifies the command identifier. The range is 0 to 2147483647.
target *pwwn*	Specifies the target port WWN. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
transfer-size *bytes*	Specifies the transfer size in multiples of 512 bytes. The range is 512 to 8388608.
outstanding-ios *value*	Specifies the number of outstanding I/Os. The range is 1 to 1024.
continuous	Specifies that the command is performed continuously.
num-transactions *number*	Specifies a number of transactions. The range is 1 to 2147483647.

Defaults

The default for outstanding I/Os is 1.

Command Modes

SAN extension N port configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To stop a SCSI write command in progress, use the **stop** command.

Examples

The following example configures a continuous SCSI write command.

```
switch# san-ext-tuner
switch(san-ext)# nWWN 10:00:00:00:00:00:00:00
switch(san-ext)# nport pwwn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2
switch(san-ext-nport)# write command-id 100 target 22:22:22:22:22:22:22:22 transfer-size
512000 outstanding-ios 2 continuous
```

Related Commands

Command	Description
nport pwwn	Configures a SAN extension tuner N port.
san-ext-tuner	Enables the SAN extension tuner feature.
show san-ext-tuner	Displays SAN extension tuner information.
stop	Cancels a SCSI command in progress on a SAN extension tuner N port.

write-accelerator

To enable write acceleration and tape acceleration for the FCIP interface, use the **write-accelerator** command in configuration mode. To disable this feature or revert to the default values, use the **no** form of the command.

write-accelerator [**tape-accelerator** [**flow-control-butter-size** *bytes*]]

no write-accelerator [**tape-accelerator** [**flow-control-butter-size**]]

Syntax Description

tape-accelerator	Enables tape acceleration.
flow-control-butter-size *bytes*	Specifies the flow control buffer size.

Defaults

Disabled.

The default flow control buffer size is 256 bytes.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.0(1b)	Added **tape-accelerator** and **flow-control-butter-size** options.

Usage Guidelines

The write acceleration feature is disabled by default and must be enabled on both sides of the FCIP link. If it is only enabled on one side of the FCIP tunnel, then the tunnel will not initialize.

In Cisco MDS SAN-OS Release 3.x, the **write-accelerator** command enables read acceleration if both ends of an FCIP tunnel are running SAN-OS Release 3.x.

If one end of an FCIP tunnel is running SAN-OS Release 3.x, and the other end is running SAN-OS Release 2.x, the **write-accelerator** command enables write acceleration only.

Tip FCIP Tape acceleration does not work if the FCIP port is part of a PortChannel or if there are multiple paths between the initiator and the target port. Such a configuration might cause SCSI discovery failure or broken write or read operations.

Examples

The following command enables write acceleration on the specified FCIP interface.

```
switch# config terminal
switch(config)# interface fcip 51
switch(config-if)# write-accelerator
```

The following command enables write acceleration and tape acceleration on the specified FCIP interface.

```
switch# config terminal
switch(config)# interface fcip 51
switch(config-if)# write-accelerator tape-accelerator
```

The following command disables tape acceleration on the specified FCIP interface.

```
switch# config terminal
switch(config)# interface fcip 51
switch(config-if)# no write-accelerator tape-acceleration
```

The following command disables both write acceleration and tape acceleration on the specified FCIP interface.

```
switch# config terminal
switch(config)# interface fcip 51
switch(config-if)# no write-accelerator
```

Related Commands

Command	Description
show interface fcip	Displays an interface configuration for a specified FCIP interface.

write erase

To clear a startup configuration, enter the **write erase** command from the EXEC mode prompt.

write erase [boot | debug]

Syntax Description

boot	Destroys boot configuration.
debug	Clears the existing debug configuration.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Once this command is issued, the switch's startup configuration reverts to factory defaults. The running configuration is not affected. The **write erase** command erases the entire startup configuration with the exception of any configuration that affects the loader functionality.

The **write erase boot** command only erases the configuration that affects the loader functionality. The loader functionality configuration includes the boot variables and the mgmt0 IP configuration information (IP address, netmask, and default gateway).

Examples

The following example clears the existing startup configuration completely.

```
switch# write erase
```

The following example clears the loader functionality configuration.

```
switch# write erase boot
This command will erase the boot variables and the ip configuration of interface mgmt 0
```

wwn secondary-mac

To allocate secondary MAC addresses, use the **wwn secondary-mac** command.

www secondary-mac *wwn-id* **range** *address-range*

Syntax Description

secondary-mac *wwn-id*	The secondary MAC address with the format *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
range *address-range*	The range for the specified WWN. The only valid value is 64.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command cannot be undone.

Changes to the worldwide names are only performed as required. They should not be changed on a daily basis. These changes should be made by an administrator or individual who is completely familiar with switch operations.

For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

Examples

The following example allocates a secondary range of MAC addresses.

```
switch(config)# wwnm secondary-mac 00:99:55:77:55:55 range 64
This command CANNOT be undone.
Please enter the BASE MAC ADDRESS again: 00:99:55:77:55:55
Please enter the mac address RANGE again: 64
From now on WWN allocation would be based on new MACs.
Are you sure? (yes/no) no
You entered: no. Secondary MAC NOT programmed
```

wwn vsan

To configure a WWN for a suspended VSAN that has interop mode 4 enabled, use the **wwn vsan** command in configuration mode. To discard the configuration, use the **no** form of the command.

wwn vsan *vsan-id* **vsan-wwn** *wwn*

no wwn vsan *vsan-id* **vsan-wwn** *wwn*

Syntax Description

vsan-id	Specifies the VSAN ID. The range is 1 to 4093.
vsan-wwn *wwn*	Specifies the WWN for the VSAN. The format is hh:hh:hh:hh:hh:hh:hh:hh.

Defaults

None.

Command Modes

Configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

This command can succeed only if the following conditions are satisfied:

- The VSAN must be suspended.
- The VSAN must have interop mode 4 enabled before you can specify the switch WWN for it.
- The switch WWN must be unique throughout the entire fabric.
- The configured switch WWN must have McData OUI [08:00:88].

Examples

The following example shows how to assign a WWN to a VSAN.

```
switch# config t
switch(config)# wwn vsan 100 vsan-wwn 20:64:08:00:88:0d:5f:81
WWN can be configured for vsan in suspended state only
switch(config)# vsan database
switch(config-vsan-db)# vsan 100 suspend
switch(config-vsan-db)# exit
switch(config)# wwn vsan 100 vsan-wwn 20:64:08:00:88:0d:5f:81
switch(config)#
```

Related Commands

Command	Description
vsan database	Creates multiple fabrics sharing the same physical infrastructure, assigns ports to a VSAN, turns on or off interop mode, and load balances either per originator exchange or source-destination ID.

CHAPTER 27

Z Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "Command Modes" section to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

zone broadcast enable vsan

To enable zone broadcast frames for a VSAN in basic zoning mode, use the **zone broadcast enable** command in configuration mode. To disable this feature, use the **no** form of the command.

zone broadcast enable vsan *vsan-id*

no zone broadcast enable vsan *vsan-id*

Syntax Description

vsan-id	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

```
Broadcast frames are sent to all Nx Ports.
If any NL port attached to an FL port shares a broadcast zone with the source of the
broadcast frame,
```

then the frames are broadcast to all devices in the loop.

This command only applies to basic zoning mode.

Examples

The following example shows how to enable zone configuration broadcasting over the fabric.

```
switch# config terminal
switch(config)# zone broadcast enable vsan 10
```

Related Commands

Command	Description
show zone	Displays zone information.

zone clone

To clone a zone name, use the **zone clone** command in configuration mode.

zone clone *origZone-Name cloneZone-Name* **vsan** *vsan-id*

Syntax Description

origZone-Name cloneZone-Name	Clones a zone attribute group from the current name to a new name. Maximum length of names is 64 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

Use the **no** form of the **zone name (configuration mode)** command to delete the zone name.

Examples

The following example creates a clone of the original zone group named origZone into the clone zone group cloneZone on VSAN 45.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# zone clone origZone cloneZone vsan 45
```

Related Commands

Command	Description
show zone	Displays zone information.

zone commit vsan

To commit zoning changes to a VSAN, use the **zone commit vsan** command in configuration mode. To negate the command, use the **no** form of the command.

zone commit vsan *vsan-id* [**force**]

no zone commit vsan *vsan-id* [**force**]

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
force	Forces the commit.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1a)	This command was introduced.

Usage Guidelines

Use the **no** form of the **zone commit vsan** command to clear a session lock on a switch where the lock originated.

Examples

The following example commits zoning changes to VSAN 200.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# zone commit vsan 200
```

Related Commands

Command	Description
show zone	Displays zone information.

zone compact vsan

To compact a zone database in a VSAN, use the **zone compact vsan** command.

zone compact vsan *vsan-id*

Syntax Description

vsan-id	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Prior to Cisco MDS SAN-OS Release 3.0(1), only 2000 zones were supported per VSAN. Starting with SAN-OS Release 3.0(1), 8000 zones are supported.

If more than 2000 zones are added, then a configuration check is registered to indicate that downgrading to a previous release could cause you to lose the zones over the limit. To avoid the configuration check, you can delete the excess zones and compact the zone database for the VSAN. If there are 2000 zones or fewer after you delete excess zones, the compacting process reissues zone IDs and the configuration can be supported by previous versions.

If you want to downgrade, you should configure less than 2001 zones across all VSANs and then issue the **zone compact vsan** command on all VSANs.

If you attempt to merge VSANs, the merge will fail if more than 2000 zones are present in a VSAN and the neighboring VSAN cannot support more than 2000 zones.

Activation will fail if more than 2000 zones are present in the VSAN and all the switches in the fabric cannot support more than 2000 zones.

Examples

The following example shows how to compact a zone database in VSAN 1.

```
switch# config terminal
switch(oongif)# zone compact vsan 1
```

Related Commands

Command	Description
show zone	Displays zone information.
show zone analysis	Displays detailed analysis and statistical information about the zoning database.

zone copy

To copy the active zone set to the full zone set, use the **zone copy** command in EXEC mode. Use the **no** form of the command to negate the command or revert to the factory defaults.

zone copy active -zoneset full-zoneset vsan *vsan-id*

zone copy vsan *vsan-id* **active-zoneset** {**bootflash: ftp: | full-zoneset | scp: | sftp: | tftp: | volatile:**}

Syntax Description

active-zoneset	Copies from the active zone set.
vsan *vsan-id*	Configures to copy active zone set on a VSAN to full zone set.The ID of the VSAN is from 1 to 4093.
full-zoneset	Copies the active-zone set to the full-zone set.
bootflash:	Copies the active-zone set to a location in the bootflash: directory.
ftp:	Copies the active-zone set to a remote location using the FTP protocol.
scp:	Copies the active-zone set to a remote location using the SCP protocol.
sftp:	Copies the active-zone set to a remote location using the SFTP protocol.
slot0:	Copies the active-zone set to a location in the slot0: directory.
tftp:	Copies the active-zone set to a remote location using the TFTP protocol.
volatile:	Copies the active-zone set to a location in the volatile: directory.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was modified.

Usage Guidelines

None.

Examples

The following example copies the active zone set to the full zone set.

```
switch# zone copy active-zoneset full-zoneset vsan 1
```

The following example copies the active zone set in VSAN 3 to a remote location using SCP.

```
switch# zone copy vsan 3 active-zoneset scp://guest@myserver/tmp/active_zoneset.txt
```

Related Commands

Command	Description
show zone	Displays zone information.

zone default-zone

To define whether a default zone (nodes not assigned a created zone) permits or denies access to all in the default zone, use the **zone default-zon**e command in configuration mode. Use the **no** form of the command to negate the command or revert to the factory defaults.

zone default-zone [**permit**] **vsan** *vsan-id*

no zone default-zone [**permit**] **vsan** *vsan-id*

Syntax Description

permit	Permits access to all in the default zone.
vsan *vsan-id*	Sets default zoning behavior for the specified VSAN. The ID of the VSAN is from 1 to 4093.

Defaults

All default zones are permitted access.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use the **zone default-zone permit vsan** command to define the operational values for the default zone in a VSAN. This command applies to existing VSANs; it has no effect on VSANs that have not yet been created.

Use the **system default zone default-zone permit** command to use the default values defined for the default zone for all VSANs. The default values are used when you initially create a VSAN and it becomes active.

Examples

The following example permits default zoning in VSAN 2.

```
switch# config terminal
switch(config)# zone default-zone permit vsan 2
```

Related Commands

Command	Description
system default zone default-zone permit	Configures default values for a zone.
show zone	Displays zone information.

zone merge-control restrict vsan

To restrict zone database merging, use the **zone merge-control restrict vsan** command in configuration mode. To disable this feature, use the **no** form of the command.

zone merge-control restrict vsan *vsan-id*

no zone merge-control restrict vsan *vsan-id*

Syntax Description

vsan-id	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

If merge control setting is restricted and the two databases are not identical, the ISLs between the switches are isolated.

Examples

The following example shows how to configure zone merge control.

```
switch# config terminal
switch(config)# zone merge-control restrict vsan 10
```

Related Commands

Command	Description
show zone	Displays zone information.

zone mode enhanced vsan

To enable enhanced zoning for a VSAN, use the **zone mode enhanced vsan** command in configuration mode. To disable this feature, use the **no** form of the command.

zone mode enhanced vsan *vsan-id*

no zone mode enhanced vsan *vsan-id*

Syntax Description

vsan-id	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

Before using the **zone mode enhanced vsan** command, verify that all switches in the fabric are capable of working in enhanced zoning mode. If one or more switches are not capable of working in enhanced zoning mode, then the request to enable enhanced zoning mode is rejected.

When the **zone mode enhanced vsan** command completes successfully, the software automatically starts a session, distributes the zoning database using the enhanced zoning data structures, applies the configuration changes, and sends a release change authorization (RCA) to all switches in the fabric. All switches in the fabric then enable enhanced zoning mode.

Examples

The following example shows how to enable enhanced zoning mode.

```
switch# config terminal
switch(config)# zone mode enhanced vsan 10
```

Related Commands

Command	Description
show zone	Displays zone information.

zone name (configuration mode)

To create a zone, use the **zone name** command in configuration mode. Use the **no** form of the command to negate the command or revert to the factory defaults.

zone name *zone-name* **vsan** *vsan-id*
attribute {**broadcast** | **qos priority** {**high** | **low** | **medium**} | **read-only**}

attribute-group *group-name*

member {**device-alias** *alias-name* [**lun** *lun-id*] |
domain-id *domain-id* **port-number** *port-number* |
fcalias *name* | **fcid** *fcid-value* [**lun** *lun-id*] | **fwwn** *fwwn-id* |
interface fc *slot/port* [**domain-id** *domain-id* | **swwn** *swwn-id*] |
ip-address *ip-address* [*subnet-mask*] | **pwwn** *pwwn-id* [**lun** *lun-id*] |
symbolic-nodename *identifier*}

zone name *zone-name* **vsan** *vsan-id*
no attribute {**broadcast** | **qos priority** {**high** | **low** | **medium**} | **read-only**}

no attribute-group *group-name*

no member {**device-alias** *alias-name* [**lun** *lun-id*] |
domain-id *domain-id* **port-number** *port-number* |
fcalias *name* | **fcid** *fcid-value* [**lun** *lun-id*] | **fwwn** *fwwn-id* |
interface fc *slot/port* [**domain-id** *domain-id* | **swwn** *swwn-id*] |
ip-address *ip-address* [*subnet-mask*] | **pwwn** *pwwn-id* [**lun** *lun-id*] |
symbolic-nodename *identifier*}

no zone name *zone-name* **vsan** *vsan-id*

Syntax Description

zone-name	Specifies the name of the zone. Maximum length is 64 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
attribute	(Optional) Sets zone attributes.
read-only	Sets read-only attribute for the zone (default is read-write).
broadcast	Sets broadcast attribute for the zone.
qos priority {**high** | **low** | **medium**}	Sets QoS attribute for the zone (default is low).
attribute-group *group-name*	Configures an attribute group. Maximum length is 64 characters.
member	(Optional) Adds a member to a zone.
device-alias *alias-name*	Adds a member using the device alias name.
lun *lun-id*	Specifies the LUN number in hexadecimal format.
domain-id *domain-id*	Adds a member using the domain ID.
port-number *port-number*	Adds a member using the port number of the domain ID portnumber association.
fcalias *name*	Adds a member using the fcalias name.
fcid *fcid-id*	Adds a member using the FCID member in the format *0***x***hhhhhh*.

fwwn *fwwn-id*	Adds a member using the fabric port WWN in the format *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
interface fc *slot/port*	Adds a member using the Fibre Channel interface.
swwn *swwn-id*	Specifies the switch WWN in the format *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
ip-address *ip-address*	Adds a member using the IP address.
subnet-mask	Specifies an optional subnet mask.
pwwn *pwwn-id*	Adds a member using the port WWN in the format *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
symbolic-nodename *identifier*	Adds a member using the symbolic node name in the form of a name or an IP address.

Defaults

Zone attribute is read-only.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
1.2(1)	Added the **attribute**, **interface**, and **lun** subcommands.
2.0(1b)	• Added the **broadcast** and **qos priority** options to the **attribute** subcommand. • Added the **attribute-group** subcommand. • Added the **device-alias** *aliasname* [**lun** *lun-id*] option to the **member** subcommand.

Usage Guidelines

Zones are assigned to zone sets, zone sets are then activated from one switch and propagate across the fabric to all switches. Zones allow security by permitting and denying access between nodes (hosts and storage). **zone name** commands are issued from the configuration mode. Configure a zone for a VSAN from the config-zone submode.

Use the **show wwn switch** command to retrieve the sWWN. If you do not provide a sWWN, the software automatically uses the local sWWN.

```
Broadcast frames are sent to all Nx ports.
If any NL port attached to an FL port shares a broadcast zone with the source of the
broadcast frame,
```

then the frames are broadcast to all devices in the loop.

Examples

The following example configures attributes for the specified zone (Zone1) based on the member type (pWWN, fabric pWWN, FCID, or FC alias) and value specified.

```
switch# config terminal
switch(config)# zone name Zone1 vsan 10
switch(config-zone)# attribute broadcast
switch(config-zone)# attribute read-only
```

The following example configures members for the specified zone (Zone2) based on the member type (pWWN, fabric pWWN, FCID, or FC alias) and value specified.

```
switch# config terminal
switch(config)# zone name Zone2 vsan 10
switch(config-zone)# attribute broadcast
switch(config-zone)# attribute read-only
pWWN example:
switch(config-zone)# member pwwn 10:00:00:23:45:67:89:ab
Fabric pWWN example:
switch(config-zone)# member fwwn 10:01:10:01:10:ab:cd:ef
FC ID example:
switch(config-zone)# member fcid 0xce00d1
FC alias example:
switch(config-zone)# member fcalias Payroll
Domain ID example:
switch(config-zone)# member domain-id 2 portnumber 23
FC alias example:
switch(config-zone)# member ipaddress 10.15.0.0 255.255.0.0
Local sWWN interface example:
switch(config-zone)# member interface fc 2/1
Remote sWWN interface example:
switch(config-zone)# member interface fc2/1 swwn 20:00:00:05:30:00:4a:de
Domain ID interface example:
switch(config-zone)# member interface fc2/1 domain-id 25
```

Related Commands

Command	Description
show zone	Displays zone information.
zone rename	Renames zones.
zone-attribute-group name	Configures zone attribute groups.

zone name (zone set configuration submode)

To configure a zone in a zone set, use the **zone name** command in zone set configuration submode. To delete the zone from the zone set, use the **no** form of the command.

zone name *zone-name*

no zone name *zone-name*

Syntax Description

zone-name	Specifies the name of the zone. Maximum length is 64 characters.

Defaults

None.

Command Modes

Zone set configuration mode.

Command History

Release	Modification
1.0(2)	This command was modified.

Usage Guidelines

None.

Examples

The following example configure a zone in a zone set.

```
switch# config terminal
switch(config)# zoneset name Sample vsan 1
switch(config-zoneset)# zone name MyZone
```

The following example deletes a zone from a zone set.

```
switch(config-zoneset)# no zone name Zone2
```

Related Commands

Command	Description
show zoneset	Displays zone set information.
zone name (configuration mode)	Configure zones.
zoneset	Configures zone set attributes.

zone rename

To rename a zone, use the **zone rename** command in configuration mode.

zone rename *current-name new-name* **vsan** *vsan-id*

Syntax Description

current-name	Specifies the current fcalias name. Maximum length is 64 characters.
new-name	Specifies the new fcalias name. Maximum length is 64 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

Configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to rename a zone.

```
switch# zone rename ZoneA ZoneB vsan 10
```

Related Commands

Command	Description
show zone	Displays zone information.
zone name	Creates and configures zones.

zone-attribute-group clone

To clone a zone attribute group, use the **zone-attribute-group clone** command in configuration mode.

zone attribute clone *origAttGrp-Name cloneAttGrp-Name* **vsan** *vsan-id*

Syntax Description

origAttGrp-Name *cloneAttGrp-Name*	Clones a zone attribute group from the current name to a new name. Maximum length of names is 64 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

To remove the zone attribute group, use the **no** form of the **zone-attribute-group name** command.

Examples

The following example shows how to clone a zone attribute group with the original name origZoneAttGrp to a copy named cloneZoneAttGrp on VSAN 45.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# zone-attribute-group clone origZoneAttGrp cloneZoneAttGrp vsan 45
```

Related Commands

Command	Description
show zone-attribute-group	Displays zone attribute group information.

zone-attribute-group name

To create and configure a zone attribute group for enhanced zoning, use the **zone-attribute-group name** command in configuration mode. To remove the zone attribute group, use the **no** form of the command.

zone attribute group name *zone-name* **vsan** *vsan-id*

no zone attribute group name *zone-name* **vsan** *vsan-id*

Syntax Description

zone-name	Specifies the zone attribute name. Maximum length is 64 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

You can use this command to create a zone attribute group and to modify an existing zone attribute group.

Zone attribute groups are only supported for enhanced zoning. You can enable enhanced zoning using the **zone mode enhanced vsan** command.

Examples

The following example shows how to create a zone attribute group and enter attribute group configuration submode.

```
switch# config terminal
switch(config)# zone-attribute-group name admin-attributes vsan 10
switch(config-attribute-group)#
```

Related Commands

Command	Description
show zone-attribute-group	Displays zone attribute group information.
zone mode enhanced vsan	Enables enhanced zoning for a VSAN.

zone-attribute-group rename

To rename a zone attribute group, use the **zone-attribute-group rename** command in configuration mode.

zone attribute group rename *current-name new-name* **vsan** *vsan-id*

Syntax Description

current-name	Specifies the current zone attribute name. Maximum length is 64 characters.
new-name	Specifies the new zone attribute name. Maximum length is 64 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to rename a zone attribute group.

```
switch# config terminal
switch(config)# zone-attribute-group rename Group1 Group2 vsan 10
```

Related Commands

Command	Description
show zone-attribute-group	Displays zone attribute group information.

zonename (iSLB initiator configuration)

To assign a zone name for the initiator, use the **zonename** command in iSLB initiator configuration submode. To remove the zone name for the initiator, use the **no** form of the command.

zonename *name*

no zonename *name*

Syntax Description

zonename *name*	Assigns the zone name for the initiator. The maximum size is 55.

Defaults

Automatically generated.

Command Modes

iSCSI initiator configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can configure a zone name where the iSLB initiators and initiator targets are added. If you do not specify a zone name, the IPS manager creates one dynamically. iSLB zone sets have the following considerations:

- Auto-zoning of the initiator with the initiator targets is enabled by default.
- A zone set must be active for a VSAN for auto-zones to be created in that VSAN. The **zoneset activate** command creates auto-zones only if at least one other change has been made to the zone set.
- iSLB zone set activation might fail if another zone set activation is in process or if the zoning database is locked. Retry the iSLB zone set activation if a failure occurs. To avoid this problem, only perform only one zoning related operation (normal zones, IVR zones, or iSLB zones) at a time.
- If IVR and iSLB are enabled in the same fabric, at least one switch in the fabric must have both features enabled. Any zoning related configuration or activation operation (for normal zones, IVR zones, or iSLB zones) must be performed on this switch. Otherwise, traffic might be disrupted in the fabric.

Examples

The following example assigns the zone name for the iSLB initiator.

```
switch# config t
switch(config)# islb initiator ip-address 100.10.10.10
ips-hac2(config-iscsi-islb-init)# zonename ?
  <WORD>  Enter zone name <Max Size - 55>
ips-hac2(config-islb-init)# zonename testzone1
```

The following example removes the zone name and reverts to the default zone name for the iSLB initiator.

```
switch (config-islb-init)# no zonename testzone1
```

Related Commands

Command	Description
islb initiator	Assigns an iSLB name and IP address to the iSLB initiator and enters iSLB initiator configuration submode.
show islb initiator	Displays iSCSI server load balancing (iSLB) CFS information.
show islb initiator detail	Displays detailed iSLB initiator information.
show islb initiator summary	Displays iSLB initiator summary information.

zoneset (configuration mode)

To group zones under one zone set, use the **zoneset** command in configuration mode. To negate the command or revert to the factory defaults, use the **no** form of the command.

zoneset {**activate name** *zoneset-name* **vsan** *vsan-id* |
clone *zoneset-currentName zoneset-cloneName* |
distribute full vsan *vsan-id* |
name *zoneset-name* **vsan** *vsan-id* |
rename *current-name new-name* **vsan** *vsan-id*}

no zoneset {**activate name** *zoneset-name* **vsan** *vsan-id* |
clone *zoneset-currentName zoneset-cloneName* |
distribute full vsan *vsan-id* |
name *zoneset-name* **vsan** *vsan-id* |
rename *current-name new-name* **vsan** *vsan-id*}

Syntax Description

activate	Activates a zone set
clone *zoneset-currentName zoneset-cloneName*	Clones a zone set from the current name to a new name. Maximum length of names is 64 characters.
name *zoneset-name*	Specifies a name for a zone set. Maximum length is 64 characters.
distribute full	Enables zone set propagation.
vsan *vsan-id*	Activates a zone set on the specified VSAN. The range is 1 to 4093.
rename	Renames a zone set.
current-name	Specifies the current fcalias name.
new-name	Specifies the new fcalias name.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
2.0(1b)	Added the **rename** option.
2.1(1a)	Added the **clone** option.

Usage Guidelines

Zones are activated by activating the parent zone set.

The **zoneset distribute full vsan** command distributes the operational values for the default zone to all zone sets in a VSAN. If you do not want to distribute the operation values, use the **system default zone distribute full** command to distribute the default values.The default values are used when you initially create a VSAN and it becomes active.

The **zoneset distribute full vsan** command applies to existing VSANs; it has no effect on VSANs that have not yet been created.

Note To replace the active IVR zone set with a new IVR zone set without disrupting traffic, activate the new IVR zone set without deactivating the current active IVR zone set.

Examples

The following example activates a zone set named gottons in VSAN 333.

```
switch# config terminal
switch(config)# zoneset activate name gottons vsan 333
Zoneset Activation initiated. check zone status
```

The following example clones a zone set named zSet1 into a new zoneset named zSetClone in VSAN 45.

```
switch(config)# zoneset clone existing zSet1 zSetClone vsan 45
```

The following example distributes the operational values for the default zone to all zone sets in VSAN 22.

```
switch(config)# zoneset distribute full vsan 22
```

Related Commands

Command	Description
system default zone distribute full	Configures default values for distribution to a zone set
show zoneset	Displays zone set information.

zoneset (EXEC mode)

To merge zone set databases, use the **zoneset** command in EXEC mode.

zoneset {**distribute** | **export** | **import interface** {**fc** *slot-number* | **fcip** *interface-number* | **port-channel** *port-number*}} **vsan** *vsan-id*

Syntax Description

distribute	Distributes the full zone set in the fabric.
export	Exports the zone set database to the adjacent switch on the specified VSAN. The active zone set in this switch becomes the activated zone set of the merged SAN.
import	Imports the zone set database to the adjacent switch on the specified interface. The active zone set in the adjacent switch becomes the activated zone set of the merged SAN.
interface	Configures the interface.
fc *slot-number*	Configures a Fibre Channel interface for the specified slot number and port number.
fcip *interface-number*	Selects the FCIP interface to configure the specified interface from 1 to 255.
port-channel *port-number*	Specifies PortChannel interface.
vsan *vsan-id*	Merges the zone set database of a VSAN on the specified interface. The ID of the VSAN is from 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(2)	This command was introduced.

Usage Guidelines

You can also issue the **zoneset import** and the **zoneset export** commands for a range of VSANs.

The **zoneset distribute vsan** *vsan-id* command is supported in **interop 2** and **interop 3** modes—not in **interop 1** mode.

Examples

The following example imports the zone set database from the adjacent switch connected through the VSAN 2 interface.

```
switch# zoneset import interface fc1/3 vsan 2
```

The following example exports the zone set database to the adjacent switch connected through VSAN 5.

```
switch# zoneset export vsan 5
```

The following example distributes the zone set in VSAN 333.

```
switch# zoneset distribute vsan 333
Zoneset distribution initiated. check zone status
```

Related Commands

Command	Description
show zone status vsan	Displays the distribution status for the specified VSAN.
show zoneset	Displays zone set information.

CHAPTER 28

Caching Services Module Commands

The commands in this chapter apply to the SAN Volume Controller (SVC) software and the Caching Services Module (CSM) in Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode.

For more information on virtualization using the CSM, see the "Related Documentation" section on page xliv.

cluster add

To create a cluster with a specified SVC node, use the **cluster add** command in SVC configuration mode.

cluster add *cluster-name* **ip** *ip-address* **node svc** *slot-number*/*node-number*

Syntax Description

cluster	Provides access to cluster commands
add *cluster-name*	Specifies a new cluster addition. The cluster name must start with an alphabet and is restricted to 15 alphanumeric characters, including dash (-) and underscore (_). The cluster name cannot be Cluster*X*, where *X* is a number.
ip *ip-address*	Specifies the IP address of the specified cluster. The IP address must be in the same subnet as the switch management IP address.
node svc	Specifies the node's SVC interface
slot-number	Specifies the slot number of the Caching Service Module (CSM).
node-number	Specifies the node number of the SVC instance running on the CSM. This number ranges from 1 to 2 nodes per module.

Defaults

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

Enter this command while connected to the switch management IP address of a node at which the cluster is being created.

Examples

The following example enters the SVC configuration mode, verifies the status of previously-configured clusters, and adds a cluster called SampleCluster.

```
switch# svc-config

switch(svc)# show nodes local
--------------------------------------------------------------------------------
Node             cluster          config   cluster      node            sw
                                  node     status       status          version
--------------------------------------------------------------------------------
svc2/1                            No       unconfigured free            1.3(1)
svc2/2                            No       unconfigured free            1.3(1)

switch(svc)# cluster add SampleCluster ip 10.10.0.1 node svc 2/1
cluster creation going on. Please wait....
```

The status of the newly-added cluster can be verified using the **show nodes local** command.

```
switch(svc)# show nodes local
--------------------------------------------------------------------------------
Node        cluster            config  cluster         node        sw
                               node    status          status      version
--------------------------------------------------------------------------------
svc2/1      SampleCluster      Yes     active          active      1.3(1)
svc2/2                         No      unconfigured    free        1.3(1)
```

Related Commands

Command	Description
show nodes local	Displays the cluster name and status for all nodes in the switch.

cluster config

To manage cluster configurations on a specified cluster, use the **cluster config** configuration submode.

cluster config *cluster-name*

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submode (`switch(svc-cluster)#`).

Defaults

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following example enters the SVC configuration mode and adds a cluster called SampleCluster.

```
switch(svc)# cluster config SampleCluster
switch(svc-cluster)#
```

Related Commands

Command	Description
show cluster	Displays configured cluster information.

cluster name

To perform operations on a previously-configured cluster, use the **cluster name** command in SVC configuration mode.

cluster name *cluster-name* **flash-copy** *fc-grp-name* **[prepare | start | stop]**

cluster name *cluster-name* **remote-copy** *rc-grp-name* **{failover | start [aux | clean | force] | stop aux-enable}**

cluster name *cluster-name* **shutdown [node** *node-name***]**

cluster name *cluster-name* **start discovery**

cluster name *cluster-name* **upgrade svc-system [force]}**

Syntax Description

cluster	Provides access to cluster commands
name *cluster-name*	Identifies a previously created cluster to perform an operation.
flash-copy*fc-grp-name*	Specifies a previously-configured FlashCopy relationship.
prepare	Prepares the FlashCopy consistency group.
start	Starts the FlashCopy for the specified cluster. Starts the background copy for the specified remote copy group
stop	Stops the FlashCopy for the specified cluster. Stops the remote copy relationships for the specified remote copy group.
remote-copy *rc-grp-name*	Specifies the remote copy consistency group name.
failover	Reverses to using the auxiliary VDisks for the specified relationship.
shutdown	Shuts down the entire cluster (gracefully).
node *node-name*	Specifies a particular node for a graceful shutdown.
start discovery	Starts the background copy for the specified remote copy group.
aux	Makes the auxiliary VDisks as primary.
clean	Marks the intended secondary VDisks as clean.
upgrade svc-system	Upgrades the specified cluster. The new version of the software image is specified to the FTP:, SCP:, SFTP:, TFTP:, bootflash:, or slot0: directories
force	Permits the remote copy operation to start—even if it leads to the loss of data consistency between the primary and secondary.
aux-enable	Enables write access o the secondary (or auxiliary) VDisks.

Defaults

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following example enters the SVC configuration mode and displays all options under the **cluster name** command.

```
switch# svc-config

switch(svc)# cluster name SampleCluster ?
  flash-copy   Flash-copy
  remote-copy  Remote copy
  shutdown     Shutdown
  start        Start discovery
  upgrade      Upgrade uri

switch(svc)# cluster name SampleCluster flash-copy f1 prepare

switch(svc)# cluster name SampleCluster flash-copy f1 start

switch(svc)# cluster name SampleCluster flash-copy f1 stop

switch(svc)# cluster name SampleCluster remote-copy f1 failover

switch(svc)# cluster name SampleCluster remote-copy f1 start

switch(svc)# cluster name SampleCluster remote-copy f1 stop

switch(svc)# cluster name SampleCluster shutdownn

switch(svc)# cluster name SampleCluster shutdown node svc2/1

switch(svc)# cluster name SampleCluster start discovery

switch(svc)# cluster name SampleCluster upgrade svc-system
bootflash:m9000-ek9-csm-svc_mz.1.3.1.bin
```

dir modflash:

To display the contents of the modflash: file system, use the **dir modflash:** command in EXEC mode.

dir modflash://*module-number***-***node-number***-***path*

Syntax Description

modflash:	Flash image that resides on the Caching Services Module (CSM).
module-number	Specifies the slot number in which the CSM resides.
node-number	Specifies one of the two nodes in the CSM (SVC node). The options are **1** or **2**.
path	Specifies the **volatile** or the **cores** paths.
volatile	Displays the /var and /tmp of the SVC node on the supervisor module and can be used to move files from/to the SVC node.
cores	Displays process, kernel crash dumps, and other trace information used to debug software issues.

Defaults

None.

Command Modes

EXEC mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following example shows how to list the files on the bootflash directory.

```
switch# dir modflash://2-2-cores

switch# dir modflash://2-2-volatile
```

Related Commands

Command	Description
delete	Deletes a file on a Flash memory device.

feature enable

To enable a specified feature in a cluster, use the **feature enable** command in the cluster configuration submode.

cluster config *cluster-name*

feature enable {capacity *number* **| flash-copy | remote-copy}**

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submode.
feature enable	Enables a specified feature on this cluster. Three features can be enabled: **capacity**, **flash-copy**, or **remote-copy**
capacity	Configures the virtualization capacity of this cluster.
number	Provides a range from 1- 1677215 Gigabytes.
flash-copy	Enables the flash-copy feature for this cluster.
remote-copy	Enables the remote-copy feature for this cluster.

Defaults

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The cluster configuration submode prompt is (`switch(svc-cluster)#`).

By default, flash-copy and remote-copy are disabled and 0 (zero) GB of virtualization capacity is enabled.

Examples

The following example enters the cluster configuration submode for the SampleCluster cluster and assigns a size of 4000 Gigabytes. The next two commands enables the flash-copy and remote-copy features for this cluster.

```
switch(svc)# cluster config SampleCluster

switch(svc-cluster)# feature enable ?
  capacity     Cluster enable feature capacity
  flash-copy   Cluster enable feature flash-copy
  remote-copy  Cluster enable feature remote-copy

switch(svc-cluster)# feature enable capacity ?
  <0-2147483647>  Enter the capacity

switch(svc-cluster)# feature enable capacity 4000
```

```
switch(svc-cluster)# feature enable flash-copy

switch(svc-cluster)# feature enable remote-copy
```

Related Commands

Command	Description
show cluster *name* **flash-copy**	Displays configured flash-copy information for a specified cluster.
show cluster *name* **remote-copy**	Displays configured remote copy information for a specified cluster.

flash-copy

To create a snapshot (or point-in-time copy) of a specified VDisk or group of VDisks, use the **flash-copy** command in the cluster configuration submode.

cluster config *cluster-name*

flash-copy add *fcopy-name*

flash-copy name *fcopy-name*
map src-vdisk *vdisk-name* **dst-vdisk** *vdisk-name* |
[mode copy-on-write | full rate *rate***]**

flash-copy rename *old-name* **newname** *new-name*

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submode.
flash-copy add *fcopy-name*	Creates a FlashCopy instance.
flash-copy *fcopy-name*	Enters the FlashCopy submode for an existing copy name.
map	Creating a mapping between the source and destination VDisks.
src-vdisk *vdisk-name*	Specifies the source VDisk for the flash copy.
dst-vdisk *vdisk-name*	Specifies the destination VDisk for the flash copy.
mode	Controls the FlashCopy mode.
copy-on-write	Copies to the source VDisk only if new information in written to it after FlashCopy is initiated (default).
full rate *rate*	Specifies the background copy rate (ranges from 1 to 100) at which the source VDisk is copied to the destination VDisk even if no new information is written to the source.

Defaults

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The cluster configuration submode prompt is (`switch(svc-cluster)#`.

The flash-copy submode prompt is `switch(svc-cluster-flash-copy)#`.

Examples

The following example enters the enters the cluster configuration mode for the SampleCluster 1 cluster.

```
switch(svc)# cluster config SampleCluster
```

```
switch(svc-cluster)# flash-copy f2
switch(svc-cluster-flash-copy)# ?
Submode Commands:
  exit  Exit from this mode
  map   Flash-copy map
  mode  Flash-copy mode
  no    Negate a command or set its defaults

switch(svc-cluster-flash-copy)# map src-vdisk VDISK1 dst-vdisk DDISK1

switch(svc-cluster-flash-copy)# mode copy-on-write
switch(svc-cluster-flash-copy)# exit

switch(svc-cluster)# flash-copy add FlashC2

switch(svc-cluster)# exit


switch(svc)# show SampleCluster flash-copy
--------------------------------------------------------------------------------
name             status
--------------------------------------------------------------------------------
fccstgrp0        idle_or_copied
f2               idle_or_copied

switch(svc)# show SampleCluster flash-copy f2
Flash-copy mapping 1:
    src vdisk is v2
    dest vdisk is v3
    state is idle_or_copied
    copy rate is 50
    progress 0% done
```

Related Commands

Command	Description
show SampleCluster *name* **flash-copy**	Displays configured flash-copy information for a specified SampleCluster.

host

To create or configure hosts, use the **host** command in the cluster configuration submode.

cluster config *cluster-name*

host add *host-name* **hostport** *port-wwn*

host name *host-name*
hostport *port-wwn* |
map vdisk *vdisk-name* **[SCSI-lun** *lun-number***]**

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submode.
host add *host-name*	Creates a host with one port and assigns the host name.
hostport *port-wwn*	Specifies a port using the port WWN
host name *host-name*	Enters the host submode for an existing host name.
map	Maps a previously configured disk to this host.
vdisk *vdisk-name*	Specifies the VDisk to be mapped to the host.
SCSI-lun *lun-number*	Specifies a LUN to map the host port. If the LUN number is not specified, the next available number is assigned automatically.

Defaults

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The cluster configuration submode prompt is (`switch(svc-cluster)#`).

The host submode prompt is `switch (svc-cluster-host)#`

Examples

The following example enters the cluster configuration mode for SampleCluster and creates a host called Host 1with one port, adds a second port, and maps the VDisk for Host1, and verifies the configured information for Host1.

```
switch(svc)# cluster config SampleCluster

switch(svc-cluster)# host add Host1 hostport 11:22:33:44:aa:bb:cc:dd

switch(svc-cluster)# host Host1
switch(svc-cluster-host)# ?
Submode Commands:
  exit      Exit from this mode
```

```
  hostport  Add pWWN to host
  map       Map vdisk to host
  no        Negate a command or set its defaults

switch(svc-cluster-host)# hostport 22:11:33:55:11:aa:bb:cc

switch(svc-cluster)# host add Host1 hostport 35:66:11:22:aa:bb:22:cc

switch(svc-cluster)# host Host1

switch(svc-cluster-host)# hostport 35:66:11:22:aa:bb:22:11

switch(svc-cluster-host)# map vdisk Vdisk1

switch(svc-cluster-host)# map vdisk Vdisk1 ssci-lun 10
```

Related Commands

Command	Description
show cluster *name* **host**	Displays configured host information for a specified cluster.

install module node

To install the SVC node image, use the **install module node** command.

install module *module-number* **node** *node-number* **image svc-system [bootflash: | slot0: | ftp: | sftp: | scp: |** *svc-image*]

Syntax Description

install module	Installs the specified image for the CSM.
module-number	Switching modules: From slot 1 to 4 and 7 to 9 in a Cisco MDS 9500 Series switch. For slot 2 in a Cisco MDS 9200 Series switch. Supervisor modules: Slot 5 or 6—only on the active supervisor module in a Cisco MDS 9500 Series switch. Slot 1—upgrades both the supervisor and switching parts of the module in a Cisco MDS 9200 Series switch.
node	Selects the SVC node to install the image.
node-number	Specifies the node number.
image svc-system	Specifies the file name of an SVC image.
bootflash:	Source location for internal bootflash memory
ftp	URI containing SVC Image.
scp	URI containing SVC Image.
sftp	URI containing SVC Image.
tftp	URI containing SVC Image.
slot0:	Source location for the CompactFlash memory or PCMCIA card.
svc-image	The name of the SAN Volume Controller (SVC) image.

Defaults

None.

Command Modes

EXEC mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.0(3).

Usage Guidelines

The **install module** *module-number* **node** command installs the new image in the specified node on the CSM module. All previous data in that node is lost.

Examples

The following example shows how to install a new image on an SVC node.

```
switch# install module 2 node 1 image svc-system
scp://root@172.22.93.174/auto/isan-src/MAIN_1_3_0_17t/VegasSW/build/gdb.sb-svc/isan/targetfs/sb-svc.bin
```

```
SVC reimage going on. Please wait
root@172.22.93.174's password:
sb-svc.bin        100% |****************************| 45408 KB    00:53
svc 2/1 software reimage succeeded
```

Related Commands

Command	Description
show version compatibility	Shows the system software that is currently running on the switch

interface svc

To configure a SAN Volume Controller (SVC) interface on the Cisco MDS 9000 Family of switches, use the **interface svc** command.

interface svc *slot_number/node-number*

interface svc *slot_number/node-number* **initiator | mgmt | nwwn** *nwwn-id* **target vsan** *vsan-id*

interface svc *slot_number/node-number* **switchport description | shutdown]**

Syntax Description

interface	Configures a new interface.
svc	Specifies the new interface to be a SVC interface.
slot-number	Specifies the slot number of the Caching Service Module (CSM).
node-number	Specifies the node number of the SVC instance running on the CSM. This number ranges from 1 to 2 nodes per module.
initiator	Configures the initiator or port in the specified VSAN.
mgmt	Configures the management or port in the specified VSAN.
target	Configures the target or port in the specified VSAN.
vsan *vsan-id*	Specifies the VSAN ID ranging from 1 to 4093.
shutdown	Enables or disables an interface.
nwwn *nwwn-id*	Configured a non-system allocated nWWN for SVC Node.
switchport description	Assigns a description to the switchport. Restricted to 80 alphanumeric characters.

Defaults

None.

Command Modes

Configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

By default, all three N-port types (initiator, mgmt, and target) are in VSAN 1. Explicitly remove it from VSAN 1 if this is not required by your network.

The VSAN number can be any number from 1 to 4096. Only 64 VSANs for all initiator/mgmt/target are allowed (meaning, you can have initiator in VSANs 1-30, target in VSANs 31-60, and mgmt in VSANs 61-64). If the target, initiator, and mgmt overlap in VSANs, each overlap is also included in the total VSAN count.

A mgmt N-port can only exist in 4 of these 64 VSANs.

You can specify a range of interfaces by issuing a command with the following example format:

interface svc 1/1 *space* **,** *space* **svc 2/1-2**

This command configures Slot 1 Node 1 as an SVC interface and simultaneously configures Slot 2, Nodes 1and 2 as SVC interfaces.

Place the disk, host, and other SVC nodes in the appropriate VSAN for any configuration to be completely established

Examples

The following example configures the initiator N-port on VSAN 1, the target N-port on VSAN 2, and the management N-port on VSAN 3.

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface svc 2/1
switch(config-if)# ?
Interface configuration commands:
    do          EXEC command
    exit        Exit from this submode
    initiator    Configure Initiator traffic for SVC Node
    mgmt         Configure traffic for communication with other SVC Nodes
    no           Negate a command or set its defaults
    nwwn         Configured a non-system allocated nWWN for SVC Node
    shutdown     Enable/disable an interface
    switchport   Configure switchport parameters
    target       Configure Target traffic for SVC Node

switch(config-if)# initiator vsan 1
switch(config-if)# target vsan 2
switch(config-if)# mgmt vsan 3
```

Related Commands

Command	Description
show interface	Displays an interface configuration for a specified interface.

iogroup

To assign a name to I/O groups, use the **iogroup** command in the cluster configuration submode. Use the **no** form of this command to delete the configured I/O group alias.

cluster config *cluster-name*

iogroup *group-id* **alias** *alias-name*

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submode.
iogroup *group-id*	Identifies one of four I/O groups in the specified cluster. The ID ranges from 1 to 4.
alias *alias-name*	Assigns a name to the selected I/O group. The name is restricted to 15 alphanumeric characters.

Defaults

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The **no iogroup** command deletes the alias name, not the I/O group itself.

The cluster configuration submode prompt is (`switch(svc-cluster)#`).

Examples

The following example enters the cluster configuration mode for SampleCluster and configures a new I/O group. The created group is verified using the **show cluster** *name* **iogroup** command

```
switch(svc)# cluster config SampleCluster

switch(svc-cluster)# iogroup 1 alias SampleIOgroup

switch(svc-cluster)# exit
```

Related Commands

Command	Description
show cluster *name* **iogroup**	Displays configured I/O group information for a specified cluster.

ip

To modify the IP address for a cluster, use the **ip** command in the cluster configuration submode.

cluster config *cluster-name*

ip *ip-address*

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submodes.
ip *ip-address*	Specifies the IP address of the cluster.

Defaults

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The IP address of the cluster can be changed, but not deleted. If you connect using the current cluster IP address, that session is lost when the command completes. You must then reconnect using the new IP address.

The **no** form of this command is not allowed.

The cluster configuration submode prompt is (`switch(svc-cluster)#`).

Examples

The following example enters the cluster configuration mode for SampleCluster, configures the IP address, and verifies by displaying this information

```
switch(svc)# cluster config SampleCluster

switch(svc-cluster)# ip 172.22.92.32

switch(svc)# show cluster SampleCluster ip
cluster ip address is 172.22.92.32
```

Related Commands

Command	Description
show cluster *name* **ip**	Displays configured -- information for a specified cluster.

mdisk-grp

To create and configure a mdsik group, use the **mdisk-grp** command in the cluster configuration submode.

cluster config *cluster-name*

mdisk-grp add *grp-name* **extent** *size*

mdisk-grp name *grp-name* **-> mdisk id** *mdisk-id*

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submode.
mdisk-grp add *grp-name*	Adds a mdisk group.
extent *size*	Assigns the extent size of the storage allocation for MDisks in this cluster. The extent size can be 16, 32, 64, 128, 256, or 512 MB.
mdisk-grp name *grp-name*	Enters the mdisk submode of an existing MDisk group.
mdisk id *mdisk-id*	Assigns the disk ID ranging from 1 to 4096 to the mdisk in the MDisk group submode.

Defaults

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The cluster configuration submode prompt is (`switch(svc-cluster)#`).

The submode prompt for the MDisk group is `switch (svc-cluster-mdisk-grp)#`

Examples

The following example enters the cluster configuration mode for SampleCluster, creates an MDisk group, and adds an MDisk to the group.

```
switch(svc)# cluster config SampleCluster

switch(svc-cluster)# mdisk-grp add Mdisk1 extent 512

switch(svc-cluster)# mdisk-grp name Mdisk1

switch(svc-cluster-mdisk-grp)# mdisk id 3

switch(svc)# show cluster SampleCluster mdisk-grp
--------------------------------------------------------------------------------
name             Capacity      free     extent   number    number    status
```

```
                                        size(MB) of mdisks of vdisks
-------------------------------------------------------------------------------
finance          7.56 GB       7.56 GB  16       5         0         online
marketing        6.48 GB       6.48 GB  16       5         0         online
```

Related Commands

Command	Description
show cluster *name* **mdisk**	Displays configured MDisk group information for a specified cluster.

migrate vdisk

To configure data migration from a VDisk, use the **migrate vdisk** command in the cluster configuration submode.

cluster config *cluster-name*

migrate vdisk *vdisk-name* **new-mdisk-grp** *grp-name*

migrate vdisk *vdisk-name* **src-mdisk id** *mdisk-id* **num-extents** *number* **tgt-mdisk id** *mdisk-id*

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submode.
migrate vdisk *vdisk-name*	Migrates data from the specified VDisk to a MDisk or MDisk group.
new-mdisk-grp *grp-name*	Migrates data to a newly specified MDisk group.
src-mdisk id *mdisk-id*	Specifies the source MDisk for data migration.
num-extents *number*	Specifies the extents of a VDisk for data migration.
tgt-mdisk id *mdisk-id*	Specifies the target MDisk for data migration.

Defaults

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The cluster configuration submode prompt is (`switch(svc-cluster)#`).

Examples

The following example enters the cluster configuration mode for SampleCluster, migrates a VDisk to a new MDisk group.

```
switch(svc)# cluster config SampleCluster

switch(svc-cluster)# migrate vdisk Vdisk2 new-mdisk-grp Group5

switch(svc-cluster)# migrate vdisk Vdisk2 src-mdisk id 3 num-extents 2 tgt-mdisk id 4
```

Related Commands

Command	Description
show cluster *name* **status migrate**	Displays configured MDisk migration status information for a specified cluster.

node

To add a node to a cluster or to assign a name to a preconfigured node, use the **node** command in the cluster configuration submode.

cluster config *cluster-name*

node name *node-name*

node nwwn *node-wwn*

node iogroup *group-id* **[alias** *alias-name***]**

Syntax Description

cluster config	Provides access to cluster commands
node	Adds a specified node to the cluster being configured.
name *node-name*	Specifies the node using a 15 alphanumeric characters.
nwwn *node-wwn*	Specifies the node using the nWWN with the format hh:hh:hh:hh:hh:hh:hh:hh.
iogroup *group-id*	Identifies one of four I/O groups in the specified cluster. The ID ranges from 1 to 4.
alias *alias-name*	Assigns a name to the selected node. The name is restricted to 156 alphanumeric characters.

Defaults

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The cluster configuration submode prompt is `(switch(svc-cluster)#)`.

The node must first be added before assigning an alias name.

The no form of the command deletes the node from the cluster.

Examples

The following example enters the cluster configuration mode for SampleCluster, adds a node by assigning the nWWN, and associates the node with an alias.

```
switch(svc)# cluster config SampleCluster

switch(svc-cluster)# node nwwn 20:00:00:04:cf:e6:e4:df iogroup 1

switch(svc-cluster)# node nwwn 20:00:00:04:cf:e6:e4:df alias NodeAlias
```

Related Commands

Command	Description
show cluster *name* **nodes**	Displays configured node information for a specified cluster.

node svc delete

To delete all cluster configurations from a specific node, use the **node svc delete** command in SVC configuration mode.

node svc *slot-number/node-number* **delete**

Syntax Description

node svc	Specifies the node's SVC interface
slot-number	Specifies the slot number of the Caching Service Module (CSM).
node-number	Specifies the node number of the SVC instance running on the CSM. This number ranges from 1 to 2 nodes per module.
delete	Deletes a cluster information from the specified node.

Defaults

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

Use this command if the node has lost communication with a configured cluster.

Examples

The following example enters the SVC configuration mode and adds a cluster called SampleCluster.

```
switch# svc-config
switch(svc)# node svc 2/1 delete
```

Related Commands

Command	Description
show nodes local	Displays configured node information.

node svc recover

To initiate cluster recovery on a specified SVC node, use the **recover cluster** command in SVC configuration mode.

node svc *slot-number*/*node-number* **recover**

Syntax Description

node svc	Specifies the node's SVC interface
slot-number	Specifies the slot number of the Caching Service Module (CSM).
node-number	Specifies the node number of the SVC instance running on the CSM. This number ranges from 1 to 2 nodes per module.
recover	Initiates recovery for a specified node.

Defaults

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

Use this command to initiate cluster recovery after a failure. If the output of the **show nodes local** command displays `recovery pause` in the node status column.

Examples

The following example initiates recovery for the SVC node 1 in slot 2.

```
switch# svc-config
switch(svc)# node svc 2/1 recover
```

Related Commands

Command	Description
show nodes local	Displays configured node information.

node svc servicemode

To place a node in service mode, use the **servicemode node svc** command in SVC configuration mode. Use the **no** form of the command to remove a node from service mode.

node svc *slot-number/node-number* **servicemode**

Syntax Description

node svc	Specifies the node's SVC interface
slot-number	Specifies the slot number of the Caching Service Module (CSM).
node-number	Specifies the node number of the SVC instance running on the CSM. This number ranges from 1 to 2 nodes per module.
servicemode	Places a node in service mode.

Defaults

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following example enters the SVC configuration mode and places the specified node in service mode.

```
switch# svc-config
switch(svc)# node svc 2/2 servicemode
```

Related Commands

Command	Description
show nodes local	Displays configured node information.

node svc upgrade

To upgrade the software on a specified SVC node, use the **upgrade node svc** command in SVC configuration mode.

node svc *slot-number*/*node-number url* **upgrade svc-system** *url*

Syntax Description

node svc	Specifies the node's SVC interface
slot-number	Specifies the slot number of the Caching Service Module (CSM).
node-number	Specifies the node number of the SVC instance running on the CSM. This number ranges from 1 to 2 nodes per module.
upgrade	Upgrades the image on the specified node.
svc-system *url*	Specifies the SVC image to be used. The new version of the software image is specified to the FTP:, SCP:, SFTP:, TFTP:, bootflash:, or slot0: directories

Defaults

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

This command is valid only if the node is in service mode or the node has been shutdown.

Examples

The following example enters the SVC configuration mode and displays all options in this mode.

```
switch# svc-config
switch(svc)# node svc 2/1 upgrade svc-system ?
  bootflash:  URI containing the system image for SVC
  ftp:        URI containing the system image for SVC
  scp:        URI containing the system image for SVC
  sftp:       URI containing the system image for SVC
  slot0:      URI containing the system image for SVC
  tftp:       URI containing the system image for SVC
```

quorum

To set the quorum disk for a cluster, use the **quorum** command in the cluster configuration submode.

cluster config *cluster-name*

quorum disk [1 | 2 | 3] mdisk *disk-id*

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submode.
quorum disk *id*	Configures one of three quorum disks for the specified cluster. The quorum ID ranges from 1 to 3.
mdisk *mdisk-id*	Specifies the MDisk ID (ranges form 1 to 4096).

Defaults

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The cluster configuration submode prompt is (`switch(svc-cluster)#`).

You can assign one of 3 possible quorum IDs in any desired order.

Examples

The following example enters the cluster configuration mode for SampleCluster and sets the quorum disk ID.

```
switch(svc)# cluster config SampleCluster

switch(svc-cluster)# quorum disk 2 mdisk 1
```

remote-copy

To create a synchronous copy of a specified VDisk or group of VDisks, use the **remote-copy** command in the cluster configuration submode.

cluster config *cluster-name*

remote-copy add *rcopy-name* **[cluster** *rcluster-name]*

remote-copy *rcopy-name*
map src-vdisk *vdisk-name* **aux-vdisk** *vdisk-name*

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submode.
remote-copy add *rcopy-name*	Creates a remote copy instance and assigns a name.
remote-copy cluster *rcluster-name*	Specifies the remote cluster name for the consistency group.
remote-copy *rcopy-name*	Enters the remote-copy submode for an existing copy object.
map	Establishes a relationship between the source and destination VDisks.
src-vdisk *vdisk-name*	Specifies the source VDisk for the copy creation.
aux-vdisk *vdisk-name*	Specifies a VDisk in the remote copy cluster.

Defaults

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The cluster configuration submode prompt is (`switch(svc-cluster)#`).

The remote-copy submode prompt is `switch(svc-cluster-remote-copy)#`

Examples

The following example enters the cluster configuration mode for SampleCluster and creates a synchronous copy of a specified disk.

```
switch(svc)# cluster config SampleCluster

switch(svc-cluster)# remote-copy add Rcopy1

switch(svc-cluster)# remote-copy r1
switch(svc-cluster-remote-copy)# ?
Submode Commands:
  exit  Exit from this mode
```

```
  map   Remote-copy map
  no    Negate a command or set its defaults

switch(svc-cluster-remote-copy)# map src-vdisk SrcVdisk1 aux-vdisk AuxVdisk1

switch(svc-cluster)# remote-copy add Rcopy1 cluster remote-cluster

switch(svc-cluster)# remote-copy name Rcopy1
```

Related Commands

Command	Description
show cluster *name* **remote-copy**	Displays configured remote-copy information for a specified cluster.

show cluster flash-copy

To display configured FlashCopy information for a specified cluster, use the **show cluster** *cluster-name* **flash-copy** command.

show cluster *cluster-name* **flash-copy** [*fcopy-name*]

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
flash-copy *fcopy-name*	Displays FlashCopy relationships configured for the specified FlashCopy object.

Defaults

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following examples display configured cluster information.

```
switch(svc)# show cluster SampleCluster flash-copy
-------------------------------------------------------------------------------
name             status
-------------------------------------------------------------------------------
fccstgrp0        idle_or_copied
f2               idle_or_copied

switch(svc)# show cluster SampleCluster flash-copy f2
Flash-copy mapping 1:
    src vdisk is v2
    dest vdisk is v3
    state is idle_or_copied
    copy rate is 50
    progress 0% done
```

show cluster host

To display configured host information for a specific cluster, use the **show cluster** *cluster-name* **host** command.

show cluster *cluster-name* **host** [*host-name* | **candidate**]

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
host	Displays information about hosts and host ports.
candidate	Lists all candidates that are not part of this entity but are visible to the cluster.
host-name	Displays information about the specified host.

Defaults

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following examples display configured cluster host information.

```
switch(svc)# show SampleCluster host
-------------------------------------------------------------------------------
name             number of ports
-------------------------------------------------------------------------------
oasis15          1
Host1            2


switch(svc)# show SampleCluster host Host1
host Host1:
    Number of port is 2
    Port WWN is 11:22:33:44:aa:bb:cc:dd
    Port WWN is 22:11:33:55:11:aa:bb:cc
    LUN 0:  vdisk V1
    LUN 10: vdisk V2

switch(svc)# show cluster SampleCluster host candidate
-------------------------------------------------------------------------------
id       pwwn
-------------------------------------------------------------------------------
1        21:00:00:e0:8b:09:e7:04
```

show cluster iogroup

To display configured I/O group information for a specified cluster, use the **show cluster** *cluster-name* **iogroup** command.

show cluster *cluster-name* **iogroup** [*group-id*]

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
iogroup	Identifies one of four I/O groups in the specified cluster.
group-id	Specifies the iogroup ID (ranges from 1 to 4).

Defaults

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following examples display configured cluster iogroup information.

```
switch(svc)# show SampleCluster iogroup
--------------------------------------------------------------------------------
ID   NAME                                NODE-COUNT       VLUN_COUNT
--------------------------------------------------------------------------------
1    Sampleio1                           2                3
2    io_grp1                             0                0
3    io_grp2                             0                0
4    io_grp3                             0                0
5    recovery_io_grp                     0                0
```

Note Only four IDs can be used, the fifth I/O group is internally created and is only used for cluster recovery.

```
switch(svc)# show SampleCluster iogroup id 2
Io group id 2:
    Node count is 0
    Host LUN count is 0
    Contains no nodes
```

show cluster ip

To displays configured ip information for a specified cluster, use the **show** *cluster-name* **ip** command.

show cluster *cluster-name* **ip**

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
ip	Displays the IP address of the specified cluster.

Defaults

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following example displays configured cluster ip information.

```
switch(svc)# show SampleCluster ip
cluster ip address is 172.22.92.32
```

show cluster mdisk

To display configured MDisk information for a specified cluster, use the **show cluster** *cluster-name* **mdisk** command.

show cluster *cluster-name* **mdisk {candidate | id** *mdisk-id* **[extent]}**

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
mdisk	Displays MDisk specific information.
candidate	Displays all MDisks that are not assigned to a group.
id *mdisk-id*	Displays details of the specified MDisk ID.
extent	Displays information about the specified MDisk's extent.

Defaults

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following examples display configured cluster MDisk information.

```
switch(svc)# show SampleCluster mdisk
--------------------------------------------------------------------------------
id       nwwn                    mdisk-grp       capacity      status
--------------------------------------------------------------------------------
1        20:00:00:04:cf:e6:1b:5b mg1             68.37 GB      online
2        20:00:00:04:cf:e6:e5:32 mg1             68.37 GB      online
3        20:00:00:04:cf:e6:21:a2 mg1             68.37 GB      online
4        20:00:00:04:cf:e6:e1:81 mg1             68.37 GB      online
5        20:00:00:04:cf:e6:e4:df                 68.37 GB      online
6        20:00:00:04:cf:e6:1c:fb                 68.37 GB      online
7        20:00:00:04:cf:e6:1a:4c                 68.37 GB      online
8        20:00:00:04:cf:e6:e4:6b                 68.37 GB      online

switch(svc)# show SampleCluster mdisk candidate
--------------------------------------------------------------------------------
id       nwwn                    capacity
--------------------------------------------------------------------------------
5        20:00:00:04:cf:e6:e4:df 68.37 GB
6        20:00:00:04:cf:e6:1c:fb 68.37 GB
7        20:00:00:04:cf:e6:1a:4c 68.37 GB
8        20:00:00:04:cf:e6:e4:6b 68.37 GB

switch(svc)# show cluster SampleCluster mdisk id 1
mdisk id 1 is online
```

```
   Is member of mdisk-grp mg1
   Controller node WWN is 20:00:00:04:cf:e6:e4:6b
   Controller port WWN is 22:00:00:04:cf:e6:e4:6b, LUN 00:00:00:00:00:00:00:00
   Controller serial number is 3HZ0KZ8W
   Capacity is 68.37 GB
   Number of free extents is 2231

switch(svc)# show cluster SampleCluster mdisk id 1 extent
-------------------------------------------------------------------------------
vdisk            number of extents
-------------------------------------------------------------------------------
v1              2144
```

show cluster mdsik-grp

To display configured MDisk group information for a specified cluster, use the **show cluster** *cluster-name* **mdisk-grp** command.

show cluster *cluster-name* **mdisk-grp** [*grp-name*]

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
mdisk-grp *grp-name*	Displays information about a specified MDisk group.

Defaults

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following examples display configured cluster information for a MDisk group.

```
switch(svc)# show cluster SampleCluster mdisk-grp
-------------------------------------------------------------------------------
name           Capacity       free        extent     number     number     status
                                          size(MB)   of mdisks  of vdisks
-------------------------------------------------------------------------------
mg1            410.16 GB      309.16 GB   16         6          1          online

switch(svc)# show cluster SampleCluster mdisk-grp mg1
mdisk-grp mg1 is online
   Total capacity is 410.16 GB
   Free capacity is 309.16 GB
   Extent size is 16 MB
   Number of mdisks is 6
   Number of vdisks using this group is 1
```

show cluster nodes

To display configured node information for a specified cluster, use the **show cluster** *cluster-name* **nodes** command.

show cluster *cluster-name* **nodes [candidate]**

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
nodes	Displays information about nodes in this cluster.
candidate	Lists all candidates that are not part of this entity but are visible to the cluster.

Defaults

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following example displays configured cluster information for a specified node.

```
switch(svc)# show cluster SampleCluster nodes
Node node1 is online(3)
    Node WWN is 20:06:00:0b:be:57:73:42
    Serial number is JAB072705JH
    Unique id is 01:00:07:27:30:35:4a:48
    Node is in config mode
    Node is part of iogroup id 1 name io_grp0

Node node2 is online(3)
    Node WWN is 20:08:00:0b:be:57:73:42
    Serial number is JAB076605JH
    Unique id is 01:00:07:66:30:35:4a:48
    Node is in non config mode
    Node is part of iogroup id 1 name io_grp0

switch1(svc)# show cluster SampleCluster nodes candidate
--------------------------------------------------------------------------------
NODE                              NWWN
--------------------------------------------------------------------------------
switch1.2.1                  20:06:00:05:30:00:8d:e0
```

show cluster remote-copy

To display configured remote-copy information for a specified cluster, use the **show cluster** *cluster-name* **remote-copy** command.

show cluster *cluster-name* **remote-copy** [*rcopy-name*]

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
remote-copy	Displays remote copy relationships configured for a specified cluster.
rcopy-name	Displays the specified remote copy object.

Defaults

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following example displays configured cluster information for the specified copy instance.

```
switch(svc)# show cluster SampleCluster remote-copy r1
Remote-copy mapping 1:
    master cluster is SampleCluster
    master vdisk is v6
    aux cluster is c1
    aux vdisk is v7
    status is inconsistent_stopped
    progress 0% done

Remote-copy mapping 2:
    master cluster is SampleCluster
    master vdisk is v8
    aux cluster is c1
    aux vdisk is v9
    status is inconsistent_stopped
    progress 0% done
```

show cluster remote-copy-cluster

To display configured remote-copy partnership information for a specified cluster, use the **show cluster** *cluster-name* **remote-copy-cluster** command.

show cluster *cluster-name* **remote-copy-cluster** [*rcopy-name*]

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
remote-copy-cluster	Displays remote copy relationships configured for a specified cluster.
rcopy-name	Displays the specified remote copy object.

Defaults

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following example displays configured cluster information for the specified copy instance.

```
switch(svc)# show cluster SampleCluster remote-copy-cluster
-----------------------------------------------
Cluster          Local/remote     Bandwidth
-----------------------------------------------
local-cluster    local             10
remote-cluster   remote            50
```

show cluster status

To displays progress information for a specified cluster, use the **show cluster** *cluster-name* **status** command.

show cluster *cluster-name* **status [flash-copy** *fcopy-name* **| remote-copy** *rcopy-name***]**

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
status	Displays the status of a upgrade or copy process.
flash-copy	Displays FlashCopy relationships configured for the specified cluster.
fcopy-name	Displays the specified FlashCopy object.
remote-copy	Displays remote copy relationships configured for a specified cluster.
rcopy-name	Displays the specified remote copy object.

Defaults

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following examples display configured cluster information.

```
switch(svc)# show cluster SampleCluster status flash-copy fc1
--------------------------------------------------------------------------------
src vdisk        dest vdisk       progress
--------------------------------------------------------------------------------
v1               v2               100% done
v3               v4               100% done

switch(svc)# show cluster SampleCluster status remote-copy rc1
--------------------------------------------------------------------------------
src vdisk        aux vdisk        progress
--------------------------------------------------------------------------------
v5               v6               100% done
v7               v8               100% done
```

show cluster vdisk

To display configured VDisk information for a specified cluster, use the **show cluster** *cluster-name* **vdisk** command.

show cluster *cluster-name* **vdisk** {*vdisk-id* **[extent | mapped_hosts]**}

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
vdisk	Displays configured VDisks in the cluster
vdisk-id	Displays details of the specified VDisk ID.
extent	Displays information about the specified MDisk's extent.
mapped_hosts	Displays information about which hosts are mapped to the specified VDisk.

Defaults

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following examples display configured cluster information for VDisks.

```
switch(svc)# show cluster SampleCluster vdisk v1 extent
--------------------------------------------------------------------------------
mdisk id  number of extents
--------------------------------------------------------------------------------
1         2144
2         2144
3         2144
5         11
6         11
7         10
switch(svc)# show cluster SampleCluster vdisk v1 mapped_hosts
--------------------------------------------------------------------------------
host             LUN
--------------------------------------------------------------------------------
oasis15          0
```

show environment battery

To display status of a battery module for the Caching Services Module (CSM), use the **show environment battery** command.

show environment battery module *slot-number* **[detail]**

Syntax Description

show environment	Displays the hardware environment in any Cisco MDS 9000 Family switch.
battery	Displays the status of the battery in a CSM.
module *slot-number*	Specifies the slot number of the CSM.
detail	Provides detailed information about the CSM battery status.

Defaults

None.

Command Modes

EXEC mode.

Command History

This command was modified in Release 1.3(1).

Usage Guidelines

None.

Examples

The following example displays the current contents of the boot variable.

```
switch# show environment battery module 2
Battery 1:
----------
Voltage             : 10.343 V
Current             : 0.000 A
Temperature         : 23.7 C
Current Capacity    : 1571 mAHr
Full Capacity       : 2057 mAHr
CySampleClustere Count         : 3
Last conditioned in : Week 22 2003
Serial Num          : AMB0722009C

Battery 2:
----------
Voltage             : 10.596 V
Current             : 0.000 A
Temperature         : 26.6 C
Current Capacity    : 1701 mAHr
Full Capacity       : 2032 mAHr
CySampleClustere Count         : 6
Last conditioned in : Week 22 2003
Serial Num          : AMB0722009R

switch## show environment battery module 2 detail
Battery 1:
```

```
----------
Voltage             : 10.338 V
Current             : 0.000 A
Temperature         : 23.7 C
Current Capacity    : 1571 mAHr
Full Capacity       : 2057 mAHr
Caching Capacity    : 6463 MB
CySampleClustere Count         : 3
Last conditioned in : Week 22 2003
Serial Num          : AMB0722009C
EEPROM version      : 1

Manufacturer Access            : 0x0
Remaining Capacity Alarm       : 0xc8
Remaining Time Alarm           : 0xa
Battery Mode                   : 0x6000
AtRate                         : 0x0
AtRate Time To Full            : 0xffff
AtRate Time To Empty           : 0xffff
AtRate OK                      : 0x1
Temperature                    : 0xb97
Voltage                        : 0x2862
Current                        : 0xd
Average Current                : 0x6
Max Error                      : 0x2
Relative State of Charge       : 0x4c
Absolute State of Charge       : 0x4f
Remaining Capacity             : 0x623
Full Charge Capacity           : 0x809
Run Time To Empty              : 0xffff
Average Time To Empty          : 0xffff
Average Time To Full           : 0x13f2
Charging Current               : 0x44c
Charging Voltage               : 0x3840
Battery Status                 : 0xc0
CySampleClustere Count                    : 0x3
Design Capacity                : 0x7d0
Design Voltage                 : 0x2580
Specification Info             : 0x21
Manufacture Date               : 0x3037
Serial Number                  : 0x0
Manufacturer Name              : 0x430a
Device Name                    : 0x4207
Device Chemistry               : 0x4e04
Manufacturer Data              : 0x7507
Pack Status & Configuration    : 0x2020
VCELL4                         : 0x0
VCELL3                         : 0x0
VCELL2                         : 0x0
VCELL1                         : 0x0
...
```

show interface svc

You can check the status of a SVC interface at any time by using the **show interface svc** command.

show interface svc *slot-number/node-number* [**brief | counters | description**]

Syntax Description

interface range	Displays the interfaces in the specified range.
brief	Displays brief info of interface.
counters	Displays the interface counter information.
description	Displays a description of interface.
svc	Displays the SAN Volume Controller (SVC) interface.
slot-number	Specifies the slot number of the Caching Service Module (CSM).
node-number	Specifies the node number of the SVC instance running on the CSM. This number ranges from 1 to 2 nodes per module.

Defaults

None

Command Modes

EXEC

Command History

This command was modified in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following examples display configured SVC interface information.

```
switch# show interface svc 2/1
svc2/1 is up
    Node WWN is 10:00:00:00:00:00:00:00
    Fabric WWN is 20:41:00:05:30:00:33:1e
    Target N-port WWN is 27:39:00:05:30:00:33:2a, vsan is 1, FCID is 0x010006
    Initiator N-port WWN is 27:3a:00:05:30:00:33:2a, vsan is 1, FCID is 0x010007
    Mgmt N-port WWN is 27:3b:00:05:30:00:33:2a, vsan is 1, FCID is 0x010008
    5 minutes input rate 16 bits/sec, 2 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      7 frames input, 736 bytes
        0 discards, 0 errors
      3 frames output, 276 bytes
        0 discards, 0 errors

switch# show interface svc 8/1-2
svc8/1 is down (Administratively down)
    Node WWN is 23:34:00:05:30:00:00:02
    Fabric WWN is 21:c1:00:05:30:00:00:00
    Target N-port WWN is 23:2e:00:05:30:00:00:02, vsan is 1, FCID is 0x000000
    Initiator N-port WWN is 23:2f:00:05:30:00:00:02, vsan is 1, FCID is 0x000000
    Mgmt N-port WWN is 23:30:00:05:30:00:00:02, vsan is 1, FCID is 0x000000
```

```
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      0 frames input, 0 bytes
        0 discards, 0 errors
      0 frames output, 0 bytes
        0 discards, 0 errors

svc8/2 is up
    Node WWN is 23:35:00:05:30:00:00:02
    Fabric WWN is 21:c2:00:05:30:00:00:00
    Target N-port WWN is 23:31:00:05:30:00:00:02, vsan is 1, FCID is 0x650003
    Initiator N-port WWN is 23:32:00:05:30:00:00:02, vsan is 1, FCID is 0x650004
    Mgmt N-port WWN is 23:33:00:05:30:00:00:02, vsan is 1, FCID is 0x650005
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      3268061 frames input, 6602103068 bytes
        0 discards, 2 errors
      3208131 frames output, 6598470800 bytes
        0 discards, 0 errors

switch# show interface brief
--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          FCOT   Oper  Oper   Port
                  Mode   Trunk                         Mode  Speed  Channel
                         Mode                          (Gbps)
--------------------------------------------------------------------------------
fc8/1      1      FX     --      fcotAbsent       --     --           --
...
fc8/32     1      FX     --      fcotAbsent       --     --           --
--------------------------------------------------------------------------------
Interface          Status                          Speed
                                                   (Gbps)
--------------------------------------------------------------------------------
sup-fc0            up                              1
--------------------------------------------------------------------------------
Interface              Status     IP Address        Speed        MTU
--------------------------------------------------------------------------------
mgmt0                  up         172.22.90.21/24   100 Mbps     1500
--------------------------------------------------------------------------------
Interface          Status
--------------------------------------------------------------------------------
svc2/1             down
svc2/2             up
svc4/1             up
svc4/2             up

switch# show interface svc 2/1 counters
svc2/1
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec 0 ios/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec 0 ios/sec
    272 frames input, 89764 bytes
      39 input session management frames
        19 plogi, 1 plogi_acc, 13 prli, 1 prli_acc
        2 logo, 0 logo_acc, 0 prlo, 0 prlo_acc
        3 abts, 0 ba_acc, 0 ls_rjt
      28 input I/Os, 28 cmd complete, 0 cmd fail
        24 reads, 4 writes
        0 input errors
        0 input discards
          FCP cmd errors
            0 sess not up, 0 no resources, 0 bad frames
            0 up layer rjt, 0 out of order, 0 proc unexp exch st
            0 drop unexp exch st, 0 no exch match
          FCP Xrdy errors
```

```
            0 sess not up, 0 no resources, 0 bad frames
            0 up layer rjt, 0 out of order, 0 proc unexp exch st
            0 drop unexp exch st, 0 no exch match
          FCP status errors
            0 sess not up, 0 no resources, 0 bad frames
            0 up layer rjt, 0 out of order, 0 proc unexp exch st
            0 drop unexp exch st, 0 no exch match
          FCP Data errors
            0 sess not up, 0 no resources, 0 bad frames
            0 up layer rjt, 0 out of order, 0 proc unexp exch st
            0 drop unexp exch st, 0 no exch match
          0 Incoming Aborts
    232 frames output, 84176 bytes
      35 output session management frames
        6 plogi, 13 plogi_acc, 1 prli, 12 prli_acc
        0 logo, 0 logo_acc, 0 prlo, 0 prlo_acc
        1 abts, 2 ba_acc, 0 ls_rjt
      103 out I/Os, 103 cmd complete, 0 cmd fail
        63 reads, 4 writes
      0 output errors
      0 output discards
        0 out ls aborts
           LS requests while sess not up
             0 cmds 0 data xfers 0 status xfers 0 ds xfers

switch# show interface svc 4/2 description

--------------------------------------------------------------------------------
Interface          Description
--------------------------------------------------------------------------------
svc4/2             SampleInt1
```

show nodes

To displays configured information for the CSM, use the **show svc** command.

show nodes {local [detail] | svc *slot_number/node-number* **| version}**

Syntax Description

show nodes	Displays information about the specified nodes.
local	Displays SVC nodes in the switch.
detail	Displays detailed node information.
svc	Displays node information specific to the SVC interface.
slot-number	Specifies the slot number of the Caching Service Module (CSM).
node-number	Specifies the node number of the SVC instance running on the CSM. This number ranges from 1 to 2 nodes per module.
version	Displays software version information for each node.

Defaults

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following example display configured SVC information and statistics.

```
switch(svc)# show nodes local detail
svc2/1:
  Is a config node for cluster SampleCluster
  cluster Status is active
  Node Status is active

svc2/2:
  Is member of cluster SampleCluster
  cluster Status is active
  Node Status is active

switch(svc)# show nodes ?
  local    Show nodes in the switch
  svc      SVC Interface
  version  Show node sw versions in the switch
  <cr>     Carriage Return

switch(svc)# show nodes svc 2/2
svc2/2:
  Is not a member of any cluster
  Cluster Status is unconfigured
```

```
  Node Status is free

switch(svc)# show nodes version
------------------------------------------------------
Node             sw version       state
------------------------------------------------------
svc2/1           1.3(1)       Runtime code    (5)
svc2/2           1.3(1)       Runtime code    (5)
```

Related Commands

Command	Description
svc config	Configures SVC nodes.

show svc

To displays configured information for the CSM, use the **show svc** command.

show svc
port svc *slot_number/node-number* **[detail | initiator | mgmt | target** [**detail | vsan** *vsan-id*]] **|**
session [detail | initiator | mgmt | peer-wwn *pwwn-id* **| target** [**detail | vsan** *vsan-id*]] **|**
stats xipc [interface svc *slot_number/node-number*] **| [module** *slot-number*]

Syntax Description

show svc	Displays configured SVC information.
port	Displays N-port specific SVC information.
svc	Specifies the new interface to be a SVC interface.
slot-number	Specifies the slot number of the Caching Service Module (CSM).
node-number	Specifies the node number of the SVC instance running on the CSM. This number ranges from 1 to 2 nodes per module.
detail	Displays detailed information for all N ports
initiator	Displays a SVC node as an initiator in the specified VSAN.
mgmt	Displays a SVC node as a management node in the specified VSAN.
target	Displays a SVC node as a target in the specified VSAN.
vsan *vsan-id*	Specifies the VSAN ID ranging from 1 to 4093.
session	Displays information specific to the SVC session.
peer-pwwn *pwwn-id*	Specifies the port WWN of the target or host, with the format hh:hh:hh:hh:hh:hh:hh:hh.
stats	Displays SVC statistical information generally used for debugging.
module *slot-number*	Specifies the slot number containing the CSM.

Defaults

None.

Command Modes

EXEC mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following examples display configured SVC information and statistics.

```
switch# show svc session svc 2/1
svc2/1:
   Target N-port WWN is 21:00:00:05:30:00:8d:e0, vsan is 2, FCID is 0x610100
     pWWN 21:00:00:e0:8b:09:f0:04, nWWN 20:00:00:e0:8b:09:f0:04, FCID 0x610000
   Initiator N-port WWN is 20:01:00:05:30:00:8d:e0, vsan is 1, FCID is 0xec0100
```

```
      pWWN 22:00:00:04:cf:e6:e4:6b, nWWN 20:00:00:04:cf:e6:e4:6b, FCID 0xec00d4
      pWWN 22:00:00:04:cf:e6:1a:4c, nWWN 20:00:00:04:cf:e6:1a:4c, FCID 0xec00d5
      pWWN 22:00:00:04:cf:e6:1c:fb, nWWN 20:00:00:04:cf:e6:1c:fb, FCID 0xec00d6
      pWWN 22:00:00:04:cf:e6:e1:81, nWWN 20:00:00:04:cf:e6:e1:81, FCID 0xec00d9
      pWWN 22:00:00:04:cf:e6:e4:df, nWWN 20:00:00:04:cf:e6:e4:df, FCID 0xec00da
      pWWN 22:00:00:04:cf:e6:21:a2, nWWN 20:00:00:04:cf:e6:21:a2, FCID 0xec00dc
      pWWN 22:00:00:04:cf:e6:e5:32, nWWN 20:00:00:04:cf:e6:e5:32, FCID 0xec00e0
      pWWN 22:00:00:04:cf:e6:1b:5b, nWWN 20:00:00:04:cf:e6:1b:5b, FCID 0xec00e1
    Mgmt N-port WWN is 21:02:00:05:30:00:8d:e0, vsan is 3, FCID is 0x7a0000
      pWWN 21:03:00:05:30:00:8d:e0, nWWN 20:07:00:05:30:00:8d:e0, FCID 0x7a0001

switch# show svc session svc 2/1 peer-pwwn 22:00:00:04:cf:e6:e4:6b detail
svc2/1:
    Initiator N-port WWN is 20:01:00:05:30:00:8d:e0, vsan is 1, FCID is 0xec0102
      pWWN 22:00:00:04:cf:e6:e4:6b, nWWN 20:00:00:04:cf:e6:e4:6b, FCID 0xec00d4
        47 frames input, 920 data bytes
          2 ELS pkts, 0 BLS pkts
          0 FCP commands, 0 FCP xfer ready
          20 FCP data frames, 25 FCP status
          0 FCP overrun, 15 FCP underrun
          0 aborts, 0 bad FC2 drops
          0 data excess
        27 frames output, 0 data bytes
          2 ELS pkts, 0 BLS pkts
          25 FCP commands, 0 FCP xfer ready
          0 FCP data frames, 0 FCP status
          0 aborts
        0 open exchanges

switch#  show svc port svc 2/1
svc2/1:
    Target N-port in vsan 2 is up
      Port WWN is 21:00:00:05:30:00:8d:e0, FCID is 0x610101
    Initiator N-port in vsan 1 is up
      Port WWN is 20:01:00:05:30:00:8d:e0, FCID is 0xec0102
    Mgmt N-port in vsan 1 is up
      Port WWN is 20:02:00:05:30:00:8d:e0, FCID is 0xec0103

switch# show svc port svc 2/1 target detail
svc2/1:
    Target N-port in vsan 1 is up
      Port WWN is 27:39:00:05:30:00:33:2a, FCID is 0x010006
      0 sessions, 0 closed, 0 in transition
        5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec 0 ios/sec
        5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec 0 ios/sec
      9 frames input, 1064 bytes
        0 input session management frames
          0 plogi, 0 prli
          0 logo, 0 logo_acc
          0 prlo, 0 prlo_acc
          0 abts, 0 ls_rjt
        0 input I/Os, 0 cmd complete, 0 cmd fail
          0 reads, 0 writes
        0 input errors
        0 input discards
      5 frames output, 388 bytes
        0 output session management frames
          0 plogi_acc, 0 prli_acc
          0 logo, 0 logo_acc
          0 prlo, 0 prlo_acc
          0 ba_acc, 0 ls_rjt
        0 output I/Os, 0 cmd complete, 0 cmd fail
        0 output errors
        0 output discards
```

```
switch# show svc session svc 2/1 peer-pwwn 27:46:00:05:30:00:33:2a detail

svc2/1:
    Mgmt N-port WWN is 27:3b:00:05:30:00:33:2a, vsan is 1, FCID is 0x010008
      pWWN 27:46:00:05:30:00:33:2a, nWWN 27:48:00:05:30:00:33:2a, FCID 0x010011
        19 frames input, 16517 data bytes
          2 ELS pkts, 0 BLS pkts
          3 FCP commands, 1 FCP xfer ready
          10 FCP data frames, 3 FCP status
          0 FCP overrun, 2 FCP underrun
          0 aborts, 0 bad FC2 drops
          0 data excess
        19 frames output, 16520 data bytes
          2 ELS pkts, 0 BLS pkts
          3 FCP commands, 1 FCP xfer ready
          10 FCP data frames, 3 FCP status
          0 aborts
        0 open exchanges
        FCP Error Stats
          FCP cmd errors
            0 sess not up, 0 no resources, 0 bad frames
            0 up layer rjt, 0 out of order, 0 proc unexp exch st
            0 drop unexp exch st, 0 no exch match
          FCP Xfer Rdy errors
            0 sess not up, 0 no resources, 0 bad frames
            0 up layer rjt, 0 out of order, 0 proc unexp exch st
            0 drop unexp exch st, 0 no exch match
          FCP Status errors
            0 sess not up, 0 no resources, 0 bad frames
            0 up layer rjt, 0 out of order, 0 proc unexp exch st
            0 drop unexp exch st, 0 no exch match
          FCP Data errors
            0 sess not up, 0 no resources, 0 bad frames
            0 up layer rjt, 0 out of order, 0 proc unexp exch st
            0 drop unexp exch st, 0 no exch match
```

svc-config

To perform SAN Volume Controller (SVC) configurations, use the **svc-config** command.

svc-config

Syntax Description

svc-config	Enters the SVC configuration mode.
cluster	Provides access to cluster commands.
node	Provides access to node commands.
show	Displays configured SVC information for the specified node.

Defaults

None.

Command Modes

EXEC mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following example enters the SVC configuration mode and displays all options in this mode.

```
switch# svc-config
switch-sw6(svc)# ?
Submode Commands:
  cluster  Cluster commands
  exit     Exit from this mode
  no       Negate a command or set its defaults
  node     Node commands
  show     Show
```

svc-ibmcli

To perform SAN Volume Controller (SVC) configurations by using IBM's CLI, use the **svc-ibmcli** command.

svc-ibmcli {cluster-name *cluster-name* [*IBM-CLI-command*] **| node svc** *slot-number/node-number* [*IBM-CLI-command*]**}**

Syntax Description

svc-ibmcli	Enters the IBM CLI configuration mode.
cluster-name	Specifies a new cluster.
cluster-name	Specifies a cluster name.
node svc	Specifies a node in the SVC interface.
slot-number	Specifies the slot number of the Caching Service Module (CSM).
node-number	Specifies the node number of the SVC instance running on the CSM. This number ranges from 1 to 2 nodes per module.
IBM-CLI-command	Specifies the IBM TotalStorage command to be executed

Defaults

None.

Command Modes

EXEC mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

When you enter the IBM TotalStorage shell, all future commands are interpreted directly by this shell. Type **exit** to return to the Cisco MDS switch prompt.

Examples

The following example enters the SVC configuration mode and displays all options in this mode.

```
switch# svc-ibmcli cluster-name SampleCluster
Attaching to config node for cluster SampleCluster
To exit type 'exit', to abort type '$.'
IBM_svc:admin>

switch# svc-ibmcli node svc 2/1
Attaching to node 2/1
To exit type 'exit', to abort type '$.'
IBM_svc:admin>
```

svc-purge-wwn module

To remove all configured WWNs for the CSM from the running configuration, use the **svc-purge-wwn module** command.

svc-purge-wwn module *module-number*

Syntax Description

svc-purge-wwn	Purges the WWN for the CSM.
module *module-number*	Specifies the slot number for the CSM.

Defaults

None.

Command Modes

EXEC mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

This command also purges all system allocated pWWNs and nWWNs from the system and will never be used again (by the system or by SVC interfaces). New system values will be allocated for all pWWN/nWWNs for the module.

Examples

The following example enters the SVC configuration mode and displays all options in this mode.

```
switch# svc purge-wwn module 2
!!!WARNING!  This command will purge all SVC system allocated
    WWNs for the specified module.  These WWNs will be lost.
    All user configured WWNs will be removed from the
    running-config, but not from the startup-config.
This operation can take a long time.  Other CLI commands
    on the system may be stopped while this operation is
    in progress.
Are you sure you want to do this? [Y/N] [N] y
switch#
```

vdisk

To create a new VDisk or access a new VDisk, use the **vdisk** command in the cluster configuration submode.

cluster config *cluster-name*

vdisk add *vdisk-name* **iogroup** *group-id* **mdisk-grp** *grp-name* **capacity** *number* **| import [clean | mdisk-list | preferred-node | sequential]**

vdisk name *vdisk-name* **-> expand [capacity | extent mdisk** *disk-id* **offset** *number*] **| io-throttle** *number* **[MB] | iogroup | shrink**

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submode.
vdisk add *vdisk-name*	Creates a VDisk of the specified name.
iogroup *group-id*	Identifies one of four I/O groups in the specified cluster. The ID ranges from 1 to 4. The I/O for the VDisk is serviced by node belonging to that I/O group.
mdisk-grp *grp-name*	Specifies an existing MDisk group from which the VDisk storage originates.
capacity	Configures the size of this VDisk.
number	Provides a range from 0- 1677215 Gigabytes.
import	Imports a previously unmanaged disk that contains SVC virtualization data.
clean	Clears all data in the VDisk.
mdisk-list	Specifies a list of MDisks. All disks in this list must be part of the MDisk group
preferred-node	specifies the preferred node within the two nodes in this group to send I/Os for this VDisk
sequential	Specifies a sequential virtualization policy. If this option is not specified, the striped (default) virtualization policy is used.
vdisk *vdisk-name*	Enters the VDisk submode of an existing VDisk.
expand capacity	Expands the MDisk capacity.
extent	Expands the MDisk by a single extent.
offset *number*	Offsets the extent.
io-throttle	Limits the amount of I/Os allowed for this VDisk. If MB is not specified, the unit is calculated in I/Os per second.
MB	Specifies the I/O throttling in Megabytes.
shrink	Shrinks the capacity of the VDisk as specified.

Defaults

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The cluster configuration submode prompt is (`switch(svc-cluster)#`).

The VDisk submode prompt is `switch (svc-cluster-vdisk)#`

Extents are allowed from all MDisks in the list

Examples

The following example enters the cluster configuration mode for SampleCluster and ---

```
switch(svc)# cluster config SampleCluster

switch(svc-cluster)# vdisk add Vdisk1 iogroup 1 mdisk-grp Mdisk1 ?
  capacity  Vdisk add name iogroup mdisk-grp
  import    Vdisk add import

switch(svc-cluster)# vdisk add Vdisk1 iogroup 1 mdisk-grp Mdisk1 capacity ?
  <0-2147483647>  Enter the capacity

switch(svc-cluster)# vdisk add Vdisk1 iogroup 1 mdisk-grp Mdisk1 capacity 5000 ?
  gb  Vdisk add name iogroup mdisk-grp capacity
  mb  Vdisk add name iogroup mdisk-grp capacity
  pb  Vdisk add name iogroup mdisk-grp capacity
  tb  Vdisk add name iogroup mdisk-grp capacity
switch(svc-cluster)# vdisk add Vdisk1 iogroup 1 mdisk-grp Mdisk1 capacity 5000 gb ?
  clean           Vdisk add clean
  mdisk-list      Vdisk add mdisk-list
  preferred-node  Vdisk add sequential mdisk
  sequential      Vdisk add sequential
  <cr>            Carriage Return

switch(svc-cluster)# vdisk add VDISK1 iogroup 1 mdisk-grp Mdisk1 capacity 0 gb
switch(svc-cluster)# vdisk VDISK1
switch(svc-cluster-vdisk)# ?
Submode Commands:
  exit         Exit from this mode
  expand       Expand
  io-throttle  Io throttle
  iogroup      Move vdisk to iogroup
  no           Negate a command or set its defaults
  shrink       Shrink capacity

switch(svc-cluster-vdisk)# expand ?
  capacity  Expand capacity
  extent    Expand extent

switch(svc-cluster-vdisk)# io-throttle 0

switch(svc-cluster-vdisk)# shrink capacity 1 ?
  gb  Expand capacity
  mb  Expand capacity
  pb  Expand capacity
  tb  Expand capacity

switch(svc-cluster-vdisk)# exit

switch(svc)# show cluster SampleCluster vdisk
--------------------------------------------------------------------------------
name             capacity     iogroup mdisk-grp name    policy      status
--------------------------------------------------------------------------------
```

```
Vdisk1          100.00 GB    1       Group1           striped     online
Vdisk2          50.00 GB     1       Group2           striped     online

switch(svc)# show cluster SampleCluster vdisk Vdisk1
vdisk Vdisk1 is online
    Capacity is 100.00 GB
    Using storage from mdisk-grp Group1
    Processed by io group 1
    Virtualization policy is striped
    Preferred node is 2

switch(svc)# show cluster SampleCluster vdisk Vdisk1 extent
-------------------------------------------------------------------------------
mdisk id  number of extents
-------------------------------------------------------------------------------
1         2134
2         2133
3         2133

switch(svc)# show cluster SampleCluster vdisk Vdisk1 mapped_hosts
-------------------------------------------------------------------------------
host             LUN
-------------------------------------------------------------------------------
Host1            0
```

Related Commands

Command	Description
show cluster *name* **vdisk**	Displays configured vdisk information for a specified cluster.