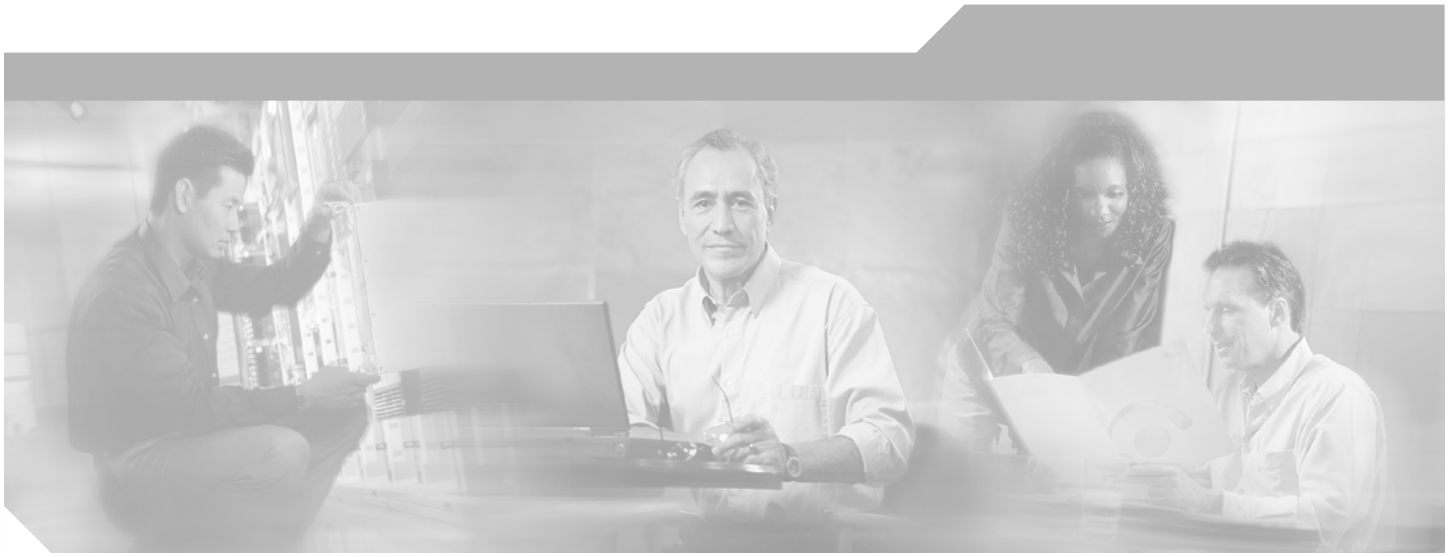
Cisco Systems

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



Cisco MDS 9020 Fabric Switch Configuration Guide and Command Reference, Release 2.x

Cisco MDS 9000 FabricWare Release 2.1(2)
June 2005

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-6988-01

Cisco MDS 9020 Fabric Switch Configuration Guide and Command Reference

CONTENTS

Preface

This preface describes the audience, organization, and conventions of the *Cisco MDS 9020 Fabric Switch Configuration Guide and Command Reference*. It also provides information on how to obtain related documentation.

Audience

This guide is for experienced network administrators who are responsible for configuring and maintaining the Cisco MDS 9020 Fabric Switch.

Organization

This guide is organized as follows:

Chapter	Title	Description
Chapter 1	Product Overview	Presents an overview of the Cisco MDS 9020 Fabric Switch.
Chapter 2	Before You Begin	Describes the command-line interface (CLI).
Chapter 3	Initial Configuration	Provides initial switch configuration options and switch access information.
Chapter 4	Software Images	Describes how to upgrade the Cisco MDS 9020 Fabric Switch, install software image files, use the Flash file system on the supervisor engine, and recover a corrupted bootflash image.
Chapter 5	Managing System Hardware	Explains switch hardware inventory, power usage, power supply, module temperature, fan and clock modules, and environment information.
Chapter 6	Configuring Interfaces	Explains port and operational state concepts in the Cisco MDS 9020 Fabric Switch and provides details on configuring ports and interfaces.

Chapter	Title	Description
Chapter 7	Configuring and Managing Zones	Defines various zoning concepts and provides details on configuring a zone set and zone management features.
Chapter 8	Managing FLOGI and FDMI	Describes the fabric login database and the Fabric-Device Management Interface information.
Chapter 9	Configuring Switch Security	Discusses the AAA parameters, user profiles, RADIUS authentication, SSH services, and SNMP security options, and provides configuration information for these options.
Chapter 10	Configuring SNMP	Provides details on configuring users, passwords, and roles for all CLI and SNMP users.
Chapter 11	Configuring Fibre Channel Routing Services and Protocols	Provides details and configuration information on Fibre Channel routing services and protocols.
Chapter 12	Configuring IP Services	Provides details on network management services configuration.
Chapter 13	Configuring Domain Parameters	Explains the Fibre Channel domain (fcdomain) feature, which includes principal switch selection, domain ID distribution, FC ID allocation, and fabric reconfiguration functions.
Chapter 14	Configuring System Message Logging	Describes how system message logging is configured and displayed.
Chapter 15	Advanced Features and Concepts	Describes the advanced configuration features—time out values and interoperating switches.
Chapter 16	Monitoring System Processes and Logs	Provides information on displaying system processes and status.
Appendix A	Command Reference	Describes the commands of the CLI in alphabetical order.

Document Conventions

Command descriptions use these conventions:

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]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Screen examples use these conventions:

`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.

Related Documentation

The documentation set for the Cisco MDS 9000 Family includes the following documents:

- *Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Releases*
- *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 VERITAS Storage Foundation for Networks Software*
- *Cisco MDS SAN-OS Release Compatibility Matrix for Storage Service Interface Images*
- *Cisco MDS 9000 Family SSM Configuration Note*

- *Cisco MDS 9000 Family ASM Configuration Note*
- *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*
- *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*
- *Cisco MDS 9000 Family Software Upgrade and Downgrade Guide*
- *Cisco MDS 9000 Family Configuration Guide*
- *Cisco MDS 9000 Family Command Reference*
- *Cisco MDS 9020 Fabric Switch Configuration Guide and Command Reference*
- *Cisco MDS 9000 Family Fabric Manager Configuration Guide*
- *Cisco MDS 9000 Family Fabric and Device Manager Online Help*
- *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide*
- *Cisco MDS 9000 Family Quick Configuration Guide*
- *Cisco MDS 9000 Family Fabric Manager Quick Configuration Guide*
- *Cisco MDS 9000 Family MIB Quick Reference*
- *Cisco MDS 9020 Fabric Switch MIB Quick Reference*
- *Cisco MDS 9000 Family CIM Programming Reference*
- *Cisco MDS 9000 Family System Messages Reference*
- *Cisco MDS 9020 Fabric Switch System Messages Reference*
- *Cisco MDS 9000 Family Troubleshooting Guide*
- *Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and 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.

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

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same 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=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

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

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

Ordering Documentation

Beginning June 30, 2005, 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/

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Instructions for ordering documentation using the Ordering tool are at this URL:

  http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

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 send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments 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 can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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

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

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 might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies — 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.

- 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 to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*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.

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)—Your 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 operation 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 your network is impaired, but 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.

- 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

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

CHAPTER 1

Product Overview

The Cisco MDS 9020 Fabric Switch offers Fibre Channel fabric-switching services that enable maximum performance and ensure high reliability. This switch combines robust and flexible hardware architecture and storage management intelligence. This powerful combination enables highly available, scalable storage networks that provide advanced security and unified management features.

The Cisco MDS 9020 Fabric Switch provides essential storage networking features that include advanced security, debug analysis tools, and unified SAN management.

This chapter lists the hardware features for the Cisco MDS 9020 Fabric Switch and describes its software features. It includes the following sections:

Hardware Overview

The Cisco MDS 9020 Fabric Switch provides these hardware features:

- 20 4-Gbps Fibre Channel ports per 1 RU
- Autodiscovery of Fibre Channel connections to single devices, loop devices, or other switches
- Autonegotiation of port transmission speeds of 1 Gbps, 2 Gbps, or 4 Gbps
- Port interfaces that support field-replaceable, hot-swappable, small form-factor pluggable (SFP) transceivers
- Front to back airflow
- Cisco MDS 9000 FabricWare software
- Full compatibility with the Cisco MDS 9000 Family

Refer to the *Cisco MDS 9020 Fabric Switch Hardware Installation Guide*.

Software Features

This section provides an overview of the major software features of the Cisco MDS 9020 Fabric Switch.

Switch Reliability

The Cisco MDS 9020 Fabric Switch maintains internally controlled reliability services that ensure continued service with no degradation. This reliability service includes the following functions:

- Provides power-on self testing (POST)
- Detects errors, isolates faults, performs parity checking, and checks illegal addresses
- Displays LEDs that summarize the status of the power supply and fan assembly

Intelligent Zoning

Intelligent zoning can control access between devices, and it accomplishes the following:

- Partitions devices that use different operating systems. In a heterogeneous environment, it is often necessary to separate servers and storage devices to avoid accidentally transferring information between devices with different operating systems. Such transfers could result in data corruption or deletion.
- Creates logical subsets of closed user groups. Closed user groups enforce security or to separate functional areas across the fabric.
- Configures groups of devices that are separate from the rest of the fabric. Based on the assigned zone membership, devices outside the zone cannot access devices inside the zone.
- Provides temporary access between devices (zone sets). Zone restrictions can be imposed temporarily and then restored to revert to normal operation, if desired.

See Chapter 7, “Configuring and Managing Zones.”

IP Services

The Cisco MDS 9020 Fabric Switch supports the following IP services:

- IP over Ethernet—These services are limited to traffic management.
- The Network Time Protocol (NTP) server—This server synchronizes the system clocks of network devices.

See Chapter 12, “Configuring IP Services.”

Switch Management Features

Along with the software features already listed, additional management features fall into these categories: fabric management and security management.

Fabric Management

The Cisco MDS 9020 Fabric Switch offers fabric management and control through the command-line interface (CLI) by using Telnet, SSH, or a serial console. The switch also offers fabric management through the Cisco MDS 9000 Family Fabric Manager tool by using Simple Network Management Protocol (SNMP):

- SNMP versions 1 and 2 are supported. See Chapter 9, "Configuring Switch Security."
- System log (syslog) messages are viewed through a console or Telnet session for asynchronous events such as an interface transition. System messages are directed to an internal log and optionally to an external server (refer to the *Cisco MDS 9020 Fabric Switch System Messages Reference)*. See Chapter 14, "Configuring System Message Logging."

Security Management

The Cisco MDS 9020 Fabric Switch offers secure switch management through user authentication and roles.

Switch Access Security

Each switch can be accessed through the CLI or SNMP.

- Secure switch access—Available when you explicitly enable Secure Shell Protocol (SSH) access to the switch. SSH access provides additional controlled security by encrypting data, user IDs, and passwords. By default, Telnet access is enabled on each switch.
- IP access control lists (IP-ACLs)—IP-ACLs enhance network security to the Cisco MDS 9020 Fabric. IP-ACLs restrict IP-related out-of-band management traffic based on IP addresses (Layer 3 and Layer 4 information). You can use IP-ACLs to control transmissions on management interfaces.

See Chapter 9, "Configuring Switch Security."

User Authentication

A strategy known as authentication, authorization, and accounting (AAA) verifies the identity of remote users, grant access, and tracks their actions. The Remote Access Dial-In User Service (RADIUS) provides a centralized AAA solution.

See Chapter 9, "Configuring Switch Security."

Role-Based Access

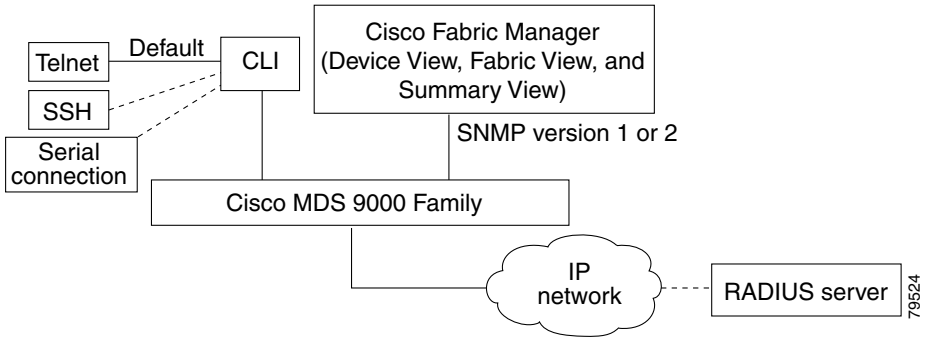
The Cisco MDS 9020 Fabric Switch performs authentication based on roles. Role-based authentication limits access to switch operations by assigning users to roles. There are two roles: network-operator and network-administrator. The network operator has permission to view the configuration only. The network administrator has permission to execute all commands and make configuration changes.

See Chapter 9, "Configuring Switch Security."

Tools for Software Configuration

You can use one of two configuration management tools to configure your SANs: the CLI and the Cisco MDS 9000 Family Fabric Manager graphical user interface. (See Figure 1-1.)

Figure 1-1 Tools for Configuring Software



CLI

With the CLI, you can type commands at the switch prompt, and the commands are executed when you press the Enter key. The CLI parser provides command help, command completion, and keyboard sequences that allow you to access previously executed commands from the buffer history.

Continue reading this guide for more information on configuring the Cisco MDS 9020 Fabric Switch using the CLI.

Cisco MDS 9000 Family Fabric Manager

The Cisco MDS 9000 Family Fabric Manager application is a set of network management tools that support secure Simple Network Management Protocol and legacy versions. It provides a graphical user interface (GUI) that displays real-time views of your network fabric and lets you manage the configuration of the Cisco MDS 9020 Fabric Switch. The Fabric Manager applications are as follows:

- Fabric Manager Server—Performs advanced monitoring, troubleshooting, and configuration for multiple fabrics. The server must be started before running the Fabric Manager. The server can be accessed by up to 16 Fabric Manager clients at a time.
- Device Manager—Presents the Device View of the a switch. Device View displays a continuously updated physical representation of the switch configuration and provides access to statistics and configuration information for a single switch.
- Fabric Manager Web Client—Allows operators to monitor MDS events, performance, and inventory from a remote location using a web browser.

The Cisco Fabric Manager applications are an alternative to the CLI for most switch configuration commands.

Refer to the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.

CHAPTER 2

Before You Begin

This chapter prepares you to configure switches from the CLI. It also lists the information that you need before you begin, and it describes the CLI command modes.

This chapter includes the following sections:

About the Switch Prompt

Note Refer to the *Cisco MDS 9020 Fabric Switch Hardware Installation Guide* for installation and connection instructions.

When the switch is powered on successfully, you see the default switch prompt (`switch#`), as shown in Example 2-1.

Example 2-1 Output When Switch Boots Up

```
INIT: Switching to runlevel: 6
Stopping sshd:[  OK  ]
Stopping xinetd: [  OK  ]
Saving random seed:  [  OK  ]
Shutting down kernel logger: [  OK  ]
Shutting down system logger: [  OK  ]
Starting killall:  [  OK  ]
Sending all processes the TERM signal...
Sending all processes the KILL signal...
Unmounting loopback filesystems:  umount: /dev/loop0: not mounted

Unmounting loopback filesystems (retry):
Unmounting file systems:
Please stand by while rebooting the system...
Restarting system.


U-Boot 0.2.0 Revision 1.3.0.08  (Mar  8 2005 - 10:21:12)

Kernel Source Revision 2.4.18_mvl30-amazon-0034

CPU:   MPC8245 Revision 1.4 at 249.999 MHz: 16 kB I-Cache 16 kB D-Cache
Board: Amazon-8245
I2C:   ready
DRAM:  256 MB
FLASH:  1 MB
Env:   default
In:    serial
Out:   serial
Err:   serial
Net:   DP83815
NAND device: Manufacture ID: 0x98, Chip ID: 0x79 (Toshiba NAND 128MiB 3,3V)
Creating 2 MTD partitions on "NAND 128MiB 3,3V":
Partition 0: 0x00000000-0x05000000 : "Amazon Image Partition"
Partition 1: 0x05000000-0x08000000 : "Amazon Config Partition"
Mounting partition '0' offset 0x0 size 80MB
### YAFFS booting: kernel=kernel.1 root=ramdisk.1 args="ramdisk=38056"
### YAFFS loading 'kernel.1' to 0x1000000
### YAFFS loading 'ramdisk.1' to 0x1100000
helper entry, hp @ 0x0x1000000, data @ 0x0x100025c, magic num 0x27051956
## Booting image at 01000000 ...
   Image Name:   Linux-2.4.18_mvl30-amazon
   Image Type:   PowerPC Linux Kernel Image (gzip compressed)
   Data Size:    638540 Bytes = 623.6 kB
   Load Address: 00000000
   Entry Point:  00000000
   Verifying Checksum ... OK
   Uncompressing Kernel Image ... OK
## Loading RAMDisk Image at 01100000 ...
```

```
   Image Name:   Amazon RAMDisk
   Image Type:   PowerPC Linux RAMDisk Image (gzip compressed)
   Data Size:    12874182 Bytes = 12.3 MB
   Load Address: 00000000
   Entry Point:  00000000
   Verifying Checksum ... OK
   Loading Ramdisk to 0f258000, end 0fe9f1c6 ... OK
Memory BAT mapping: BAT2=256Mb, BAT3=0Mb, residual: 0Mb
Linux version 2.4.18_mvl30-amazon (builds@gotham) (gcc version 3.2.1 20020930
(MontaVista)) #1 Tue F
eb 8 12:50:15 CST 2005
Amazon platform
On node 0 totalpages: 65536
zone(0): 65536 pages.
zone(1): 0 pages.
zone(2): 0 pages.
Kernel command line:   ramdisk=38056
OpenPIC Version 1.2 (1 CPUs and 26 IRQ sources) at fc040000
time_init: decrementer frequency = 25.011598 MHz
Calibrating delay loop... 166.29 BogoMIPS
Memory: 243920k available (1100k kernel code, 376k data, 60k init, 0k highmem)
Dentry-cache hash table entries: 32768 (order: 6, 262144 bytes)
Inode-cache hash table entries: 16384 (order: 5, 131072 bytes)
Mount-cache hash table entries: 4096 (order: 3, 32768 bytes)
Buffer-cache hash table entries: 16384 (order: 4, 65536 bytes)
Page-cache hash table entries: 65536 (order: 6, 262144 bytes)
POSIX conformance testing by UNIFIX
PCI: Probing PCI hardware
Linux NET4.0 for Linux 2.4
Based upon Swansea University Computer Society NET3.039
Initializing RT netlink socket
Starting kswapd
Disabling the Out Of Memory Killer
i2c-core.o: i2c core module version 2.6.2 (20011118)
i2c-dev.o: i2c /dev entries driver module version 2.6.2 (20011118)
i2c-proc.o version 2.6.2 (20011118)
pty: 256 Unix98 ptys configured
adm1021.o version 2.6.2 (20011118)
adm9240.o version 2.6.2 (20011118)
eeprom.o version 2.6.2 (20011118)
ds1339.o version 2.6.2 (20011118)
mic74.o version 2.6.2 (20011118)
Serial driver version 5.05c (2001-07-08) with MANY_PORTS SHARE_IRQ SERIAL_PCI enabled
ttyS00 at 0xfc004500 (irq = 137) is a 16550A
Generic RTC Driver v1.07
block: 128 slots per queue, batch=32
RAMDISK driver initialized: 16 RAM disks of 38056K size 1024 blocksize
loop: loaded (max 8 devices)
natsemi.c:v1.07 1/9/2001  Written by Donald Becker <becker@scyld.com>
  http://www.scyld.com/network/natsemi.html
  (unofficial 2.4.x kernel port, version 1.07+LK1.0.14, Nov 27, 2001  Jeff Garzik, Tjeerd
Mulder)
eth0: NatSemi DP8381[56] at 0xd1000000, 00:c0:dd:07:12:9f, IRQ 16.
Amazon Boot Flash: Probing for AMD compatible flash...
Amazon Boot Flash: Found 1 x 1MiB AMD AM29LV800BB at 0x0
Creating 1 MTD partitions on "Amazon Boot Flash":
0x00000000-0x00100000 : "BootFlash"
NAND device: Manufacture ID: 0x98, Chip ID: 0x79 (Toshiba NAND 128MiB 3,3V)
Creating 2 MTD partitions on "NAND 128MiB 3,3V":
0x00000000-0x05000000 : "Amazon Image Partition"
0x05000000-0x08000000 : "Amazon Config Partition"
MPC10x I2C - interrupt vector 129
NET4: Linux TCP/IP 1.0 for NET4.0
IP Protocols: ICMP, UDP, TCP, IGMP
```

```
IP: routing cache hash table of 2048 buckets, 16Kbytes
TCP: Hash tables configured (established 16384 bind 32768)
NET4: Unix domain sockets 1.0/SMP for Linux NET4.0.
RAMDISK: Compressed image found at block 0
Freeing initrd memory: 12572k freed
VFS: Mounted root (ext2 filesystem).
Freeing unused kernel memory: 60k init
INIT:version 2.78 bootinWelcome to Red Hat Linux
Mounting proc filesystem:  [  OK  ]
Configuring kernel parameters:  [  OK  ]
Setting hostname switch:  [  OK  ]
Finding module dependencies:  [  OK  ]
mke2fs 1.23, 15-Aug-2001 for EXT2 FS 0.5b, 95/08/09
Filesystem label=
OS type: Linux
Block size=1024 (log=0)
Fragment size=1024 (log=0)
9520 inodes, 38056 blocks
1902 blocks (5.00%) reserved for the super user
First data block=1
5 block groups
8192 blocks per group, 8192 fragments per group
1904 inodes per group
Superblock backups stored on blocks:
    8193, 24577

Writing inode tables: 0/51/52/53/54/5done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 33 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
Mounting local filesystems:  [  OK  ]
Running logRotate...
Enabling swap space:  [  OK  ]
INIT: Entering runlevel: 3
Initializing random number generator:  [  OK  ]
Starting system logger: [  OK  ]
Starting kernel logger: [  OK  ]
Starting xinetd: [  OK  ]
Starting fcswitch:  [  OK  ]

switch login: admin
Password:

Cisco MDS 9000 FabricWare
Copyright (C) 2002-2005, by Cisco Systems, Inc.
and its suppliers.  All rights reserved.
Copyrights to certain works contained herein are owned by
third parties, and used and distributed under license.
Portions of this software are governed by the GNU Public License,
which is available at http://www.gnu.org/licenses/gpl.html.

        ---- 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 is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

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): y

  Create another login account (yes/no) [n]: n

  Configure read-only SNMP community string (yes/no) [n]: y

    SNMP community string: public

  Configure read-write SNMP community string (yes/no) [n]: y

    SNMP community string: private

  Enter the switch name: rtp-9020-top

  Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: y

    Mgmt0 IP address: 172.18.172.160

    Mgmt0 IP netmask: 255255.255.255.0

  Configure the default gateway? (yes/no) [y]: y

  IP address of the default gateway: 172.18.172.1

  Enable the telnet service? (yes/no) [y]: y

  Enable SSH service? (yes/no) [n]: y

  Configure ntp server? (yes/no) [n]: n

  Configure default switchport interface state (shut/noshut) [shut]:

  Configure default zone policy (permit/deny) [deny]:

The following configuration will be applied:
  snmp-server community public ro
  snmp-server community private rw
  switchname rtp-9020-top
  interface mgmt0
    ip address 172.18.172.160 255.255.255.0
  ip default-gateway 172.18.172.1
  telnet server enable
  ssh server enable
  system default switchport shutdown
  no zone default-zone permit

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]:

[########################################] 100%
```

You can perform embedded CLI operations, access command histories, 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.

Default Switch Roles

The following roles are available in all switches:

- Network operator—Has permission to view the configuration.
- Network administrator—Has permission to perform all functions.

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. (See Chapter 9, "Configuring Switch Security.")

About the CLI Command Modes

Switches in the Cisco MDS 9020 Fabric Switch 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 2-1 lists and describes the two commonly used modes, how to enter the modes, and the resulting system prompts. The system prompt helps you to identify which mode you are in and which commands are available to you.

Table 2-1 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. See the "Saving a Configuration" section on page 2-14.	From EXEC mode, enter the **config terminal** command.	`switch(config)#`

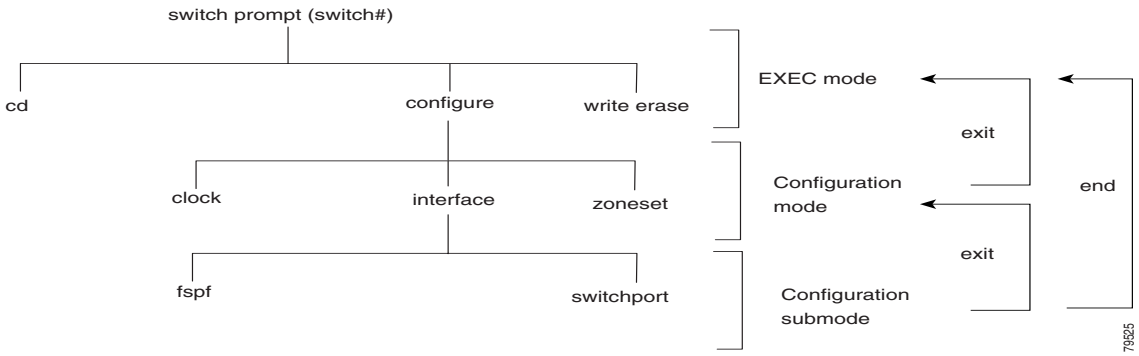
You can abbreviate commands and keywords by entering just enough characters to make the command unique from other commands. For example, you can abbreviate the **config terminal** command to **conf t**.

Note Do not enter percent (%), pound (#), ellipsis (...), vertical bar (|), less than or great than (< >), brackets ([ ]), semicolor (;), period (.), comma (,), or braces ({ }) in command lines. These characters have special meaning in Cisco MDS 9000 FabricWare text strings.

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 2-1 illustrates a portion of the **config terminal** command hierarchy.

Figure 2-1 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. When you are in configuration mode, enter 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 t
Enter configuration commands, one per line.
switch(config)# interface fc1/1
switch(config-if)# ?
  do                          EXEC command
  end                         Exit from configure mode
  exit                        Exit from this submode
  fspf                        Configure fspf
  help                        Press '?' key to display available commands
  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 Authorization" section on page 9-5.) From 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# ?
  cd                        Change current directory
  clear                     Reset functions
  clock                     Manage the system clock
  config                    Enter configuration mode
  copy                      Copy from one file to another
  delete                    Delete a file
  dir                       List files in a directory
  exit                      Exit from the EXEC
  help                      Press '?' key to display available commands
  install                   Upgrade software
  move                      Move files
  ping                      Send echo messages
  reload                    Reboot the entire box
  run-script                Run shell scripts
  setup                     Run the basic SETUP command facility
  show                      Show running system information
  sleep                     Sleep for the specified number of seconds
  system                    System management commands
  terminal                  Set terminal line parameters
  write                     Write current configuration
  zone                      Execute zone server commands
  zoneset                   Execute zoneset commands
```

Configuration Mode

In configuration mode, you can make changes to the existing configuration. When you save the configuration, these commands are preserved across switch reboots. When 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

Here is a list of configuration mode commands:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ?
  clock                    Configure time-of-day clock
  do                       EXEC command
  end                      Exit from configure mode
  exit                     Exit from configure mode
  fcalias                  Fcalias configuration commands
  fcdomain                 Enter the fcdomain configuration mode
  fctimer                  Configure fibre channel timers
  help                     Press '?' key to display available commands
  interface                Select an interface to configure
  ip                       Configure IP features
  logging                  Modify message logging facilities
  no                       Negate a command or set its defaults
  ntp                      NTP Configuration
  snmp-server              Configure snmp server
  ssh                      Configure SSH parameters
  switchname               Configure system's network name
  telnet                   Enable telnet
  username                 Configure user information.
  zone                     Zone configuration 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 execute an EXEC mode command from a configuration mode or submode prompt. You can enter 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 entering 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 entering a **do** command along with the EXEC command.

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

Table 2-2 Useful Command Key Description

Command	Description
Ctrl-P	Up history.
Ctrl-N	Down history.
Ctrl-R	Refreshes the current line and reprints it.
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-L	Clear screen.

CLI Command Navigation

To redisplay a command that you previously entered, press the **Up Arrow** key. You can continue to press the **Up Arrow** key to see more previously entered 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)# sh<Tab>
switch(config)# show in<tab>
switch(config)# show interface
```

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><Tab>
fcalias   fcdomain  fctimer
switch(config)# fcdo<Tab>
switch(config)# fcdomain
```

File System Completion

You can use the **Tab** key to complete schemes, servers, and file names that are available in the file system, as shown in this example.

```
switch# dir b<Tab>
switch# dir bootflash:
        962     May  2 19:42:32 2005  running-config
         26     May  1 20:16:45 2005  startup-config

Usage for bootflash://
15360       bytes used
2667520     bytes free
2682880     bytes total
```

The no and Default Forms of Commands

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

- Undo a wrongly entered command.

  If you enter the **zone member** command, you can undo the results as shown in the following example:

  ```
  switch(config)# zone name test
  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, enter the **no zone name** command, as shown in the following example:

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

CLI Command Configuration Options

You can configure the software in one of two ways:

- You can create the configuration for the switch interactively by entering commands at the CLI prompt.
- You can create an ASCII file containing a switch configuration and then load this file on the required system.

Displaying the Switch Configuration

You can view the ASCII form of the configuration file when required. To view the current configuration tree from the EXEC prompt, enter the **show running-config** command. If the running configuration is different from the startup configuration, enter the **show startup-config** command to view the ASCII version of the current startup configuration that was used to boot the switch if a **copy run start** command was not entered after the reboot. Use the **show startup** command to view the contents of the current startup configuration.

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

Examples 2-2 to 2-5 display **show** command examples.

Example 2-2 Displays Details on the Specified Interface

```
switch# show interface fc1/1
fc1/1 is Down (Administratively down)
    Hardware is Fibre Channel, SFP is long wave laser
    Port WWN is 20:00:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
```

Example 2-3 Displays the Software and Hardware Version

```
switch# show version
Cisco MDS 9000 FabricWare
Copyright (C) 2002-2005, by Cisco Systems, Inc.
and its suppliers.  All rights reserved.
Copyrights to certain works contained herein are owned by
third parties, and used and distributed under license.
Portions of this software are governed by the GNU Public License,
which is available at http://www.gnu.org/licenses/gpl.html.

Software
  system:   2.1(2)
  system compile time:   Thu Apr 21 12:48:49 2005

Hardware
  switch uptime is 0 days 11 hours 34 minute(s) 3 second(s)

  Last reset at 41643 usecs after Mon Apr 25 11:01:12 2005
    Reason: PowerUp
```

Example 2-4 Displays the Running Configuration

```
switch# show running
ip default-gateway 10.20.83.1
logging level fcdomain 2
logging level fspf 2
logging level fcns 2
logging level fcs 2
logging level port 2
logging level zone 2
logging level auth 2
logging level ipconf 2
logging level module 2
logging level ntp 2
logging level sysmgr 2
interface mgmt0
  ip address 10.20.83.122 255.255.255.0
interface fc1/1
interface fc1/2
interface fc1/3
interface fc1/4
interface fc1/5
interface fc1/6
interface fc1/7
interface fc1/8
interface fc1/9
interface fc1/10
interface fc1/11
interface fc1/12
interface fc1/13
interface fc1/14
interface fc1/15
interface fc1/16
interface fc1/17
interface fc1/18
interface fc1/19
interface fc1/20
```

Example 2-5 Displays the Difference Between the Running and Startup Configuration

```
switch# show running diff
switchname rtp-9020-top
  ip default-gateway 172.18.172.1
  ssh server enable
  logging level fcdomain 2
  logging level fspf 2
  logging level fcns 2
  logging level fcs 2
  logging level port 2
  logging level zone 2
  logging level auth 2
  logging level ipconf 2
  logging level module 2
  logging level ntp 2
  logging level sysmgr 2
  snmp-server community public ro
  snmp-server community private rw
  interface mgmt0
    ip address 172.18.172.160 255.255.255.0
    no shutdown
  interface fc1/1
+   no shutdown
  interface fc1/2
  interface fc1/3
  interface fc1/4
  interface fc1/5
  interface fc1/6
  interface fc1/7
  interface fc1/8
  interface fc1/9
  interface fc1/10
  interface fc1/11
  interface fc1/12
  interface fc1/13
  interface fc1/14
  interface fc1/15
  interface fc1/16
  interface fc1/17
  interface fc1/18
  interface fc1/19
  interface fc1/20
```

Saving a Configuration

Use the **copy running-config startup-config** command to save the new configuration into nonvolatile storage. When this command is entered, the running and the startup copies of the configuration are identical.

See the "Copying Files" section on page 3-20.

Clearing a Configuration

Use the **write erase** command to clear a startup configuration. When this command is entered, the switch's startup configuration reverts to factory defaults. The running configuration is not affected.

Caution 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 erases the startup configuration and any 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
```

Displaying Users

Use the **show users** command to display all users currently accessing the switch.

```
switch# show users
  snmp@IB-session2     Mon Apr 25 11:02:07 2005 (Unknown)
  snmp@OB-session3     Mon Apr 25 11:02:07 2005 (Unknown)
  admin@OB-session11   Wed Apr 27 13:50:49 2005 (10.20.32.70)
```

Using the ping Command

Use the **ping** command to verify 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 10.20.83.107
PING 10.20.83.107 (10.20.83.107): 10 data bytes
18 bytes from 10.20.83.107: icmp_seq=0 ttl=64 time=0.5 ms

--- 10.20.83.107 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.5/0.5/0.5 ms
```

Setting the 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 Terminal Length

Use the **terminal length** command in EXEC mode to set the terminal screen length for the current session. 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 20 lines.

Displaying Terminal Settings

Use the **show terminal** command to display the terminal settings for the current session:

```
switch# show terminal

Length: 10 lines
Session Timeout: 0 minutes
```

Internal bootflash:

The Cisco MDS 9020 Fabric Switch has two locations within the internal bootflash: file system.

- The volatile: file system provides temporary storage, and it is also the default location for file system commands. Files in temporary storage (volatile:) are erased when the switch reboots.
- The bootflash: (nonvolatile storage) file system provides permanent storage. The files in bootflash: are preserved through reboots and power outages.

Using the File System

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

Setting the Current File System

The **cd** command changes the current file system to a specified file system. CLI defaults to the volatile: file system. This command requires a file system name input.

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

The syntax for this command is **cd** *file system.*

This example changes the current file system to the volatile: file system:

```
switch# cd volatile:
```

Listing the Files in a File System

The **dir** command displays the contents of the current file system. The syntax for this command is **dir** *filesystem.*

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

```
switch# dir bootflash:
        962     May  5 15:26:49 2005  running-config
         26     May  1 20:16:45 2005  startup-config

Usage for bootflash://
15360       bytes used
2667520     bytes free
2682880     bytes total
```

Moving Files

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

This example moves the file called latest_mpc from the bootflash: file system to the volatile: file system:

```
switch# move bootflash:latest_mpc volatile:latest_mpc
```

Copying Files

The **copy** command copies a file. (See the "Copying Files" section on page 3-20.)

This example saves your configuration to the startup configuration:

```
switch# copy running-config startup-config
```

The following example saves a copy of the startup configuration on a remote host:

```
switch# copy startup-config ftp://10.20.102.98/configs/q100-startup
```

Deleting Files

The **delete** command deletes a specified file. (See the "Deleting Files" section on page 3-21.)

This example shows how to delete a file from the current working directory:

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

This example deletes the `my-file` file from the bootflash: file system:

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

Caution If you specify a file system, the **delete** command deletes the file system contents.

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: file system. This section assumes that the script file resides in the bootflash: file system.

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

The file, testfile, contains the following commands.

```
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 testfile
'conf t'
Enter configuration commands, one per line.
'interface fc1/1'
'no shutdown'
'end'
'sh interface fc1/1'
fc1/1 is Up (Link failure or not connected)
    Hardware is Fibre Channel, SFP is long wave laser
    Port WWN is 20:00:00:0d:ec:19:cb:0e
    Admin port mode is auto
    Port mode is Unknown, FCID is 0x690000
    Speed is Auto
    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 frames input, 0 bytes
        0 discards, 154096 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      1 input OLS, 1 LRR, 11 loop inits
      13 output OLS, 4 LRR, 11 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, consider a script called test-script with the following contents:

```
clear counters interface all
sleep 5
show interface counters brief
```

When you execute the test-script, the switch software executes the **clear counters interface all** command and then waits for 5 seconds before executing the **show interface counters brief** command.

```
switch# run-script test-script
```

CHAPTER 3

Initial Configuration

This chapter describes how to initially configure switches so they can be accessed by other devices. This chapter includes the following sections:

Starting a Cisco MDS 9020 Fabric Switch

The following procedure is a review of the tasks you should have completed during hardware installation, including starting up the switch. These tasks must be completed before you can configure the switch.

Before you can configure a switch, follow these steps:

Step 1 Verify the following physical connections for the new Cisco MDS 9020 Fabric Switch:

- The console port is physically connected to a computer terminal (or terminal server).
- The management 10/100 Ethernet port (mgmt0) is connected to an external hub, switch, or router.

Refer to the *Cisco MDS 9020 Fabric Switch Hardware Installation Guide* for more information.

Tip Save the host ID information for future use (for example, to enable licensed features). The host ID information is provided in the Proof of Purchase document that accompanies the switch.

Step 2 Verify that the default console port parameters are identical to those of the computer terminal (or terminal server) attached to the switch console port:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity

Step 3 Power on the switch. The switch boots automatically and the `switch#` prompt appears in your terminal window.

Initial Setup Routine

The first time that you access a Cisco MDS 9020 Fabric Switch, it runs a setup program that prompts you for the IP address and other configuration information necessary for the switch to communicate over the Ethernet interface. This information is required to configure and manage the switch.

Note The IP address can be configured from the CLI only. When you power up the switch for the first time, assign the IP address. After you perform this step, the Cisco Fabric Manager can reach the switch through the Ethernet port.

Preparing to Configure the Switch

Before you configure a Cisco MDS 9020 Fabric Switch for the first time, you need the following information:

- Administrator password, including:
  - Creating a password for the administrator (required).
  - Creating an additional login account and password (optional).
- IP address for the switch management interface. The management interface is an out-of-band Ethernet interface.
- Subnet mask for the switch's management interface (optional).
- IP addresses, including:
  - Destination prefix, destination prefix subnet mask, and next hop IP address, if you want to enable IP routing. Also, provide the IP address of the default network (optional).
  - Otherwise, provide an IP address of the default gateway (optional).
- SSH service on the switch—To enable this optional service, select the SSH key (rsa) and the number of key bits (768 to 2048).
- Default domain name (optional).
- NTP server IP address (optional).
- SNMP community string (optional).
- Switch name—This is your switch prompt (optional).

Note Be sure to configure the IP route, the IP default network address, and the IP default gateway address to enable SNMP access. If IP routing is enabled, the switch uses the IP route and the default network IP address. If IP routing is disabled, the switch uses the default gateway IP address.

Default Login

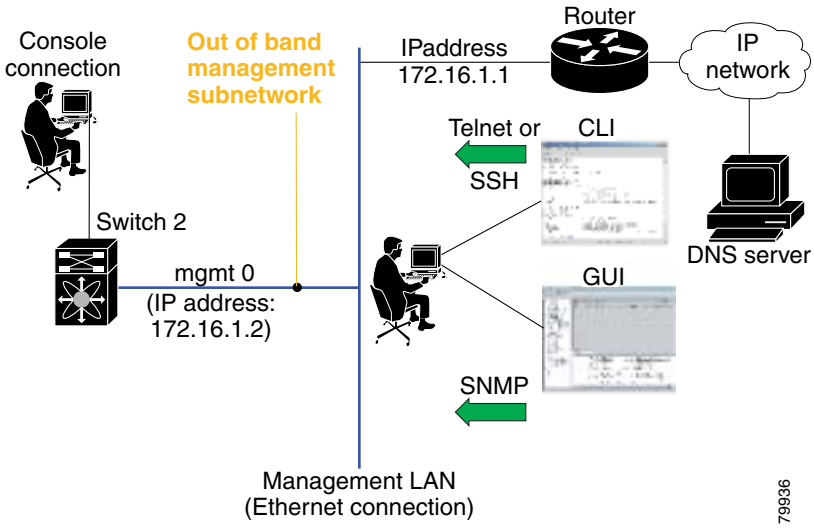
The Cisco MDS 9020 Fabric Switch has the network administrator as a default user (admin). You cannot change the default user at any time. (See the "Role-Based Authorization" section on page 9-5.)

You must explicitly configure a strong password for the Cisco MDS 9020 Fabric Switch. If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a strong password. (See "Configuring User Accounts" section on page 9-6.) If you configure and subsequently forget this new password, you have the option to recover this password. (See the "Recovering the Administrator Password" section on page 9-10.)

Setup Options

The setup scenario differs based on the subnet to which you are adding the new switch. You must configure a Cisco MDS 9020 Fabric Switch with an IP address to enable management connections from outside of the switch. Figure 3-1 shows a switch that is managed out-of-band over a connection to the network through an Ethernet port.

Figure 3-1 Management Access to Switches



Assigning Setup Information

This section describes how to initially configure the switch for both out-of-band and in-band management.

Note Press **Ctrl-C** at any prompt to skip the remaining configuration options and proceed with what is configured until that point. Entering the new password for the administrator is a requirement and cannot be skipped.

Tip 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 previously configured value and skips to the next question.

Configuring Out-of-Band Management

To configure the switch for first time out-of-band access, follow these steps:

Step 1 Power on the switch. The Cisco MDS 9020 Fabric Switch boots automatically.

Step 2 Enter the password for the administrator.

```
Enter the password for admin: admin123
```

Step 3 Enter **yes** to enter the setup mode.

```
---- 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 is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

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
```

The setup utility guides you through the basic configuration process. Press **Ctrl-C** at any prompt to end the configuration process.

Step 4 Enter **yes** (no is the default) to create additional accounts.

Note Only the admin user name can create or modify user accounts.

```
Create another login account (yes/no) [n]: yes
```

While configuring your initial setup, you can create an additional user account (in the network-admin role) besides the administrator's account. See the "Role-Based Authorization" section on page 9-5 for information on default roles and permissions.

a. Enter the user login ID.

```
Enter the user login ID: user_name
```

b. Enter the user password.

```
Enter the password for user_name: user-password
Confirm the password for user_name: user-password
```

c. Enter the user role.

```
Enter the user role [network-operator]:network_admin
```

Step 5 Enter **yes** (no is the default) to configure the read-only or read-write SNMP community string.

```
Configure read-only SNMP community string (yes/no) [n]: yes
```

a. Enter the SNMP community string.

```
SNMP community string: snmp_community
```

Step 6 Enter a name for the switch.

Note The switch name is limited to 32 alphanumeric characters.

```
Enter the switch name: switch_name
```

Step 7 Enter **yes** (yes is the default) to configure out-of-band management.

```
Continue with Out-of-band (mgmt0) management configuration? [yes/no]: yes
```

a. Enter the mgmt0 IP address.

```
Mgmt0 IP address: ip_address
```

b. Enter the mgmt0 subnet mask.

```
Mgmt0 IP netmask: subnet_mask
```

Step 8 Enter **yes** (yes is the default) to configure the default gateway (recommended).

```
Configure the default-gateway: (yes/no) [y]: yes
```

a. Enter the default gateway IP address.

```
IP address of the default-gateway: default_gateway
```

Step 9 Enter **yes** (yes is the default) to enable Telnet service.

```
Enable the telnet service? (yes/no) [y]: yes
```

Step 10 Enter **no** (no is the default) to disable the SSH service.

```
Enabled SSH service? (yes/no) [n]: no
```

Step 11 Enter **no** (no is the default) to not configure the NTP server.

```
Configure NTP server? (yes/no) [n]: no
```

Step 12 Enter **noshut** (shut is the default) to configure the default switchport interface to the noshut state.

```
Configure default switchport interface state (shut/noshut) [shut]: noshut
```

Step 13 Enter **deny** (deny is the default) to deny a default zone policy configuration.

```
Configure default zone policy (permit/deny) [deny]: deny
```

Deny prevents traffic flow to all members of the default zone.

Step 14 You see the new configuration. Review and edit the configuration that you have just entered. Enter **no** (no is the default) if you are satisfied with the configuration.

```
The following configuration will be applied:
username admin password admin_pass role network-admin
switchname switch
interface mgmt0
    ip address ip_address subnet_mask
ip default-gateway 10.0.0.254
telnet server enable
no ssh server enable
no system default switchport shutdown
no zone default-zone permit

Would you like to edit the configuration? (yes/no) [n]: no
```

Step 15 Enter **yes** (yes is default) to use and save this configuration:

```
Use this configuration and save it? (yes/no) [y]: yes
```

Caution If you do not save the configuration at this point, none of your changes are updated the next time the switch is rebooted. Type **yes** to save the new configuration and ensure that the system images are also automatically configured. (See Chapter 4, “Software Images”.)

Using the setup Command

To make changes to the initial configuration at a later time, you can enter the **setup** command in EXEC mode.

Note The setup utility is mainly used for the initial configuration when no configuration is present. The setup utility assumes system defaults and not the current system configuration values.

```
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 in case 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
```

The setup utility guides you through the basic configuration process.

Accessing the Switch

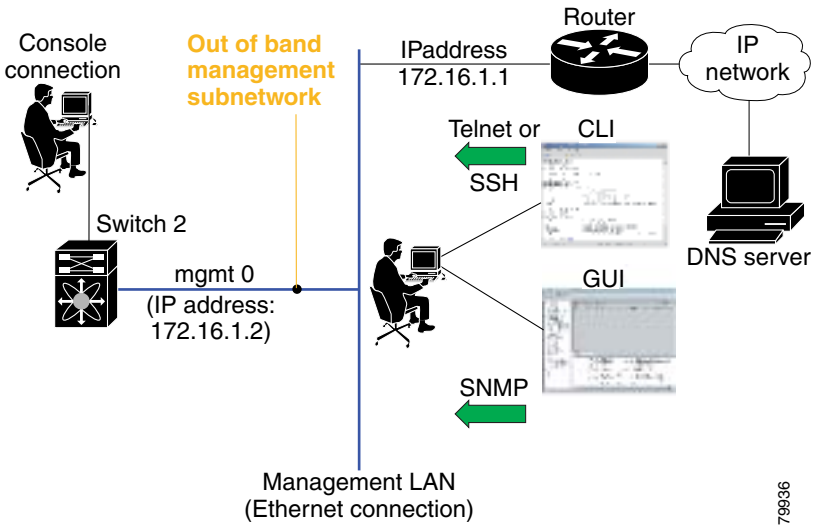
After initial configuration, you can access the switch in the following ways:

- Serial console access—You can use a serial port connection to access the CLI.
- Out-of-band (10/100BASE-T Ethernet) access—You can use Telnet or SSH to access a Cisco MDS 9020 Fabric Switch or use SNMP to connect to Cisco Fabric Manager.

Note To use Cisco Fabric Manager, refer to the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.

Figure 3-2 illustrates serial console access and out-of-band access.

Figure 3-2 Switch Access Options



Assigning a Switch Name

Each switch in the fabric requires a unique name. You can assign names to easily identify the switch by its physical location, its SAN association, or the organization to which it is deployed. The assigned name is displayed in the command-line prompt. The switch name is limited to 32 alphanumeric characters.

Note This guide refers to the Cisco MDS 9020 Fabric Switch as *switch*, and it uses the `switch#` prompt.

To change the name of the switch, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# switchname myswitch1` `myswitch1(config)#`	Changes the switch name prompt as specified.
Step 3	`myswitch1(config)# no switchname` `switch(config)#`	Reverts the switch name prompt to its default (switch#).

Where Do You Go Next?

After reviewing the default configuration, you can change it or perform other configuration or management tasks. The initial setup can be performed at the CLI only. However, you can continue to configure other software features or access the switch after initial configuration by using either the CLI or the Device Manager and Fabric Manager applications.

To use the Cisco Fabric Manager, refer to the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.

Verifying the Status of the Switch

Before you begin configuring the switch, you need to ensure that the switch is functioning as designed. To verify the status of a switch at any time, enter the **show module** command in EXEC mode. A sample output of the **show module** command follows:

```
switch# show module
Mod  Ports  Module-Type                       Model              Status
---  -----  -------------------------------- ------------------ ------------
1    20     1/2/4 Gbps FC/Supervisor         DS-C9020-20K9      active *

Mod  Sw             Hw      World-Wide-Name (WWN)
---  -------------  ------  --------------------------------------------------
1    2.1(2)         -------  10:00:00:0d:ec:19:cb:01


Mod  MAC-Address                               Serial-Num
---  ----------------------------------------  ----------
1    00-c0-dd-03-d4-e4                         0426a07855

* this terminal session
```

If the status is OK or active, you can continue with your configuration.

Configuring Date and Time

A Cisco MDS 9020 Fabric Switch uses Universal Coordinated Time (UTC), which is the same as Greenwich Mean Time (GMT). To change the default time on the switch, enter the **clock** command from EXEC mode.

```
switch# clock set <HH:MM:SS> <DD> <Month in words> <YYYY>
```

The following example sets the time on the switch:

```
switch# clock set 15:58:09 23 May 2005
Mon May 23 15:58:09 UTC 2005
```

Where *HH* represents hours in military format (15 for 3 p.m.), *MM* is minutes (58), *SS* is seconds (09), *DD* is the date (23), *Month* is the month in words (May), and *YYYY* is the year (2005).

Note The **clock** command changes are saved across system resets.

Configuring the Time Zone

You can specify a time zone for the switch.

To specify the local time without the daylight savings feature, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.

Step 2	`switch(config)# clock timezone <timezone name> <-23 to 23 hours offset from UTC time> <0 to 50 minutes offset from UTC>`
	
	Example:
	`switch(config)# clock timezone PST -8 0`
		Sets the time zone with a specified name, specified hours, and specified minutes.
		
		This example sets the time zone to Pacific Standard Time (PST) and offsets the UTC time by negative eight hours and 0 minutes.

Step 3	`switch(config)# exit` `switch#`	Returns to EXEC mode.
Step 4	`switch# show clock`	Verifies the time zone configuration.
Step 5	`switch# show run`	Displays changes made to the time zone configuration along with other configuration information.

Adjusting for Daylight Saving Time

Following U.S. standards, the switch can advance the clock one hour at 2:00 a.m. on the first Sunday in April and move the clock back one hour at 2:00 a.m. on the last Sunday in October. You can also explicitly specify the start and end dates and times, and you can specify whether or not the time adjustment recurs every year.

To enable the daylight saving time clock adjustment according to the U.S. rules, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# clock timezone` *timezone_name hour_offset_from_UTC minute_offset_from_UTC* Example: `switch(config)# clock timezone PST -8 0`	Offsets the time zone as specified. This example sets the Pacific standard offset time as negative 8 hours and 0 minutes.
	`switch(config)# no clock timezone`	Disables the time zone adjustment feature.

Step 3	`switch(config)# clock summer-time` *daylight_timezone_name start_week start_day start_month start_time end_week end_day end_month end_time daylight_offset_inminutes*
	
	Follow this example:
	`switch(config)# clock summer-time PDT 1 Sun Apr 02:00 5 Sun Oct 02:00 60`
	`switch(config)#`
		Sets the daylight savings time for a specified time zone.
		The start and end values are as follows:
		• Week ranging from 1 through 5
		• Day ranging from Sunday through Saturday
		• Month ranging from January through December
		The daylight offset ranges from 1 through 1440 minutes, which are added to the start time and deleted time from the end time.
		This example adjusts the daylight savings time for the Pacific daylight time by 60 minutes, starting the first Sunday in April at 2 a.m. and ending the last Sunday in October at 2 a.m.

	`switch(config)# no clock summer-time`	Disables the daylight saving time adjustment feature.
Step 4	`switch(config)# exit` `switch#`	Returns to EXEC mode.
Step 5	`switch# show clock`	Verifies the time zone configuration.

NTP Configuration

A Network Time Protocol (NTP) server provides a precise time source (radio clock or atomic clock) to synchronize the system clocks of network devices. NTP is transported over User Datagram Protocol UDP/IP. All NTP communications use UTC. An NTP server receives its time from a reference time source, such as a radio clock or atomic clock, attached to the time. NTP distributes this time across the network.

In a large enterprise network, having one time standard for all network devices is critical for management reporting and event logging functions when trying to correlate interacting events logged across multiple devices. Many enterprise customers with extremely mission-critical networks maintain their own stratum-1 NTP source.

Time synchronization happens when several frames are exchanged between clients and servers. The switches in client mode know the address of one or more NTP servers. The servers act as the time source and receive client synchronization requests.

To configure NTP in a server association, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# ntp server 10.10.10.10` `switch(config)#`	Forms a server association with a server.
Step 3	`switch(config)# exit` `switch#`	Returns to EXEC mode.
Step 4	`switch# copy running-config startup-config`	Saves your configuration changes to nonvolatile memory. **Tip** This is one instance where you can save the configuration as a result of an NTP configuration change. You can enter this command at any time.

Management Interface Configuration

A single IP address is used to manage the switch. The switch management (mgmt0) interface uses this IP address. The management interface on the switch allows multiple, simultaneous Telnet or SNMP sessions. You can remotely configure the switch through the management interface, but first you must configure some IP parameters (IP address, subnet mask) so that the switch is reachable. You can manually configure the management interface from the CLI.

The management port (mgmt0) is autosensing and operates in full duplex mode at a speed of 10/100 Mbps. The speed and mode cannot be configured.

Note Before you begin to configure the management interface manually, obtain the switch's IP address and IP subnet mask. Also make sure the console cable is connected to the console port.

Obtaining Remote Management Access

In some cases, a switch interface might be administratively shut down. You can check the status of an interface at any time by using the **show interface mgmt 0** command.

To obtain remote management access, perform this task:

	Command	Command
Step 1	`switch# config terminal` `switch(config)#`	Enters configuration mode. You can also abbreviate the command to **config t**.
Step 2	`switch(config)# interface mgmt 0`	Enters the interface configuration mode on the specified interface (mgmt0). You can use the management Ethernet interface on the switch to configure the management interface.
Step 3	`switch(config)# ip address 10.1.1.0 255.255.255.0`	Enters the IP address and IP subnet mask for the interface specified in Step 2.
Step 4	`switch(config-if)# no shutdown`	Enables the interface.
Step 5	`switch(config-if)# exit`	Returns to configuration mode.
Step 6	`switch(config)# ip default-gateway 10.1.1.1`	Configures the default gateway address.

Using the force Option

When you try to shut down a management interface (mgmt0), a follow-up message confirms your action before performing the operation. You can use the **force** option to bypass this confirmation. The following example shuts down the interface without using the **force** option:

Caution Do not shut down the mgmt0 port unless you have direct console access. If the management interface is shutdown, a console connection is the only way to regain access to the switch.

```
switch# config t
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:

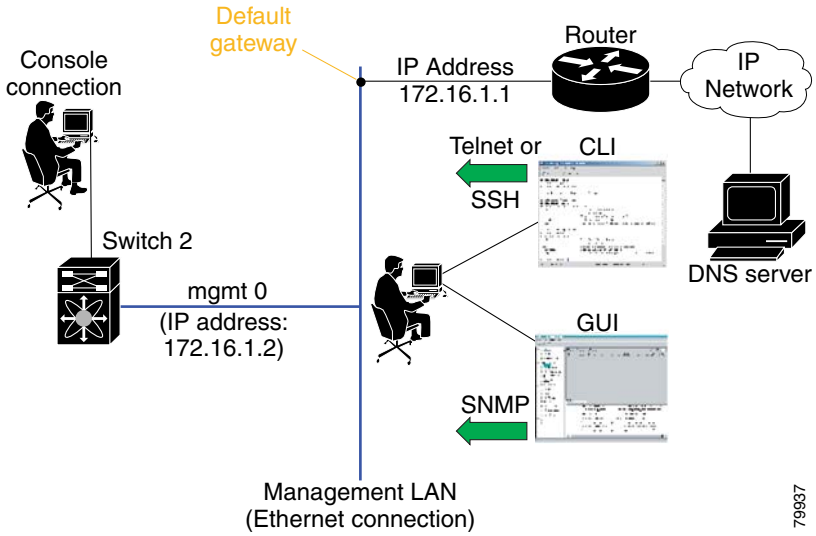
```
switch# config t
switch(config)# interface mgmt 0
switch(config-if)# shutdown force
```

Note You need to explicitly configure a default gateway to connect to the switch and send IP packets or add a route for each subnet.

Default Gateway Configuration

The switch sends IP packets with unresolved destination IP addresses to the default gateway. Figure 3-3 shows the default gateway.

Figure 3-3 Default Gateway



Configuring the Default Gateway

To configure the IP address of the default gateway, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# ip default-gateway 172.16.1.1`	Configures the 172.16.1.1 IP address.

Telnet Server Connection

The Telnet server is enabled by default on a Cisco MDS 9020 Fabric Switch. If you require a secure SSH connection, you need to disable the default Telnet connection and then enable the SSH connection. (See the "Enabling SSH Service" section on page 9-9.)

Tip A maximum of nine Telnet sessions are allowed on a Cisco MDS 9020 Fabric Switch.

Make sure the terminal is connected to the switch and that the switch and terminal are both powered on.

Disabling a Telnet Connection

To disable Telnet connections to the switch, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# no telnet server enable` `updated`	Disables the Telnet server.

Working with Configuration Files

Configuration files can contain some or all of the commands needed to configure one or more switches. For example, you might want to download the same configuration file to several switches that have the same hardware configuration so that they have identical module and port configurations.

This section describes how to work with configuration files and has the following topics:

Displaying Configuration Files

Use the **show running-config** command to view the running configuration file.

```
switch# show running-config
ip default-gateway 10.20.83.1
logging level fcdomain 2
logging level fspf 2
logging level fcns 2
logging level fcs 2
logging level port 2
logging level zone 2
logging level auth 2
logging level ipconf 2
logging level module 2
logging level ntp 2
logging level sysmgr 2
no snmp-server contact
no snmp-server location
zone name asdfa
zoneset name dave
interface mgmt0
  ip address 10.20.83.122 255.255.255.0
interface fc1/1
interface fc1/2
interface fc1/3
interface fc1/4
interface fc1/5
interface fc1/6
interface fc1/7
interface fc1/8
interface fc1/9
interface fc1/10
interface fc1/11
interface fc1/12
interface fc1/13
interface fc1/14
interface fc1/15
interface fc1/16
interface fc1/17
interface fc1/18
interface fc1/19
interface fc1/20
```

Use the **show startup-config** command to view the startup configuration file.

```
switch# show startup-config
interface fc1/1
       no shutdown
       Auto

interface fc1/2
       no shutdown
       Auto

interface fc1/3
       no shutdown
       Fx

interface fc1/4
       no shutdown
       Auto
```

```
interface fc1/5
       no shutdown
       Auto

interface fc1/6
       no shutdown
       Auto

interface fc1/7
       no shutdown
       Auto

interface fc1/8
       no shutdown
       Auto

interface fc1/9
       no shutdown
       Auto

interface fc1/10
       no shutdown
       Auto

interface fc1/11
       no shutdown
       Auto

interface fc1/12
       no shutdown
       Auto
interface fc1/13
       no shutdown
       Auto

interface fc1/14
       no shutdown
       Auto

interface fc1/15
       no shutdown
       Auto

interface fc1/16
       no shutdown
       Auto

interface fc1/17
       no shutdown
       Auto

interface fc1/18
       no shutdown
       Auto

interface fc1/19
       no shutdown
       Auto

interface fc1/20
       no shutdown
       Auto
```

Downloading Configuration Files to the Switch

You can configure a Cisco MDS 9020 Fabric Switch by using configuration files that you create or download from another switch. Before you begin downloading a configuration file using a remote server, do the following:

- Ensure that the configuration file to be downloaded is in the correct directory on the remote server.
- Ensure that the permissions on the file are set correctly. Permissions on the file should be set to world-read.
- Ensure that the switch has a route to the remote server. The switch and the remote server must be in the same subnetwork if you do not have a router or default gateway to route traffic between subnets.

  Check connectivity to the remote server using the **ping** command.

From a Remote Server

To configure a Cisco MDS 9020 Fabric Switch using a configuration file downloaded from a remote server using TFTP or FTP, follow these steps:

Step 1 Log in to the switch through the console port or through a Telnet or SSH session.

Step 2 Configure the switch using the configuration file downloaded from the remote server using the **copy <***scheme***> :// <***server address***> running-config** command, where *scheme* is TFTP or FTP.

The configuration file downloads and the commands are executed as the file is parsed line by line.

Saving Configuration Files to an External Device

You can save a configuration file stored on internal storage to a remote server.

To a Remote Server

To save a configuration file to a remote server such as FTP, follow these steps:

Step 1 Log into the switch through the console port or through a Telnet or SSH session.

Step 2 Save the configuration using the **copy running-config <***scheme***> :// <***server address***>** command, where *scheme* is FTP.

Step 3 Specify the IP address or host name of the remote server and the name of the file to download.

The configuration file is saved to the remote server.

Use the following command to save a running configuration file to a remote server:

```
switch# copy running-config <scheme>://<server address>
```

Use the following command to save a startup configuration file to a remote server:

```
switch# copy bootflash:startup-config <scheme>://<server address>
```

Saving the Configuration

After you have created a running configuration in system memory, you can save it to the startup configuration in the bootflash: file system using the following **copy** command:

```
switch# copy running-config bootflash:startup-config
```

The **copy running-config startup-config** command is an alias to the previous command and is used frequently throughout this guide.

Copying Files

The syntax for the **copy** command follows and is explained in Table 3-1.

```
switch# copy <scheme>://<server>/<file name> <scheme>://<server>/<file name>
```

Table 3-1 copy Command Syntax

Scheme	Server	File Name
volatile	—	User-specified
bootflash	—	User-specified
tftp	IP address or DNS name	User-specified
ftp		

- This example shows how to copy a running configuration to the bootflash: file system:

  ```
  switch# copy running-config bootflash:my-config
  ```

- This example shows how to overwrite the contents of an existing configuration in the nonvolatile file system:

  ```
  switch# copy bootflash:my-config bootflash:startup-config
  ```

Backing Up the Current Configuration

Before installing or migrating to any software configuration, back up the startup configuration.

- This example shows how to back up the startup configuration copy in the bootflash: file system (ASCII file):

  ```
  switch# copy startup-config bootflash:my-config
  ```

- This example shows how to back up the startup configuration to the TFTP server (ASCII file):

  ```
  switch# copy startup-config tftp://172.16.10.100/my-config
  ```

- This example shows how to back up the running configuration to the bootflash: file system (ASCII file):

  ```
  switch# copy running-config bootflash:my-config
  ```

Rolling Back to a Previous Configuration

All switch configurations reside in the internal bootflash: file system. If your internal bootflash: file system is corrupted, you could potentially lose your configuration. Save and back up your configuration file periodically.

- This example shows how to roll back to a snapshot copy of a previously saved running configuration (binary file):

```
switch# copy bootflash:snapshot-config bootflash:startup-config
```

Note You can enter a rollback command only when a snapshot is already created. Otherwise, you will receive the `No snapshot-config found` error message.

- This example shows how to roll back to a configuration copy that was previously saved in the bootflash: file system (ASCII file):

```
switch# copy bootflash:my-config startup-config
```

Note Each time a **copy running-config startup-config** command is entered, a binary file is created and the ASCII file is updated. A valid binary configuration file reduces the overall boot time significantly. A binary file cannot be uploaded, but its contents can be used to overwrite the existing startup configuration. The **write erase** command clears the binary file.

Deleting Files

Assuming you are already in the bootflash: file system, use the **delete** command to delete a file from the bootflash: file system:

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

CHAPTER 4

Software Images

This chapter describes how to install and upgrade software images. It includes the following sections:

About Software Images

Each switch is shipped with Cisco MDS 9000 FabricWare software. The software image install procedure is dependent on the following factors:

- Software images—The image file must reside in the volatile: file system.
- Image version—Each image file has a version.

Essential Upgrade Prerequisites

Before attempting to migrate to any software image version, follow these guidelines to ensure a nondisruptive upgrade:

Caution Failure to follow these guidelines could result in a disruptive upgrade.

- Customer Service

  Before performing any software upgrade, contact your respective customer service representative to review your software upgrade requirements and to provide recommendations based on your current operating environment.

Note If you purchased Cisco support through a Cisco reseller, contact the reseller directly. If you purchased support directly from Cisco Systems, contact Cisco Technical Support at this URL: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

- Scheduling

  Schedule the upgrade when the fabric is stable and steady. Ensure that everyone who has access to the switch or the network is not configuring the switch or the network during this time. All configurations are disallowed at this time.

- Space

  Verify that sufficient space is available in the volatile: file system where you are copying the firmware image.

- Hardware

  Avoid power interruption during any install procedure. This type of problem can corrupt the software image.

- Connectivity (to retrieve images from remote servers)
  - Configure the IP address for the 10/100BASE-T Ethernet port connection (interface mgmt0).
  - Ensure that the switch has a route to the remote server. The switch and the remote server must be in the same subnetwork if you do not have a router to route traffic between subnets.

- Retrieve an image in one of two ways:

  Locally—Image is locally available on the switch.

  Remotely—Image is in a remote location, and the user specifies the destination using the remote server parameters and the file name to be used locally.

- Terminology

  Table 4-1 summarizes terms used in this chapter with specific reference to the install and upgrade process.

Table 4-1 Terms Specific to This Chapter

Term		Definition
bootable		The module's ability to boot or not boot based on image compatibility.
impact		The type of software upgrade mechanism—disruptive or nondisruptive.
install-type	reset	Resets the switch.

- Commands
  - Verify connectivity to the remote server using the **ping** command.
  - Use the **dir** command to ensure that the required space is available for the image file to be copied.
  - Use the one-step **install all** command to upgrade your software.
  - Only one **install all** command can be running on a switch at any time.
  - No other command can be entered while running the **install all** command.

Note When you enter the **install all** command, the switch displays a summary of changes that are made to your configuration.

Software Upgrade Methods

You can upgrade software without disruptions by using the Cisco MDS 9000 FabricWare software designed for high availability environments. You can upgrade a Cisco MDS 9020 Fabric Switch using the **install all** command. The **install all** command will attempt a nondisruptive upgrade; if a nondisruptive upgrade is not possible, a disruptive upgrade will occur. (See the "Automated Upgrades" section on page 4-3.)

Automated Upgrades

The **install all** command upgrades the Cisco MDS 9020 Fabric Switch. The **install all** command provides the following features:

- You can upgrade the entire switch using just one command.
- The command performs a platform validity check to verify that a wrong image is not used.
- After entering the command, if any step in the sequence fails, the command completes the step in progress and ends.

  For example, if a switching module fails to be updated for any reason (for example, due to an unstable fabric state), then the command sequence disruptively updates that module and ends. In such cases, you can investigate the problem on the affected switching module and upgrade the other switching modules.

Recognizing Failure Cases

The following situations cause the **install all** command to end:

- If the volatile: file system does not have sufficient space to accept the updated image.
- If the switch has any power disruption while the upgrade is in progress.
- If the entire path for the remote location is not specified accurately.

Tip Most configurations are disallowed while the **install all** command is in progress.

Using the install all Command

To perform an automated software upgrade on a switch, follow these steps:

Step 1 Log in to the switch through the console.

Step 2 Create a backup of your existing configuration file, if required. (See the "Working with Configuration Files" section on page 3-16.)

Step 3 Download the firmware image file to the volatile: file system:

```
switch# copy ftp://10.20.102.98/firmware/latest_mpc volatile:latest_mpc
```

Step 4 Perform the upgrade by entering the **install all** command.

```
switch# install all system volatile:latest_mpc
Performing configuration copy.
[########################################] 100%

Unpacking image - this may take several seconds...
```

Step 5 Exit the switch console, and open a new terminal session to view the upgraded switch using the **show module** command.

If the configuration meets all guidelines when the **install all** command is entered, the switch is upgraded.

Caution If a nondisruptive upgrade operation fails for any reason other than those listed in the "Recognizing Failure Cases" section on page 4-3, contact your reseller or Cisco representative for further assistance.

If you purchased Cisco support through a Cisco reseller, contact the reseller directly. If you purchased support directly from Cisco Systems, contact Cisco Technical Support at this URL: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Corrupted Bootflash Recovery

In the event that the switch bootflash is corrupted, the file system must be recreated. To recreate the file system, you must enter maintenance mode and choose **Remake Filesystem** option. The **Remake Filesystem** recreates the file system and resets the switch to the factory default values, including user accounts and zoning.

Caution The **Remake Filesystem** option deletes the running-config and startup-config files. You must then restore the switch from an archived configuration or reconfigure the portions of the fabric that involve the switch.

To recreate the file system, follow these steps:

Step 1 Isolate the switch from the fabric.

Step 2 Connect the PC console to the switch using a serial console connection.

Step 3 Place the switch in maintenance mode. Press and hold the **Maintenance** button with a pointed tool. When the Heartbeat LED turns on continuously, release the button.

Step 4 Enter the account name (prom) and password (prom), and press the **Enter** key.

```
Switch login: prom
Password:xxxx
```

Step 5 Enter **6** (Remake Filesystem) on the maintenance menu, and press the **Enter** key to recreate the configuration file.

```
0)  Exit
1)  Image Unpack
2)  Reset Network Config
3)  Reset User Accounts to Default
4)  Copy Log Files
5)  Remove Switch Config
6)  Remake Filesystem
7)  Reset Switch
8)  Update Boot Loader
Option: 6
```

Step 6 When the process is complete, enter **7** (Reset Switch) to reset the switch and exit maintenance mode.

```
0)  Exit
1)  Image Unpack
2)  Reset Network Config
3)  Reset User Accounts to Default
4)  Copy Log Files
5)  Remove Switch Config
6)  Remake Filesystem
7)  Reset Switch
8)  Update Boot Loader
Option: 7
```

CHAPTER 5

Managing System Hardware

This chapter provides details on monitoring the health of the switch. It includes the following sections:

Displaying Switch Hardware Inventory

Use the **show hardware** command to display switch hardware inventory details. (See Example 5-1.)

Note To display modules, see the "Verifying the Status of the Switch" section on page 3-10.

Example 5-1 Displays the Hardware Information

```
switch# show hardware
Cisco MDS 9000 FabricWare
Copyright (C) 2002-2005, by Cisco Systems, Inc.
and its suppliers.  All rights reserved.
Copyrights to certain works contained herein are owned by
third parties, and used and distributed under license.
Portions of this software are governed by the GNU Public License,
which is available at http://www.gnu.org/licenses/gpl.html.

Software
  system:   2.1(2)
  system compile time:   Thu Apr 21 12:48:49 2005

Hardware
  switch uptime is 2 days 4 hours 25 minute(s) 20 second(s)

  Last reset at 188720 usecs after Mon Apr 25 11:01:12 2005
    Reason: PowerUp

--------------------------------
Switch hardware ID information
--------------------------------

MDS Switch is booted up
  Model number is DS-C9020-20K9
  H/W version is -------
  Part Number is 74-3811-01
  Part Revision is A0
  Serial number is 0426a07855
  CLEI code is COMMM00ARA
```

Displaying the Switch Serial Number

The serial number of your Cisco MDS 9020 Fabric Switch can be obtained by looking at the serial number label on the back of the switch or by executing the operating system **show sprom mgmt-module** command.

```
switch# show sprom mgmt-module
DISPLAY SAM sprom contents:
Common block:
 OEM String      : Cisco Systems, Inc.
 Product Number  : DS-C9020-20K9
 Serial Number   : 0426a07855
 Part Number     : 74-3811-01
 Part Revision   : A0
 Mfg Deviation   : 0
 H/W Version     : -------
 snmpOID         : 1.3.6.1.4.1.1663.1.1.1.1.26
 CLEI Code       : COMMM00ARA
```

```
VID             : V01
MAC Address     : 00-c0-dd-03-d4-e4
WWN             : 10:00:00:0d:ec:19:cb:0e
```

Displaying Power Supply Status

Use the **show environment power** command to display the power supply status. (See Example 5-2.)

Example 5-2 Displays Power Supply Status

```
switch# show environment power
-------------
PS      Status
-------------
1       ok
```

Displaying Environment Information

Use the **show environment** command to display all environment-related switch information. (See Example 5-3.)

Example 5-3 Displays All Environment Information

```
switch# show environment
Temperature:
---------------------------
Module   CurTemp     Status
         (Celsius)
---------------------------
1        36          ok

Power Supply:
-------------
PS      Status
-------------
1       ok
```

CHAPTER 6

Configuring Interfaces

A switch's main function is to relay frames from one data link to another. To do that, the characteristics of the interfaces through which the frames are received and sent must be defined. The configured interfaces can be Fibre Channel interfaces or the management interface (mgmt0).

This chapter describes the basic interface configuration to get your switch up and running. It includes the following sections:

Note See Chapter 3, "Initial Configuration," and Chapter 12, "Configuring IP Services," for more information on configuring mgmt0 interfaces.

Tip Before you begin configuring the switch, ensure that the switch functioning as designed. To verify the status of a switch at any time, enter the **show module** command in EXEC mode. (See the "Verifying the Status of the Switch" section on page 3-10.)

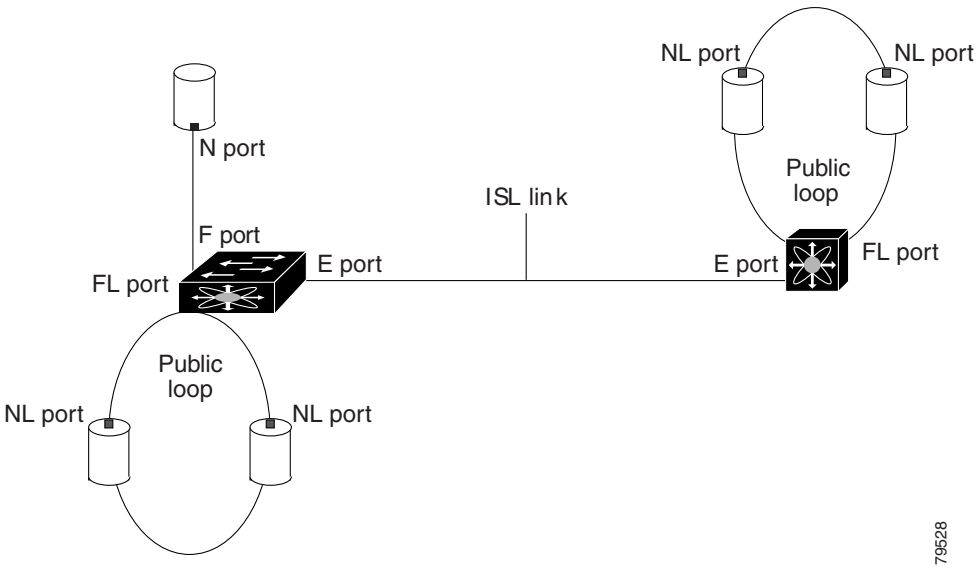
Fibre Channel Interfaces

This section describes Fibre Channel interface characteristics, including (but not limited to) modes, states, and speeds. It includes the following sections:

About Interface Modes

Each physical Fibre Channel interface in a switch may operate in one of several port modes: E port, F port, and FL port (see Figure 6-1). Each interface may be configured in auto or Fx port modes. These two modes determine the port type during interface initialization.

Figure 6-1 Cisco MDS 9020 Fabric Switch Port Modes



Each interface has an associated administrative configuration and an operational status:

- The administrative configuration does not change unless you modify it. This configuration has various attributes that you can configure in administrative mode.
- The operational status represents the current status of a specified attribute, such as the interface speed. This status cannot be changed and is read-only. Some values may not be valid when the interface is down (for example, the operational speed).

A brief description of each interface mode follows.

E Port

In expansion port (E port) mode, an interface functions as a fabric expansion port. This port may be connected to another E port to create an Inter-Switch Link (ISL) between two switches. E ports carry frames between switches for configuration and fabric management. They serve as conduits between switches for frames that are destined to remote N ports and NL ports. E ports support class 2, class 3, and class F service.

F Port

In fabric port (F port) mode, an interface functions as a fabric port. This port may be connected to a peripheral device (host or disk) operating as an N port. An F port can be attached to only one N port. F ports support class 2 and class 3 service.

FL Port

In fabric loop port (FL port) mode, an interface functions as a fabric loop port. This port may be connected to one or more NL ports (including FL ports in other switches) to form a public arbitrated loop. If more than one FL port is detected on the arbitrated loop during initialization, only one FL port becomes operational and the other FL ports enter nonparticipating mode. FL ports support class 2 and class 3 service.

Fx Port

Interfaces that are configured as Fx ports can operate in either F port or FL port mode. The Fx port mode is determined during interface initialization depending on the attached N port or NL port. This administrative configuration disallows interfaces to operate in any other mode—for example, preventing an interface to connect to another switch.

Auto

Interfaces that are configured in auto mode can operate in one of the following modes: F port, FL port, or E port. The port mode is determined during interface initialization. For example, if the interface is connected to a node (host or disk), it operates in F port or FL port mode depending on the N port or NL port mode. If the interface is attached to a third-party switch, it operates in E port mode.

About Interface States

The interface state depends on the administrative configuration of the interface and the dynamic state of the physical link.

Administrative States

The administrative state refers to the administrative configuration of the interface, as described in Table 6-1.

Table 6-1 Administrative States

Administrative State	Description
Up	Interface is enabled.
Down	Interface is disabled. If you administratively disable an interface by shutting down that interface, the physical link layer state change is ignored.

Operational States

The operational state indicates the current operational state of the interface, as described in Table 6-2.

Table 6-2 Operational States

Operational State	Description
Up	Interface is transmitting or receiving traffic as desired. To be in this state, an interface must be administratively up, the interface link layer state must be up, and the interface initialization must be completed.
Down	Interface cannot transmit or receive (data) traffic.

Reason Codes

Reason codes are dependent on the operational state of the interface, as described in Table 6-3.

Table 6-3 Reason Codes for Interface States

Administrative Configuration	Operational Status	Reason Code
Up	Up	None.
Down	Down	Administratively down—If you administratively configure an interface as down, you disable the interface. No traffic is received or transmitted.
Up	Down	See Table 6-4.

If the administrative state is up and the operational state is down, the reason code differs based on the nonoperational reason code, as described in Table 6-4.

Table 6-4 Reason Codes for Nonoperational States

Reason Code	Description	Applicable Modes
Link failure or not connected	The physical layer link is not operational.	All
SFP not present	The small form-factor pluggable (SFP) hardware is not plugged in.	
Initializing	The physical layer link is operational, and the protocol initialization is in progress.	
Reconfigure fabric in progress	The fabric is currently being reconfigured.	
Offline	The Cisco MDS 9000 FabricWare software waits for the specified R_A_TOV time before retrying initialization.	
Inactive	The interface is deleted or is in a suspended state.	
Hardware failure	A hardware failure is detected.	
Error disabled	Error conditions require administrative attention. Interfaces may be error-disabled for various reasons. For example: • Configuration failure. • Incompatible buffer-to-buffer credit configuration. To make the interface operational, you must first fix the error conditions causing this state; and next, administratively shut down or enable the interface.	
Isolation due to ELP failure	The port negotiation failed.	E ports
Isolation due to ESC failure	The port negotiation failed.	
Isolation due to domain overlap	The Fibre Channel domains (fcdomain) overlap.	
Isolation due to domain ID assignment failure	The assigned domain ID is not valid.	
Isolation due to other side E port isolated	The E port at the other end of the link is isolated.	
Isolation due to invalid fabric reconfiguration	The port is isolated due to fabric reconfiguration.	
Isolation due to domain manager disabled	The fcdomain feature is disabled.	
Isolation due to zone merge failure	The zone merge operation failed.	
Nonparticipating	FL ports cannot participate in loop operations. It may happen if more than one FL port exists in the same loop, in which case all but one FL port in that loop automatically enters nonparticipating mode.	FL ports

Fibre Channel Interface Configuration

To configure a Fibre Channel interface, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# interface fc1/1`	Configures the specified interface. **Note** When a Fibre Channel interface is configured, it is automatically assigned a unique world wide name (WWN). If the interface's operational state is up, it is also assigned a Fibre Channel ID (FC ID).

To configure a range of interfaces, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# interface fc1/1-4`	Configures the range of specified interfaces.

Graceful Shutdown

Interfaces on a port are shut down by default (unless you modified the initial configuration). The Cisco MDS 9000 FabricWare software implicitly performs a graceful shutdown in response to either of the following actions for interfaces operating in the E port mode:

- If you shut down an interface
- If a Cisco MDS 9000 FabricWare application executes a port shutdown as part of its function

A graceful shutdown ensures that no frames are lost when the interface is shutting down. When a shutdown is triggered either by you or the Cisco MDS 9000 FabricWare software, the switches connected to the shutdown link coordinate with each other to ensure that all frames in the ports are safely sent through the link before shutting down. This enhancement reduces the chance of frame loss.

A graceful shutdown is not possible if the Min_LS_interval interval is higher than 10 seconds. (See "Displaying Global FSPF Information" section on page 11-4.)

To shut down an interface, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# interface fc1/1`	Configures the specified interface.
Step 3	`switch(config-if)# shutdown`	Shuts down the interface and administratively disables traffic flow (default).

To enable traffic flow, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# interface fc1/1`	Configures the specified interface.
Step 3	`switch(config-if)# no shutdown`	Enables traffic flow to administratively allow traffic when the **no** prefix is used (provided the operational state is up).

Interface Modes

To configure the interface mode, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# interface fc1/1` `switch(config-if)#`	Configures the specified interface.
Step 3	`switch(config-if)# switchport mode F` `switch(config-if)#`	Configures the administrative mode of the port. You can set the interface mode to auto, E, F, FL, or Fx port mode. **Note** Fx ports refers to an F port or an FL port (host connection only), but not E ports.
	`switch(config-if)# switchport mode auto` `switch(config-if)#`	Configures the interface mode to autonegotiate an E, F, or FL port mode of operation.

Administrative Speeds

By default, the administrative speed for an interface is automatically calculated by the switch.

To configure the administrative speed of the interface, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config-if)# switchport speed 1000` `switch(config-if)#`	Configures the administrative speed of the interface to 1000 Mbps. The number indicates the speed in megabits per second (Mbps). You can set the speed to 1000 Mbps (for 1-Gbps interfaces), 2000 Mbps (for 2-Gbps interfaces), 4000 Mbps (for 4-Gbps interfaces), or auto (default).
	`switch(config-if)# switchport speed auto` `switch(config-if)#`	Reconfigures the factory default (auto) administrative speed of the interface.

Interface Descriptions

To configure a description for an interface, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# interface fc1/1` `switch(config-if)#`	Configures the specified interface.
Step 3	`switch(config-if)# switchport description cisco-HBA2`	Configures the description of the interface. The string may be up to 32 characters long.
	`switch(config-if)# no switchport description`	Clears the description of the interface.

Beacon Mode

By default, the beacon mode is disabled on all switches. The beacon mode is indicated by a flashing green light that helps you identify the physical location of the specified interface.

The **beacon** command has no effect on the operation of the interface.

To enable beacon mode for a specified interface or range of interfaces, perform this task:

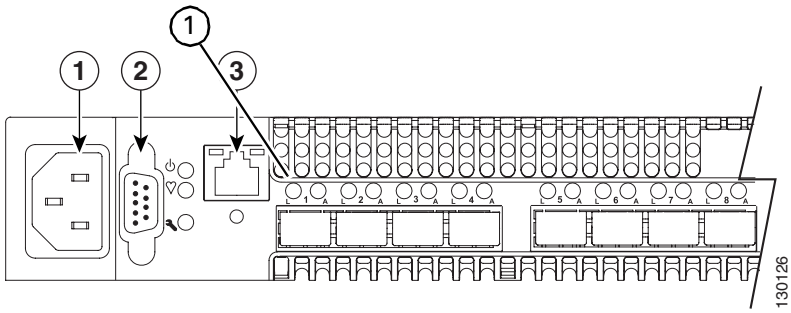
	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# interface fc1/1` `switch(config-if)#`	Configures the specified interface.
Step 3	`switch(config-if)# switchport beacon`	Enables the beacon mode for the interface.
	`switch(config-if)# no switchport beacon`	Disables the beacon mode for the interface.

The flashing green light indication turns on automatically when an external loopback is detected that causes the interfaces to be isolated. The flashing green light indication overrides the beacon mode configuration. The state of the LED is restored to reflect the beacon mode configuration after the external loopback is removed.

Beacon LED Identification

Figure 6-2 displays the Logged-In LED for port 1 in a Cisco MDS 9020 Fabric Switch. The beacon flashes the Logged-In LEDs on all ports.

Figure 6-2 Cisco MDS 9020 Fabric Logged-In LED (Beacon)



1	Logged-In LED (Green)

SFP Transmitter Types

The SFP hardware transmitters are identified by their acronyms when displayed in the **show interface brief** command. If the related SFP has a Cisco-assigned extended ID, then the **show interface** and **show interface brief** commands display the ID instead of the transmitter type. The **show interface transceiver** command and the **show interface fc***slot/port* **transceiver** command display both values for Cisco supported SFPs. Table 6-5 defines the acronyms used in the command output. (See the "Displaying Interface Information" section on page 6-12.)

Table 6-5 SFP Transmitter Acronym Definitions

Definition	Acronym
Standard transmitters defined in the GBIC specifications	
short wave laser	swl
long wave laser	lwl
long wave laser cost reduced	lwcr
electrical	elec
Extended transmitters assigned to Cisco-supported SFPs	
CWDM-1470	c1470
CWDM-1490	c1490
CWDM-1510	c1510
CWDM-1530	c1530
CWDM-1550	c1550
CWDM-1570	c1570

Table 6-5 SFP Transmitter Acronym Definitions (continued)

Definition	Acronym
Standard transmitters defined in the GBIC specifications	
CWDM-1590	c1590
CWDM-1610	c1610

Management Interface Configuration

You can remotely configure the switch through the management interface (mgmt0). To configure a connection remotely, you must configure the IP parameters (IP address, subnet mask, and default gateway) from the CLI so that the switch is reachable.

Note Before you begin to configure the management interface manually, obtain the switch's IP address and IP subnet mask.

To configure the mgmt0 Ethernet interface, perform this task:

	Command	Purpose
Step 1	`switch# config terminal` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# interface mgmt0` `switch(config-if)#`	Configures the management Ethernet interface on the switch to configure the management interface.
Step 3	`switch(config-if)# ip address 172.16.1.2 255 255.255.0`	Enters the IP address and IP subnet mask for the interface specified in Step 2.
Step 4	`switch(config-if)# no shutdown`	Enables the interface.
Step 5	`switch(config-if)# exit` `switch(config)#`	Returns to configuration mode.
Step 6	`switch(config)# ip default-gateway 10.1.1.4 switch(config)#`	Configures the default gateway IP address.
Step 7	`switch(config)# exit` `switch#`	Returns to EXEC mode.
Step 8	`switch# copy running-config startup-config`	(Optional) Saves your configuration changes to the file system. **Note** If you wish to save your configuration, you can enter this command at any time.

The management port (mgmt0) is autosensing and operates in full duplex mode at a speed of 10/100 Mbps. The speed and mode cannot be configured.

Note You need to explicitly configure a default gateway to connect to the switch and send IP packets or add a route for each subnet.

Displaying Interface Information

The **show interface** command is invoked from the EXEC mode and displays the interface configurations. Without any arguments, this command displays the information for all the configured interfaces in the switch. (See Examples 6-1 to 6-8.)

Example 6-1 Displays All Interfaces

```
switch# show interface
fc1/1 is Down (Administratively down)
    Hardware is Fibre Channel, SFP is long wave laser
    Port WWN is 20:00:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits

fc1/2 is Down (Administratively down)
    Hardware is Fibre Channel, SFP is short wave laser without OFC
    Port WWN is 20:01:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits

fc1/3 is Down (Administratively down)
    Port WWN is 20:02:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits

fc1/4 is Down (Administratively down)
    Port WWN is 20:03:00:0d:ec:19:cb:0e
```

```
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits

fc1/5 is Down (Administratively down)
    Port WWN is 20:04:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits

fc1/6 is Down (Administratively down)
    Port WWN is 20:05:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits

fc1/7 is Down (Administratively down)
    Port WWN is 20:06:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits

fc1/8 is Down (Administratively down)
    Port WWN is 20:07:00:0d:ec:19:cb:0e
```

```
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits

fc1/9 is Down (Administratively down)
    Hardware is Fibre Channel, SFP is short wave laser without OFC
    Port WWN is 20:08:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits

fc1/10 is Down (Administratively down)
    Port WWN is 20:09:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits

fc1/11 is Down (Administratively down)
    Port WWN is 20:0a:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits

fc1/12 is Down (Administratively down)
```

```
    Port WWN is 20:0b:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits

fc1/13 is Down (Administratively down)
    Hardware is Fibre Channel, SFP is unknown
    Port WWN is 20:0c:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits

fc1/14 is Down (Administratively down)
    Port WWN is 20:0d:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits

fc1/15 is Down (Administratively down)
    Port WWN is 20:0e:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
```

```
fc1/16 is Down (Administratively down)
    Hardware is Fibre Channel, SFP is short wave laser without OFC
    Port WWN is 20:0f:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits

fc1/17 is Down (Administratively down)
    Port WWN is 20:10:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits

fc1/18 is Down (Administratively down)
    Port WWN is 20:11:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits

fc1/19 is Down (Administratively down)
    Port WWN is 20:12:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
```

```
fc1/20 is Down (Administratively down)
    Hardware is Fibre Channel, SFP is electrical
    Port WWN is 20:13:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits

mgmt0 is up
    Hardware is FastEthernet
    Internet address is 10.20.83.122/24
```

You can specify a range of interfaces by entering the following example format:

```
interface fc1/1-3
```

Example 6-2 Displays Multiple, Specified Interfaces

```
switch# show interface fc1/1-3
fc1/1 is Up (Link failure or not connected)
    Hardware is Fibre Channel, SFP is long wave laser
    Port WWN is 20:00:00:0d:ec:19:cb:0e
    Admin port mode is auto
    Port mode is Unknown, FCID is 0x690000
    Speed is Auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      7 output OLS, 0 LRR, 3 loop inits

fc1/2 is Up (Link failure or not connected)
    Hardware is Fibre Channel, SFP is short wave laser without OFC
    Port WWN is 20:01:00:0d:ec:19:cb:0e
    Admin port mode is auto
    Port mode is Unknown, FCID is 0x690100
    Speed is Auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
```

```
      0 errors
    0 input OLS, 0 LRR, 0 loop inits
    6 output OLS, 0 LRR, 2 loop inits

fc1/3 is Up (SFP not present)
    Port WWN is 20:02:00:0d:ec:19:cb:0e
    Admin port mode is auto
    Port mode is Unknown, FCID is 0x690200
    Speed is Auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      6 output OLS, 0 LRR, 2 loop inits
```

Example 6-3 Displays a Specific Interface

```
switch# show interface fc1/2
fc1/2 is Down (Administratively down)
    Hardware is Fibre Channel, SFP is short wave laser without OFC
    Port WWN is 20:01:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
```

Example 6-4 Displays Port Description

```
switch# show interface description
-------------------------------------------------
Interface Description
-------------------------------------------------
fc1/1     fc1/1
fc1/2     fc1/2
fc1/3     fc1/3
fc1/4     fc1/4
fc1/5     fc1/5
fc1/6     fc1/6
fc1/7     fc1/7
fc1/8     fc1/8
fc1/9     fc1/9
fc1/10    fc1/10
fc1/11    fc1/11
fc1/12    fc1/12
```

```
fc1/13    fc1/13
fc1/14    fc1/14
fc1/15    fc1/15
fc1/16    fc1/16
fc1/17    fc1/17
fc1/18    fc1/18
fc1/19    fc1/19
fc1/20    fc1/20
```

Example 6-5 Displays Interface Information in a Brief Format

```
switch# show interface brief
--------------------------------------------------------------------
Interface  Admin       Status            FCOT  Oper     Oper
           Mode                                Mode     Speed
                                                        (Gbps)
--------------------------------------------------------------------
fc1/1      auto        down              lwl    --
fc1/2      auto        down              swl    --
fc1/3      auto        down              --     --
fc1/4      auto        down              --     --
fc1/5      auto        down              --     --
fc1/6      auto        down              --     --
fc1/7      auto        down              --     --
fc1/8      auto        down              --     --
fc1/9      auto        down              swl    --
fc1/10     auto        down              --     --
fc1/11     auto        down              --     --
fc1/12     auto        down              --     --
fc1/13     auto        down              unk    --
fc1/14     auto        down              --     --
fc1/15     auto        down              --     --
fc1/16     auto        down              swl    --
fc1/17     auto        down              --     --
fc1/18     auto        down              --     --
fc1/19     auto        down              --     --
fc1/20     auto        down              elec   --

-------------------------------------------
Interface               Status     IP Address
-------------------------------------------
mgmt0                   up         10.20.83.122
```

Example 6-6 Displays Interface Counters

```
switch# show interface counters

fc1/1
    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
      0 frames input, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 discards, 0 errors, 0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
      0 link failures, 0 sync losses
```

```
fc1/2
    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
      0 frames input, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 discards, 0 errors, 0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
      0 link failures, 0 sync losses

fc1/3
    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 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 discards, 0 errors, 0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
      0 link failures, 0 sync losses

fc1/4
    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
      0 frames input, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 discards, 0 errors, 0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
      0 link failures, 0 sync losses

fc1/5
    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
      0 frames input, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 discards, 0 errors, 0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
      0 link failures, 0 sync losses
```

```
fc1/6
    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
      0 frames input, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 discards, 0 errors, 0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
      0 link failures, 0 sync losses

fc1/7
    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
      0 frames input, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 discards, 0 errors, 0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
      0 link failures, 0 sync losses

fc1/8
    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
      0 frames input, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 discards, 0 errors, 0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
      0 link failures, 0 sync losses

fc1/9
    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 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 discards, 0 errors, 0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
      0 link failures, 0 sync losses
```

```
fc1/10
    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 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 discards, 0 errors, 0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
      0 link failures, 0 sync losses

fc1/11
    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 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 discards, 0 errors, 0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
      0 link failures, 0 sync losses

fc1/12
    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 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 discards, 0 errors, 0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
      0 link failures, 0 sync losses

fc1/13
    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 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 discards, 0 errors, 0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
      0 link failures, 0 sync losses
```

```
fc1/14
    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 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 discards, 0 errors, 0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
      0 link failures, 0 sync losses

fc1/15
    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 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 discards, 0 errors, 0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
      0 link failures, 0 sync losses

fc1/16
    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 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 discards, 0 errors, 0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
      0 link failures, 0 sync losses

fc1/17
    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 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 discards, 0 errors, 0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
      0 link failures, 0 sync losses
```

```
fc1/18
    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 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 discards, 0 errors, 0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
      0 link failures, 0 sync losses

fc1/19
    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 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 discards, 0 errors, 0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
      0 link failures, 0 sync losses

fc1/20
    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 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 discards, 0 errors, 0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 class-2 frames, 0 bytes
        0 class-3 frames, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
      0 link failures, 0 sync losses
```

Example 6-7 Displays Interface Counters in Brief Format

```
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
-------------------------------------------------------------------------------
fc1/1            0                0                       0                0
fc1/2            1.12E-04         2844                    1.12E-04         2840
fc1/3            0                0                       0                0
fc1/4            0                0                       0                0
fc1/5            0                0                       0                0
```

```
fc1/6           0                   0                   0                   0
fc1/7           0                   0                   0                   0
fc1/8           0                   0                   0                   0
fc1/9           0                   0                   0                   0
fc1/10          0                   0                   0                   0
fc1/11          0                   0                   0                   0
fc1/12          0                   0                   0                   0
fc1/13          0                   0                   0                   0
fc1/14          0                   0                   0                   0
fc1/15          0                   0                   0                   0
fc1/16          0                   0                   0                   0
fc1/17          0                   0                   0                   0
fc1/18          0                   0                   0                   0
fc1/19          0                   0                   0                   0
fc1/20          0                   0                   0                   0
```

Note The **show interface transceiver** command will display information only if a transceiver is present. (See Example 6-8.)

Example 6-8 Displays Transceiver Information

```
switch# show interface transceiver
fc1/1 sfp is present but not supported
    name is FINISAR CORP.
    part number is FTRJ-8519-3-2.5
    revision is X1
    serial number is E113LSF
    vendor specific data (bytes 96-127)
      0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF
      0xFF 0xFF 0xFF 0xFF 0xFF 0x00 0x00 0x00
      0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0x00
      0x00 0x00 0xFF 0xFF 0xFF 0xFF 0xA7 0xCE

fc1/2 sfp is present but not supported
    name is FINISAR CORP.
    part number is FTRJ-8519-3-2.5
    revision is X1
    serial number is H112UZ3
    vendor specific data (bytes 96-127)
      0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF
      0xFF 0xFF 0xFF 0xFF 0xFF 0x00 0x00 0x00
      0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0x00
      0x00 0x00 0xFF 0xFF 0xFF 0xFF 0xA7 0xCE

fc1/3 sfp is not present
fc1/4 sfp is not present
fc1/5 sfp is not present
fc1/6 sfp is not present
fc1/7 sfp is not present
fc1/8 sfp is not present
fc1/9 sfp is present but not supported
    name is FINISAR CORP.
    part number is FTRJ8524P2BNL
    revision is A
    serial number is P6G2333
    vendor specific data (bytes 96-127)
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
```

```
fc1/10 sfp is not present
fc1/11 sfp is not present
fc1/12 sfp is not present
fc1/13 sfp is present but not supported
    name is
    part number is
    revision is
    serial number is
    vendor specific data (bytes 96-127)
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

fc1/14 sfp is not present
fc1/15 sfp is not present
fc1/16 sfp is present but not supported
    name is FINISAR CORP.
    part number is FTRJ-8519-3-2.5
    revision is X1
    serial number is E113GL5
    vendor specific data (bytes 96-127)
      0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF
      0xFF 0xFF 0xFF 0xFF 0xFF 0x00 0x00 0x00
      0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0x00
      0x00 0x00 0xFF 0xFF 0xFF 0xFF 0xA7 0xCE

fc1/17 sfp is not present
fc1/18 sfp is not present
fc1/19 sfp is not present
fc1/20 sfp is present but not supported
    name is Molex Inc.
    part number is 74720-0502
    revision is D
    serial number is 33281334
    vendor specific data (bytes 96-127)
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
```

Example 6-9 displays the running configuration for a specified interface.

Example 6-9 Displays the Running Configuration

```
switch# show running-config
ip default-gateway 10.20.83.1
logging level fcdomain 2
logging level fspf 2
logging level fcns 2
logging level fcs 2
logging level port 2
logging level zone 2
logging level auth 2
logging level ipconf 2
logging level module 2
logging level ntp 2
logging level sysmgr 2
no snmp-server contact
no snmp-server location
zone name asdfa
zoneset name dave
```

```
interface mgmt0
  ip address 10.20.83.122 255.255.255.0
interface fc1/1
interface fc1/2
interface fc1/3
interface fc1/4
interface fc1/5
interface fc1/6
interface fc1/7
interface fc1/8
interface fc1/9
interface fc1/10
interface fc1/11
interface fc1/12
interface fc1/13
interface fc1/14
interface fc1/15
interface fc1/16
interface fc1/17
interface fc1/18
interface fc1/19
interface fc1/20
```

Default Settings

Table 6-6 lists the default settings for Fibre Channel interface parameters.

Table 6-6 Default Interface Parameters

Parameters	Default
Interface mode	Auto
Interface speed	Auto
Administrative state	Shutdown (unless changed during initial setup)
Beacon mode	Off (disabled)
Data field size	2112 bytes

CHAPTER 7

Configuring and Managing Zones

Zoning enables you to set up access control between storage devices or user groups. If you have administrator privileges in your fabric, you can create zones to increase network security and to prevent data loss or corruption. Zoning is enforced by examining the source-destination ID field.

This chapter includes the following sections:

Zoning Features

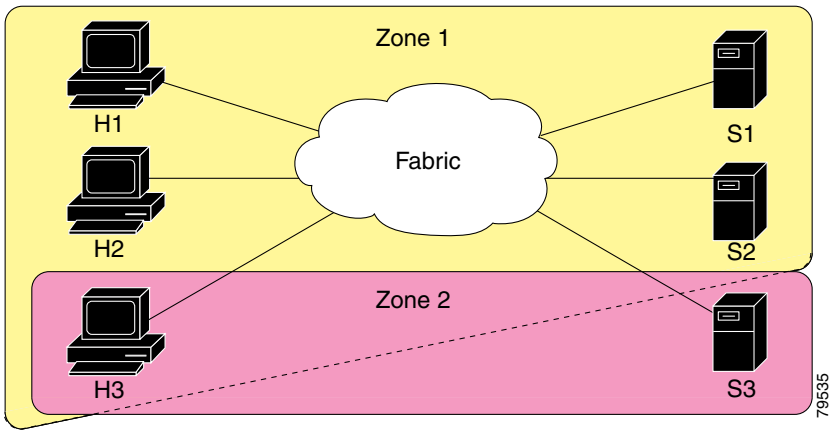
Zoning has the following features:

- A zone consists of multiple zone members.
  - Members in a zone can access each other; members in different zones cannot access each other.
  - If zoning is not activated, all devices are members of the default zone.
  - If zoning is activated, any device that is not in an active zone (a zone that is part of an active zone set) is a member of the default zone.
  - Zones can vary in size.
  - Devices can belong to more than one zone.
- A zone set consists of one or more zones.
  - A zone set can be activated or deactivated as a single entity across all switches in the fabric.
  - Only one zone set can be activated at any time.
  - A zone can be a member of more than one zone set.
- Zoning can be administered from any switch in the fabric.
  - When you activate a zone set (from any switch), all switches in the fabric receive the active zone set. Additionally, full zone sets are distributed to all switches in the fabric if this feature is enabled in the source switch.
  - If a new switch is added to an existing fabric, zone sets are acquired by the new switch.
- Zone changes can be configured nondisruptively. New zones and zone sets can be activated without interrupting traffic on unaffected ports or devices.
- Zone membership criteria is based on Port world wide name (pWWN). The pWWN of an N port is attached to the switch as a member of the zone.
- Default zone membership includes all ports or WWNs that do not have a specific membership association. Access between default zone members is controlled by the default zone policy.

Zoning Example

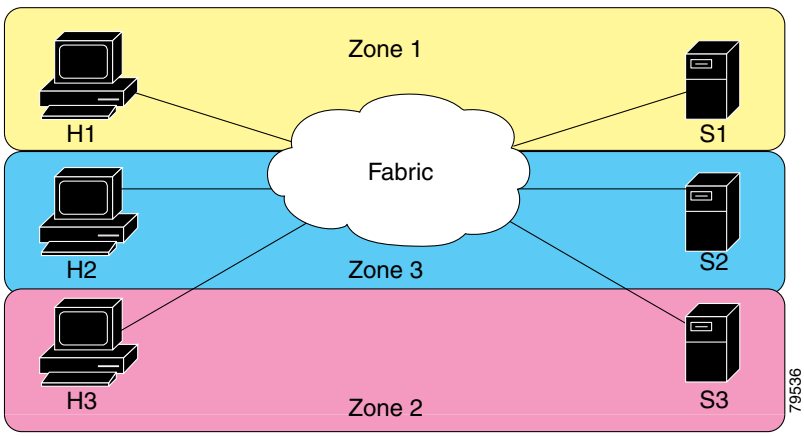
Figure 7-1 illustrates a zone set with two zones, zone 1 and zone 2, in a fabric. Zone 1 provides access from all three hosts (H1, H2, H3) to the data residing on storage systems S1 and S2. Zone 2 restricts the data on S3 to access only by H3. Note that H3 resides in both zones.

Figure 7-1 Fabric with Two Zones



Of course, there are other ways to partition this fabric into zones. Figure 7-2 illustrates another possibility. Assume that there is a need to isolate storage system S2 for the purpose of testing new software. To achieve this, zone 3 is configured, which contains only host H2 and storage S2. You can restrict access to just H2 and S2 in zone 3, and to H1 and S1 in zone 1.

Figure 7-2 Fabric with Three Zones



Zone Implementation

The Cisco MDS 9020 Fabric Switch automatically supports the following basic zone features (no additional configuration is required):

- Name server queries are soft-zoned.
- Only active zone sets are distributed.
- Unzoned devices cannot access each other.
- Active zone sets cannot be changed without activating a full zone database.
- Active zone sets are preserved across switch reboots.
- Changes to the full database must be explicitly saved.
- Zone reactivation (a zone set is active and you activate another zone set) does not disrupt existing traffic.

If required, you can additionally configure the following zone features:

- Propagate full zone sets to all switches.
- Change the default policy for unzoned members.
- Bring E ports out of isolation.

Zone Configuration

A zone can be configured using one of the following types to assign members:

- pWWN—The WWN of the N or NL port in hex format (for example, 10:00:00:23:45:67:89:ab).
- FC alias—The alias name is in alphabetic characters (for example, Payroll) and denotes a WWN. The alias can also include multiple WWN members.

Configuring a Zone

To configure a zone and assign a zone name, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zone name Zone1` `switch(config-zone)#`	Creates a zone called Zone 1.

Step 3	`switch(config-zone)# member <type> <value>`
	`pWWN example:`
	`sswitch(config-zone)# member pwwn 10:00:00:23:45:67:89:ab`
	`FC alias example:`
	`switch(config-zone)# member fcalias Payroll`
		Configures a member for the specified zone (Zone1) based on the type (pWWN or FC alias) and value specified.

Tip Use a relevant display command (for example, **show interface** or **show flogi database**) to obtain the required value in hex format.

Alias Configuration

You can assign an alias name and configure an alias member using pWWN values.

Tip The Cisco MDS 9020 Fabric Switch supports a maximum of 2500 aliases.

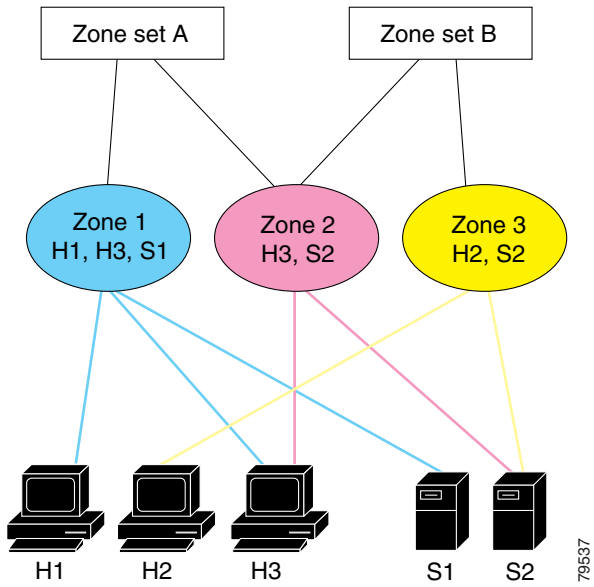
To create an alias using the **fcalias** command, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# fcalias name AliasSample` `switch-config-fcalias#`	Configures an alias name (AliasSample).
Step 3	`switch-config-fcalias# member pwwn 10:00:00:23:45:67:89:ab`	Configures alias members based on the specified port WWN type and value (pWWN 10:00:00:23:45:67:89:ab).

Zone Set Creation

In Figure 7-3, two separate sets are created, each with its own membership hierarchy and zone members.

Figure 7-3 Hierarchy of Zone Sets, Zones, and Zone Members



Zones provide a mechanism for specifying access control, while zone sets are a grouping of zones to enforce access control in the fabric. Either zone set A or zone set B can be activated (but not together).

To create a zone set to include several zones, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zoneset name Zoneset1` `switch-config-zoneset#`	Configures a zone set called Zoneset1. **Tip** A zone set must have member zones before you can activate the zone set.
Step 3	`switch-config-zoneset# member Zone1`	Adds Zone1 as a member of the specified zone set (Zoneset1). **Tip** If the specified zone name was not previously configured, this command will return the `Zone not present` error message.
Step 4	`switch-config-zoneset# zone name InlineZone1` `switch-config-zoneset-zone#`	Adds a zone (InlineZone1) to the specified zone set (Zoneset1). **Tip** Execute this step only if you need to create a zone from a zone set prompt.

Active and Full Zone Set Considerations

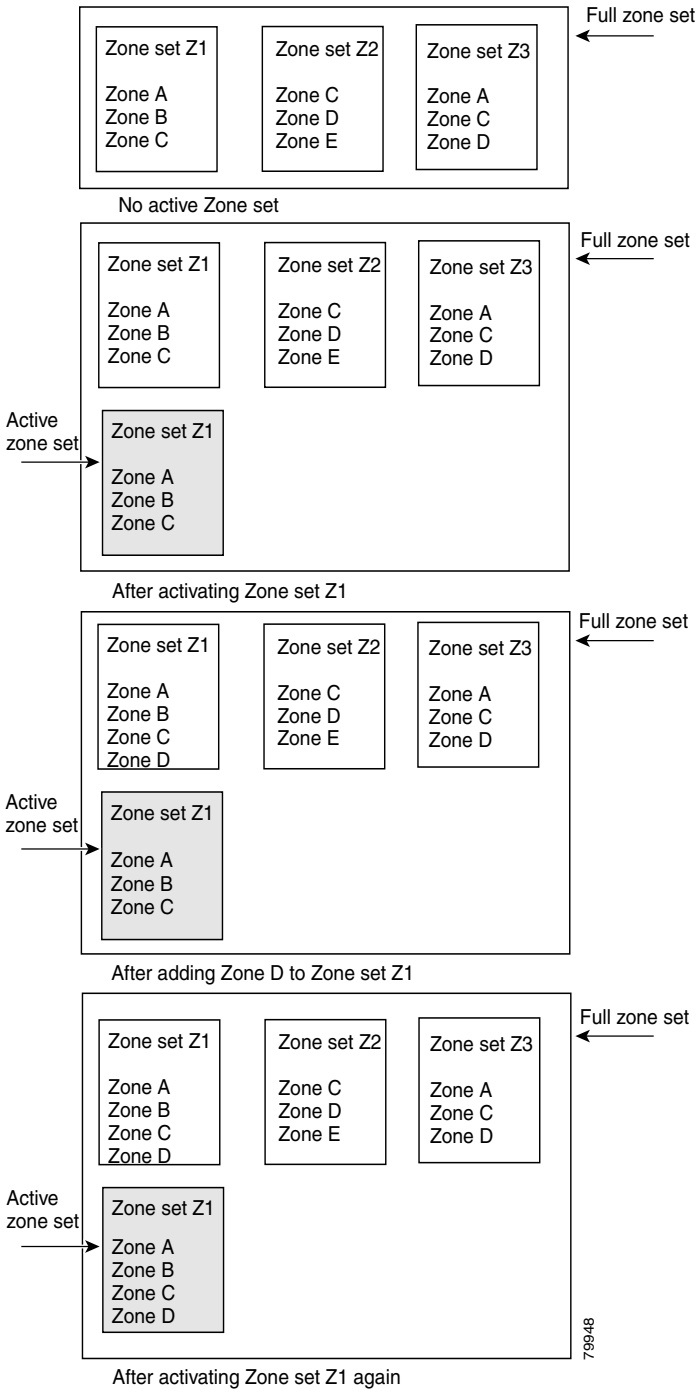
Before configuring a zone set, consider the following guidelines:

- When you create a zone set, that zone set becomes a part of the full zone set.
- When you activate a zone set, a copy of the zone set from the full zone set is used to enforce zoning and is called the active zone set. An active zone set cannot be modified. A zone that is part of an active zone set is called an active zone.
- The administrator can modify the full zone set even if a zone set with the same name is active. However, the modification will be enforced only upon reactivation.
- When the activation is done, the active zone set is automatically stored in persistent configuration. This enables the switch to preserve the active zone set information across switch resets.
- All other switches in the fabric receive the active zone set so they can enforce zoning in their respective switches.
- Soft zoning is implemented using the active zone set. Modifications take effect during zone set activation.

Note You must explicitly deactivate the currently active zone set before activating a new zone set.

Figure 7-4 shows a zone being added to an activated zone set.

Figure 7-4 Active and Full Zone Sets



Activating a Zone Set

You can activate a zone set using the **zoneset activate name** command. The changes to a full zone set do not take effect until the zone set is activated with the **zoneset activate name** command.

Tip You do not have to enter the **copy running-config startup-config** command to store the active zone set. However, you need to enter the **copy running-config startup-config** command to explicitly store full zone sets. It is not available across switch resets.

To activate a zone set, perform this task:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# zoneset activate name Zoneset1`	Activates the specified zone set.
	`switch(config)# no zoneset activate name Zoneset1`	Deactivates the specified zone set.

Zone Enforcement

Zoning is enforced in the form of soft zones. Each end device (N port or NL port) discovers other devices in the fabric by querying the name server. When a device logs in to the name server, the name server returns the list of other devices that can be accessed by the querying device. If an Nx port does not know about the FC IDs of other devices outside of its zone, it cannot access those devices. Zoning restrictions are applied only during interaction between the name server and the end device. If an end device somehow knows the FC ID of a device outside its zone, it can access that device.

The Default Zone

Each member of a fabric (in effect a device attached to an Nx port) can belong to any zone. If a member is not part of any active zone, it is considered to be part of the default zone. Therefore, if no zone set is active in the fabric, all devices are considered to be in the default zone. Even though a member can belong to multiple zones, a member that is part of the default zone cannot be part of any other zone. The switch determines whether or not a port is a member of the default zone when the attached port comes up.

Note Unlike configured zones, default zone information is not distributed to the other switches in the fabric.

Traffic can either be permitted or denied among members of the default zone. This information is not distributed to all switches; it must be configured in each switch.

Note When the switch is initialized for the first time, no zones are configured and all members are considered to be part of the default zone. Members are not permitted to talk to each other.

Configure the default zone policy on each switch in the fabric. If you change the default zone policy on one switch in a fabric, be sure to change it on all the other switches in the fabric.

Note The default settings for default zone configurations can be changed.

To permit or deny traffic in the default zone, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zone default-zone permit`	Permits traffic flow to default zone members.
	`switch(config)# no zone default-zone permit`	Denies traffic flow to default zone members and reverts to factory default.

Full Zone Set Propagation

The Cisco MDS 9020 Fabric Switch distributes active zone sets when new E port links come up or when a new zone set is activated. The zone set distribution takes effect while sending merge requests to the adjacent switch or while activating a zone set.

The **zoneset distribute full** command in configuration mode distributes the full zone set along with the active zone set.

To propagate full zone sets to all switches, perform this task:

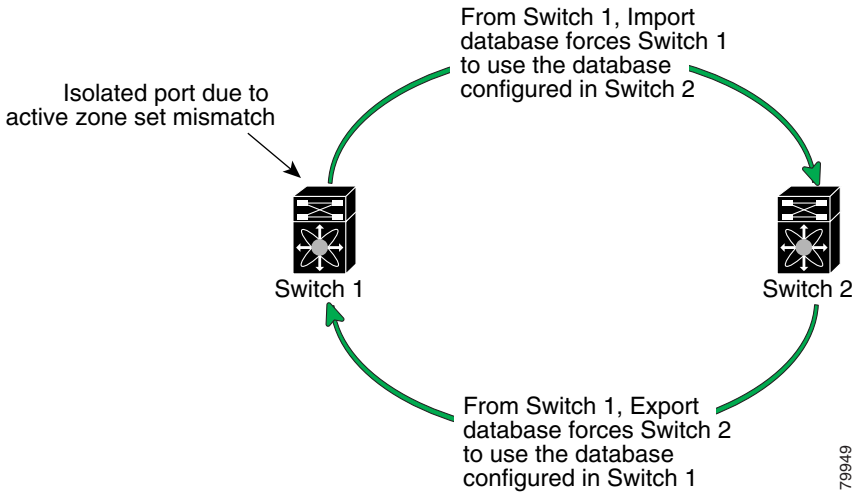
	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zoneset distribute full`	Enables sending a full zone set along with an active zone set.

Recovering from Link Isolation

When two switches in a fabric are merged using an E port, the E ports may become isolated when the active zone sets are different between the two switches or fabrics. When an E port becomes isolated, you can recover that port from its isolated state using one of three options:

- Import the neighboring switch's active zone set database, and replace the current active zone set.. (See Figure 7-5.)
- Export the current database to the neighboring switch. (See Figure 7-5.)
- Manually resolve the conflict by editing the full zone set, activating the corrected zone set, and then bringing up the link.

Figure 7-5 Importing and Exporting the Database



Zone Database Information

If required, you can clear configured information stored in the zone server database.

Note Clearing a zone set only erases the full zone database, not the active zone database.

Clearing the Zone Server Database

To clear the zone server database, use the **clear zone database** command:

```
switch# clear zone database
```

This command clears all configured information in the zone server.

Note After entering a **clear zone database** command, you need to explicitly enter the **copy running-config startup-config** to ensure that the running configuration is used when you next start the switch.

Renaming Zone Sets, Zones and, fcaliases

To rename a zone set, zone, or fcalias, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zoneset rename oldname newname`	Renames a zone set in the specified.
	`switch(config)# zone rename oldname newname`	Renames a zone in the specified.
	`switch(config)# fcalias rename oldname newname`	Renames a fcalias in the specified.

Displaying Zone Information

You can view any zone information by using the **show** command. If you request information for a specific object (for example, a specific zone, zone set, fcalias, or even a keyword like **brief** or **active**), only information for the specified object is displayed. If you do not request specific information, all available information is displayed. (See Examples 7-1 to 7-8.)

Example 7-1 Displays Zone Information

```
switch# show zone
zone name Z1
        pwwn 10:00:00:c0:dd:07:00:f8
        fcalias name A1
                  pwwn 10:00:00:c0:dd:07:00:f9
```

Use the **show zoneset** command to view the configured zone sets.

Example 7-2 Displays Configured Zone Set Information

```
switch# show zoneset
zoneset name ZS1
         zone name Z1
               pwwn 10:00:00:c0:dd:07:00:f8
               fcalias name A1
                         pwwn 10:00:00:c0:dd:07:00:f9
```

Use the **show zone name** command to display members of a specific zone.

Example 7-3 Displays Members of a Zone

```
switch# show zone name Zone1
```

```
zone name Z1
      pwwn 10:00:00:c0:dd:07:00:f8
      fcalias name A1
               pwwn 10:00:00:c0:dd:07:00:f9
```

Use the **show fcalias** command to display fcalias configuration.

Example 7-4 Displays fcalias Configuration

```
switch# show fcalias
fcalias name Alias2

fcalias name Alias1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:9c:48:e5
```

Use the **show zone member** command to display all zones to which a member belongs using the pWWN.

Example 7-5 Displays Membership Status

```
switch# show zone member pwwn 10:00:00:c0:dd:07:00:f9
fcalias name A1
          pwwn 10:00:00:c0:dd:07:00:f9
```

Example 7-6 Displays Active Zones

```
switch# show zone active
zone name zone1
  pwwn 10:11:22:33:44:55:66:77
  pwwn 10:11:22:33:44:55:66:88
  pwwn 10:11:22:33:44:55:66:99

zone name zone2
  pwwn 20:11:22:33:44:55:66:00
  pwwn 20:11:22:33:44:55:66:01
  pwwn 20:11:22:33:44:55:66:02
  pwwn 20:11:22:33:44:55:66:03
```

Example 7-7 Displays Active Zone Sets

```
switch# show zoneset active
zoneset name circus
  zone name bozo
    pwwn 10:11:22:33:44:55:66:77
    pwwn 10:11:22:33:44:55:66:88
    pwwn 10:11:22:33:44:55:66:99

  zone name clown
    pwwn 20:11:22:33:44:55:66:00
    pwwn 20:11:22:33:44:55:66:01
    pwwn 20:11:22:33:44:55:66:02
    pwwn 20:11:22:33:44:55:66:03
```

Example 7-8 Displays Zone Status

```
switch# show zone status
Full Zoning Database :
        Zonesets: 1 Zones: 1 Aliases: 1
        Active Zoning Database:
                Name: ZS1 Zonesets: 1 Zones: 1
                Status:
```

Merging the Database

The merge behavior is governed by the merge rules specified in Table 7-1.

Table 7-1 Database Zone Merge Status

Local Database	Adjacent Database	Merge Status	Results of the Merge
The databases contain zone sets with the same name but different zones, aliases, and attributes groups.		Successful.	The union of the local and adjacent databases.
The databases contains a zone, zone alias, or zone attribute group object with same name but different members.		Failed.	ISLs are isolated.
Empty.	Contains data.	Successful.	The adjacent database information populates the local database.
Contains data.	Empty.	Successful.	The local database information populates the adjacent database.

Default Zone Policies

To permit or deny traffic in the default zone, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zone default-zone permit`	Permits traffic flow to default zone members.
	`switch(config)# no zone default-zone permit`	Denies traffic flow to default zone members and reverts to factory default.

Default Settings

Table 7-2 lists the default settings for basic zone parameters.

Table 7-2 Default Basic Zone Parameters

Parameters	Default
Default zone policy	Denied to all members.
Full zone set distribute	The full zone set(s) is not distributed.

CHAPTER 8

Managing FLOGI and FDMI

This chapter describes the fabric login database and the Fabric-Device Management Interface information provided in the Cisco MDS 9020 Fabric Switch. It includes the following sections:

Displaying FLOGI Details

In a Fibre Channel fabric, each host or disk requires an FC ID. Use the **show flogi** command to verify if a storage device is displayed in the fabric login (FLOGI) table, as in the following examples. 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. (See Examples 8-1.)

Example 8-1 Displays Details on the FLOGI Database

```
switch# show flogi database
--------------------------------------------------------------------------------
INTERFACE FCID PORT NAME NODE NAME
--------------------------------------------------------------------------------
fc1/2 0x6101e1 21:00:00:04:cf:03:36:2f 20:00:00:04:cf:03:36:2f
fc1/2 0x6101e2 21:00:00:04:cf:03:38:6e 20:00:00:04:cf:03:38:6e
fc1/2 0x6101e4 21:00:00:04:cf:03:38:24 20:00:00:04:cf:03:38:24
fc1/2 0x6101e8 21:00:00:04:cf:03:38:4b 20:00:00:04:cf:03:38:4b
Total number of flogi = 4
```

Displaying Name Server Database Entries

The name server stores name entries for all hosts in the Fibre Channel Network Switch (FCNS) database. The name server permits an Nx port to register attributes during a port login (PLOGI) (to the name server) to obtain attributes of other hosts. These attributes are deregistered when the Nx port logs out either explicitly or implicitly.

In a multiswitch fabric configuration, the name server instances running on each switch share information in a distributed database. One instance of the name server process runs on each switch.

Use the **show fcns** command to display the name server database and statistical information. (See Examples 8-2 and 8-3.)

Example 8-2 Displays the Name Server Database

```
switch# show fcns database
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x010000    N     50:06:0b:00:00:10:a7:80                 scsi-fcp fc-gs
0x010001    N     10:00:00:05:30:00:24:63 (Cisco)         ipfc
0x010002    N     50:06:04:82:c3:a0:98:52 (Company 1)     scsi-fcp 250
0x010100    N     21:00:00:e0:8b:02:99:36 (Company A)     scsi-fcp
0x020000    N     21:00:00:e0:8b:08:4b:20 (Company A)
0x020100    N     10:00:00:05:30:00:24:23 (Cisco)         ipfc
0x020200    N     21:01:00:e0:8b:22:99:36 (Company A)     scsi-fcp
```

Example 8-3 Displays the Name Server Database Details

```
switch# show fcns database detail
-------------
FCID:0x0101e1
-------------
port-wwn (vendor) :      21:00:00:20:37:d9:4f:66 ()
node-wwn :               20:00:00:20:37:d9:4f:66
class :                  3
node-ip-addr :           0.0.0.0
fc4-types:fc4_features : FCP
symbolic-port-name :     (NULL)
symbolic-node-name       (NULL)
port-type :              NL
port-ip-addr :           0.0.0.0
fabric-port-wwn :        20:01:00:c0:dd:06:fc:00
-------------
FCID:0x0101e2
-------------
port-wwn (vendor) :      21:00:00:20:37:d9:4d:61 ()
node-wwn :               20:00:00:20:37:d9:4d:61
class :                  3
node-ip-addr :           0.0.0.0
fc4-types:fc4_features : FCP
symbolic-port-name :     (NULL)
symbolic-node-name :     (NULL)
port-type :              NL
port-ip-addr :           0.0.0.0
fabric-port-wwn :        20:01:00:c0:dd:06:fc:00
-------------
FCID:0x0101e4
-------------
port-wwn (vendor) :      21:00:00:20:37:d9:4a:fa ()
node-wwn :               20:00:00:20:37:d9:4a:fa
```

```
class :                   3
node-ip-addr :            0.0.0.0
fc4-types:fc4_features : FCP
symbolic-port-name :      (NULL)
symbolic-node-name :      (NULL)
port-type :               NL
port-ip-addr :            0.0.0.0
fabric-port-wwn :         20:01:00:c0:dd:06:fc:00
-------------
FCID:0x0101e8
-------------
port-wwn (vendor) :       21:00:00:20:37:d9:4c:02 ()
node-wwn :                20:00:00:20:37:d9:4c:02
class :                   3
node-ip-addr :            0.0.0.0
fc4-types:fc4_features : FCP
symbolic-port-name :      (NULL)
symbolic-node-name :      (NULL)
port-type :               NL
port-ip-addr :            0.0.0.0
fabric-port-wwn :         20:01:00:c0:dd:06:fc:00
```

Displaying FDMI

Cisco MDS 9000 FabricWare provides support for the Fabric-Device Management Interface (FDMI) functionally, as described in the FC-GS-4 standard. FDMI enables management of devices such as Fibre Channel Host Bus Adapters (HBAs) through in-band communications. This addition complements the existing Fibre Channel name server and management server functions.

Using the FDMI functionality, the Cisco MDS 9000 FabricWare software can extract the following management information about attached HBAs and host operating systems without installing proprietary host agents:

- Manufacturer, model, and serial number
- Node name and node symbolic name
- Hardware, driver, and firmware versions
- Host operating system (OS) name and version number

All FDMI entries are stored in persistent storage and are retrieved when the FDMI process is started.

Use the **show fdmi** command to display the FDMI database information. (See Example 8-4.)

Example 8-4 Displays All HBA Management Servers

```
switch# show fdmi database
Registered HBA List
  10:00:00:00:c9:32:8d:77
  21:01:00:e0:8b:2a:f6:54

switch# show fdmi database detail
Registered HBA List
-------------------------------
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
```

CHAPTER 9

Configuring Switch Security

The authentication, authorization, and accounting (AAA) mechanism verifies the identity of, grants access to, and tracks the actions of users managing a switch. The Cisco MDS 9020 Fabric Switch uses Remote Access Dial-In User Service (RADIUS) protocols to provide solutions using remote AAA servers.

Based on the user ID and password combination provided, switches perform local authentication or authorization using the local database or remote authentication or authorization using AAA server(s). A preshared secret key provides security for communication between the switch and AAA servers. This secret key can be configured for all AAA servers or for only a specific AAA server. This security mechanism provides a central management capability for AAA servers.

This chapter includes the following sections:

Switch Management Security

Management security in the Cisco MDS 9020 Fabric Switch provides security to all management access methods including the command-line interface (CLI) or Simple Network Management Protocol (SNMP).

CLI Security Options

You can access the CLI using the console (serial connection), Telnet, or Secure Shell (SSH). For each management path (console or Telnet and SSH), you can configure one or more of the following security control options: local or remote (RADIUS).

- Remote security control. (See the "Configuring RADIUS" section on page 9-3.)
- Local security control. (See the "Local AAA Services" section on page 9-4.)

SNMP Security Options

The SNMP agent supports security features for SNMP v1 and SNMP v2c. Normal SNMP security mechanisms apply to all applications that use SNMP (for example, Cisco MDS 9000 Family Fabric Manager).

CLI security options also apply to the Cisco MDS Fabric Manager and Device Manager. (See Chapter 10, "Configuring SNMP".)

Refer to the *Cisco MDS 9000 Family Fabric Manager Configuration Guide* for information on the Cisco Fabric or Device Managers.

Switch AAA Functionalities

Using the CLI or an SNMP application, you can configure authentication, authorization, and accounting (AAA) switch functionalities in the Cisco MDS 9020 Fabric Switch.

Authentication

Authentication is the process of verifying the identity of the person managing the switch. This identity verification is based on the user ID and password combination provided by the person trying to manage the switch. The Cisco MDS 9020 Fabric Switch allows you to perform local authentication (using the local lookup database) or remote authentication (using one or more RADIUS servers).

Authorization

Two roles exist in all Cisco MDS switches:

- Network operator (**`network-operator`**)—Has permission to view the configuration only. The operator cannot make any configuration changes.
- Network administrator (**`network-admin`**)— Has permission to execute all commands and make configuration changes.

Accounting

The accounting feature tracks and maintains a log of every management session used to access the switch. This information can be used to generate reports for troubleshooting and auditing purposes. Accounting logs are stored locally.

Configuring RADIUS

The Cisco MDS 9020 Fabric Switch can use the RADIUS protocol to communicate with remote AAA servers. You can configure multiple RADIUS servers and set timeout and retry counts. This section defines the RADIUS operation, identifies its network environments, and describes its configuration possibilities. RADIUS is a distributed client/server protocol that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on the switch and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

You can add up to five RADIUS servers. RADIUS keys are always stored in encrypted form in persistent storage. The running configuration also displays encrypted keys. To specify the host RADIUS server address and the options, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode
Step 2	`switch(config)# radius-server host 10.10.0.0 key abcdefgh01234567`	Specifies the preshared key for the selected RADIUS server. In this example, the host is 10.10.0.0 and the shared secret is abcdefgh01234567. The shared secret must be exactly 16 characters.
Step 3	`switch(config)# radius-server host 10.10.0.0 auth-port 2003`	Specifies the destination UDP port number to which the RADIUS authentication messages should be sent. In this example, the host is 10.10.0.0 and the authentication port is 2003. The default authentication port is 1812, and the valid range is 0 to 65,366.
Step 4	`switch(config)# radius-server host 10.10.0.0 accounting`	Specifies this server to be used only for accounting purposes. **Note** If neither the authentication nor the accounting options are specified, the server is used for both accounting and authentication purposes.
Step 5	`switch(config)# radius-server host 10.10.0.0 timeout 30`	Specifies the time (in seconds) between retransmissions to the RADIUS server. The default timeout is one (1) second. The time ranges from 1 to 60 seconds.
Step 6	`switch(config)# radius-server host 10.10.0.0 retransmit 3`	Configures the number of times (3) the switch tries to connect to the RADIUS server before reverting to local authentication.

Local AAA Services

The system maintains the user name and password locally and stores the password information in encrypted form. You are authenticated based on the locally stored user information.

Use the **username** command to configure local users and their roles. (See the "Creating or Updating Users" section on page 9-6.)

Use the **show accounting log** command to view the local accounting log. (See Example 9-1.)

Example 9-1 Displays the Accounting Log Information

```
switch# show accounting log
[1][Thu Jan 20 21:30:20.599 UTC 2005][AU][0000.00FF][None][Zoning Default Zone changed in
Config default to False]
[2][Thu Jan 20 21:30:35.119 UTC 2005][AU][0000.0001][None][IP Unknown User
snmp@IB-session1 User Login]
[3][Thu Jan 20 21:30:35.122 UTC 2005][AU][0000.0001][None][IP Unknown User
snmp@OB-session2 User Login]
[4][Thu Jan 20 21:30:50.409 UTC 2005][AU][0000.0001][None][IP 10.0.0.254 User
admin@OB-session3 User Login]
[5][Thu Jan 20 21:31:14.514 UTC 2005][AU][0000.0001][None][IP 10.0.0.254 User
maint@OB-session4 User Login]
...
```

Authentication and Authorization Process

Authentication is the process of verifying the identity of the person managing the switch. This identity verification is based on the user ID and password combination provided by the person trying to manage the switch. The Cisco MDS 9020 Fabric Switch allows you to perform local authentication (using the lookup database) or remote authentication (using one or more RADIUS servers).

The following steps explain the authorization and authentication process. Figure 9-1 shows a flow chart of the process.

Step 1 If you can log in to the required Cisco MDS 9020 Fabric Switch, then you can use the Telnet, SSH, Fabric Manager/Device Manager, or console login options.

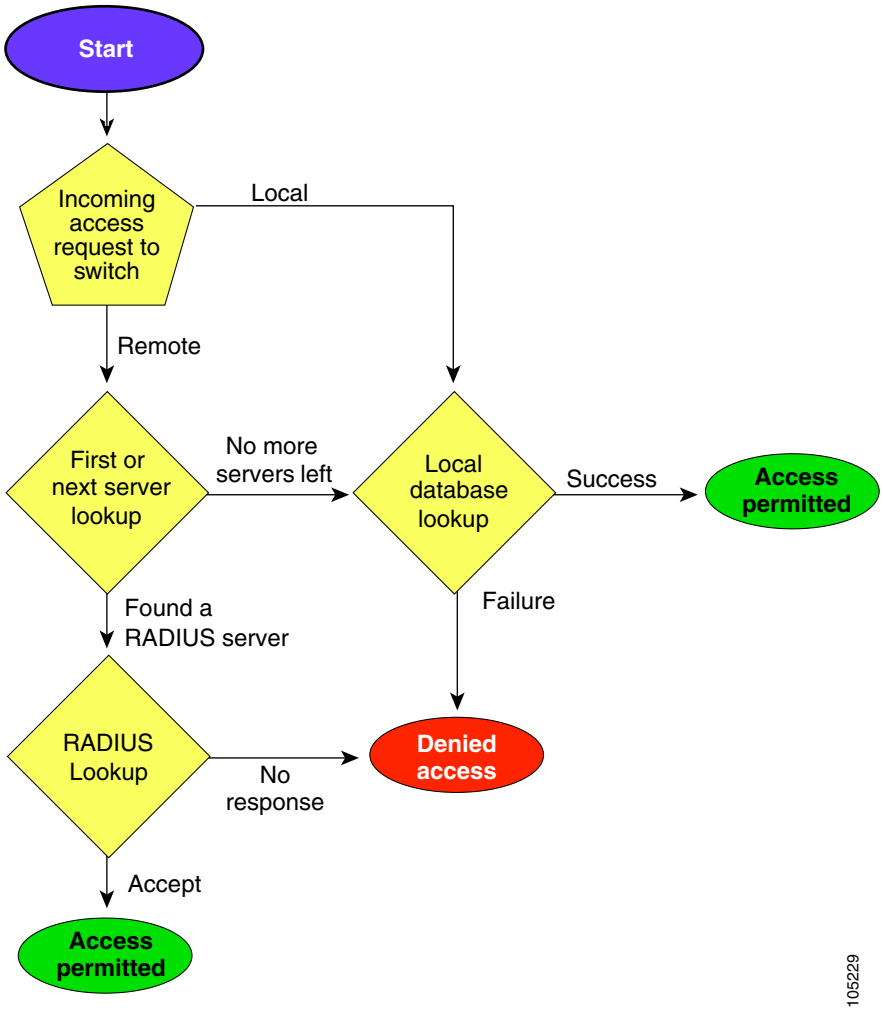
Step 2 An authentication request is sent to the first RADIUS server.

- If a RADIUS server fails to respond, then another RADIUS server is tried and so on until a RADIUS server responds to the authentication request.
- If all RADIUS servers fail to respond, then the local database is used for authentication.

Step 3 If you are successfully authenticated through a RADIUS server, then user roles are downloaded with an authentication response. If user roles are not successfully retrieved from the RADIUS server, then the user is assigned the network-operator role.

Step 4 If your user name and password are successfully authenticated locally, you are allowed to log in, and you are assigned the roles configured in the local database.

Figure 9-1 Switch Authorization and Authentication Flow



Role-Based Authorization

The Cisco MDS 9020 Fabric Switch performs authentication based on roles. The Cisco MDS 9020 Fabric Switch supports two roles: network-administrator and network operator. Role-based authorization limits access to switch operations by assigning users to roles. When you execute a command, perform command completion, or obtain context sensitive help, the switch software allows the operation to progress if you have permission to access that command.

Note Only the admin user name can create or modify user accounts. Users can change their own passwords.

Displaying Role-Based Information

Use the **show role** command to display rules configured on the switch. (See Example 9-2.)

Example 9-2 Displays 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
```

Configuring User Accounts

Every Cisco MDS 9020 Fabric Switch user has the account information stored by the system. Your authentication information, user name, user password, password expiration date, and role membership are stored in your user profile.

The tasks explained in this section enable you to create users and modify the profile of an existing user. These tasks are restricted to privileged users as determined by your administrator.

Creating or Updating Users

By default, the user account does not expire unless you explicitly configure it to expire. The **expire** option determines the date on which the user account is disabled. The date is specified in the YYYY-MM-DD format.

Tip The following words are reserved and cannot be used to configure users: bin, daemon, adm, lp, sync, shutdown, halt, mail, news, uucp, operator, games, gopher, ftp, nobody, nscd, mailnull, rpc, rpcuser, xfs, gdm, mtsuser, ftpuser, man, and sys.

Note User passwords are not displayed in the switch configuration file.

Tip If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a strong password, as shown in the sample configuration. Passwords are case-sensitive. Admin is not the default password for the Cisco MDS 9020 Fabric Switch. You must explicitly configure a password that meets the above requirements.

To configure a new user or to modify the profile of an existing user, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# username usam password abcd123AAA expire 2005-05-31`	Creates or updates the user account (usam), along with a password (abcd123AAA) that is set to expire on 2003-05-31. The password is limited to 20 characters.
	`switch(config)# username msam password abcd12AAA role network-operator`	Creates or updates the user account (msam), along with a password (abcd12AAA) specified in clear text. The password can be from 8 to 20 characters.
Step 3	`switch(config)# username usam role network-admin`	Adds the specified user (usam) to the network-admin role.

Displaying User Account Information

Use the **show user-account** command to display configured information about user accounts. (See Examples 9-3 to 9-4.)

Example 9-3 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
```

Example 9-4 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 28 00:00:00 2005
        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
```

Configuring Accounting Services

Accounting refers to the log information that is kept for each management session in a switch. This information may be used to generate reports for troubleshooting and auditing purposes. Accounting can be implemented locally or remotely (using RADIUS).

Tip The Cisco MDS 9020 Fabric Switch uses interim-update RADIUS accounting-request packets to communicate accounting log information to the RADIUS server. The RADIUS server must be appropriately configured to log the information communicated in these packets. Several servers typically have log update/watchdog packets flags in the AAA client configuration. Turn on this flag to ensure proper RADIUS accounting.

Note Configuration operations are automatically recorded in the accounting log if they are performed in configuration mode. Additionally, important system events (for example, configuration save and system switchover) are also recorded in the accounting log.

Displaying the Accounting Log

The **show accounting log** command displays the contents of the accounting log. (See Example 9-5.) To display the size of the local accounting log, use the **show accounting logsize** command.

Example 9-5 Displays the Entire Log File

```
switch# show accounting log
[1][Mon Apr 25 11:01:59.888 UTC 2005][AU][0000.00FF][None][Zoning Default Zone changed in
Config default to False]
[2][Mon Apr 25 11:02:03.228 UTC 2005][AU][0000.0001][None][IP Unknown User
admin@OB-session1 User Login]
[3][Mon Apr 25 11:02:07.376 UTC 2005][AU][0000.0001][None][IP Unknown User
snmp@IB-session2 User Login]
[4][Mon Apr 25 11:02:07.379 UTC 2005][AU][0000.0001][None][IP Unknown User
snmp@OB-session3 User Login]
[5][Mon Apr 25 15:58:40.548 UTC 2005][AU][0000.0001][None][IP 10.20.33.160 User
admin@OB-session4 User Login]
[6][Mon Apr 25 16:08:38.188 UTC 2005][AU][0000.0001][None][IP 10.20.32.70 User
admin@OB-session5 User Login]
[7][Mon Apr 25 16:38:23.054 UTC 2005][AU][0000.0001][None][IP 10.20.32.70 User
admin@OB-session6 User Login]
[8][Mon Apr 25 20:02:43.211 UTC 2005][AU][0000.0001][None][IP 10.20.32.70 User
admin@OB-session7 User Login]
[9][Tue Apr 26 13:49:28.317 UTC 2005][AU][0000.0001][None][IP 10.20.32.70 User
admin@OB-session8 User Login]
[10][Tue Apr 26 18:47:00.064 UTC 2005][AU][0000.0001][None][IP 10.20.32.70 User
admin@OB-session9 User Login]
...
```

Configuring SSH Services

The Telnet service is enabled by default on the Cisco MDS 9020 Fabric Switch. Before enabling the SSH service, generate a server key pair. (See the "Generating the SSH Server Key Pair" section on page 9-9.)

Use the **ssh key** command to generate a server key.

Generating the SSH Server Key Pair

Be sure to have an SSH server key pair with the appropriate version before enabling the SSH service. Generate the SSH server key pair according to the SSH client version used. The number of bits specified for each key pair ranges from 768 to 2048. The **rsa** option generates the RSA key pair for the SSH version 2 protocol.

Caution If you delete all of the SSH keys, you cannot start a new SSH session.

To generate the SSH server key pair, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.

Step 2	`switch(config)# ssh key rsa`
	`generating rsa key.....`
	`generated rsa key`
		Generates the RSA server key pair.

	`switch(config)# no ssh key rsa` `cleared RSA keys`	Clears the RSA server key pair configuration.

Enabling SSH Service

By default, the SSH service is disabled.

To enable or disable the SSH service, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# ssh server enable` `updated`	Enables the use of the SSH service.
	`switch(config)# no ssh server enable` `updated`	Disables (default) the use of the SSH service and resets the switch to its factory defaults.

Caution If you are logging in to a switch through SSH and you have entered the **aaa authentication login default none** command, you must enter one or more keystrokes to log in. If you press the **Enter** key without entering at least one keystroke, your log in will be rejected.

Displaying SSH Protocol Status

Use the **show ssh server** command to display the status of the SSH protocol (enabled or disabled). (See Example 9-6.)

Example 9-6 Displays SSH Protocol Status

```
switch# show ssh server
ssh service is enabled
```

Recovering the Administrator Password

To recover the administrator password, you must restore the factory account name password using maintenance mode. This restores the password for the Admin account name to the default (admin123) and removes all other user accounts from the switch. To reset the switch password, follow these steps:

Step 1 Isolate the switch from the fabric.

Step 2 Establish a serial connection from the PC console to the switch console port.

a. Configure the baud rate and character format of the PC terminal emulation program to match the following management port default characteristics:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- Flow control: none

b. Connect a null-modem F/F DB9 cable from the switch console port to the PC serial port.

Step 3 Place the switch in maintenance mode. Press and hold the **Maintenance** button with a pointed tool. The Maintenance button is located under the Ethernet port. When the Heartbeat LED alone turns on, release the button. The switch will reboot and display the `Switch Login:` prompt.

Step 4 Enter the maintenance mode account name and password (prom, prom), and press **Enter**.

```
Switch login: prom
Password:xxxx
```

Step 5 Enter `3` for **Reset User Accounts to Default**.

```
0)  Exit
1)  Image Unpack
2)  Reset Network Config
3)  Reset User Accounts to Default
4)  Copy Log Files
5)  Remove Switch Config
6)  Remake Filesystem
7)  Reset Switch
8)  Update Boot Loader
Option: 3
```

Step 6 Enter `7` for **Reset Switch**.

```
0)  Exit
1)  Image Unpack
2)  Reset Network Config
3)  Reset User Accounts to Default
4)  Copy Log Files
5)  Remove Switch Config
6)  Remake Filesystem
7)  Reset Switch
8)  Update Boot Loader
Option: 7
```

Step 7 Enter **yes** when prompted to reset the switch.

Configuring Cisco Access Control Server

The Cisco Access Control Server (ACS) uses RADIUS protocols to provide AAA services that ensure a secure environment. When using the AAA server, user management is normally done using Cisco ACS. Figure 9-2 and Figure 9-3 display ACS server user setup configurations for network-administsrator roles and multiple roles using RADIUS.

Figure 9-2 Configuring the network-admin Role When Using RADIUS

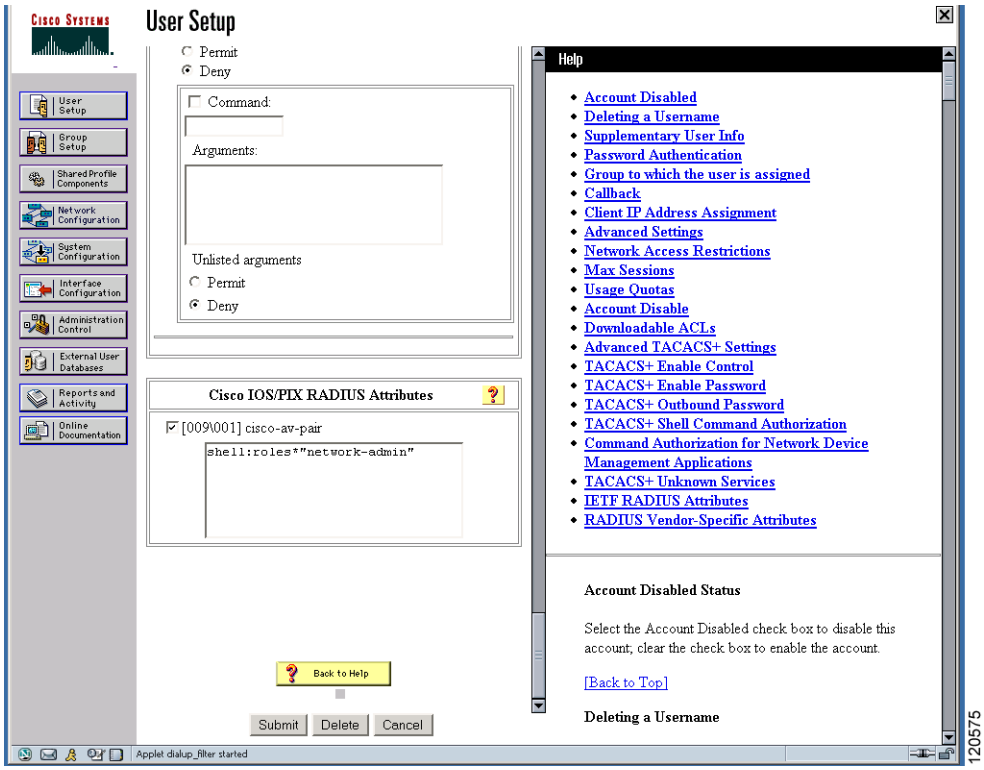
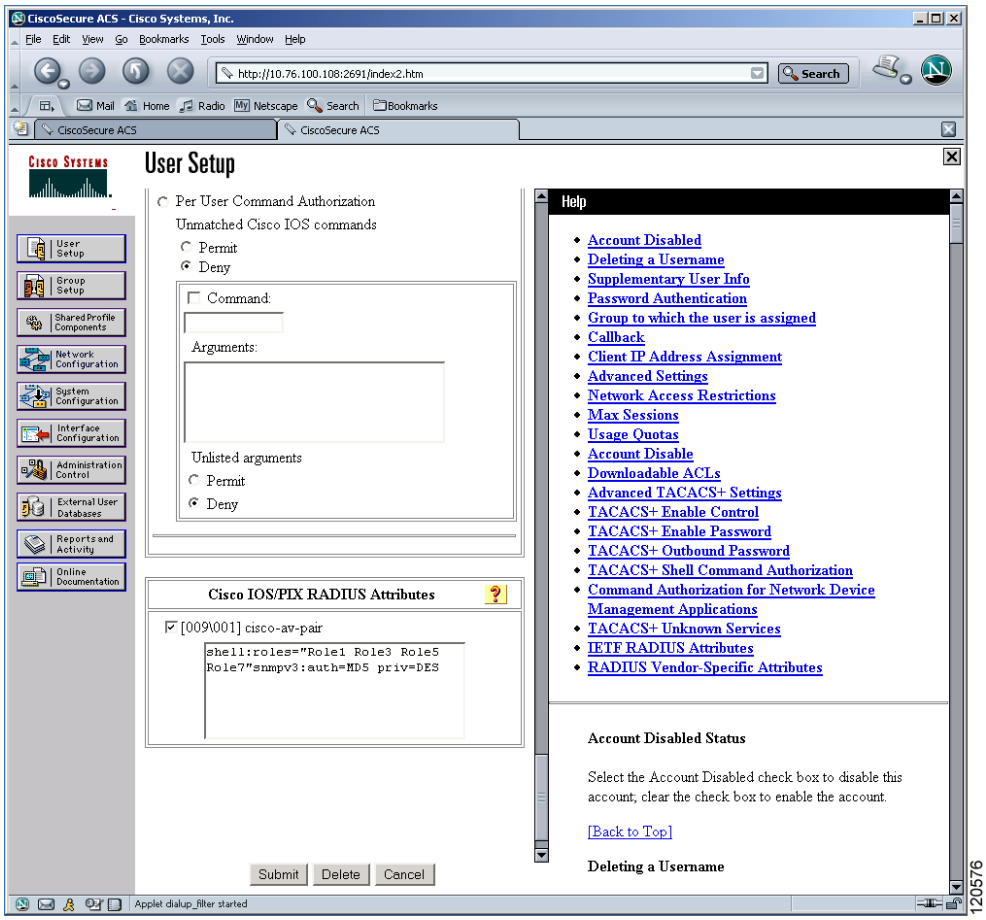


Figure 9-3 Configuring Multiple Roles with SNMPv3 Attributes When Using RADIUS



Default Settings

Table 9-1 lists the default settings for all switch security features in any switch.

Table 9-1 Default Switch Security Settings

Parameters	Default
Roles in a Cisco MDS 9020 Fabric Switch	Network operator (network-operator).
AAA configuration services	Local.
Authentication port	1821.
Accounting port	1813.
Preshared key communication	Clear text.
RADIUS server time out	1 (one) second.
RADIUS server retries	Once.
User account	No expiry (unless configured).
Password	None.
Accounting log size	250 KB.
SSH service	Disabled.
Telnet service	Enabled.

CHAPTER 10

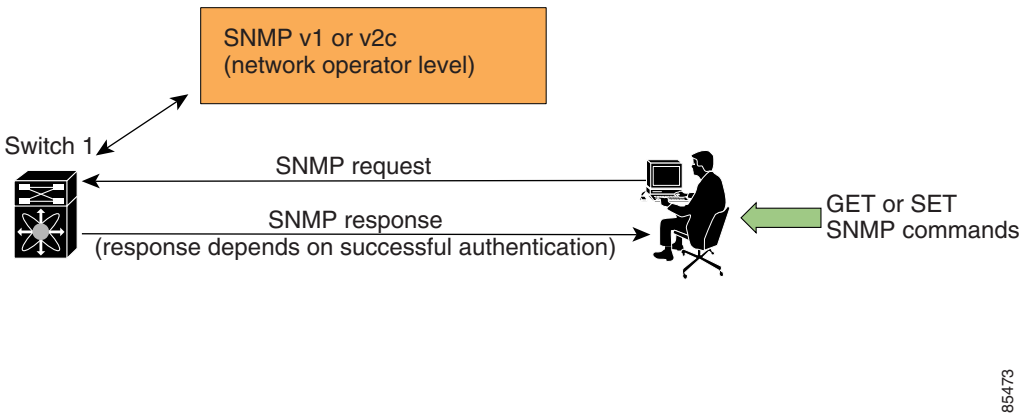
Configuring SNMP

This chapter includes the following sections:

SNMP Security

SNMP is an application layer protocol that facilitates the exchange of management information between network devices. In the Cisco MDS 9020 Fabric Switch, two SNMP versions are available: SNMPv1 and SNMPv2c. (See Figure 10-1.)

Figure 10-1 SNMP Security



Adding or Deleting Communities

You can configure read-only or read-write access for SNMP users. To create an SNMPv1 or SNMPv2c community, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# snmp-server community snmp_Community ro`	Adds read-only access for the specified SNMP community.
	`switch(config)# snmp-server community snmp_Community rw`	Adds read-write access for the specified SNMP community.
	`switch(config)# no snmp-server community snmp_Community`	Deletes access for the specified SNMP community (default).

Assigning SNMP Switch Contact Information

The switch contact information is limited to 32 characters (without spaces).

Use the **snmp-server** command to set the contact information and the switch location. Use the **no** form of the command to remove the system contact information.

To configure contact information, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# snmp-server contact NewUser`	Assigns the contact name for the switch.
	`switch(config)# no snmp-server contact NewUser`	Deletes the contact name for the switch.
Step 3	`switch(config)# snmp-server location SanJose`	Assigns the switch location.
	`switch(config)# no snmp-server location SanJose`	Deletes the switch location.

Configuring SNMP Notifications

You can configure the Cisco MDS 9020 Fabric Switch using the CLI to send notifications to SNMP managers when changes occur that affect the switch configuration or status. You can send these notifications as traps.

To configure notifications, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# snmp-server host 172.16.187.101 traps version 2c private udp-port 1163`	Configures the specified host to receive SNMP version 2c trap notifications on a private port number 1163.
	`switch(config)# no snmp-server host 172.18.2.247 version 2c public udp-port 2162`	Prevents the specified host to receive SNMP version 2c inform notifications on a private port number 2162.
	`switch(config)# snmp-server host 10.1.1.1 fsdf`	Configures the specified host to receive SNMP inform notifications with the default **noauth** option on the default UDP port (162).

Enabling SNMP Notifications

Notifications (traps) are system alerts that the switch generates when selected changes occur that affect the switch configuration or status. By default, no notification is defined or issued.

To enable notifications, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# snmp-server enable traps`	Enables SNMP traps.
	`switch(config)# no snmp-server enable traps`	Disables SNMP traps.

Displaying SNMP Security Information

Use the **show snmp** commands to display configured SNMP information. (See Example 10-1 to 10-3.)

Example 10-1 Displays SNMP User Details

```
switch# show snmp user
Host                            Port Version  Type   SecName
____                            ____ _______  _____  ______
10.0.0.254                      162  2c       trap   public
```

Example 10-2 Displays SNMP Community Information

```
switch# show snmp community
Community Group/Access
--------- ------------
public    network-operator
```

Example 10-3 Displays SNMP Host Information

```
switch# show snmp host
Host                            Port Version  Level  Type   SecName
____                            ____ _______  ______ ____   ______
172.16.126.34                   2162 v2c      noauth trap   public
172.16.75.106                   2162 v2c      noauth trap   public
...
172.31.58.97                    2162 v2c      auth   trap   public
...
```

The **show snmp** command displays counter information for SNMP contact, location, and packet settings. This command provides information that is used entirely by the Cisco MDS 9000 Family Fabric Manager (refer to the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*). (See Example 10-4.)

Example 10-4 Displays SNMP

```
switch# show snmp
sys contact: <sysContact undefined>

sys location: <sysLocation undefined>

Community  Group/Access
---------  ------------
public     network-operator
```

CHAPTER 11

Configuring Fibre Channel Routing Services and Protocols

Fabric Shortest Path First (FSPF) is the standard path selection protocol used by Fibre Channel fabrics. The FSPF feature is enabled by default on all Fibre Channel switches. Except in configurations that require special consideration, you do not need to configure any FSPF services. FSPF automatically calculates the best path between any two switches in a fabric. Specifically, FSPF is used to do the following:

- Dynamically compute routes throughout a fabric by establishing the shortest and quickest path between any two switches.
- Select an alternative path in the event of the failure of a given path. FSPF supports multiple paths and automatically computes an alternative path around a failed link. It provides a preferred route when two equal paths are available.

This chapter provides details on Fibre Channel routing services and protocols. It includes the following sections:

FSPF Features

FSPF is the protocol currently standardized by the T11 committee for routing in Fibre Channel networks. The FSPF protocol has the following characteristics and features:

- Supports multipath routing.
- Bases path status on a link state protocol.
- Routes hop by hop, based only on the domain ID.
- Runs only on E ports and provides a loop free topology.
- Uses a topology database to keep track of the state of the links on all switches in the fabric and associates a cost with each link.
- Guarantees a fast reconvergence time in case of a topology change. It uses the standard Dijkstra's algorithm, but there is a static dynamic option for a more robust, efficient, and incremental Dijkstra's algorithm.

FSPF Examples

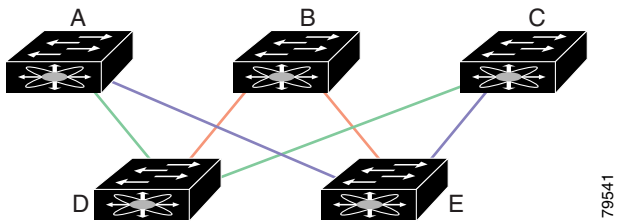
This section provides examples of topologies and applications that demonstrate the benefits of FSPF.

Note The FSPF feature can be used on any topology.

Fault Tolerant Fabric

Figure 11-1 depicts a fault tolerant fabric using a partial mesh topology. If a link goes down anywhere in the fabric, any switch can still communicate with all others in the fabric. In the same way, if any switch goes down, the connectivity of the rest of the fabric is preserved.

Figure 11-1 Fault Tolerant Fabric

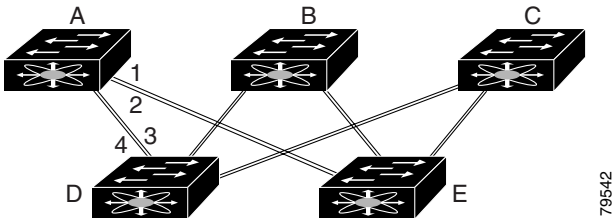


For example, if all links are of equal speed, the FSPF calculates two equal paths from A to C: A-D-C (green) and A-E-C (blue).

Redundant Links

To further improve on the topology in Figure 11-1, each connection between any pair of switches can be replicated; two or more links can be present between a pair of switches. Figure 11-2 shows this arrangement.

Figure 11-2 Fault Tolerant Fabric with Redundant Links



For example, if all links are of equal speed, the FSPF calculates four equal paths from A to C: A1-E-C, A2-E-C, A3-D-C, and A4-D-C.

Link State Record Defaults

Each time a new switch enters the fabric, a link state record (LSR) is sent to the neighboring switches and then flooded throughout the fabric. Table 11-1 displays the default settings for switch responses.

Table 11-1 LSR Default Settings

LSR Option	Default	Description
Acknowledgment interval (RxmtInterval)	5 seconds	The time a switch waits for an acknowledgment from the LSR before retransmission.
Refresh time (LSRefreshTime)	30 minutes	The time a switch waits before sending an LSR refresh transmission.
Maximum age (MaxAge)	60 minutes	The time a switch waits before dropping the LSR from the database.

Clearing FSPF Counters

To clear the FSPF statistics counters for one interface, perform this task:

	Command	Purpose
Step 1	`switch# clear fspf counters` `switch#`	Clears the FSPF statistics counters. If an interface reference is not specified, all counters are cleared.
	`switch# clear fspf counters interface fc1/1` `switch#`	Clears the FSPF statistics counters for the specified interface.

Displaying Global FSPF Information

Example 11-1 displays global FSPF information:

- Domain number of the switch.
- Autonomous region for the switch.
- Min_LS_arrival: minimum time that must elapse before the switch accepts LSR updates.
- Min_LS_interval: minimum time that must elapse before the switch can transmit an LSR.

Tip If the Min_LS_interval is higher than 10 seconds, the graceful shutdown feature is not implemented.

- LS_refresh_time: interval time lapse between refresh LSR transmissions.
- Max_age: maximum time aa LSR can stay before being deleted.

Example 11-1 Displays FSPF Information

```
switch# show fspf
FSPF routing administration status is enabled
FSPF routing operational status is UP
MinLsArrival = 1000 msec , MinLsInterval = 5000 msec
Local Domain is 0x61(97)
Number of LSRs = 0
Protocol constants :
     LS_REFRESH_TIME = 30 minutes (1800 sec)
     MAX_AGE         = 60 minutes (3600 sec)
Statistics counters :
     Number of LSR that reached MaxAge = 0
     Number of SPF computations = 0
     Number of Checksum Errors = 0
     Number of Transmitted packets : LSU 0 LSA 0 Hello 0 Retranmsitted LSU 0
     Number of Received packets : LSU 0 LSA 0 Hello 0 Error Packets 0
```

Displaying FSPF Interfaces

Example 11-2 displays the following information for each selected interface.

- Link cost
- Timer values
- Neighbor's domain ID (if known)
- Local interface number
- Remote interface number (if known)
- FSPF state of the interface
- Interface counters

Example 11-2 Displays FSPF Interface Information

```
switch# show fspf interface
FSPF interface fc1/1
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
      Number of packets received : LSU 0 LSA 0 Hello 0 Error packets 0
      Number of packets transmitted : LSU 0 LSA 0 Hello 0 Retransmitted LSU 0

FSPF interface fc1/2
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
      Number of packets received : LSU 0 LSA 0 Hello 0 Error packets 0
      Number of packets transmitted : LSU 0 LSA 0 Hello 0 Retransmitted LSU 0

FSPF interface fc1/3
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
      Number of packets received : LSU 0 LSA 0 Hello 0 Error packets 0
      Number of packets transmitted : LSU 0 LSA 0 Hello 0 Retransmitted LSU 0
```

Default Settings

Table 11-2 lists the default settings for FSPF features.

Table 11-2 Default FSPF Settings

Parameters	Default
FSPF	Enabled on all E ports.
SPF computation	Dynamic.
SPF hold time	0.
Backbone region	0.
Acknowledgment interval (RxmtInterval)	5 seconds.
Refresh time (LSRefreshTime)	30 minutes.
Maximum age (MaxAge)	60 minutes.
Hello interval	20 seconds.
Dead interval	80 seconds.
Distribution tree information	Derived from the principal switch (root node).
Routing table	FSPF stores up to 4 equal cost paths to a given destination.
Load balancing	Based on destination ID, source ID, and oxID (switch by exchange) on different, equal cost paths.
Static route cost	If the cost (metric) of the route is not specified, the default is 10.
Remote destination switch	If the remote destination switch is not specified, the default is direct.
Multicast routing	Uses the principal switch to compute the multicast tree.

CHAPTER 12

Configuring IP Services

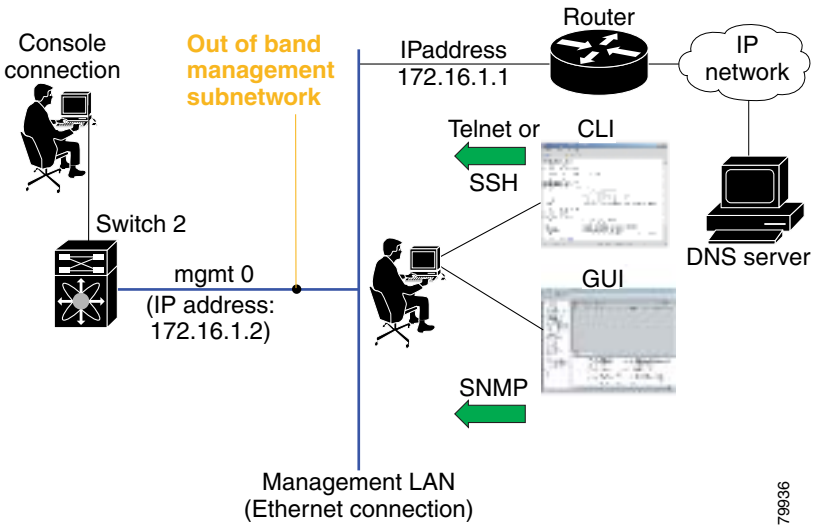
Cisco MDS 9020 Fabric Switches can route IP traffic between Ethernet and Fibre Channel interfaces.

This chapter includes the following sections:

Traffic Management Services

All traffic management is performed through the console connection or the mgmt0 Ethernet interface. (See Figure 12-1.)

Figure 12-1 Management Access to Switches



Management Interface Configuration

The management interface on the switch allows multiple simultaneous Telnet or SNMP sessions. You can remotely configure the switch through the management interface, but first you must configure some IP parameters (IP address, subnet mask) so that the switch is reachable. You can manually configure the management interface from the CLI.

Note Before you begin to configure the management interface manually, obtain the switch's IP address and IP subnet mask. Also make sure the console cable is connected to the console port.

To configure the mgmt0 Ethernet interface, perform this task:

	Command	Purpose
Step 1	`switch# config terminal` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# interface mgmt0` `switch(config-if)#`	Enters the interface configuration mode on the management Ethernet interface (mgmt0).
Step 3	`switch(config-if)# ip address 10.1.1.1 255.255.255.0`	Enters the IP address (10.1.1.1) and IP subnet mask (255.255.255.0) for the management interface.
Step 4	`switch(config-if)# no shutdown`	Enables the interface.

Default Gateway Configuration

The default gateway IP address should be configured along with the IP static routing commands (IP default network, destination prefix, destination mask, and next hop address).

Tip If you configure the static route IP forwarding and the default-network details, these IP addresses will be used regardless of the default-gateway being enabled or disabled. If these IP addresses are configured but not available, the switch will fall back to using the default gateway IP address if you have configured it. Be sure to configure IP addresses for all entries in the switch.

See the "Initial Setup Routine" section on page 3-2 for more information on configuring the IP addresses for all entries in the switch.

Use the **IP default-gateway** command to configure the IP address for a switch's default gateway and the **show ip route** command to verify that the IP address for the default gateway is configured.

To configure default gateways, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# ip default-gateway 10.12.11.1`	Configures the IP address for the default gateway.

IP Access Control Lists

IP access control lists (IP-ACLs) enhance network security for Cisco MDS 9020 Fabric Switches. IP-ACLs restrict IP-related traffic based on the configured IP filters. A filter contains the rules to match an IP packet, and if the packet matches, the rule also stipulates whether the packet should be permitted or denied.

Each Cisco MDS 9020 Fabric Switch can have a maximum of 64 IP-ACLs, and each IP-ACL can have a maximum of 256 filters.

IP-ACL Configuration Guidelines

When configuring IP-ACLs in a Cisco MDS 9020 Fabric Switch, configure the order of conditions accurately. Because the IP-ACL filters are sequentially applied to the IP flows, only 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.

Filter Contents

An IP filter contains rules for matching an IP packet based on the protocol, address, port, ICMP type, and type of service (TOS).

Protocol Information

The protocol information is required in each filter. It identifies the IP name or number. You can specify the IP in one of two ways:

- Specify a number ranging from 0 to 255. This number represents the IP number.
- Specify the name of a protocol including, but not restricted to, Internet Protocol (IP, keyword **ip),** Transmission Control Protocol (TCP, keyword **tcp**), User Datagram Protocol (UDP, keyword **udp**), and Internet Control Message Protocol (ICMP, keyword **icmp**).

Address Information

The address information is required in each filter. It identifies the following details:

- Source: The address of the network or host from which the packet is being sent.
- Source-wildcard: The wildcard bits applied to the source.
- Destination: The number of the network or host to which the packet is being sent.
- Destination-wildcard: The wildcard bits applied to the destination.

You can specify the source and source-wildcard or the destination and destination-wildcard in one of two ways:

- Using the 32-bit quantity in four-part, dotted decimal format (10.1.1.2/0.0.0.0 is the same as host 10.1.1.2).
  - 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 bit position in the source.
  - Each wildcard bit set to one indicates that both a zero bit and a one bit in the corresponding position of the packet's IP address will be considered a match to this access list entry. Place ones in the bit positions that you want to ignore. For example, use 0.0.255.255 to require an exact match of only the first 16 bits of the source. Wildcard bits set to one do not need to be contiguous in the source-wildcard. For example, a source-wildcard of 0.255.0.64 would be valid.
- Using the **any** option as an abbreviation for a source and source-wildcard or destination and destination-wildcard (0.0.0.0/255.255.255.255).

Port Information

The port information is optional. To compare the source and destination ports, use the **eq** (equal) option, the **gt** (greater than) option, the **lt** (less than) option, or the **range** (range of ports) option. You can specify the port information in one of two ways:

- Specify the number of the port. Port numbers range from 0 to 65535. Table 12-1 displays the port numbers recognized by the Cisco MDS 9000 FabricWare software for associated TCP and UDP ports.
- Specify the name of a TCP or UDP port as follows:
  - TCP port names can only be used when filtering TCP.
  - UDP port names can only be used when filtering UDP.

Table 12-1 TCP and UDP Port Numbers

Protocol	Port	Number
UDP	dns	53
	tftp	69
	ntp	123
	radius accounting	1646 or 1813
	radius authentication	1645 or 1812
	snmp	161
	snmp-trap	162
	syslog	514

Table 12-1 TCP and UDP Port Numbers (continued)

Protocol	Port	Number
TCP **Note** If the TCP connection is already established, use the **established** option to find matches. A match occurs if the TCP datagram has the ACK, FIN, PSH, RST, or URG control bit set.	ftp	20
	ftp-data	21
	ssh	22
	telnet	23
	smtp	25
	tasacs-ds	65
	www	80
	sftp	115
	http	143
	wbem-http	5988
	wbem-https	5989

ICMP Information

IP packets can be filtered based on the following optional ICMP conditions:

- The icmp-type: ICMP message type. The type is a number from 0 to 255.
- The icmp-code: ICMP message code. The code is a number from 0 to 255.

Table 12-2 displays the value for each ICMP type.

Table 12-2 ICMP Type Value

ICMP Type[1]	Code
echo	8
echo-reply	0
destination unreachable	3
traceroute	30
time exceeded	11

1. ICMP redirect packets are always rejected.

TOS Information

IP packets can be filtered based on the following optional TOS conditions:

- The TOS level, as specified by a number from 0 to 15
- The TOS name: max-reliability, max-throughput, min-delay, min-monetary-cost, and normal

IP-ACL Creation

Traffic coming into the switch is compared with IP-ACL filters based on the order that the filters occur in the switch. New filters are added to the end of the IP-ACL. The switch keeps looking until it has a match. If no matches are found when the switch reaches the end of the filter, the traffic is denied. For this reason, you should have the frequently hit filters at the top of the filter. There is an *implied deny* for traffic that is not permitted. A single-entry IP-ACL with only one **deny** entry has the effect of denying all traffic.

To configure an IP-ACL, you must complete the following tasks:

1. Create an IP-ACL by specifying a filter name and one or more access condition(s). Filters require the source and destination address to match a condition. Use optional keywords to configure finer granularity.
2. Apply the access filter to specified interfaces.

To create an IP-ACL, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# ip access-list List1 permit ip any any`	Configures an IP-ACL called List1 and permits IP traffic from any source address to any destination address.
	`switch(config)# no ip access-list List1 permit ip any any`	Removes the IP-ACL called List1.
Step 3	`switch(config)# ip access-list List1 deny tcp any any`	Updates List1 to deny TCP traffic from any source address to any destination address.

To define an IP-ACL that permits a specified network, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# ip access-list List1 permit udp 192.168.32.0 0.0.7.255 any`	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.

To use the operand and port options, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# ip access-list List2 deny tcp 10.2.3.0 0.0.0.255 eq port 5 any`	Denies TCP traffic from 10.2.3.0 through source port 5 to any destination.

Adding filters to an Existing IP-ACL

After you create an IP-ACL, you place subsequent additions at the end of the IP-ACL. You cannot insert filters in the middle of an IP-ACL. Each configured entry is automatically added to the end of an IP-ACL.

To add entries to an existing IP-ACL, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# ip access-list List1 permit tcp 10.1.1.2 0.0.0.0 172.16.1.1 0.0.0.0 eq port telnet`	Permits TCP for Telnet traffic.
	`switch(config)# ip access-list List1 permit tcp 10.1.1.2 0.0.0.0 172.16.1.1 0.0.0.0 eq port http`	Permits TCP for HTTP traffic.
	`switch(config)# ip access-list List1 permit udp 10.1.1.2 0.0.0.0 172.16.1.1 0.0.0.0`	Permits UDP for all traffic.

Removing Entries from an Existing IP-ACL

To remove configured entries from an IP-ACL, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# no ip access-list List2 deny tcp 10.2.3.0 0.0.0.255 eq port 5 any`	Removes this entry from the IP-ACL.
	`switch(config)# no ip access-list x3 deny ip any any`	Removes this entry from the IP-ACL.
	`switch(config)# no ip access-list x3 permit ip any any`	Removes this entry from the IP-ACL.

Reading the IP-ACL Log Dump

Use the **log-deny** option at the end of a filter condition to log information about packets that match dropped entries. The log output displays the ACL number, permit or deny status, and port information.

For the input ACL, the log displays the raw MAC information. The keyword **MAC=** does not refer to showing an Ethernet MAC frame with MAC address information. It refers to the Layer 2 MAC-layer information dumped to the log. For the output ACL, the raw Layer 2 information is not logged.

The following example shows an input ACL log dump:

```
Jul 17 20:38:44 excal-2
%KERN-7-SYSTEM_MSG:
%IPACL-7-DENY:IN=vsan1 OUT=
MAC=10:00:00:05:30:00:47:df:10:00:00:05:30:00:8a:1f:aa:aa:03:00:00:00:08:00:45:00:00:54:00
:00:40:00:40:01:0e:86:0b:0b:0b:0c:0b:0b:0b:02:08:00:ff:9c:01:15:05:00:6f:09:17:3f:80:02:01
:00:08:09:0a:0b:0c:0d:0e:0f:10:11:12:13:14:15:16:17:18:19:1a:1b:1c:1d:1e:1f:20:21:22:23:24
:25:26:27:28:29:2a:2b SRC=11.11.11.12 DST=11.11.11.2 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=0
DF PROTO=ICMP TYPE=8 CODE=0 ID=277 SEQ=1280
```

The following example is an output ACL log dump:

```
Jul 17 20:38:44 excal-2
%KERN-7-SYSTEM_MSG:
%IPACL-7-DENY:IN= OUT=vsan1 SRC=11.11.11.2 DST=11.11.11.12 LEN=84 TOS=0x00 PREC=0x00
TTL=255 ID=38095 PROTO=ICMP TYPE=0 CODE=0 ID=277 SEQ=1280
```

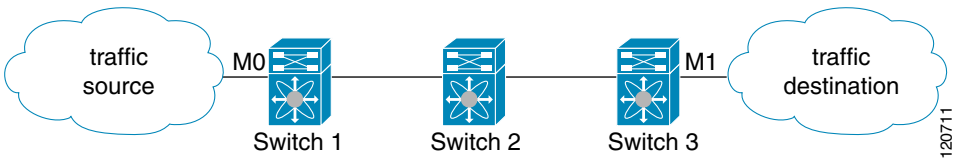
IP-ACL Interface Application

You can define IP-ACLs without applying them. However, the IP-ACLs will have no effect until they are applied to the switch's interface.

Tip Apply the IP-ACL on the interface closest to the source of the traffic.

When you are trying to block traffic from source to destination, you can apply an inbound IP-ACL to M0 on Switch 1 instead of an outbound filter to M1 on Switch 3. (See Figure 12-2.)

Figure 12-2 Denying Traffic on the Inbound Interface



The **access-group** option controls access to an interface. Each interface can only be associated with one access filter per direction. The ingress direction can have a different ACL than the egress direction. The access group becomes active on creation.

Tip Create all conditions in an access filter before creating the access group that uses this filter.

Caution If you create an access group before an access-filter, all packets in that interface are dropped because the access filter is empty.

The terms *in*, *out*, *source*, and *destination* are used as referenced by the switch.

- In—Traffic that is arriving on the interface and which will go through the switch; the source would be where it's been and the destination is where it's going (on the other side of the router).

Tip The access-group configuration for the ingress traffic applies to both local and remote traffic.

- Out—Traffic that has already been through the switch and is leaving the interface; the source would be where it's been (on the other side of the router) and the destination is where it's going.

Tip The access-group configuration for the egress traffic applies only to local traffic.

To create an access group, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch (config)# interface mgmt0`	Configures the management interface (mgmt0).
Step 3	`switch (config-if)#ip access-group SampleName`	Creates an access group called SampleName for both the ingress and egress traffic (default).
	`switch(config-if)# no ip access-group NotRequired`	Deletes the access group called NotRequired.
Step 4	`switch(config-if)# ip access-group SampleName1 in`	Creates an access group called SampleName (if it does not already exist) for ingress traffic.
	`switch(config-if)# no ip access-group SampleName1 in`	Deletes the access group called SampleName for ingress traffic.
	`switch(config-if)# ip access-group SampleName2 out`	Creates an access group called SampleName (if it does not already exist) for local egress traffic.
	`switch(config-if)# no ip access-group SampleName2 out`	Deletes the access group called SampleName for local egress traffic.

IP-ACL Configuration Verification

Use the **show ip access-list** command to view the contents of configured access filters. Each access filter can have several conditions. (See Examples 12-1 and 12-2.)

Example 12-1 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
```

Example 12-2 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)
```

IP-ACL Counter Cleanup

Use the **clear** command to clear the counters for a specified IP-ACL entry.

Note You cannot use this command to clear the counters for each individual filter.

```
switch# clear ip access-list counters abc
```

Displaying IP Interface Information

Use the following **show** commands to view configured IP interface information. (See Examples 12-3 and 12-4.)

Example 12-3 Displays the Interface

```
switch# show interface mgmt0
mgmt0 is up
    Hardware is FastEthernet
    Internet address is 10.20.83.122/24
```

Example 12-4 Displays the Connected and Static Route Details

```
switch# show ip route
Codes: C - connected, S - static

Default gateway is 10.20.83.1

C 10.20.83.0/24 is directly connected, mgmt0
```

CHAPTER 13

Configuring Domain Parameters

The Fibre Channel domain (fcdomain) feature performs principal switch selection, domain ID distribution, FC ID allocation, and fabric reconfiguration functions as described in the FC-SW-2 standards. If you do not configure a domain ID, the local switch uses a random ID.

Caution Changes to fcdomain parameters should not be performed on a daily basis. These changes should be made by an administrator or individual who is completely familiar with switch operations.

Tip When you change the configuration, be sure to save the running configuration. The next time you reboot the switch, the saved configuration is used. If you do not save the configuration, the previously saved startup configuration is used.

This chapter includes the following sections:

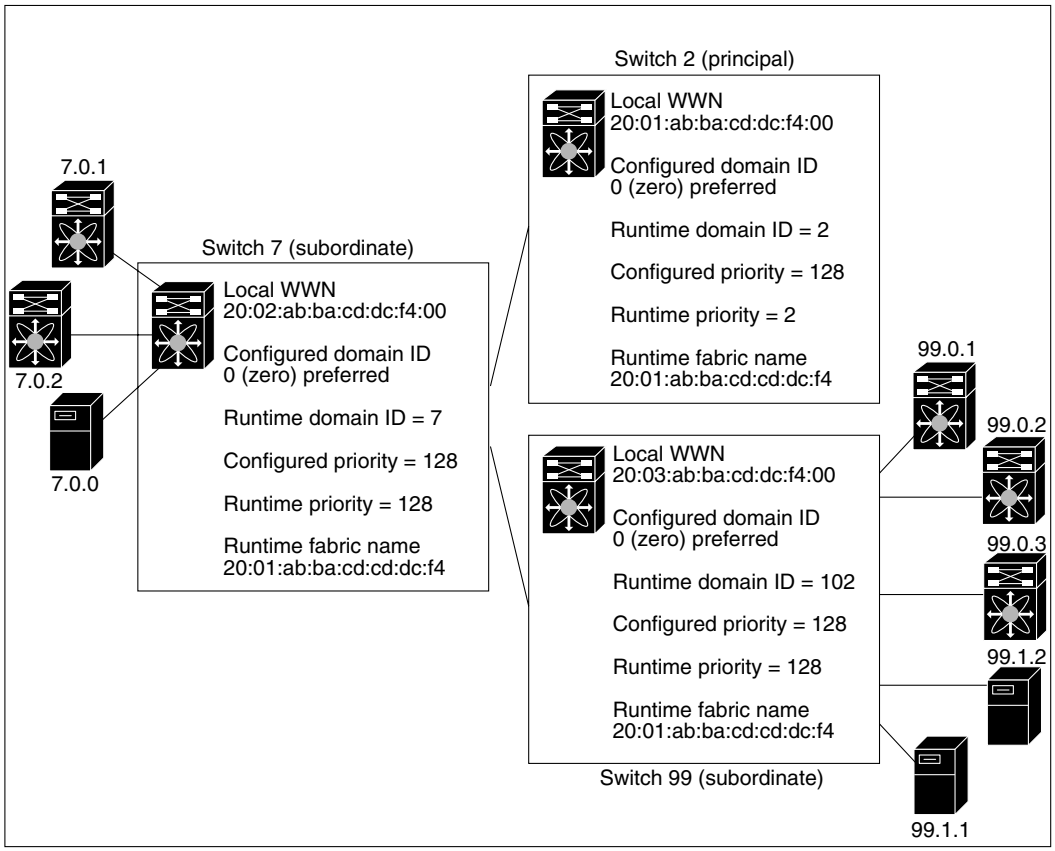
About fcdomain Phases

This section describes each fcdomain phase:

- Principal switch selection—This phase guarantees the selection of a unique principal switch across the fabric.
- Domain ID distribution—This phase guarantees each switch in the fabric obtains a unique domain ID.
- FC ID allocation—This phase guarantees a unique FC ID assignment to each device attached to the corresponding switch in the fabric.
- Fabric reconfiguration—This phase guarantees a resynchronization of all switches in the fabric to ensure they simultaneously restart a new principal switch selection phase.

Figure 13-1 shows a sample fcdomain configuration.

Figure 13-1 Sample fcdomain Configuration



Note Domain ID values used in all procedures are only provided as examples. Be sure to use IDs and values that apply to your configuration.

Domain Restart

Fibre Channel domains can be started disruptively or nondisruptively. If you perform a disruptive restart, reconfigured fabric (RCF) frames are sent to other switches in the fabric. If you perform a nondisruptive restart, build fabric (BF) frames are sent to other switches in the fabric.

Note A static domain is specifically configured by the user and may be different from the runtime domain. If the domain IDs are different, the runtime domain ID changes to take on the static domain ID after the next restart.

You can apply most of the configurations to their corresponding runtime values. Each of the following sections provide further details to show how the fcdomain parameters are applied to the runtime values.

The **fcdomain restart** command applies your changes to the runtime settings. Use the **restart disruptive** option to apply most of the configurations to their corresponding runtime values.

To restart the fabric disruptively or nondisruptively, perform this task:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# fcdomain restart`	Reconfigures the fabric without traffic disruption.
	`switch(config)# fcdomain restart disruptive`	Reconfigures the fabric with data traffic disruption.

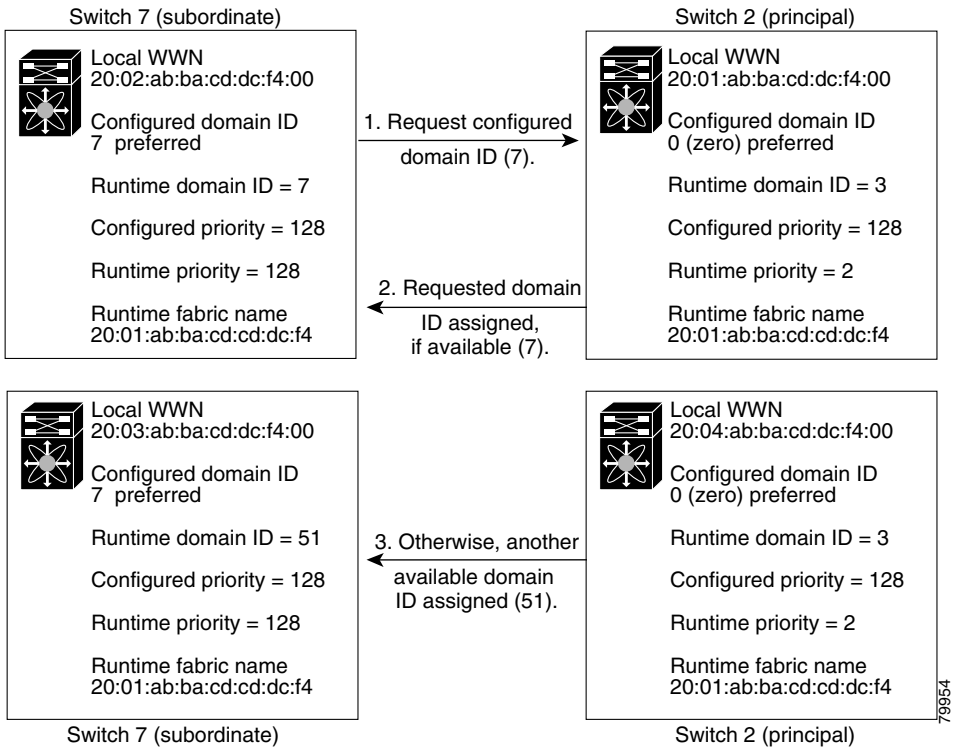
Domain Configuration

The configured domain ID can be **preferred** or **static**. By default, the configured domain is **0** and the configured type is **preferred**. If you do not configure a domain ID, the local switch sends a random ID in its request.

When a subordinate switch requests a domain, the following process takes place:

1. The local switch sends a configured domain ID request to the principal switch.
2. The top portion of Figure 13-2 shows the principal switch assigning the requested domain ID as requested. If the requested ID is unavailable, the principal switch assigns another ID as shown in the bottom portion of Figure 13-2.

Figure 13-2 Configuration Process Using the preferred Option



The behavior of a subordinate switch depends on the allowed domain ID lists, the configured domain ID, and the domain ID assigned by principal switch.

- When the received domain ID is not within the allowed list, the requested domain ID becomes the runtime domain ID and all interfaces are isolated.
- When the assigned and requested domain IDs are the same, the **preferred** and **static** options are not relevant, and the assigned domain ID becomes the runtime domain ID.
- When the assigned and requested domain IDs are different, the following cases apply:
  - If the configured type is **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.
  - If the configured type is **preferred**, the local switch accepts the domain ID assigned by the principal switch, and the assigned domain ID becomes the runtime domain ID.

If you change the configured domain ID, the change is accepted only if the new domain ID is included in all the allowed domain ID lists. Alternatively, you can also configure zero-preferred domain ID.

Note The 0 (zero) value can be configured only if you use the **preferred** option.

While the **static** option can be applied to runtime after a disruptive or nondisruptive restart, the **preferred** option is applied to runtime only after a disruptive restart. (See the "Domain Restart" section on page 13-3.)

Caution You must enter the **fcdomain restart** command if you want to apply the configured domain changes to the runtime domain.

To specify a **preferred** or a **static** domain ID, perform this task:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# fcdomain domain 3 preferred`	Configures the switch to request a preferred domain ID 3 and accepts any value assigned by the principal switch.
	`switch(config)# no fcdomain domain 3 preferred`	Resets the configured domain ID to 0 (default). The configured domain ID becomes 0 preferred.
Step 3	`switch(config)# fcdomain domain 2 static`	Configures the switch to accept only a specific value and moves the local interfaces to an isolated state if the requested domain ID is not granted.
	`switch(config)# no fcdomain domain 18 static`	Resets the configured domain ID to factory defaults. The configured domain ID becomes 0 preferred.

Switch Priority

By default, the configured priority is 128. The valid range to set the priority is between 1 and 254. Priority 1 has the highest priority. Value 255 is accepted from other switches but cannot be locally configured.

Any new switch cannot become the principal switch when it joins a stable fabric. During the principal switch selection phase, the switch with the highest priority becomes the principal switch. If two switches have the same configured priority, the switch with the lower WWN becomes the principal switch.

The priority configuration is applied to runtime when the fcdomain is restarted. (See the "Domain Restart" section on page 13-3.) This configuration is applicable to both disruptive and nondisruptive restarts.

To configure the priority for the principal switch, perform this task:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# fcdomain priority 25`	Configures a priority of 25 for the local switch.
	`switch(config)# no fcdomain priority 25`	Reverts the priority to the factory default (128).

fcdomain Initiation

By default, the fcdomain feature is enabled on each switch. If you disable the fcdomain feature in a switch, that switch can no longer participate with other switches in the fabric. The fcdomain configuration is applied to runtime through a disruptive restart.

Use the **no fcdomain** command to disable the fcdomain feature.

To disable fcdomains, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# no fcdomain`	Disables the fcdomain configuration.
	`switch(config)# fcdomain`	Enables the fcdomain configuration.

Displaying fcdomain Information

Use the **show fcdomain** command to display global information about fcdomain configurations. (See Example 13-1.)

Note In Example 13-1, the fcdomain feature is disabled. Consequently, the runtime fabric name is the same as the configured fabric name.

Example 13-1 Displays the Global fcdomain Information

```
switch# show fcdomain
The local switch is the Principal Switch.
Local switch run time information:
        Local switch WWN:    10:00:00:0d:ec:19:cb:0e
        Running fabric name: 10:00:00:0d:ec:19:cb:0e
        Running priority:    128
        Current domain ID:   0x69(105)

Local switch configuration information:
        Configured fabric name:
        Configured priority:    128
        Configured domain ID:   0x0(0) (preferred)

Principal switch run time information:
        Running priority: 128
```

Use the **show fcdomain domain-list** command to display the list of domain IDs of all switches. This list provides the WWN of the switches owning each domain ID. (See Example 13-2.)

Example 13-2 Displays the fcdomain Lists

```
switch# show fcdomain domain-list
Domain ID           WWN
---------  ------------------------
0x2(2)     10:00:00:c0:dd:00:90:a3
0x61(97)   10:00:00:c0:dd:07:00:f7 [Local] [Principal]
Number of domains: 2
```

Default Settings

Table 13-1 lists the default settings for all fcdomain parameters.

Table 13-1 Default fcdomain Parameters

Parameters	Default
fcdomain feature	Enabled.
Configured domain ID	0 (zero).
Configured domain	Preferred.
Priority	128.

CHAPTER 14

Configuring System Message Logging

This chapter describes how to configure system message logging on the Cisco MDS 9020 Fabric Switch. It includes the following sections:

About System Message Logging

The system message logging software saves messages in a log file or directs the messages to other devices. This feature provides you with the following capabilities:

- Provides logging information for monitoring and troubleshooting
- Allows you to select the types of captured logging information
- Allows you to select the destination server to forward the captured logging information

By default, the switch logs normal but significant system messages to a log file and sends these messages to the system console. You can specify which system messages should be saved based on the type of facility (see Table 14-1) and the severity level (see Table 14-2). Messages are time-stamped to enhance real-time debugging and management.

You can access logged system messages using the CLI or by saving them to a properly configured system message logging server. The switch software saves system messages in a file that can save up to 1200 entries. You can monitor system messages remotely by accessing the switch through Telnet, SSH, or the console port, or by viewing the logs on a system message logging server.

Note When the switch first initializes, the network is not connected until initialization completes. Therefore, messages are not redirected to a system message logging server for a few seconds.

Table 14-1 describes some samples of the facilities supported by the system message logs.

Table 14-1 Internal Logging Facilities

Facility Keyword	Description
all	All facilities
auth	Authorization system
fcdomain	fcdomain
fcns	Name server
fcs	FCS
fspf	FSPF
ipconf	IP configuration
module	Switching module
ntp	NTP
port	Port
sysmgr	System manager
user	User process
zone	Zone server

Table 14-2 describes the severity levels supported by the system message logs.

Table 14-2 Error Message Severity Levels

Level Keyword	Level	Description	System Message Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Note Refer to the *Cisco MDS 9020 Fabric Switch System Messages Reference* for details on the error log message format.

System Message Logging Configuration

System logging messages are sent to the console based on the default (or configured) logging facility and severity values.

Facility Severity Level

To configure the severity level for a logging facility, perform this task:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# logging level all 4`	Configures Telnet or SSH logging for the all facilities at level 4 (warning). As a result, logging messages with a severity level of 4 or above are displayed.

Log Files

You can display the log file using the **show logging logfile** command.

System Message Logging Servers

You can configure a maximum of three system message logging servers.

To send log messages to a UNIX system message logging server, you must configure the system message logging daemon on a UNIX server. Log in as root, and follow these steps:

Step 1 Add the following line to the /etc/syslog.conf file.

local1.debug /var/log/*myfile*.log

Note Be sure to add five tab characters between **local1.debug** and **/var/log/*myfile*.log**. Refer to entries in the /etc/syslog.conf file for further examples.

The switch sends messages according to the specified facility types and severity levels. The **local1** keyword specifies the UNIX logging facility used. The messages from the switch are generated by user processes. The **debug** keyword specifies the severity level of the condition being logged. You can set UNIX systems to receive all messages from the switch.

Step 2 Create the log file by entering these commands at the UNIX shell prompt:

```
$ touch /var/log/myfile.log
$ chmod 666 /var/log/myfile.log
```

Step 3 Make sure the system message logging daemon reads the new changes by entering this command:

```
$ kill -HUP ~cat /etc/syslog.pid~
```

To configure system message logging servers, perform this task:

	Command	Purpose
Step 1	`switch# config t` `switch#`	Enters configuration mode.
Step 2	`switch(config)# logging server 172.22.00.00`	Configures the switch to forward log messages according to the specified facility types and severity levels to remote multiple servers specified by its hostname or IP address (172.22.00.00).
	`switch(config)# no logging server 172.16.00.00`	Removes the specified server (172.16.00.00) and reverts to factory default.

Outgoing System Message Logging Server Facilities

All system messages have a logging facility and a level. The logging facility can be thought of as *where* and the level can be thought of as *what*.

The single system message logging daemon (syslogd) sends the information based on the configured **facility** option. If no facility is specified, local7 is the default outgoing facility.

The internal facilities are listed in Table 14-1 and the outgoing logging facilities are listed in Table 14-3.

Table 14-3 External Logging Facilities

Facility Keyword	Description	Standard or Cisco MDS Specific
auth	Authorization system	Standard
authpriv	Authorization (private) system	Standard
cron	Cron or at facility	Standard
daemon	System daemons	Standard
ftp	File Transfer Protocol	Standard
kernel	Kernel	Standard
local0 to local7	Locally defined messages	Standard (local7 is the default)
lpr	Line printer system	Standard
mail	Mail system	Standard
news	USENET news	Standard
syslog	Internal system messages	Standard
user	User process	Standard
uucp	UNIX-to-UNIX Copy Program	Standard

Displaying System Message Logging Information

Use the **show logging** command to display the current system message logging configuration. (See Examples 14-1 to 14-7.)

Example 14-1 Displays Current System Message Logging

```
switch# show logging
Logging monitor:                 disabled
Logging server:                  disabled
Logging logfile:                 enabled (Severity: information)

Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
fcns                    6                       6
fcs                     6                       6
zone                    6                       6
auth                    6                       6
ipconf                  6                       6
module                  6                       6
ntp                     6                       6
sysmgr                  6                       6
user                    6                       6
port                    6                       6
fcdomain                6                       6
fspf                    6                       6
[1][Fri Jan 21 17:50:12.072 UTC 2005][I][8400.0001][Switch][Modifying configured DomainID
1 to negotiated value 97]
[2][Fri Jan 21 17:50:18.629 UTC 2005][A][1005.0040][Port: 1][Unsupported SFP within port.]
[3][Fri Jan 21 17:50:18.662 UTC 2005][A][1005.0040][Port: 2][Unsupported SFP within port.]
[4][Fri Jan 21 18:47:27.879 UTC 2005][I][8400.0023][Switch][Successful login user
(admin@OB-session4) with admin privilege from address 10.0.0.254]
[5][Fri Jan 21 19:24:27.097 UTC 2005][I][8400.0023][Switch][Successful login user
(maint@OB-session5) with admin privilege from address 10.0.0.254]
...
```

Example 14-2 Displays the Log File

```
switch# show logging logfile
Jul 16 21:06:50 %DAEMON-3-SYSTEM_MSG: Un-parsable frequency in /mnt/pss/ntp.drift
Jul 16 21:06:56 %DAEMON-3-SYSTEM_MSG: snmpd:snmp_open_debug_cfg: no snmp_saved_dbg_uri ;
Jul 16 21:06:58 172.22.91.204 %PORT-5-IF_UP: Interface mgmt0 is up
Jul 16 21:06:58 172.22.91.204 %MODULE-5-ACTIVE_SUP_OK: Supervisor 5 is active
...
```

Example 14-3 Displays Logging Facility

```
switch# show logging level

Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
fcns                    6                       2
fcs                     6                       2
zone                    6                       2
auth                    6                       2
ipconf                  6                       2
module                  6                       2
ntp                     6                       2
sysmgr                  6                       2
user                    6                       2
port                    6                       2
fcdomain                6                       2
fspf                    6                       2
```

Example 14-4 Displays Logging Information

```
switch# show logging info
Logging monitor:                disabled
Logging server:                 disabled
Logging logfile:                enabled (Severity: critical)

Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
fcns                    6                       2
fcs                     6                       2
zone                    6                       2
auth                    6                       2
ipconf                  6                       2
module                  6                       2
ntp                     6                       2
sysmgr                  6                       2
user                    6                       2
port                    6                       2
fcdomain                6                       2
fspf                    6                       2
```

Example 14-5 Displays Last Few Lines of a Log File

```
switch# show logging last 2
[7][Fri Jan 21 22:45:07.672 UTC 2005][I][8400.0023][Switch][Successful login user
(admin@OB-session3) with admin privilege from address 10.0.0.254]
[8][Fri Jan 21 22:49:06.768 UTC 2005][I][8400.0023][Switch][Successful login user
(maint@OB-session4) with admin privilege from address 10.0.0.254]
```

Example 14-6 Displays Monitor Logging Status

```
switch# show logging monitor
Logging monitor:                enabled
```

Example 14-7 Displays Server Information

```
switch# show logging server
Logging server:                 disabled
```

Default Settings

Table 14-4 lists the default settings for system message logging.

Table 14-4 Default System Message Log Setting

Parameters	Default
System message logging to the console	Enabled for messages at the critical severity level.
System message logging to Telnet sessions	Disabled.
Logging file size	1200 entries.
Log file name	Message (change to a name with up to 200 characters).
Logging server	Disabled.
Syslog server IP address	Not configured.
Number of servers	Three servers.
Server facility	Local 7.

CHAPTER 15

Advanced Features and Concepts

This chapter describes the advanced features provided in the Cisco MDS 9020 Fabric Switch. It includes the following sections:

Fibre Channel Time Out Values

You can modify Fibre Channel protocol related timer values for the switch by configuring the following time out values (TOVs):

- Distributed services TOV (D_S_TOV)—The valid range is from 5,000 to 10,000 milliseconds. The default is 5,000 milliseconds.
- Error detect TOV (E_D_TOV)—The valid range is from 1,000 to 10,000 milliseconds. The default is 2,000 milliseconds. This value is matched with the other end during port initialization.
- Resource allocation TOV (R_A_TOV)—The valid range is from 5,000 to 10,000 milliseconds. The default is 10,000 milliseconds. This value is matched with the other end during port initialization.

Note The fabric stability TOV (F_S_TOV) constant cannot be configured.

Timer Configuration

You can modify Fibre Channel protocol related timer values for the switch.

To configure FC timers, perform this task:

	Command	Purpose
Step 1	`switch# config t` `switch(config)`	Enters configuration mode.
Step 2	`switch(config)# fctimer R_A_TOV 6000`	Configures the R_A_TOV value to be 6000 ms.

Displaying Configured FC Timer Values

Use the **show fctimer** command to display the configured FC timer values (see Example 15-1).

Example 15-1 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
```

Note The F_S_TOV constant, though not configured, is displayed in the output of the **show fctimer** command.

The show tech-support Command

The **show tech-support** command is useful when collecting a large amount of information about your switch for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem.

The **show tech-support** command displays the output of several **show** commands at once. The output from this command varies depending on your configuration. Use the **show tech-support** command in EXEC mode to display general information about the switch when reporting a problem.

You can choose to have detailed information for each command or even specify the output for a particular interface. Each command output is separated by line and the command precedes the output.

Note Explicitly set the **terminal length** command to 0 (zero) to disable auto-scrolling and enable manual scrolling. Use the **show terminal** command to view the configured the terminal size. After obtaining the output of this command, remember to reset you terminal length as required (see the "Setting the Terminal Length" section on page 2-16).

Tip You can save the output of this command to a file named dump_support.tgz and send it to a remote host by entering the **show tech-support create** command. If you save this file, verify you have sufficient space to do so. Each of these files may take about 1.8 MB.

The default output of the **show tech-support** command includes the output of the following commands:

- **show version**
- **show environment**
- **show module**
- **show hardware**
- **show running-config**
- **show interface**
- **show accounting log**
- **show processes**

Each command is discussed in Appendix A, "Command Reference." Refer to the *Cisco MDS 9000 Family Troubleshooting Guide* to obtain debug processes, procedures, and examples.

The show tech-support brief Command

Use the **show tech-support brief** command to obtain a quick, condensed review of your switch configurations. This command provides a summary of the current running state of the switch.

The **show tech-support brief** command is useful when collecting information about your switch for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem. Example 15-2 shows an example of the **show tech-support brief** command.

Example 15-2 Displays the Condensed View of Switch Configurations

```
switch# show tech-support brief
CMD: show fcs database
  ---

FCS Local Database
------------------
Switch WWN          : 1000000dec19cb0e
Switch Domain Id    : 105
Fabric-Name         :
Switch Logical-Name : switch
Switch Ports:
-----------------------------------------------------------------
Interface  fWWN                     Type     Attached-pWWNs
-----------------------------------------------------------------
fc1/1      20:00:00:0d:ec:19:cb:0e  Unknown  None
fc1/2      20:01:00:0d:ec:19:cb:0e  Unknown  None
fc1/3      20:02:00:0d:ec:19:cb:0e  Unknown  None
fc1/4      20:03:00:0d:ec:19:cb:0e  Unknown  None
fc1/5      20:04:00:0d:ec:19:cb:0e  Unknown  None
fc1/6      20:05:00:0d:ec:19:cb:0e  Unknown  None
fc1/7      20:06:00:0d:ec:19:cb:0e  Unknown  None
fc1/8      20:07:00:0d:ec:19:cb:0e  Unknown  None
fc1/9      20:08:00:0d:ec:19:cb:0e  Unknown  None
fc1/10     20:09:00:0d:ec:19:cb:0e  Unknown  None
fc1/11     20:0a:00:0d:ec:19:cb:0e  Unknown  None
fc1/12     20:0b:00:0d:ec:19:cb:0e  Unknown  None
fc1/13     20:0c:00:0d:ec:19:cb:0e  Unknown  None
fc1/14     20:0d:00:0d:ec:19:cb:0e  Unknown  None
fc1/15     20:0e:00:0d:ec:19:cb:0e  Unknown  None
fc1/16     20:0f:00:0d:ec:19:cb:0e  Unknown  None
```

```
fc1/17     20:10:00:0d:ec:19:cb:0e  Unknown  None
fc1/18     20:11:00:0d:ec:19:cb:0e  Unknown  None
fc1/19     20:12:00:0d:ec:19:cb:0e  Unknown  None
fc1/20     20:13:00:0d:ec:19:cb:0e  Unknown  None

  CMD: show version
  ---

Cisco MDS 9000 FabricWare
Copyright (C) 2002-2005, by Cisco Systems, Inc.
and its suppliers.  All rights reserved.
Copyrights to certain works contained herein are owned by
third parties, and used and distributed under license.
Portions of this software are governed by the GNU Public Licen
which is available at http://www.gnu.org/licenses/gpl.html.

Software
  system:   2.1(2)
  system compile time:   Thu Apr 21 12:48:49 2005

Hardware
  switch uptime is 0 days 11 hours 14 minute(s) 0 second(s)

  Last reset at 40440 usecs after Mon Apr 25 11:01:12 2005
    Reason: PowerUp

  CMD: show interface brief
  ---

--------------------------------------------------------------
Interface  Admin       Status            FCOT  Oper     Oper
           Mode                               Mode     Speed
                                                       (Gbps)
--------------------------------------------------------------
fc1/1      auto        down              lwl    --
fc1/2      auto        down              swl    --
fc1/3      auto        down              --     --
fc1/4      auto        down              --     --
fc1/5      auto        down              --     --
fc1/6      auto        down              --     --
fc1/7      auto        down              --     --
fc1/8      auto        down              --     --
fc1/9      auto        down              swl    --
fc1/10     auto        down              --     --
fc1/11     auto        down              --     --
fc1/12     auto        down              --     --
fc1/13     auto        down              unk    --
fc1/14     auto        down              --     --
fc1/15     auto        down              --     --
fc1/16     auto        down              swl    --
fc1/17     auto        down              --     --
fc1/18     auto        down              --     --
fc1/19     auto        down              --     --
fc1/20     auto        down              elec   --

-----------------------------------------------
Interface               Status     IP Address
-----------------------------------------------
mgmt0                   up         10.20.83.122
```

The show tech-support create Command

Use the **show tech-support create** command creates a file (dump_support.tgz) in the volatile: file system containing a summary of your switch configurations and sends the file to a remote host. Example 15-3 shows an example of the **show tech-support create** command, creating and sending the file to the host address 10.20.33.130 under the user account soper1.

Example 15-3 Creating and Sending a Support File

```
switch # show tech-support create
This may take several seconds...
FTP the dump support file to another machine? (y/n) : y
Enter IP Address of remote computer: 10.20.33.130
Login name: soper1
Enter a valid remote directory path within the user's home directory.
Otherwise the file will be place in the user's home directory:
Would you like to continue downloading support file? (y/n) : y
Connected to 10.20.33.130 (10.20.33.130).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
331 Password required for soper1.
Password:
230 User soper1 logged in.
cd /itasca/conf/images
Local directory now /itasca/conf/images
bin
200 Type set to I.
put dump_support.tgz
local: dump_support.tgz remote: dump_support.tgz
227 Entering Passive Mode (10,20,33,130,144,7)
150 Opening BINARY mode data connection for dump_support.tgz.
226 Transfer complete.
75614 bytes sent in 0.00731 secs (1e+04 Kbytes/sec)
Remote system type is UNIX.
Using binary mode to transfer files.
221-You have transferred 75614 bytes in 1 files.
221-Total traffic for this session was 76026 bytes in 1 transfers.
221 Thank you for using the FTP service on localhost.localdomain.
```

Default Settings

Table 15-1 lists the default settings for the features included in this chapter.

Table 15-1 Default Settings for Advanced Features

Parameters	Default
D_S_TOV	5,000 milliseconds.
E_D_TOV	2,000 milliseconds.
R_A_TOV	10,000 milliseconds.

CHAPTER 16

Monitoring System Processes and Logs

This chapter provides details on monitoring the health of the switch. It includes the following sections:

Displaying System Processes

Use the **show processes** command to obtain general information about all processes (see Example 16-1 to Example 16-3).

Example 16-1 Displays System Processes

```
switch# show processes
PID PPID %CPU TIME ELAPSED      COMMAND
163 141  0.0  00:00:00 16:23:32 cns
164 141  0.0  00:00:00 16:23:32 ens
169 141  0.0  00:00:00 16:23:32 dlog
170 141  0.0  00:00:04 16:23:32 ds
171 141  0.0  00:00:01 16:23:32 mgmtApp
172 141  0.0  00:00:00 16:23:32 sys2swlog
173 141  0.0  00:00:00 16:23:32 fc2
174 141  0.0  00:00:00 16:23:32 nserver
175 141  0.0  00:00:00 16:23:32 mserver
176 141  0.0  00:00:00 16:23:32 util
177 141  0.0  00:00:01 16:23:32 snmpservicepath
178 141  0.0  00:00:00 16:23:31 eport
179 141  0.0  00:00:00 16:23:31 PortApp
180 141  0.0  00:00:00 16:23:31 port_mon
181 141  0.0  00:00:00 16:23:31 zoning
182 141  0.0  00:00:00 16:23:31 diagApp
241 141  0.0  00:00:00 16:23:18 snmpd
242 141  0.0  00:00:00 16:23:18 snmpmain
244 242  0.0  00:00:00 16:23:17 snmpmain
245 244  0.0  00:00:00 16:23:17 snmpmain
```

Where:

- PID = process ID
- PPID=arent process identification number
- %CPU=CPU utilization in percentage for the last one second
- TIME ELAPSED=elapsed time
- COMMAND=name of the process

Example 16-2 Displays Process Log Information

```
switch# show processes log
Process                 Log-create-time
----------------------  ---------------
backtrace-clishco       Tue Apr 26 18:45:39 2005
```

Where:

- Process = name of the process
- Log-create-time = when the log file was generated

Example 16-3 Displays All Process Log Details

```
switch# show processes log details
================================================
Service          : backtrace-clishco
Modification time: Tue Apr 26 18:45:39 2005
----------------------------------------
  *** Segmentation fault
  Register dump:
  fp0-3:   00000008000704e0 0000000000000000 0000000000000000 0000000000000000
  fp4-7:   0000000000000000 0000000000000000 0000000000000000 0000000000000000
  fp8-11:  0000000000000000 0000000000000000 0000000000000000 0000000000000000
  fp12-15: 0000000000000000 0000000000000063 0000000000000000 0000000000000000
  fp16-19: 0000000000000000 0000000000000000 0000000000000000 0000000000000000
  fp20-23: 0000000000000000 0000000000000000 0000000000000000 0000000000000000
  fp24-27: 0000000000000000 0000000000000000 0000000000000000 0000000000000000
  fp28-31: 0000000000000000 0000000000000000 0000000000000000 0000000000000000
  r0 =00000000 sp =7fffba50 r2 =00000000 r3 =65727665  trap=00000300
  r4 =1011739c r5 =1026a2f0 r6 =00000000 r7 =00000000   sr0=0faacecc sr1=0000d032
  r8 =000000b8 r9 =0fb6b11c r10=7fffcbd9 r11=10030be0   dar=65727661 dsi=20000000
  r12=4400286c r13=1027bdc0 r14=00000000 r15=00000000   r3*=00000003
  r16=00000000 r17=00000000 r18=00000000 r19=00000000
  r20=00000000 r21=00000000 r22=7fffbf28 r23=7fffbea8    lr=0fb68ed8 xer=00000000
  r24=7fffbfa8 r25=7fffbcd8 r26=7fffbc58 r27=00000000    mq=c0160000 ctr=10030aac
  r28=00000001 r29=00000000 r30=0fb68ed8 r31=6572765d  fscr=00000000 ccr=42002860
    Backtrace:
  /lib/libc.so.6(__libc_free+0x68)[0xfaacecc]
  /lib/libstdc++.so.5(_ZdlPv+0x18)[0xfcdec5c]
  /lib/libstdc++.so.5(_ZdaPv+0x10)[0xfcdeca4]
  -clishco[0x10030b14]
  -clishco[0x1001ae98]
  /itasca/lib/libMgmtapi.so(_ZN7mgmtApi8recv_msgEP11Hsb_Message+0x138)[0xff91d3c]
  /itasca/lib/libswbApi.so(_ZN11Hsb_Handler4recvEP11Hsb_Message+0x94)[0xffd383c]
  /itasca/lib/libswbApi.so(_ZN13Vpipe_Handler12handle_inputEi+0xc8)[0xffdaae8]
  /itasca/lib/libswbApi.so(_ZN10Dispatcher12dispatch_setERi6fd_seti+0x144)[0xffcfbc0]
  /itasca/lib/libswbApi.so(_ZN10Dispatcher8dispatchEi6fd_setS0_S0_+0x98)[0xffcf9cc]
  /itasca/lib/libswbApi.so(_ZN10Dispatcher13handle_eventsEP7timeval+0x208)[0xffd0138]
  /itasca/lib/libswbApi.so(_ZN3Hsb13handle_eventsEP7timeval+0x20)[0xffd07c4]
  -clishco[0x100150ac]
```

```
-clishco[0x10014db0]
/lib/libc.so.6(__libc_start_main+0x19c)[0xfa5456c]

Process Status:
Name: clishco
State:        R (running)
Tgid: 302
Pid:  302
PPid: 301
TracerPid:    0
Uid:  10003   10003   10003   10003
Gid:  1000    1000    1000    1000
FDSize:       32
Groups:       1000
VmSize:          24132 kB
VmLck:               0 kB
VmRSS:            2528 kB
VmData:            360 kB
VmStk:              56 kB
VmExe:               0 kB
VmLib:            2488 kB
SigPnd:       0000000000000000
SigBlk:       0000000000000400
SigIgn:       0000000000080000
SigCgt:       00000000000014e2
CapInh:       0000000000000000
CapPrm:       0000000000000000
CapEff:       0000000000000000
```

Displaying System Status

Use the **show system** command to display system-related status information (see Example 16-4 and Example 16-5.

Example 16-4 Displays the System Reset Information

```
switch# Show system reset-reason
----- reset reason for module 1 -----
1) At 215435 usecs after Mon Apr 25 11:01:12 2005
    Reason: PowerUp
```

The **show system reset-reason** command displays the last reset-reason code.

Example 16-5 Displays System Uptime

```
switch# show system uptime
System Start Time:          Mon Apr 25 11:01:12 2005
System Up Time:             0 days, 10 hours, 58 minutes, 38 seconds
Active Supervisor Up Time:  0 days, 10 hours, 58 minutes, 38 seconds
```

APPENDIX A

Command Reference

The commands in this appendix apply to the Cisco MDS 9020 Fabric Switch. 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.

cd

To change the default file system, use the **cd** command in EXEC mode.

cd [**bootflash:** | **volatile:**]

Syntax Description

bootflash:	Flash image on the non-volatile file system.
volatile:	Flash image on the volatile file system.

Defaults

bootflash:

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following example changes the file system to the bootflash: file system and displays the contents.

```
switch# cd bootflash:

switch# dir
        656     Apr 25 22:04:33 2005  running-config

Usage for bootflash://
14336       bytes used
2668544     bytes free
2682880     bytes total
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.

clear counters interface

To clear the interface counters, use the **clear counters interface** command in EXEC mode.

clear counters interface {all | fc 1/*port***}**

Syntax Description

all	Clears all interface counters.
fc	Fibre Channel interface for which to clear counters.
1/*port*	Specifies slot 1 and the port number. The port number is in the range 1 to 20.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

The following table lists the keywords and number ranges for the **clear counters** interface types:

Keyword	Interface Type	Number
1/*port*	Fibre Channel	1/1 to 1/20

This command clears counters displayed in the **show interface** command output.

Examples

The following is an example of how to clear counters for a Fibre Channel interface 1/3:

```
switch# clear counters interface fc 1/3
```

Related Commands

Command	Description
show interface	Displays interface information.

clear fspf counters

To clear the Fabric Shortest Path First statistics, use the **clear fspf counters** command in EXEC mode.

clear fspf counters [**interface fc 1/***port*]

Syntax Description

interface fc	(Optional) Fibre Channel interface.
1/*port*	FC interface number where the slot number is 1 and the interface number is the port number in the range 1 to 20.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

If the interface is not specified, then all of the FC interface counters are cleared. If the interface is specified, then the counters of the specific interface are cleared.

Examples

The following example clears FSPF statistics specific to Fibre Channel interface 1/3.

```
switch#  clear fspf counters interface fc 1/3
```

Related Commands

Command	Description
show fspf	Displays global FSPF information.

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

No default behavior or values.

Command Modes

EXEC.

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

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 zone database

To clear all configured information in the zone server, use the **clear zone database** command in EXEC mode.

clear zone database

SyntaxDescription

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

After entering a **clear zone database** command, you need to explicitly enter the **copy running-config startup-config** command to ensure that the running configuration is used when you next start the switch.

Examples

The following example shows how to clear all configured information in the zone server.

```
switch# clear zone database
```

Related Commands

Command	Description
show zone	Displays zone information for any configured interface.

clock

To configure the time zone and summer-time-of-day (daylight savings), use the **clock** command in configuration mode.

clock
{summer-time *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* **|**
time-zone *timezone-name hours-offset minutes-offset***}**

To disable the daylight savings time adjustment or to set the time zone to the default, use the no form of this command.

no clock {summer-time | time-zone}

Syntax Description

summer-time	Configures daylight savings time.
daylight-timezone-name	Time zone name. The time zone name has a maximum of 8 characters.
start-week *end-week*	The week-of-the-month ranging from 1 through 4; 5 specifies the last week of the month.
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 in HH:MM:SS format.
daylight-offset-to-be-added-in-minutes	The daylight offset ranges from 1 through 1440 minutes that will be added to the start time and deleted from the end time.
time-zone	Sets the time zone.
timezone-name	Time zone name. The time zone name has a maximum of 8 characters.
hours-offset	Hours offset from Coordinated Universal Time (UTC) ranging from -23 to 23.
minutes-offset	Minutes offset from the hour ranging from -59 to 59.

Defaults

The default time zone is Coordinated Universal Time (UTC), which is the same as Greenwich Mean Time (GMT).

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following example adjusts the daylight savings time for the Pacific time zone by 60 minutes starting on the first Sunday in April at 2 a.m. and ending on the last Sunday in October at 2 a.m.

```
switch# config
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 time on the switch.
show clock	Displays the current date and time.
show running-config	Displays changes made to the time zone configuration along with other configuration information.

clock set

To change the system time, 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

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

If the system is synchronized with an NTP clock server, 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 15 August 2005
Mon Aug 15 15:58:00 PDT 2005
```

config terminal

To enter the configuration mode, use the **config** command in EXEC mode.

config terminal

Syntax Description

This command had no arguments or keywords.

Defaults

None.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following example enters the configuration mode:

```
switch# config terminal
Enter configuration commands, one per line.
switch(config)#
```

The following example enters the configuration mode using an abbreviated format of the command:

```
switch# config
Enter configuration commands, one per line.
switch(config)#
```

copy

To save a backup of the system software, use the **copy** command in EXEC mode.

copy *source destination*

Syntax Description

source	Location URL or name of the source file to be copied. Source file systems can be **bootflash:**, **running-config**, **startup-config**, and **volatile:**.
destination	Location URL or name of the copied file. Destination file systems can be **bootflash:**, **ftp:**, **running-config**, **startup-config**, **tftp:**, and **volatile:**

The following table lists the aliases for source and destination URLs.

bootflash:	Specifies the switch non-volatile file system. The syntax for this alias is **bootflash:***filename*
filename	The name of the file.
ftp:	Specifies the location for a File Transfer Protocol (FTP) network server. The syntax for this alias is **ftp:**[[*//location*]*/directory*]*/filename*.
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 bootflash. The **bootflash:startup-config** keyword represents the configuration file used during initialization.
tftp:	Specifies the location for a Trivial File Transfer Protocol (TFTP) network server. The syntax for this alias is **tftp:**[[*//location*]*/directory*]*/filename*.
volatile:	Specifies the location for the volatile file system. The syntax for this alias is **volatile:***filename*

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

This command be used to make the running and the backup copy of the configuration identical.

The copy function will not be completed if the required space is not available in the file system. First change to the required file system (for example, **cd bootflash:**) and verify the available space (for example, **dir bootflash:**).

Examples

The following example saves your configuration to the startup configuration.

```
switch# copy running-config startup-config
```

The following example creates a snapshot of the current running configuration.

```
switch# copy running-config bootflash:running-snapshot
```

The following example saves a backup copy of the startup configuration.

```
switch# copy startup-config bootflash:startup-backup
```

The following example saves a copy of the startup configuration on a remote host.

```
switch# copy startup-config ftp://10.20.102.98/configs/q100-startup
```

Related Commands

Command	Description
cd	Changes the default file system.
dir	Displays a list of files on a file system.
reload	Resets the switch.
show version	Displays the version of the running configuration file.
move	Moves a file to another filename.

delete

To delete a file, use the **delete** command in EXEC mode.

delete {**bootflash:***filename* | **volatile:***filename*}

Syntax Description

bootflash:	Flash image that resides on the non-volatile file system.
volatile:	Flash image that resides on the volatile file system.
filename	The name of the file to be deleted.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

When you delete a file, the software erases the file.

Caution If you move to a specific file system with the **cd** command and enter the **delete** command, all files in the file system will be deleted.

Examples

The following example deletes a file from the volatile file system.

```
switch# delete volatile:my_file
```

Related Commands

Command	Description
cd	Changes the default file system.
dir	Displays a list of files on a file system.
move	Moves a file to another filename.

dir

To display the contents of the current file system or the specified file system, use the **dir** command in EXEC mode.

dir [bootflash:*filename* | **volatile:***filename*]

Syntax Description

bootflash:	The non-volatile file system.
filename	(Optional) Name of the file to display on a specified file system. 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:	The volatile file system.

Defaults

The default file system is specified by the **cd** command.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following example shows how to list the files on the volatile file system.

```
switch# dir volatile:
       1446     Apr 04 20:08:06 2005  image_0
       1446     Apr 04 20:09:34 2005  image_1
       1446     Apr 04 20:09:32 2005  image_2
       1446     Apr 04 20:09:30 2005  image_3
       1446     Apr 04 20:09:28 2005  ilc1.bin
       1446     Apr 04 20:09:27 2005  startup-con_1
       1446     Apr 04 20:09:24 2005  startuup-con_2
       1446     Apr 04 20:09:22 2005  startuup-con_3
       1446     Apr 04 20:09:20 2005  startuup-con_4
       1446     Apr 04 20:10:43 2005  zzzffp

Usage for volatile://
      40960 bytes used
   20930560 bytes free
   20971520 bytes total
```

Related Commands

Command	Description
cd	Changes the default file system.

do

Use the **do** command to execute an EXEC mode command from any configuration mode or submode.

do *command*

Syntax Description

command	Specifies the EXEC command to be executed.

Defaults

No default behavior or values.

Command Modes

All

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

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 entered the **do** command.

Examples

The following example displays the logging levels using the **do** command in configuration mode.

```
switch(config)# do show logging level

Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
fcns                    6                       2
fcs                     6                       2
zone                    6                       2
auth                    6                       2
ipconf                  6                       2
module                  6                       2
ntp                     6                       2
sysmgr                  6                       2
user                    6                       2
port                    6                       2
fcdomain                6                       2
fspf                    6                       2
```

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 had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

None.

Examples

The following example sets the time zone to GMT. Entering the **end** command causes the system to exit configuration mode and return to EXEC mode.

```
switch(config)# clock timezone
george(config)# end
switch#
```

Related Commands

Command	Description
exit	Exits configuration mode, or any of the configuration modes.

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 had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

All.

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

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 submode to return to configuration mode. You also use the **end** command, from any configuration mode to return to EXEC mode.

Examples

The following example displays an exit from the interface configuration submode to return to the configuration mode.

```
switch(config-if)# exit
switch(config)#
```

The following example shows how to log out of an active session.

```
switch# exit
```

Related Commands

Command	Description
end	Returns you to EXEC mode.

fcalias name

To configure an FC alias, use the **fcalias name** command in configuration mode.

fcalias name *alias-name*

Entering the **fcalias name** command opens the config-fcalias submode which provides access to the **member** subcommand:

member pwwn *pwwn-id*

To disable an FC alias, use the **no** form of this command.

no fcalias name *alias-name*

Syntax Description

alias-name	The name of the fcalias. Maximum length is 64 characters. This opens the config-fcalias submode.
member	Adds a member to the fcalias. This command is available only in the config-fcalias submode.
pwwn *pwwn-id*	Adds a member using the port WWN in the format *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.

Defaults

No default behavior or values.

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

To include multiple members in any alias, use the pWWN value.

Examples

The following examples show how to configure an FC alias called AliasSample.

```
switch# config
switch(config)# fcalias name AliasSample
switch(config-fcalias)#
```

Related Commands

Command	Description
fcalias rename	Renames an FC alias.

fcalias rename

To rename an FC alias, use the **fcalias rename** command in configuration mode.

fcalias rename *current-name new-name*

Syntax Description

current-name	The current name of the fcalias.
new-name	The new name of the fcalias. Maximum length is 64 characters.

Defaults

No default behavior or values.

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following examples show how to rename an fcalias called AliasSample.

```
switch# config
switch(config)# fcalias rename AliasSample AliasNew
switch(config-fcalias)#
```

Related Commands

Command	Description
fcalias name	Configures an FC alias.

fcdomain

To configure the Fibre Channel domain feature, use the **fcdomain** command in configuration mode.

fcdomain {**domain** *id* {**preferred | static**} **priority** *value* | **restart** [**disruptive**]}

To disable the FC domain, use the **no** form of this command.

no fcdomain {**domain** *id* {**preferred | static**} **priority** *value* | **restart** [**disruptive**]}

Syntax Description

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.
priority *value*	Specifies the FC domain priority. The range is 1 to 254.
restart	Restarts a disruptive or nondisruptive reconfiguration.
disruptive	Forces the disruptive fabric reconfiguration.

Defaults

Enabled.

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

You can use this command to select the principle switch, domain ID distribution, reconfigure fabric, and allocate FC IDs.

Examples

The following examples show how to configure the Fibre Channel domain feature.

```
switch# config

switch(config)# fcdomain domain 3 preferred

switch(config)# no fcdomain domain 3 preferred

switch(config)# fcdomain domain 2 static

switch(config)# no fcdomain domain 2 static

switch(config)# fcdomain restart

switch(config)# fcdomain restart disruptive
```

```
switch(config)# fcdomain priority 25

switch(config)# no fcdomain priority 25
```

Related Commands

Command	Description
show fcdomain	Displays global information about the FC domain configurations.

fctimer

To change the default Fibre Channel timers, use the **fctimer** command in configuration mode.

fctimer {**d_s_tov** *milliseconds* | **e_d_tov** *milliseconds* | **r_a_tov** *milliseconds*}

To revert to the default values, use the **no** form of this command.

no fctimer {**d_s_tov** *milliseconds* | **e_d_tov** *milliseconds* | **r_a_tov** *milliseconds*}

Syntax Description

d_s_tov *milliseconds*	Specifies the distributed services time out value. The range is 5000 to 100,000 milliseconds, with a default of 5000.
e_d_tov *milliseconds*	Specifies the error detect time out value. The range is 1000 to 100,000 milliseconds, with a default of 2000.
r_a_tov *milliseconds*	Specifies the resolution allocation time out value. The range is 5000 to 100,000 milliseconds, with a default of 10,000.

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

In accordance with the FC-SW2 standard, the timeout values must be the same on each switch in the fabric.

Examples

The following example shows how to change the default Fibre Channel timers.

```
switch# config
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.

fspf cost

To configure FSPF link cost for an interface, use the **fspf cost** command in interface configuration submode.

fspf cost *link-cost*

To revert to the default value, use the **no** form of this command.

no fspf cost *link-cost*

Syntax Description

link-cost	Enters FSPF link cost. The range is 1 to 65,535.

Defaults

1000 for 1 Gbps

500 for 2 Gbps

250 for 4 Gbps

Command Modes

Interface configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

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 shows how to set the FSPF link cost to 5000.

```
switch# config
switch(config)# interface fc1/1
switch(config-if)# fspf cost 5000
```

Related Commands

Command	Description
show fspf interface	Displays information for each selected 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 in interface configuration submode.

fspf dead-interval *seconds*

To revert to the default value, use the **no** form of this command.

no fspf dead-interval *seconds*

Syntax Description

seconds	Specifies the FSPF dead interval in seconds. The range is 2 to 65,535.

Defaults

80 seconds

Command Modes

Interface configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

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

```
switch# config
switch(config)# interface fc1/1
switch(config-if)# fspf dead-interval 4000
```

Related Commands

Command	Description
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 in interface configuration submode.

fspf hello-interval *seconds*

To revert to the default value, use the **no** form of this command.

no fspf hello-interval *seconds*

Syntax Description

seconds	Specifies the FSPF hello-interval in seconds. The range is 1 to 65,535.

Defaults

20 seconds

Command Modes

Interface configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

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

This command configures FSPF for the specified FC interface.

Note This value must be the same in the ports at both ends of the ISL.

Examples

```
switch# config
switch(config)# interface fc1/1
switch(config-if)# fspf hello-interval 3
```

Related Commands

Command	Description
show fspf interface	Displays information for each selected 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 in interface configuration submode.

fspf retransmit-interval *seconds*

To revert to the default value, use the **no** form of this command.

no fspf retransmit-interval *seconds*

Syntax Description

seconds	Specifies FSPF retransmit interval in seconds. The range is 1 to 4093.

Defaults

5 seconds

Command Modes

Interface configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

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

```
switch# config
switch(config)# interface fc 1/1
switch(config-if)# fspf retransmit-interval 6
```

Related Commands

Command	Description
show fspf interface	Displays information for each selected interface.

help

To display a list of available commands and arguments in the current command mode, use the **?** command in any mode. No carriage return is needed with this command.

?

command ?

command argument ?

Syntax Description

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

All

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

The **?** command alone displays available commands based on the command mode.

To display the arguments for a command, enter the command name, then a space, then the **?** command.

To display the keywords for an argument, enter the command, the argument, a space, then the **?** command.

Examples

The following example displays the list of commands for EXEC mode.

```
switch# ?
  cd                        Change current directory
  clear                     Reset functions
  clock                     Manage the system clock
  config                    Enter configuration mode
  copy                      Copy from one file to another
  delete                    Delete a file
  dir                       List files in a directory
  exit                      Exit from the EXEC
  help                      Press '?' key to display available commands
  install                   Upgrade software
  move                      Move files
  ping                      Send echo messages
  reload                    Reboot the entire box
  run-script                Run shell scripts
  setup                     Run the basic SETUP command facility
  show                      Show running system information
  sleep                     Sleep for the specified number of seconds
  system                    System management commands
  terminal                  Set terminal line parameters
  write                     Write current configuration
  zone                      Execute zone server commands
  zoneset                   Execute zoneset commands
```

The following example displays the arguments for the **copy** command.

```
switch# copy ?
  bootflash:                Select source filesystem
  ftp:                      Select source filesystem
  running-config            Copy running configuration to destination
  startup-config            Copy startup configuration to destination
  tftp:                     Select source filesystem
  volatile:                 Select source filesystem
```

install all

To upgrade firmware on the switch, use the **install all** command in EXEC mode. The **install all** command will attempt a nondisruptive upgrade; if a nondisruptive upgrade is not possible, a disruptive upgrade will occur.

install all system volatile:*filename*

Syntax Description

system	Upgrades the system image.
volatile:	The volatile file system.
filename	The source file to be installed.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

The firmware image must be downloaded to the volatile file system before it can be installed. Use the **copy ftp:** or **copy tftp:** command to download the firmware image file.

Examples

The following example downloads the firmware image to the volatile file system, installs the firmware, and resets the switch.

```
switch# copy ftp://10.20.102.98/firmware/latest_mpc volatile:latest_mpc
switch# install all system volatile:latest_mpc
Performing configuration copy.
[########################################] 100%

Unpacking image - this may take several seconds...
```

Related Commands

Command	Description
copy	Copies a file from one location to another.
show version	Displays software image version information.

interface fc

To configure a Fibre Channel interface, use the **interface fc** command in configuration mode. This will place the switch in the interface configuration submode.

interface fc 1/*port***[** - *portn***]**

Syntax Description

port	Specifies a port number or the first port number in a range from 1 to 20.
portn	Specifies the second port in the range from 1 to 20.

Defaults

Disabled.

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

You can specify a range of interfaces by entering a command with the following example format:

interface*space***fc***space***1/1***space***-***space***5**

Use the **no shutdown** command to enable the interface.

Examples

The following example configures ports 1 to 4.

```
switch# config
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# int fc 1/1 - 4
```

The following example enables the Fibre Channel interface.

```
switch# config
switch(config)# interface fc 1/1
switch(config-if)# no shutdown
```

Related Commands

Command	Description
show interface	Displays an interface configuration for a specified interface.
shutdown	Disables and enables an interface.

interface mgmt

To configure management interface 0 on a switch, use the **interface mgmt** command in configuration mode.

interface mgmt 0

Syntax Description

0	Management interface 0.

Defaults

Disabled.

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

When you try to shutdown a management interface (mgmt0), a follow-up message confirms your action before performing the operation. Use the **shutdown force** command 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
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
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
switch(config)# interface mgmt 0
switch(config-if)# shutdown force
switch(config-if)#
```

Related Commands

Command	Description
shutdown	Disables and enables an interface.
show interface mgmt	Displays interface configuration for specified interface.

ip access-group

To create an access group to use an access list, use the **ip access-group** command in interface configuration submode.

ip access-group *group-name* **[in | out]**

To negate a previously entered command or revert to factory defaults, use the **no** form of this command.

no ip access-group *group-name* **[in | out]**

Syntax Description

group-name	Specifies the IP access-group name. 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

Groups are created for both ingress and egress traffic.

Command Modes

Interface configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

The **access-group** command controls access to an interface. Each interface can only be associated with one access list. The access group becomes active on creation.

We recommend creating all rules in an access list, before creating the access group that uses this access list.

If you create an access group before the access-list, 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 create a different access-group for each type of traffic.

Examples

The following example creates an access group called SampleName for both the ingress and egress traffic (default).

```
switch# config
switch(config)# interface mgmt 0
switch(config-if)# ip access-group SampleName
```

The following example deletes the access group called NotRequired.

```
switch(config-if)# no ip access-group NotRequired
```

The following example creates an access group called SampleName (if it does not already exist) for ingress traffic.

```
switch(config-if)# ip access-group SampleName1 in
```

The following example deletes the access group called SampleName for ingress traffic.

```
switch(config-if)# no ip access-group SampleName1 in
```

The following example creates an access group called SampleName (if it does not already exist) for local egress traffic.

```
switch(config-if)# ip access-group SampleName2 out
```

The following example deletes the access group called SampleName for local egress traffic.

```
switch(config-if)# no ip access-group SampleName2 out
```

Related Commands

Command	Description
interface mgmt	Configures the management interface and opens the config-if submode.
ip access-list	Creates IP access control lists.
show ip access-list	Displays the IP-ACL configuration information.

ip access-list

To configure IP access control lists (ACL), use the **ip access-list** command in configuration mode. The first **ip access-list** command entry creates the ACL. Subsequent **ip access-list** command entries add filters to the ACL definition.

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*]

To negate a previously entered command or revert to factory defaults, use the **no** form of this command.

no 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*]

Syntax Description

list-name	Identifies the access control list. *list-name* is case sensitive and the maximum length is 64 alphanumeric characters.
deny	Denies access if the conditions match.
permit	Provides 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 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 IP address must exactly match the bit value in the corresponding position of the packet IP address. 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 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 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 destination-wildcard of 0.0.0.0 255.255.255.255
operator	Compares source or destination ports 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 (range from 0 to 65,535) 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)

Defaults

Denied.

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following example configures an IP-ACL called List1 and permits IP traffic from any source address to any destination address.

```
switch# config
switch(config)# ip access-list List1 permit ip any any
```

The following example removes the IP-ACL called List1.

```
switch# config
switch(config)# no ip access-list List1 permit ip any any
```

The following example updates List1 to deny TCP traffic from any source address to any destination address.

```
switch# config
switch(config)# ip access-list List1 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
switch(config)# ip access-list List1 permit udp 192.168.32.0 0.0.7.255
```

The following example permits all IP traffic from and to the specified networks.

```
switch# config
switch(config)# ip access-list List1 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 10.2.3.0 through source port 5 to any destination.

```
switch# config
switch(config)# ip access-list List2 deny tcp 10.2.3.0 0.0.0.255 eq port 5 any
```

The following example removes this entry from the IP-ACL.

```
switch# config
switch(config)# no ip access-list List2 deny tcp 10.2.3.0 0.0.0.255 eq port 5 any
```

The following example creates an access group called List1 for both the ingress and egress traffic (default).

```
switch# config
switch(config)# interface mgmt0
switch(config-if)# ip access-group List1
```

The following example deletes the access group called NotRequired.

```
switch# config
switch(config)# interface mgmt0
switch(config-if)# no ip access-group NotRequired
```

Related Commands

Command	Description
ip access-group	Creates an IP access group.
show ip access-list	Displays the IP-ACL configuration information.

ip address

To assign an IP address to the Ethernet management port, use the **ip address** command in interface configuration submode. Enter the **interface mgmt** command to open the config-if submode.

ip address *address netmask*

To remove the IP address, us the **no** form of this command.

no ip address *address netmask*

Syntax Description

address	Specifies the IP address.
netmask	Specifies the network mask.

Defaults

The IP address default is 10.0.0.1. The network mask default is 255.0.0.0.

Command Modes

Interface configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

```
switch# config
switch(config)# interface mgmt 0
switch(config-if)# ip address 10.5.1.1 255.255.0.0
```

Related Commands

Command	Description
interface mgmt	Configures the management interface and opens the config-if submode.
show interface	Displays information about an interface.

ip default-gateway

To configure the IP address of the default gateway, use the **ip default-gateway** command in configuration mode.

ip default-gateway *destination-ip-address*

To disable the IP address of the default gateway, use the **no** form of this command.

no ip default-gateway *destination-ip-address*

Syntax Description

destination-ip-address	Specifies the IP address of the default gateway.

Defaults

10.0.0.254

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following examples configures the IP default gateway to 10.1.1.4.

```
switch# config
switch(config)# ip default-gateway 10.1.1.4
```

Related Commands

Command	Description
show ip route	Displays the IP address of the default gateway.

logging level

To modify message logging facilities, use the **logging level** command in configuration mode.

logging level all *severity-level*

To negate the previously entered command or to revert to factory defaults, use the **no** form of this command.

no logging level all *severity-level*

Syntax Description

all	Specifies all message facilities: authorization system, fcdomain syslog, name server, FCS, FSPF syslog, IP configuration, module manager syslog, NTP syslog, port syslog, System Manager syslog, User Process, and zone server.
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 • 7 is debugging

Defaults

The default severity level is critical (2).

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

The switch logs messages at or above the configured severity level.

Examples

Configures the logging level at level 4 (warning). As a result, logging messages with a severity level of 4 or above will be displayed.

```
switch# config
switch(config)# logging level all 4
```

logging monitor

To set monitor message logging, use the **logging monitor** command in configuration mode.

logging monitor *severity level*

To negate the previously entered command or to revert to factory defaults, use the **no** form of the command.

no logging monitor *severity level*

Syntax Description

severity level	Severity level. 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 • 7 is debugging

Defaults

Severity level: 0 - emergency; 1 - alert

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following example sets terminal line (monitor) message logging at level 2.

```
switch# config
switch(config)# logging monitor 2
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

logging server

To set the IP address of the remote message logging server, use the **logging server** command in configuration mode.

logging server *ip address*

To negate the previously entered command or to revert to factory defaults, use the **no** form of this command.

no logging server *ip address*

Syntax Description

ip address	Enters the IP address for the remote server.

Defaults

10.0.0.254

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

Change the IP address of the remote message logging server to 10.20.30.40.

```
switch# config
switch(config)# logging sever 10.20.30.40
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

move

To move a file to another filename, use the **move** command in EXEC mode.

move *source destination*

Syntax Description

source	The source file to be moved. Sources can be **bootflash:***filename* or **volatile:***filename*.
destination	The destination filename. Destinations can be **bootflash:***filename* or **volatile:***filename*
filename	The name of the source or destination file.

Defaults

The default source or destination file system is the current file system, bootflash: or volatile:.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following example moves latest_mpc from the bootflash file system to the volatile file system.

```
switch# move bootflash:latest_mpc volatile:latest_mpc
```

Related Commands

cd	Changes the default file system.
copy	Copies a file to a new location.
dir	Displays a list of files on a file system.

ntp server

To configure a Network Time Protocol (NTP) server, use the **ntp server** command in configuration mode.

ntp server *ip-address*

Syntax Description

ip-address	The IP address of the NTP server.

Defaults

0.0.0.0.

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

This example forms a server association with a server.

```
switch(config)# ntp server 10.10.10.10
switch(config)#
```

ping

To diagnose basic network connectivity, use the **ping** (packet internet groper) command in EXEC mode.

ping *ip-address*

Syntax Description

ip-address	IP address of system to ping.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

The ping 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 system 192.168.7.27.

```
switch# ping 192.168.7.27
PING 192.168.7.27 (192.168.7.27): 10 data bytes
18 bytes from 192.168.7.27: icmp_seq=0 ttl=64 time=0.5 ms

--- 192.168.7.27 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.5/0.5/0.5 ms
```

radius-server host

To configure RADIUS server, use the **radius-server host** command in configuration mode.

radius-server host {*server-name* | *ip-address*}
[**key** *shared-secret*] [**accounting**]
[**auth-port** *port-number*] [**authentication**]
[**retransmit** *count*] [**timeout** *seconds* [**retransmit** *count*]]

To revert to the factory defaults, use the **no** form of this command.

no radius-server host {*server-name* | *ip-address*}
[**key** *shared-secret*] [**accounting**]
[**auth-port** *port-number*] [**authentication**]
[**retransmit** *count*] [**timeout** *seconds* [**retransmit** *count*]]

Syntax Description

server-name	Specifies the RADIUS server DNS name. Maximum length is 256 characters.
ip-address	Specifies the RADIUS server IP address.
auth-port *port-number*	Configures the RADIUS server port for authentication
authentication	Use for authentication.
accounting	Use for accounting.
key	RADIUS server shared key.
shared-secret	Configures a preshared key to authenticate communication between the RADIUS client and server. *shared-secret* must be exactly 16 characters
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.
timeout *seconds*	Specifies the time (in seconds) between retransmissions to the RADIUS server. The default is 1 second and the valid range is 1 to 60 seconds.

Defaults

No default behavior or values.

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following example configures RADIUS server authentication parameters.

```
switch# config t
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 accounting
switch(config)# radius-server host radius2 key abcdefgh01234567
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

reload

To reboot the switch, use the **reload** command in EXEC mode.

reload

Syntax Description

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following example uses the **reload** command to reboot the system.

```
switch# reload
This command will reboot the system. (y/n)? y
```

Related Commands

Command	Description
install	Installs a new software image.
copy	Copies a file from one location to another.

run-script

To execute the commands specified in a file, use the **run-script** command in EXEC mode.

run-script [*filename* | **running-config** | **startup-config** | **volatile:***filename* | **bootflash:***filename*]

Syntax Description

filename	Name of the file containing the commands.
running-config	Specifies the configuration currently running on the switch.
startup-config	Specifies the configuration used during initialization (startup).
volatile:	Location for volatile file system.
bootflash:	Location for the bootflash file system.

Defaults

Uses the current default file system.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

You must create the script file on an external host, then use the **copy ftp** or **copy tftp** command to download the file to the volatile or bootflash file system.

Examples

The file, testfile, contains the following commands:

```
conf t
interface fc 1/1
no shutdown
end
sh interface fc1/1
```

The following example executes the CLI commands specified in the testfile.

```
switch# run-script 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 (Administratively down)
    Hardware is Fibre Channel, SFP is long wave laser
    Port WWN is 20:00:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
```

setup

To enter the switch setup mode, use the **setup** command in EXEC mode.

setup

Syntax Description

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

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 is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

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

Create another login account (yes/no) [n]: yes

    Enter the user login ID: user_name

    Enter the password for user_name: user-password

    Enter the user role [network-operator]:network_admin

Configure read-only SNMP community string (yes/no) [n]: yes

    SNMP community string: snmp_community
```

```
Enter the switch name: switch_name

Continue with Out-of-band (mgmt0) management configuration? [yes/no]: yes

    Mgmt0 IP address: ip_address

    Mgmt0 IP netmask: subnet_mask

Configure the default-gateway: (yes/no) [y]: yes

    IP address of the default-gateway: default_gateway

Enable the telnet service? (yes/no) [y]: yes

Enabled SSH service? (yes/no) [n]: no

Configure NTP server? (yes/no) [n]: no

Configure default switchport interface state (shut/noshut) [shut]: noshut

Configure default zone policy (permit/deny) [deny]: deny

The following configuration will be applied:
username admin password admin_pass role network-admin
switchname switch
interface mgmt0
    ip address ip_address subnet_mask
ip default-gateway 10.0.0.254
telnet server enable
no ssh server enable
no system default switchport shutdown
no zone default-zone permit

Would you like to edit the configuration? (yes/no) [n]: no

Use this configuration and save it? (yes/no) [y]: yes
```

show accounting log

To display the accounting log contents, use the **show accounting log** command in EXEC mode.

show accounting log

Syntax Description

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show accounting log** command.

```
switch# show accounting log
  [1][Mon Apr 25 11:01:59.888 UTC 2005][AU][0000.00FF][None][Zoning Default Zone changed
in Config default to False]
  [2][Mon Apr 25 11:02:03.228 UTC 2005][AU][0000.0001][None][IP Unknown User
admin@OB-session1 User Login]
  [3][Mon Apr 25 11:02:07.376 UTC 2005][AU][0000.0001][None][IP Unknown User
snmp@IB-session2 User Login]
  [4][Mon Apr 25 11:02:07.379 UTC 2005][AU][0000.0001][None][IP Unknown User
snmp@OB-session3 User Login]
  [5][Mon Apr 25 15:58:40.548 UTC 2005][AU][0000.0001][None][IP 10.20.33.160 User
admin@OB-session4 User Login]
  [6][Mon Apr 25 16:08:38.188 UTC 2005][AU][0000.0001][None][IP 10.20.32.70 User
admin@OB-session5 User Login]
```

show accounting logsize

To display maximum size of the accounting log file, use the **show accounting logsize** command in EXEC mode.

show accounting logsize

Syntax Description

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show accounting logsize** command.

```
switch# show accounting logsize
maximum local accounting logentries: 1200
```

show clock

To display the system date and time and verify the time zone configuration, use the **show clock** command in EXEC mode.

show clock

Syntax Description

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show clock** command..

```
switch# show clock
Fri Apr 22 00:00:49 CDT 2005
```

show environment

To display all environment-related switch information, use the **show environment** command in EXEC mode.

show environment [**power** | **temperature**]

Syntax Description

power	Displays status of power supply module, power supply redundancy mode and power usage summary.
temperature	Displays switch temperature thresholds and alarm status of temperature sensors.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show environment** command.

```
switch# show environment
Temperature:
---------------------------
Module   CurTemp     Status
         (Celsius)
---------------------------
1        36          ok

Power Supply:
-------------
PS     Status
-------------
1      ok
```

Related Commands

Command	Description
show hardware	Displays all hardware components on a system.

show fcalias

To display the member name information in a Fibre Channel alias (fcalias), use the **show fcalias** command in EXEC mode.

show fcalias [**name** *fcalias-name*]

Syntax Description

name *fcalias-name*	Displays fcalias information for a specific name. The maximum length is 64.

Defaults

Displays a list of all global fcaliases.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

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 is sample output from the **show fcalias** command.

```
switch# show fcalias
fcalias name Alias2

fcalias name Alias1
  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 fcdomain

To display the Fibre Channel domain (fcdomain) information for the local switch or for all switches in the fabric, use the **show fcdomain** command in EXEC mode.

show fcdomain [domain-list]

Syntax Description

domain-list	Displays list of domain ids granted by the principal switch for all switches in the fabric.

Defaults

Displays domain information for the local switch.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show fcdomain** command.

```
switch# show fcdomain
The local switch is the Principal Switch.
Local switch run time information:
        Local switch WWN:    10:00:00:0d:ec:19:cb:0e
        Running fabric name: 10:00:00:0d:ec:19:cb:0e
        Running priority:    128
        Current domain ID:   0x69(105)

Local switch configuration information:
        Configured fabric name:
        Configured priority:    128
        Configured domain ID:   0x0(0) (preferred)

Principal switch run time information:
        Running priority: 128
```

The following is sample output from the **show fcdomain domain-list** command.

```
switch# show fcdomain domain-list
VSAN 1
Number of domains: 1
Domain ID              WWN
---------    -----------------------
0x69(105)   10:00:00:0d:ec:19:cb:0e [Local] [Principal]
```

show fcns database

To display the results of the discovery, or to display the name server database, use the **show fcns database** command in EXEC mode.

show fcns database [detail | domain *domain-id* **| fcid** *fcid-id*]

Syntax Description

detail	Displays all objects in each entry.
domain *domain-id*	Displays entries in a domain.
fcid *fcid-id*	Displays entry for the given port.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

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.

Examples

The following is sample output from the **show fcns database detail** command.

```
switch# show fcns database detail

-------------
FCID:0x0101e1
-------------
port-wwn (vendor) :      21:00:00:20:37:d9:4f:66 ()
node-wwn :               20:00:00:20:37:d9:4f:66
class :                  3
node-ip-addr :           0.0.0.0
fc4-types:fc4_features : FCP
symbolic-port-name :     (NULL)
symbolic-node-name       (NULL)
port-type :              NL
port-ip-addr :           0.0.0.0
fabric-port-wwn :        20:01:00:c0:dd:06:fc:00
-------------
FCID:0x0101e2
-------------
port-wwn (vendor) :      21:00:00:20:37:d9:4d:61 ()
node-wwn :               20:00:00:20:37:d9:4d:61
class :                  3
node-ip-addr :           0.0.0.0
fc4-types:fc4_features : FCP
symbolic-port-name :     (NULL)
symbolic-node-name :     (NULL)
port-type :              NL
port-ip-addr :           0.0.0.0
fabric-port-wwn :        20:01:00:c0:dd:06:fc:00
-------------
FCID:0x0101e4
-------------
port-wwn (vendor) :      21:00:00:20:37:d9:4a:fa ()
node-wwn :               20:00:00:20:37:d9:4a:fa
class :                  3
node-ip-addr :           0.0.0.0
fc4-types:fc4_features : FCP
symbolic-port-name :     (NULL)
symbolic-node-name :     (NULL)
port-type :              NL
port-ip-addr :           0.0.0.0
fabric-port-wwn :        20:01:00:c0:dd:06:fc:00
-------------
FCID:0x0101e8
-------------
port-wwn (vendor) :      21:00:00:20:37:d9:4c:02 ()
node-wwn :               20:00:00:20:37:d9:4c:02
class :                  3
node-ip-addr :           0.0.0.0
fc4-types:fc4_features : FCP
symbolic-port-name :     (NULL)
symbolic-node-name :     (NULL)
port-type :              NL
port-ip-addr :           0.0.0.0
fabric-port-wwn :        20:01:00:c0:dd:06:fc:00
```

The following is sample output from the **show fcns database domain** command

```
switch# show fcns database domain 1
-------------------------------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
-------------------------------------------------------------------------------------------
0x0101e1 NL 21:00:00:20:37:d9:4f:66 FCP
0x0101e2 NL 21:00:00:20:37:d9:4d:61 FCP
0x0101e4 NL 21:00:00:20:37:d9:4a:fa FCP
0x0101e8 NL 21:00:00:20:37:d9:4c:02 FCP
Total number of entries = 4
```

show fcs database

To display the status of the fabric configuration, use the **show fcs database** command in EXEC mode.

show fcs database

Syntax Description

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show fcs database** command.

```
switch# show fcs database
FCS Local Database
------------------
Switch WWN          : 1000000dec19cb0e
Switch Domain Id    : 105
Fabric-Name         :
Switch Logical-Name : switch
Switch Ports:
-----------------------------------------------------------------
Interface  fWWN                     Type     Attached-pWWNs
-----------------------------------------------------------------
fc1/1      20:00:00:0d:ec:19:cb:0e  Unknown  None
fc1/2      20:01:00:0d:ec:19:cb:0e  Unknown  None
fc1/3      20:02:00:0d:ec:19:cb:0e  Unknown  None
fc1/4      20:03:00:0d:ec:19:cb:0e  Unknown  None
fc1/5      20:04:00:0d:ec:19:cb:0e  Unknown  None
fc1/6      20:05:00:0d:ec:19:cb:0e  Unknown  None
fc1/7      20:06:00:0d:ec:19:cb:0e  Unknown  None
fc1/8      20:07:00:0d:ec:19:cb:0e  Unknown  None
fc1/9      20:08:00:0d:ec:19:cb:0e  Unknown  None
fc1/10     20:09:00:0d:ec:19:cb:0e  Unknown  None
fc1/11     20:0a:00:0d:ec:19:cb:0e  Unknown  None
fc1/12     20:0b:00:0d:ec:19:cb:0e  Unknown  None
fc1/13     20:0c:00:0d:ec:19:cb:0e  Unknown  None
fc1/14     20:0d:00:0d:ec:19:cb:0e  Unknown  None
fc1/15     20:0e:00:0d:ec:19:cb:0e  Unknown  None
fc1/16     20:0f:00:0d:ec:19:cb:0e  Unknown  None
fc1/17     20:10:00:0d:ec:19:cb:0e  Unknown  None
fc1/18     20:11:00:0d:ec:19:cb:0e  Unknown  None
fc1/19     20:12:00:0d:ec:19:cb:0e  Unknown  None
fc1/20     20:13:00:0d:ec:19:cb:0e  Unknown  None
```

show fctimer

To view the Fibre Channel timers (fctimer), use the **show fctimer** command in EXEC mode.

show fctimer [**d_s_tov** | **e_d_tov** | **f_s_tov** | **r_a_tov**]

Syntax Description

d_s_tov	Displays the distributed services time out value (D_S_TOV) in milliseconds.
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.
r_a_tov	Displays the resource allocation time out value (R_A_TOV) in milliseconds.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show fctimer** command.

```
switch# show fctimer
F_S_TOV   D_S_TOV   E_D_TOV   R_A_TOV
----------------------------------------
5000 ms   5000 ms   2000 ms   10000 ms
```

Related Commands

Command	Description
fctimer	Configures fctimer parameters.

show fdmi database

To display the Fabric-Device Management Interface (FDMI) database information, use the **show fdmi database** command in EXEC mode.

show fdmi database [detail]

Syntax Description

detail	Specifies detailed FDMI information.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show fdmi database** command.

```
switch# show fdmi database
Registered HBA List
  10:00:00:00:c9:32:8d:77
  21:01:00:e0:8b:2a:f6:54
```

The following is sample output from the **show fdmi database detail** command.

```
switch# show fdmi database detail
Registered HBA List
-------------------------------
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
```

show flogi database

To list all the FLOGI sessions, use the **show flogi database** command in EXEC mode.

show flogi database

Syntax Description

This command had no arguments or keywords.

Defaults

Displays the entire FLOGI database.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

In a Fibre Channel fabric, each host or disk requires an FC ID. 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 is sample output from the **show flogi database** command.

```
switch# show flogi database
--------------------------------------------------------------------------
INTERFACE FCID PORT NAME NODE NAME
--------------------------------------------------------------------------
fc1/2 0x6101e1 21:00:00:04:cf:03:36:2f 20:00:00:04:cf:03:36:2f
fc1/2 0x6101e2 21:00:00:04:cf:03:38:6e 20:00:00:04:cf:03:38:6e
fc1/2 0x6101e4 21:00:00:04:cf:03:38:24 20:00:00:04:cf:03:38:24
fc1/2 0x6101e8 21:00:00:04:cf:03:38:4b 20:00:00:04:cf:03:38:4b
Total number of flogi = 4
```

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 in EXEC mode.

show fspf [interface]

Syntax Description

interface	Displays FSPF interface information for all interfaces.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

FSPF 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
- LS_refresh_time: the interval lapse between refresh LSR transmissions
- Max_age: the maximum time aa LSR can stay before being deleted

Examples

The following is sample output from the **show fspf** command.

```
switch# show fspf
FSPF routing administration status is enabled
FSPF routing operational status is UP
MinLsArrival = 1000 msec , MinLsInterval = 5000 msec
Local Domain is 0x69(105)
Number of LSRs = 0

Protocol constants :
   LS_REFRESH_TIME = 30 minutes (1800 sec)
   MAX_AGE         = 60 minutes (3600 sec)

Statistics counters :
   Number of LSR that reached MaxAge = 0
   Number of SPF computations        = 0
   Number of Checksum Errors         = 0
   Number of Transmitted packets :  LSU 0 LSA 0 Hello 0 Retranmsitted LSU 0
   Number of Received packets :  LSU 0 LSA 0 Hello 0 Error Packets 0
```

The following is sample output from the **show fspf interface** command.

```
switch# show fspf interface

FSPF interface fc1/1
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
   Number of packets received : LSU 0  LSA 0  Hello 0  Error packets 0
   Number of packets transmitted : LSU 0  LSA 0  Hello 0  Retransmitted LSU 0

FSPF interface fc1/2
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
   Number of packets received : LSU 0  LSA 0  Hello 0  Error packets 0
   Number of packets transmitted : LSU 0  LSA 0  Hello 0  Retransmitted LSU 0

FSPF interface fc1/3
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
   Number of packets received : LSU 0  LSA 0  Hello 0  Error packets 0
   Number of packets transmitted : LSU 0  LSA 0  Hello 0  Retransmitted LSU 0

FSPF interface fc1/4
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
   Number of packets received : LSU 0  LSA 0  Hello 0  Error packets 0
   Number of packets transmitted : LSU 0  LSA 0  Hello 0  Retransmitted LSU 0

FSPF interface fc1/5
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
   Number of packets received : LSU 0  LSA 0  Hello 0  Error packets 0
   Number of packets transmitted : LSU 0  LSA 0  Hello 0  Retransmitted LSU 0

FSPF interface fc1/6
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
```

```
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
   Number of packets received : LSU 0  LSA 0  Hello 0  Error packets 0
   Number of packets transmitted : LSU 0  LSA 0  Hello 0  Retransmitted LSU 0

FSPF interface fc1/7
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
   Number of packets received : LSU 0  LSA 0  Hello 0  Error packets 0
   Number of packets transmitted : LSU 0  LSA 0  Hello 0  Retransmitted LSU 0

FSPF interface fc1/8
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
   Number of packets received : LSU 0  LSA 0  Hello 0  Error packets 0
   Number of packets transmitted : LSU 0  LSA 0  Hello 0  Retransmitted LSU 0

FSPF interface fc1/9
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
   Number of packets received : LSU 0  LSA 0  Hello 0  Error packets 0
   Number of packets transmitted : LSU 0  LSA 0  Hello 0  Retransmitted LSU 0

FSPF interface fc1/10
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
   Number of packets received : LSU 0  LSA 0  Hello 0  Error packets 0
   Number of packets transmitted : LSU 0  LSA 0  Hello 0  Retransmitted LSU 0

FSPF interface fc1/11
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
   Number of packets received : LSU 0  LSA 0  Hello 0  Error packets 0
   Number of packets transmitted : LSU 0  LSA 0  Hello 0  Retransmitted LSU 0

FSPF interface fc1/12
FSPF routing administrative state is active
Interface cost is 0
```

```
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
   Number of packets received : LSU 0  LSA 0  Hello 0  Error packets 0
   Number of packets transmitted : LSU 0  LSA 0  Hello 0  Retransmitted LSU 0

FSPF interface fc1/13
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
   Number of packets received : LSU 0  LSA 0  Hello 0  Error packets 0
   Number of packets transmitted : LSU 0  LSA 0  Hello 0  Retransmitted LSU 0

FSPF interface fc1/14
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
   Number of packets received : LSU 0  LSA 0  Hello 0  Error packets 0
   Number of packets transmitted : LSU 0  LSA 0  Hello 0  Retransmitted LSU 0

FSPF interface fc1/15
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
   Number of packets received : LSU 0  LSA 0  Hello 0  Error packets 0
   Number of packets transmitted : LSU 0  LSA 0  Hello 0  Retransmitted LSU 0

FSPF interface fc1/16
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
   Number of packets received : LSU 0  LSA 0  Hello 0  Error packets 0
   Number of packets transmitted : LSU 0  LSA 0  Hello 0  Retransmitted LSU 0

FSPF interface fc1/17
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
   Number of packets received : LSU 0  LSA 0  Hello 0  Error packets 0
   Number of packets transmitted : LSU 0  LSA 0  Hello 0  Retransmitted LSU 0

FSPF interface fc1/18
```

```
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
   Number of packets received : LSU 0  LSA 0  Hello 0  Error packets 0
   Number of packets transmitted : LSU 0  LSA 0  Hello 0  Retransmitted LSU 0

FSPF interface fc1/19
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
   Number of packets received : LSU 0  LSA 0  Hello 0  Error packets 0
   Number of packets transmitted : LSU 0  LSA 0  Hello 0  Retransmitted LSU 0

FSPF interface fc1/20
FSPF routing administrative state is active
Interface cost is 0
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is DOWN
Neighbor Domain Id is 0x0(0), Neighbor Interface index is 0x00000000

Statistics counters :
   Number of packets received : LSU 0  LSA 0  Hello 0  Error packets 0
   Number of packets transmitted : LSU 0  LSA 0  Hello 0  Retransmitted LSU 0
```

show hardware

To display switch hardware inventory details, use the **show hardware** command in EXEC mode.

show hardware

Syntax Description

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show hardware** command

```
switch# show hardware
Cisco MDS 9000 FabricWare
Copyright (C) 2002-2005, by Cisco Systems, Inc.
and its suppliers.  All rights reserved.
Copyrights to certain works contained herein are owned by
third parties, and used and distributed under license.
Portions of this software are governed by the GNU Public License,
which is available at http://www.gnu.org/licenses/gpl.html.

Software
  system:   2.1(2)
  system compile time:   Thu Apr 21 12:48:49 2005

Hardware
  switch uptime is 0 days 5 hours 44 minute(s) 42 second(s)

  Last reset at 20682 usecs after Mon Apr 25 11:01:12 2005
    Reason: PowerUp

--------------------------------
Switch hardware ID information
--------------------------------

MDS Switch is booted up
  Model number is DS-C9020-20K9
  H/W version is -------
  Part Number is 74-3811-01
  Part Revision is A0
  Serial number is 0426a07855
  CLEI code is COMMM00ARA
```

show interface

You can check the status of an interface at any time by using the **show interface** command in EXEC mode.

show interface {[brief] | counters [brief] | description | fc 1/*port* **[brief] | mgmt 0 | transceiver}**

Syntax Description

brief	Displays brief information.
counters	Displays the interface counter information.
description	Displays the interface description.
fc	Displays interface information for all ports.
1/*port*	Specifies slot 1 and the port number. The port number is in the range 1 to 20.
mgmt 0	Displays management interface 0 information.
transceiver	Displays the transceiver information for all interfaces.

Defaults

Displays information for all interfaces on the switch.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show interface fc** command.

```
switch# show interface fc 1/11
fc1/11 is Down (Administratively down)
    Port WWN is 20:0a:00:0d:ec:19:cb:0e
    Admin port mode is auto
    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 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 errors
      0 input OLS, 0 LRR, 0 loop inits
      5 output OLS, 0 LRR, 1 loop inits
```

The following is sample output from the **show interface description** command.

```
switch# show interface description
------------------------------------------------
Interface Description
------------------------------------------------
fc1/1     fc1/1
fc1/2     fc1/2
fc1/3     fc1/3
fc1/4     fc1/4
fc1/5     fc1/5
fc1/6     fc1/6
fc1/7     fc1/7
fc1/8     fc1/8
fc1/9     fc1/9
fc1/10    fc1/10
fc1/11    fc1/11
fc1/12    fc1/12
fc1/13    fc1/13
fc1/14    fc1/14
fc1/15    fc1/15
fc1/16    fc1/16
fc1/17    fc1/17
fc1/18    fc1/18
fc1/19    fc1/19
fc1/20    fc1/20
```

The following is sample output from the **show interface brief** command.

```
switch# show interface brief
--------------------------------------------------------------------
Interface  Admin       Status            FCOT  Oper     Oper
           Mode                                Mode     Speed
                                                        (Gbps)
--------------------------------------------------------------------
fc1/1      auto        down              lwl    --
fc1/2      auto        down              swl    --
fc1/3      auto        down              --     --
fc1/4      auto        down              --     --
fc1/5      auto        down              --     --
fc1/6      auto        down              --     --
fc1/7      auto        down              --     --
fc1/8      auto        down              --     --
fc1/9      auto        down              swl    --
fc1/10     auto        down              --     --
fc1/11     auto        down              --     --
fc1/12     auto        down              --     --
fc1/13     auto        down              unk    --
fc1/14     auto        down              --     --
fc1/15     auto        down              --     --
fc1/16     auto        down              swl    --
fc1/17     auto        down              --     --
fc1/18     auto        down              --     --
fc1/19     auto        down              --     --
fc1/20     auto        down              elec   --

-------------------------------------------
Interface               Status     IP Address
-------------------------------------------
mgmt0                   up         10.20.83.122
```

The following is sample output from the **show interface counters brief** command.

```
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
-------------------------------------------------------------------------------
fc1/1              0        0                     0        0
fc1/2              0        0                     0        0
fc1/3              0        0                     0        0
fc1/4              0        0                     0        0
fc1/5              0        0                     0        0
fc1/6              0        0                     0        0
fc1/7              0        0                     0        0
fc1/8              0        0                     0        0
fc1/9              0        0                     0        0
fc1/10             0        0                     0        0
fc1/11             0        0                     0        0
fc1/12             0        0                     0        0
fc1/13             0        0                     0        0
fc1/14             0        0                     0        0
fc1/15             0        0                     0        0
fc1/16             0        0                     0        0
fc1/17             0        0                     0        0
fc1/18             0        0                     0        0
fc1/19             0        0                     0        0
fc1/20             0        0                     0        0
```

The following is sample output from the **show interface transceiver** command.

```
switch# show interface transceiver
fc1/1 sfp is present but not supported
    name is FINISAR CORP.
    part number is FTRJ-8519-3-2.5
    revision is X1
    serial number is E113LSF
    vendor specific data (bytes 96-127)
      0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF
      0xFF 0xFF 0xFF 0xFF 0xFF 0x00 0x00 0x00
      0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0x00
      0x00 0x00 0xFF 0xFF 0xFF 0xFF 0xA7 0xCE

fc1/2 sfp is present but not supported
    name is FINISAR CORP.
    part number is FTRJ-8519-3-2.5
    revision is X1
    serial number is H112UZ3
    vendor specific data (bytes 96-127)
      0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF
      0xFF 0xFF 0xFF 0xFF 0xFF 0x00 0x00 0x00
      0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0x00
      0x00 0x00 0xFF 0xFF 0xFF 0xFF 0xA7 0xCE

fc1/3 sfp is not present
fc1/4 sfp is not present
fc1/5 sfp is not present
fc1/6 sfp is not present
fc1/7 sfp is not present
fc1/8 sfp is not present
fc1/9 sfp is present but not supported
    name is FINISAR CORP.
    part number is FTRJ8524P2BNL
    revision is A
    serial number is P6G2333
    vendor specific data (bytes 96-127)
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

fc1/10 sfp is not present
fc1/11 sfp is not present
fc1/12 sfp is not present
fc1/13 sfp is present but not supported
    name is
    part number is
    revision is
    serial number is
    vendor specific data (bytes 96-127)
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

fc1/14 sfp is not present
fc1/15 sfp is not present
fc1/16 sfp is present but not supported
    name is FINISAR CORP.
    part number is FTRJ-8519-3-2.5
    revision is X1
    serial number is E113GL5
    vendor specific data (bytes 96-127)
```

```
        0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF
        0xFF 0xFF 0xFF 0xFF 0xFF 0x00 0x00 0x00
        0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0x00
        0x00 0x00 0xFF 0xFF 0xFF 0xFF 0xA7 0xCE

fc1/17 sfp is not present
fc1/18 sfp is not present
fc1/19 sfp is not present
fc1/20 sfp is present but not supported
    name is Molex Inc.
    part number is 74720-0502
    revision is D
    serial number is 33281334
    vendor specific data (bytes 96-127)
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
```

show ip access-list

To display the IP access control lists (IP-ACLs) currently active, use the **show ip access-list** command in EXEC mode.

show ip access-list [*list-name* | **usage**]

Syntax Description

list-name	IP access list name. Maximum length is 64 characters.
usage	Access list usage.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show ip access-list usage** command.

```
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 2005
x1                               3       1    active    Tue Jun 24 18:32:25 2005
x3                             0     1    not-ready Tue Jun 24 18:32:28 2005
```

The following is sample output from the **show ip access-list** command.

```
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 route

To display the IP routing information, use the **show ip route** command in EXEC mode.

show ip route

Syntax Description

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show ip route** command.

```
switch# show ip route
Codes: C - connected, S - static

Default gateway is 10.20.83.1

C 10.20.83.0/24 is directly connected, mgmt0
```

show logging

To display the current message logging configuration, use the **show logging** command in EXEC mode.

show logging [info | last *lines* **| level | logfile | monitor | server]**

Syntax Description

info	Displays logging configuration.
last *lines*	Displays last few lines of logfile. The range is 1 to 9999.
level	Displays logging level configuration.
logfile	Displays contents of logfile.
monitor	Displays monitor logging configuration.
server	Displays server logging configuration.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show logging** command.

```
switch# show logging
Logging monitor:                 disabled
Logging server:                  disabled
Logging logfile:                 enabled (Severity: critical)

Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
fcns                    6                       2
fcs                     6                       2
zone                    6                       2
auth                    6                       2
ipconf                  6                       2
module                  6                       2
ntp                     6                       2
sysmgr                  6                       2
user                    6                       2
port                    6                       2
fcdomain                6                       2
fspf                    6                       2

  [1][Mon Apr 25 11:02:03.228 UTC 2005][I][8400.0022][Switch][Successful login user
(admin@OB-session1) with admin privi
lege]
  [2][Mon Apr 25 11:02:03.337 UTC 2005][W][8A00.0000][CLI][Error while processing 'copy'
command: Source file does not exist]
  [3][Mon Apr 25 11:02:03.358 UTC 2005][A][1005.0040][Port: if1/2][Unsupported SFP within
port.]
  [4][Mon Apr 25 11:02:03.393 UTC 2005][A][1005.0040][Port: if1/9][Unsupported SFP within
port.]
  [5][Mon Apr 25 11:02:03.431 UTC 2005][A][1005.0040][Port: if1/13][Unsupported SFP within
port.]
```

The following is sample output from the **show logging info** command.

```
switch# show logging info
Logging monitor:                 disabled
Logging server:                  disabled
Logging logfile:                 enabled (Severity: critical)

Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
fcns                    6                       2
fcs                     6                       2
zone                    6                       2
auth                    6                       2
ipconf                  6                       2
module                  6                       2
ntp                     6                       2
sysmgr                  6                       2
user                    6                       2
port                    6                       2
fcdomain                6                       2
fspf                    6                       2
```

The following is sample output from the **show logging last** command.

```
switch# show logging last 2

[7][Fri Jan 21 22:45:07.672 UTC 2005][I][8400.0023][Switch][Successful login user
(admin@OB-session3) with admin privilege from address 10.0.0.254]
[8][Fri Jan 21 22:49:06.768 UTC 2005][I][8400.0023][Switch][Successful login user
(maint@OB-session4) with admin privilege from address 10.0.0.254]
```

The following is sample output from the **show logging monitor** command.

```
switch# show logging monitor
Logging monitor:                 enabled
```

The following is sample output from the **show logging server** command.

```
switch# show logging server

Logging server:                  disabled
```

Related Commands

Command	Description
logging level	Configures the message facility name and severity level.
logging monitor	Configures the message severity level.
logging server	Configures the IP address of the remote logging host running syslog.

show module

To verify the status of a module, use the **show module** command in EXEC mode.

show module [**uptime**]

Syntax Description

uptime	Displays the length of time that the module has been functional in the switch.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

Use the **uptime** option to display the time that a module goes online after a disruptive upgrade or reset.

Examples

The following is sample output from the **show module** command.

```
switch# show module
Mod  Ports  Module-Type                      Model              Status
---  -----  -------------------------------- ------------------ ------------
1    20     1/2/4 Gbps FC/Supervisor         DS-C9020-20K9      active *

Mod  Sw             Hw      World-Wide-Name (WWN)
---  -------------  ------  --------------------------------------------------
1    2.1(2)         -------  10:00:00:0d:ec:19:cb:01


Mod  MAC-Address                              Serial-Num
---  ---------------------------------------  ----------
1    00-c0-dd-03-d4-e4                        0426a07855

* this terminal session
```

The following is sample output from the **show module uptime** command.

```
switch#  show module uptime
------ Module 1 -----
Module Start Time:   Mon Apr 25 11:01:12 2005
Up Time:             0 days, 9 hours, 7 minutes, 56 seconds
```

show processes

To display general information about all the processes, use the **show processes** command in EXEC mode.

show processes {log [details]}

Syntax Description

log	Displays information about process logs or backtrace files.
details	Displays detailed process log information.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show processes** command.

```
switch# show processes
  PID   PPID %CPU     TIME     ELAPSED COMMAND
  178    148  0.0 00:00:00    09:46:25 cns
  179    148  0.0 00:00:00    09:46:25 ens
  180    148  0.0 00:00:00    09:46:25 dlog
  181    148  0.0 00:00:05    09:46:24 ds
  182    148  0.0 00:00:02    09:46:24 mgmtApp
  183    148  0.0 00:00:00    09:46:24 sys2swlog
  236    148  0.0 00:00:00    09:45:38 fc2
  237    148  0.0 00:00:00    09:45:38 nserver
  238    148  0.0 00:00:00    09:45:38 mserver
  239    148  0.0 00:00:00    09:45:38 util
  240    148  0.0 00:00:01    09:45:37 snmpservicepath
  241    148  0.0 00:00:00    09:45:37 eport
  242    148  0.0 00:00:00    09:45:37 PortApp
  243    148  0.0 00:00:00    09:45:37 port_mon
  244    148  0.0 00:00:00    09:45:37 zoning
  245    148  0.0 00:00:00    09:45:37 diagApp
  265    148  0.0 00:00:00    09:45:31 snmpd
  266    148  0.0 00:00:00    09:45:31 snmpmain
  269    266  0.0 00:00:00    09:45:29 snmpmain
  270    269  0.0 00:00:00    09:45:29 snmpmain
```

The following is sample output from the **show processes log** command.

```
switch# show processes log
Process                 Log-create-time
----------------------  ---------------
backtrace-clishco       Tue Apr 26 18:45:39 2005
```

show radius-server

To display all configured RADIUS server parameters, use the **show radius-server** command in EXEC mode.

show radius-server

Syntax Description

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

Only administrators can view the RADIUS pre-shared key.

Examples

The following is sample output from the **show radius-server** command.

```
switch# show radius-server
total number of servers:2
following RADIUS servers are configured:
        10.20.11.5:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:
                timeout:2
                retries:0
        10.20.11.7:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:
                timeout:2
                retries:0
```

show running-config

To display the running configuration file, use the **show running-config** command in EXEC mode.

show running-config [**diff**]

Syntax Description

diff	Displays the difference between the running and startup configurations.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

If the running configuration is different from the startup configuration, enter the **show startup-config diff** command to view the differences.

Examples

The following is sample output from the **show running-config** command.

```
switch# show running-config
ip default-gateway 10.20.83.1
logging level fcdomain 2
logging level fspf 2
logging level fcns 2
logging level fcs 2
logging level port 2
logging level zone 2
logging level auth 2
logging level ipconf 2
logging level module 2
logging level ntp 2
logging level sysmgr 2
interface mgmt0
  ip address 10.20.83.122 255.255.255.0
interface fc1/1
interface fc1/2
interface fc1/3
interface fc1/4
interface fc1/5
interface fc1/6
interface fc1/7
interface fc1/8
interface fc1/9
interface fc1/10
interface fc1/11
interface fc1/12
interface fc1/13
interface fc1/14
interface fc1/15
```

```
interface fc1/16
interface fc1/17
interface fc1/18
interface fc1/19
interface fc1/20
```

The following is sample output from the **show running-config diff** command.

```
switch# show running-config diff
switchname rtp-9020-top
  ip default-gateway 172.18.172.1
  ssh server enable
  logging level fcdomain 2
  logging level fspf 2
  logging level fcns 2
  logging level fcs 2
  logging level port 2
  logging level zone 2
  logging level auth 2
  logging level ipconf 2
  logging level module 2
  logging level ntp 2
  logging level sysmgr 2
  snmp-server community public ro
  snmp-server community private rw
  interface mgmt0
    ip address 172.18.172.160 255.255.255.0
    no shutdown
  interface fc1/1
+   no shutdown
  interface fc1/2
  interface fc1/3
  interface fc1/4
  interface fc1/5
  interface fc1/6
  interface fc1/7
  interface fc1/8
  interface fc1/9
  interface fc1/10
  interface fc1/11
  interface fc1/12
  interface fc1/13
  interface fc1/14
  interface fc1/15
  interface fc1/16
  interface fc1/17
  interface fc1/18
  interface fc1/19
  interface fc1/20
```

show snmp

To display SNMP status and setting information, use the **show snmp** command in EXEC mode.

show snmp [**community** | **host** | **user**]

Syntax Description

community	Displays SNMP community strings.
host	Displays SNMP host information.
user	Displays SNMP users.

Defaults

Displays the system contact, system location, and community information.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show snmp** command.

```
switch# show snmp

sys contact: <sysContact undefined>
sys location: <sysLocation undefined>

Community                       Group/Access
---------                       ------------
public                          network-operator
```

The following is sample output from the **show snmp community** command.

```
switch# show snmp community

Community       Group/Access
---------       ------------
public          network-operator
```

The following is sample output from the **show snmp user** command.

```
switch# show snmp user
Host                            Port Version  Type   SecName
____                            ____ _______  _____  ______

10.0.0.254                      162  2c       trap   public
```

The following is sample output from the **show snmp host** command.

```
switch# show snmp host
Host                                 Port Version  Level  Type   SecName
____                                 ____ _______  ______ ____  _______
172.16.126.34                        2162 v2c      noauth trap   public
172.16.75.106                        2162 v2c      noauth trap   public
172.31.124.81                        2162 v2c      noauth trap   public
172.31.157.193                       2162 v2c      noauth trap   public
172.31.157.98                        2162 v2c      noauth trap   public
172.31.49.25                         2162 v2c      noauth trap   public
172.31.49.32                         2188 v2c      noauth trap   public
172.31.49.49                         2162 v2c      noauth trap   public
172.31.49.49                         3514 v2c      noauth trap   public
172.31.49.54                         2162 v2c      noauth trap   public
172.31.58.54                         2162 v2c      noauth trap   public
172.31.58.81                         2162 v2c      noauth trap   public
172.31.58.97                         1635 v2c      noauth trap   public
172.31.58.97                         2162 v2c      auth   trap   public
172.31.58.97                         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 is sample output from the **show snmp user** command.

```
switch# show snmp user
User                            Group                           Auth  Priv
____                            _____                           ____  ____
sadmin2                         network-admin                   md5   des
sadmin                          network-admin                   md5   des
soper                           network-operator                md5   des
```

show sprom mgmt-module

To display the switch SPROM contents, use the **show sprom mgmt-module** command in EXEC mode.

Syntax Description

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show sprom mgmt-module** command.

```
switch# show sprom mgmt-module
DISPLAY SAM sprom contents:
Common block:
 OEM String      : Cisco Systems, Inc.
 Product Number  : DS-C9020-20K9
 Serial Number   : 0426a07855
 Part Number     : 74-3811-01
 Part Revision   : A0
 Mfg Deviation   : 0
 H/W Version     : -------
 snmpOID         : 1.3.6.1.4.1.1663.1.1.1.1.26
 CLEI Code       : COMMM00ARA
 VID             : V01
 MAC Address     : 00-c0-dd-03-d4-e4
 WWN             : 10:00:00:0d:ec:19:cb:0e
```

show ssh server

To display the status of the Secure Shell information (SSH) server, use the **show ssh server** command in EXEC mode.

show ssh server

Syntax Description

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show ssh server** command.

```
switch# show ssh server
ssh service is enabled
```

show startup-config

To display the startup configuration file, use the **show startup-config** command in EXEC mode.

show startup-config

Syntax Description

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show startup-config** command.

```
switch# show startup-config
#
# Startup config
#
switchname DS-C9020-20K9

fcdomain domain 0 preferred

interface fc1/1
       no shutdown
       Auto

interface fc1/2
       no shutdown
       Auto

interface fc1/3
       no shutdown
       Fx

interface fc1/4
       no shutdown
       Auto

interface fc1/5
       no shutdown
       Auto

interface fc1/6
       no shutdown
       Auto

interface fc1/7
       no shutdown
       Auto
```

```
interface fc1/8
       no shutdown
       Auto

interface fc1/9
       no shutdown
       Auto

interface fc1/10
       no shutdown
       Auto

interface fc1/11
       no shutdown
       Auto

interface fc1/12
       no shutdown
       Auto
```

show switchname

To display the switch network name, use the **show switchname** command in EXEC mode.

show switchname

Syntax Description

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show switchname** command.

```
switch# show switchname
switch-123
```

show system

To display the system information, use the **show system** command in EXEC mode.

show system [**reset-reason** | **uptime**]

Syntax Description

reset-reason	Displays the last reset reason code.
uptime	Displays how long the system has been up and running.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show system reset-reason** command.

```
switch# show system reset-reason
----- reset reason for module 1 -----
1) At <USECS> usecs after Fri Jan 21 23:20:11 2005
        Reason: NormalReset
```

The following is sample output from the **show system uptime** command.

```
switch# show system uptime
System Start Time:          Mon Apr 25 11:01:12 2005
System Up Time:             0 days, 10 hours, 58 minutes, 38 seconds
Active Supervisor Up Time:  0 days, 10 hours, 58 minutes, 38 seconds
```

show tech-support

To display information useful to technical support when reporting a problem, use the **show tech-support** command in EXEC mode.

show tech-support [**brief** | **create** | **details** | **interface** | **module 1**]

Syntax Description

brief	Provides a summary of the current running state of the switch.
create	Creates a technical support file (dump_support.tgz) and uses FTP to send the file to a remote host.
details	Provides detailed troubleshooting information.
interface	Displays interface status and configuration information.
module 1	Displays module1 status information.

Defaults

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 processes**

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

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 explanations for the commands listed under Defaults.

Examples

The following is sample output from the **show tech-support module** command.

```
switch# show tech-support module 1
  CMD: show module 1
  ---
Mod  Ports  Module-Type                      Model              Status
---  -----  -------------------------------- ------------------ ------------
1    20     1/2/4 Gbps FC/Supervisor         DS-C9020-20K9      active

Mod  Sw             Hw      World-Wide-Name (WWN)
---  -------------  ------  --------------------------------------------------
1    2.1(2)         -------  10:00:00:0d:ec:19:cb:0e

Mod  MAC-Address                             Serial-Num
---  --------------------------------------  ----------
1    00-c0-dd-03-d4-e4                       0426a07855

  CMD: show environment
  ---
Fan:
----------------------
Fan              Status
----------------------
1                Good
2                Good

Temperature:
---------------------------
Module   CurTemp     Status
         (Celsius)
---------------------------
1        33          ok

Power Supply:
-------------
PS     Status
-------------
1      ok
2      ok
```

The following is sample output from the **show tech-support brief** command.

```
switch# show tech-support brief
  CMD: show fcs database
  ---

FCS Local Database
------------------
Switch WWN          : 1000000dec19cb0e
Switch Domain Id    : 105
Fabric-Name         :
Switch Logical-Name : switch
Switch Ports:
-----------------------------------------------------------------
Interface  fWWN                     Type     Attached-pWWNs
-----------------------------------------------------------------
fc1/1      20:00:00:0d:ec:19:cb:0e  Unknown  None
fc1/2      20:01:00:0d:ec:19:cb:0e  Unknown  None
fc1/3      20:02:00:0d:ec:19:cb:0e  Unknown  None
fc1/4      20:03:00:0d:ec:19:cb:0e  Unknown  None
fc1/5      20:04:00:0d:ec:19:cb:0e  Unknown  None
fc1/6      20:05:00:0d:ec:19:cb:0e  Unknown  None
fc1/7      20:06:00:0d:ec:19:cb:0e  Unknown  None
fc1/8      20:07:00:0d:ec:19:cb:0e  Unknown  None
fc1/9      20:08:00:0d:ec:19:cb:0e  Unknown  None
fc1/10     20:09:00:0d:ec:19:cb:0e  Unknown  None
fc1/11     20:0a:00:0d:ec:19:cb:0e  Unknown  None
fc1/12     20:0b:00:0d:ec:19:cb:0e  Unknown  None
fc1/13     20:0c:00:0d:ec:19:cb:0e  Unknown  None
fc1/14     20:0d:00:0d:ec:19:cb:0e  Unknown  None
fc1/15     20:0e:00:0d:ec:19:cb:0e  Unknown  None
fc1/16     20:0f:00:0d:ec:19:cb:0e  Unknown  None
fc1/17     20:10:00:0d:ec:19:cb:0e  Unknown  None
fc1/18     20:11:00:0d:ec:19:cb:0e  Unknown  None
fc1/19     20:12:00:0d:ec:19:cb:0e  Unknown  None
fc1/20     20:13:00:0d:ec:19:cb:0e  Unknown  None

  CMD: show version
  ---

Cisco MDS 9000 FabricWare
Copyright (C) 2002-2005, by Cisco Systems, Inc.
and its suppliers.  All rights reserved.
Copyrights to certain works contained herein are owned by
third parties, and used and distributed under license.
Portions of this software are governed by the GNU Public Licen
which is available at http://www.gnu.org/licenses/gpl.html.

Software
  system:   2.1(2)
  system compile time:   Thu Apr 21 12:48:49 2005

Hardware
  switch uptime is 0 days 11 hours 14 minute(s) 0 second(s)

  Last reset at 40440 usecs after Mon Apr 25 11:01:12 2005
    Reason: PowerUp

  CMD: show interface brief
  ---
```

```
--------------------------------------------------------------
Interface  Admin       Status            FCOT  Oper     Oper
           Mode                                Mode     Speed
                                                        (Gbps)
--------------------------------------------------------------
fc1/1      auto        down              lwl    --
fc1/2      auto        down              swl    --
fc1/3      auto        down              --     --
fc1/4      auto        down              --     --
fc1/5      auto        down              --     --
fc1/6      auto        down              --     --
fc1/7      auto        down              --     --
fc1/8      auto        down              --     --
fc1/9      auto        down              swl    --
fc1/10     auto        down              --     --
fc1/11     auto        down              --     --
fc1/12     auto        down              --     --
fc1/13     auto        down              unk    --
fc1/14     auto        down              --     --
fc1/15     auto        down              --     --
fc1/16     auto        down              swl    --
fc1/17     auto        down              --     --
fc1/18     auto        down              --     --
fc1/19     auto        down              --     --
fc1/20     auto        down              elec   --

-------------------------------------------
Interface               Status     IP Address
-------------------------------------------
mgmt0                   up         10.20.83.122
```

The following is sample output from the **show tech-support create** command.

```
switch # show tech-support create
This may take several seconds...
FTP the dump support file to another machine? (y/n) : y
Enter IP Address of remote computer: 10.20.33.130
Login name: soper1
Enter a valid remote directory path within the user's home directory.
Otherwise the file will be place in the user's home directory:
Would you like to continue downloading support file? (y/n) : y
Connected to 10.20.33.130 (10.20.33.130).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
331 Password required for soper1.
Password:
230 User soper1 logged in.
cd /itasca/conf/images
Local directory now /itasca/conf/images
bin
200 Type set to I.
put dump_support.tgz
local: dump_support.tgz remote: dump_support.tgz
227 Entering Passive Mode (10,20,33,130,144,7)
150 Opening BINARY mode data connection for dump_support.tgz.
226 Transfer complete.
75614 bytes sent in 0.00731 secs (1e+04 Kbytes/sec)
Remote system type is UNIX.
Using binary mode to transfer files.
221-You have transferred 75614 bytes in 1 files.
221-Total traffic for this session was 76026 bytes in 1 transfers.
221 Thank you for using the FTP service on localhost.localdomain.
```

show telnet server

To display the state of the Telnet access configuration, use the **show telnet server** command in EXEC mode.

show telnet server

Syntax Description

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show telnet server** command.

```
switch# show telnet server
telnet service is enabled
```

show terminal

To display the terminal information, use the **show terminal** command

show terminal

Syntax Description

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show terminal** command.

```
switch# show terminal

Length: 10 lines
Session Timeout: 0 minutes
```

show user-account

To display configured information about user accounts, use the **show user-account** command in EXEC mode.

show user-account

Syntax Description

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show user-account** command.

```
switch# show user-account
show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
```

show users

To display all users currently accessing the switch, use the **show users** command in EXEC mode.

show users

Syntax Description

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show users** command.

```
switch# show users
  snmp@IB-session2     Mon Apr 25 11:02:07 2005 (Unknown)
  snmp@OB-session3     Mon Apr 25 11:02:07 2005 (Unknown)
  admin@OB-session11   Wed Apr 27 13:50:49 2005 (10.20.32.70)
```

show version

To display the version of system software that is currently running on the switch, use the **show version** command in EXEC mode.

show version

Syntax Description

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show version** command.

```
switch# show version
Cisco MDS 9000 FabricWare
Copyright (C) 2002-2005, by Cisco Systems, Inc.
and its suppliers.  All rights reserved.
Copyrights to certain works contained herein are owned by
third parties, and used and distributed under license.
Portions of this software are governed by the GNU Public License,
which is available at http://www.gnu.org/licenses/gpl.html.

Software
  system:   2.1(2)
  system compile time:   Thu Apr 21 12:48:49 2005

Hardware
  switch uptime is 0 days 11 hours 34 minute(s) 3 second(s)

  Last reset at 41643 usecs after Mon Apr 25 11:01:12 2005
    Reason: PowerUp
```

show zone

To display zone information, use the **show zone** command in EXEC mode.

show zone [**active** | **member** {**fcalias** *alias-name* | **pwwn** *wwn*} | **name** *string* | **status**]

Syntax Description

active	Displays zones which are part of active zone set.
member	Displays all zones to which the given member belongs.
fcalias	Displays zone members according to Fibre Channel alias.
pwwn	Displays zone members according to port worldwide name.
name	Displays members of a specified zone.
status	Displays zone server current status.
alias-name	Member alias name. Maximum length is 64 characters.
wwn	Member port worldwide name. Maximum length is 64 characters.
string	Zone name of up to 64 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show zone** command.

```
switch# show zone
zone name Z1
        pwwn 10:00:00:c0:dd:07:00:f8
        fcalias name A1
                  pwwn 10:00:00:c0:dd:07:00:f9
```

The following is sample output from the **show zone name** command.

```
switch# show zone name Zone1

zone name Z1
      pwwn 10:00:00:c0:dd:07:00:f8
      fcalias name A1
               pwwn 10:00:00:c0:dd:07:00:f9
      fcid 0x610005
```

The following is sample output from the **show zone member pwwn** command.

```
switch# show zone member pwwn 10:00:00:c0:dd:07:00:f9
fcalias name A1
          pwwn 10:00:00:c0:dd:07:00:f9
```

The following is sample output from the **show zone status** command.

```
switch# show zone status
Full Zoning Database :
        Zonesets: 1 Zones: 1 Aliases: 1
        Active Zoning Database:
                Name: ZS1 Zonesets: 1 Zones: 1
                Status:
```

show zoneset

To display the configured zone sets, use the **show zoneset** command in EXEC mode.

show zoneset [active | name *zoneset-name*]

Syntax Description

active	Displays only active zone sets.
name *zoneset-name*	Displays members of a specified zone set. Maximum length is 64 characters.

Defaults

Displays active zone set information.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following is sample output from the **show zoneset** command.

```
switch# show zoneset

zoneset name ZS1
         zone name Z1
               pwwn 10:00:00:c0:dd:07:00:f8
               fcalias name A1
                         pwwn 10:00:00:c0:dd:07:00:f9
```

The following is sample output from the **show zoneset active** command.

```
switch# show zoneset active
zoneset name ZS1
    zone name Z1
        pwwn 10:00:00:c0:dd:07:00:f8
        pwwn 10:00:00:c0:dd:07:00:f9
```

shutdown

To disable an interface, use the **shutdown** command in interface configuration submode.

shutdown [**force**]

To enable an interface, use the **no** form of this command.

no shutdown [**force**]

Syntax Description

force	Forces the shut down of the mgmt0 interface to avoid the confirmation.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

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 shut down 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
switch(config)# interface fc 1/2
switch(config-if)# no shutdown
```

The following example shows how to disable an interface.

```
switch# config
switch(config)# interface mgmt 0
switch(config-if)# shutdown
```

The following example shows how to forcefully disable the mgmt0 interface.

```
switch# config
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.

sleep

To delay an action by a specified number of seconds, use the **sleep** command in EXEC mode.

sleep *seconds*

Syntax Description		
	seconds	The number of seconds to delay an action.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

This command is useful within scripts.

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-server

To configure the SNMP server information, switch location, and switch name, use the **snmp-server** command in configuration mode.

snmp-server {**community** *string* **[ro | rw]** | **contact** [*name*] | **enable traps** | **location** [*location*]}

To remove the SNMP server information, use the **no** form of this command.

no snmp-server {**community** *string* **[ro | rw]** | **contact** [*name*] | **enable traps** | **location** [*location*]}

Syntax Description

community *string*	Specifies SNMP community string. 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.
enable traps	Enables SNMP traps.
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

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following example sets the contact information, switch location, and switch name.

```
switch# config
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 host

To specify the recipient of an Simple Network Management Protocol notification operation, use the **snmp-server host** command in configuration mode.

snmp-server host *host-address* **traps version [1 | 2c]** *community-string* **[udp-port** *port***]**

To remove the specified host, use the **no** form of this command.

no snmp-server host *host-address* **traps version [1 | 2c]** *community-string* **[udp-port** *port***]**

Syntax Description

host-address	Specifies the name or IP address of the host (the targeted recipient).
traps	Sends SNMP traps to this host.
version	Specifies the version of the Simple Network Management Protocol (SNMP) used to send the traps.
1	SNMPv1 (default).
2c	SNMPv2C.
community-string	Sends a password-like community string with the notification operation. Maximum length is 32 characters.
udp-port	Specifies the port UDP port of the host to use. The default is 162.
port	UDP port number. The range is 0 to 65,535.

Defaults

Sends SNMP traps.

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

If you use the version keyword, one of the following must be specified: **1** or **2c**.

Examples

The following example specify the recipient of an SNMP notification.

```
switch# config
switch(config)# snmp-server host 10.1.1.1 traps version 2c abcddsfsf udp-port 500
```

ssh key

To generate an SSH key, use the **ssh key** command in configuration mode.

ssh key rsa [*bits*]

To delete the SSH keys, use the **no** form of this command.

no ssh key

Syntax Description

rsa [*bits*]	Generates an RSA key. The range for the number of bits is 768 to 2048.

Defaults

No default behavior or values.

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following example shows how to generate an SSH 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.

ssh server enable

To disable the SSH service, use the **no** form of this command.

no ssh server enable

Syntax Description

This command had no arguments or keywords.

Defaults

Disabled

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following example enables the SSH server.

```
switch# config
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.

switchname

To change the name of the switch, use the **switchname** command in configuration mode.

switchname *name*

To revert the switch name to the default name, use the **no** form of this command.

no switchname

Syntax Description

name	Specifies a switch name. Maximum length is 32 characters.

Defaults

switch.

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following example changes the name of the switch to myswitch1.

```
switch# config
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 32 characters (without spaces).

switchport

To configure switchport parameter on a Fibre Channel interface, use the **switchport** command in interface configuration submode.

switchport {**beacon** |
description *text* |
mode [**auto** | **E** | **F** | **FL** | **Fx**] |
speed [**1000** | **2000** | **4000** | **auto**]}

To negate this command or revert to the factory defaults, user the **no** form of this command.

no switchport [**beacon** | **description** | **mode** | **speed**]

Syntax Description

beacon	Enables the beacon for the interface.
description *text*	Specifies the interface description. Maximum length is 32 characters with no embedded spaces.
mode	Configures the port mode.
auto	Specifies autosense mode.
E	Specifies E port mode.
F	Specifies F port mode.
FL	Specifies FL port mode.
Fx	Specifies Fx port mode.
speed	Configures the port speed.
1000	Specifies 1000 Mbps speed.
2000	Specifies 2000 Mbps speed.
4000	Specifies 4000 Mbps speed.
auto	Specifies autosense speed.

Defaults

The beacon is disabled.

The mode is **auto**.

The speed is **auto**.

Command Modes

Interface configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

You can specify a range of interfaces by entering a command with the following example format:

interface fc1/1-5

Examples

The following example configures switchport features for a Fibre Channel interface.

```
switch# config
switch(config)# interface fc1/1-4
switch(config-if)# switchport description ISLs
switch(config-if)# switchport mode E
switch(config-if)# switchport speed 4000
```

Related Commands

Command	Description
show interface	Displays an interface configuration for a specified interface.

telnet server enable

To enable the Telnet server, use the **telnet server enable** command in configuration mode.

telnet server enable

To disable this Telnet server, use the **no telnet server** command.

no telnet server enable

Syntax Description

This command had no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following example enables the Telnet server.

```
switch(config)# telnet server enable
```

terminal

To configure terminal attributes, use the **terminal** command in EXEC mode.

terminal [**length** *lines* | **session-timeout** *minutes*]

To revert to the defaults, use the **no** form of this command.

no terminal [**length** | **session-timeout**]

Syntax Description

length *lines*	Specifies the number of lines on the screen. The range is 0 to 511. Enter 0 to scroll continuously.
session-timeout	Specifies the session timeout value in minutes. The range is 0 to 525600. Enter 0 to disable.

Defaults

The default number of lines for the length is 20. The default width is 80 lines.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

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 20 and the width is not 80, then you need to set a length and width.

Examples

The following example sets the terminal length to 30.

```
switch# terminal length 30
```

Related Commands

Command	Description
show terminal	Displays terminal configuration information.

username

To define a user, use the **username** command in configuration mode.

username *name* {**password** *user-password* | [**expire** *days*] | **role** *rolename*}

To undo the configuration or revert to factory defaults, use the **no** form of this command.

no username *name* {**expire** *days* | **password** *user-password* [**expire** *date*] | **role** *rolename*}

Syntax Description

name	Specifies the name of the user. Maximum length is 16 characters.
password	Configures a password for the user.
user-password	Enters the password. The minimum password length is 8 characters and the maximum is 20.
expire *days*	Specifies the date when this user account expires (in YYYY-MM-DD format). The date can be no more than 2000 days into the future.
role	Specifies the role name of the user.
rolename	Role name. Only two role names are supported: network-operator and network-administrator. Maximum length is 32 characters.

Defaults

No default behavior or values.

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

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.

Examples

The following example shows how to define a user.

```
switch(config)# username knuckles password testpw role network-operator
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
```

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 2005-05-31
```

The following example adds the specified user (usam) to the network-admin role.

```
switch(config)# username usam role network-admin
```

Related CommandsT

Command	Description
show username	Displays user name information.

write erase

To clear a startup configuration, enter the **write erase** command in EXEC mode.

write erase [boot]

Syntax Description

boot	Destroys the startup file and mgmt0 IP configuration.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

Once this command is entered, 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 the IP configuration of the mgmt0 IP configuration (IP address, netmask, and default gateway).

The **write erase boot** command erases the mgmt0 IP configuration information (IP address, netmask, and default gateway) and the startup configuration.

Examples

The following example clears only the startup configuration.

```
switch# write erase
```

The following example clears the startup configuration and the mgmt0 IP configuration.

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

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.

zone default-zone [**permit**]

To negate the command or revert to the factory defaults, use the **no** form of this command.

no zone default-zone [**permit**]

Syntax Description

permit	Permits access to all in the default zone.

Defaults

All default zones are permitted access.

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following example permits default zoning.

```
switch# config
switch(config)# zone default-zone permit
```

Related Commands

Command	Description
show zone	Displays zone information.

zone name

To create a zone, use the **zone name** command in configuration mode.

zone name *zone-name*

To negate the command or revert to the factory defaults, use the **no** form of this command.

no zone name *zone-name*

Entering the **zone name** command opens the config-zone submode which provides access to the following subcommand:

member [fcalias *alias-name* **| pwwn** *pwwn-id***]**

Syntax Description

zone-name	Specifies the name of the zone and opens the config-zonet submode. Maximum length is 64 characters.
member	Adds a member to a zone. This command is available only in the config-zone submode.
fcalias *alias-name*	Adds a member using the device alias name.
pwwn *pwwn-id*	Adds a member using the port WWN in the format *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.

Defaults

No default behavior or values.

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

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 entered from the configuration mode.

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 members for the specified zone (Zone2) based on the member type (pWWN or FC alias) and value specified.

```
switch# config
switch(config)# zone name Zone2
switch(config-zone)# member pwwn 10:00:00:23:45:67:89:ab
switch(config-zone)# member fcalias Payroll
```

Related Commands

Command	Description
show zone	Displays zone information.
zone rename	Renames zones.

zone rename

To rename a zone, use the **zone rename** command in EXEC mode.

zone rename *current-name new-name*

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.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Examples

The following example shows how to rename a zone.

```
switch# zone rename ZoneA ZoneB
```

Related Commands

Command	Description
show zone	Displays zone information.
zone name	Creates and configures zones.

zoneset

To group zones under one zone set, use the **zoneset** command in configuration mode.

zoneset [**name** *zoneset-name* |
activate name *zoneset-name* |
distribute full |
rename *current-name new-name*]

To negate the command or revert to the factory defaults, use the **no** form of this command.

no zoneset [**name** *zoneset-name* |
activate name *zoneset-name* |
distribute full |
rename *current-name new-name*]

Entering the **zoneset name** *zoneset-name* command opens the config-zoneset submode which provides access to the member subcommand:

member [fcalias *alias-name* | **pwwn** *pwwn-id*]

Syntax Description

name *zoneset-name*	Creates the zone set and opens the config-zoneset submode. Maximum length is 64 characters.
activate *zoneset-name*	Activates a zone set.
distribute full	Enables full zone set propagation. Zone set propagation occurs when a zone set is activated.
member *zone-name*	Specifies an existing zone as a zone set member. This command is available only in the config-zoneset submode.
rename	Renames a zone set.
current-name	Specifies the current zone set name.
new-name	Specifies the new zone set name.

Defaults

No default behavior or values.

Command Modes

Configuration

Command History

This command was introduced in Cisco MDS 9000 FabricWare Release 2.1(2).

Usage Guidelines

Zones are activated by activating the parent zone set.

Examples

The following example creates a zone set named gottons, adds a zone, and activates the zone set.

```
switch# config
switch(config)# zoneset name gottons
switch(config-zone)# member zone1
switch(config-zone)# exit
switch(config)# zoneset activate name gottons
Zoneset Activation initiated. check zone status
```

Related Commands

Command	Description
show zoneset	Displays zone set information.

INDEX

A

B

C

D

E

F

L

M

S

T

U

V

W

Z