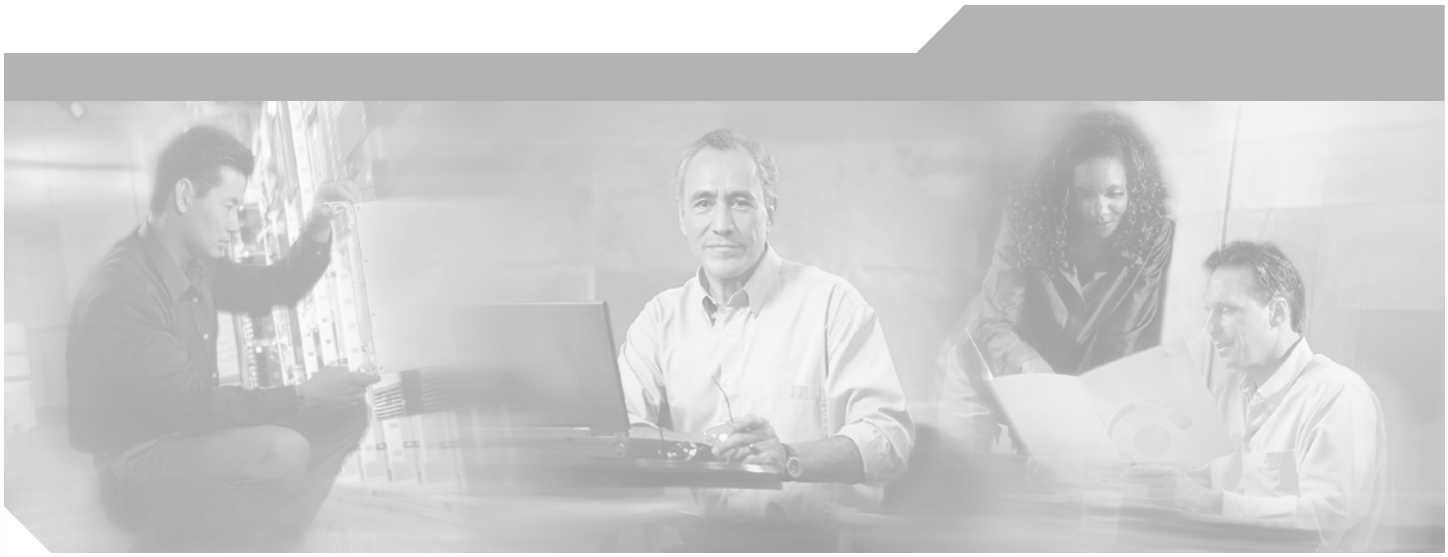


Cisco MDS 9000 Family Quick Configuration Guide

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

Customer Order Number: DOC-7816946=
Text Part Number: 78-16946-01

Cisco MDS 9000 Family Quick Configuration Guide

CONTENTS

Preface

This preface describes the audience, organization, and conventions of the *Cisco MDS 9000 Family Quick Configuration Guide*. 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 9000 Family of multilayer directors and fabric switches.

Organization

This guide is organized as follows:

Chapter	Title	Description
Chapter 1	Before You Begin	Prepares you to configure switches from the CLI.
Chapter 2	Quick Installation	Describes the basic operations required to install the Cisco MDS 9000 Family switches.
Chapter 3	Initial Configuration	Describes how to initially configure switches so they can be accessed by other devices.
Chapter 4	Configuring VSANs, Interfaces, and Zones	Describes how to configure VSANs, interfaces, and zones.
Chapter 5	Configuring Domain Parameters	Describes how to configure the Fibre Channel domain (fcdomain) feature.
Chapter 6	Configuring Trunking and PortChannels	Describes how to configure the trunking and PortChannel features.
Chapter 7	Configuring Security	Describes how to configure switch, fabric, and port security.
Chapter 8	Configuring Call Home	Describes configuration and messaging details on the Call Home feature.
Chapter 9	Configuring System Message Logging	Describes how to configure system message logging.

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 SSI Images*
- *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 9000 Family Software Upgrade and Downgrade Guide*
- *Cisco MDS 9000 Family Configuration Guide*
- *Cisco MDS 9000 Family 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 MIB Quick Reference*
- *Cisco MDS 9000 Family CIM Programming Reference*
- *Cisco MDS 9000 Family 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*

For information on VERITAS Storage Foundation™ for Networks for the Cisco MDS 9000 Family, refer to the VERITAS website: http://support.veritas.com/

For information on IBM TotalStorage SAN Volume Controller Storage Software for the Cisco MDS 9000 Family, refer to the IBM TotalStorage Support website: http://www.ibm.com/storage/support/2062-2300/

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/univercd/home/home.htm

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

Documentation DVD

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

Registered Cisco.com users (Cisco direct customers) can order a Cisco 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/

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

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

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

- 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 send comments about technical 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

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
- Nonemergencies—psirt@cisco.com

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 that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

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

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support 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 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 TAC 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 TAC 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, 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

- *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

- 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

Before You Begin

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

This chapter includes the following sections:

About the Switch Prompt

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

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

Example 1-1 Output When a Switch Boots Up

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

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

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

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

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

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

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

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

switch login:admin101
Password:*******
Cisco Storage Area Networking Operating System (SAN-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2004, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
Andiamo Systems, Inc. and/or other third parties and are used and
distributed under license. Some parts of this software are covered
under the GNU Public License. A copy of the license is available
at http://www.gnu.org/licenses/gpl.html.
switch#
```

You can perform embedded CLI operations, access command history, and use command parsing functions at this prompt. The switch gathers the command string upon detecting an **Enter** (CR) and accepts commands from the terminal.

About the CLI Command Modes

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

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

Table 1-1 Frequently Used Switch Command Modes

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

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

Understanding CLI Command Hierarchy

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

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

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

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

EXEC Mode Options

When you start a session on the switch, you begin in EXEC mode. Based on the role or group to which you belong, you have access to limited commands or to all commands. 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# ?
Exec Commands:
  attach      Connect to a specific linecard
  callhome    Callhome commands
  cd          Change current directory
  clear       Reset functions
  clock       Manage the system clock
  config      Enter configuration mode
  copy        Copy from one file to another
  debug       Debugging functions
  delete      Remove files
  dir         Directory listing for files
  discover    Discover information
  exit        Exit from the EXEC
  fcping      Ping an N-Port
  fctrace     Trace the route for an N-Port.
  find        Find a file below the current directory
  format      Format disks
  install     Upgrade software
  load        Load system image
  mkdir       Create new directory
  move        Move files
  no          Disable debugging functions
  ping        Send echo messages
  purge       Deletes unused data
  pwd         View current directory
  reload      Reboot the entire box
  rmdir       Remove existing directory
  run-script  Run shell scripts
  send        Send message to all the open sessions
  setup       Run the basic SETUP command facility
  show        Show running system information
  sleep       Sleep for the specified number of seconds
  system      System management commands
  tail        Display the last part of a file
  telnet      Telnet to another system
  terminal    Set terminal line parameters
  test        Test command
  traceroute  Trace route to destination
```

```
  undebug     Disable Debugging functions (See also debug)
  write       Write current configuration
  zone        Execute Zone Server 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. Once you are in configuration mode, you can enter interface configuration mode, zone configuration mode, and a variety of protocol-specific modes. Configuration mode is the starting point for all configuration commands. When you are in configuration mode, the switch expects configuration commands from the user.

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

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

Configuration Mode Commands and Submodes

Here is a list of configuration mode commands:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ?
Configure commands:
  aaa                 Configure AAA
  arp                 [no] remove an entry from the ARP cache
  boot                Configure boot variables
  callhome            Enter the callhome configuration mode
  clock               Configure time-of-day clock
  end                 Exit from configure mode
  exit                Exit from configure mode
  fcalias             Fcalias configuration commands
  fcanalyzer          Configure cisco fabric analyzer
  fcc                 Configure FC Congestion Control
  fcdomain            Enter the fcdomain configuration mode
  fcdroplatency       Configure switch or network latency
  fcflow              Configure  fcflow
  fcinterop           Interop commands.
  fcns                Name server configuration
  fcroute             Configure FC routes
  fcs                 Configure Fabric Config Server
  fctimer             Configure fibre channel timers
  fspf                Configure fspf
  in-order-guarantee  Set in-order delivery guarantee
  interface           Select an interface to configure
  ip                  Configure IP features
  line                Configure a terminal line
  logging             Modify message logging facilities
  no                  Negate a command or set its defaults
  ntp                 NTP Configuration
  power               Configure power supply
  poweroff            Poweroff a module in the switch
  qos                 Configure priority of FC control frames
  radius-server       Configure RADIUS related parameters
  role                Configure roles
  rscn                Config commands for RSCN
  snmp-server         Configure snmp server
  span                Enter SPAN configuration mode
```

```
ssh                 Configure SSH parameters
switchname          Configure system's network name
system              System config command
telnet              Enable telnet
trunk               Configure Switch wide trunk protocol
username            Configure user information.
vsan                Enter the vsan configuration mode
wwn                 Set secondary base MAC addr and range for additional WWNs
zone                Zone configuration commands
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.

Note In configuration mode, you can alternatively enter
— **Ctrl-Z** instead of the **end** command, and
— **Ctrl-G** instead of the **exit** command

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

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

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

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

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

Table 1-2 Useful Command Key Description

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

Table 1-3 displays the commonly used configuration submodes.

Table 1-3 Submodes Within the Configuration Mode

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

CHAPTER 2

Quick Installation

This chapter describes the basic operations required to install the Cisco MDS 9000 Family switches.

Note Before you install, operate, or service the system, read the *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family* for important safety information you should know before working with the system.

For detailed information about installing a Cisco MDS 9000 Family switch, refer to the appropriate hardware guide.

To install a Cisco MDS 9000 Family switch, follow these steps:

Step 1 Remove the Cisco MDS 9000 Family switch from the shipping container.

Note Compare the shipment to the equipment list provided by your customer service representative and verify that you have received all items. Check for damage and report any discrepancies or damage to your customer service representative.

Step 2 Install the switch in the rack.

Allow the following clearance for the switch:

- Have the following minimum vertical rack space per chassis:
  - Cisco MDS 9200 Series chassis: 1.75 inches (4.4 cm) per chassis or 1 rack unit (RU)
  - Cisco MDS 9216 chassis: 5.25 inches (13.3 cm) or 3 RUs
  - Cisco MDS 9506 chassis: 12.25 inches (31.1 cm) or 7 RUs
  - Cisco MDS 9509 chassis: 24.5 inches (62.2 cm) or 14 RUs
- Put 17.75 inches (45.1 cm) between the rack mounting rails.
- Put 6 inches (15.2 cm) between two chassis for horizontal distance.
- Put 2.5 inches (6.4 cm) between the chassis air vents and any walls .
- Have the following clearance for four-post EIA cabinets (perforated or solid-walled):
  - To ensure the minimum bend radius for fiber optic cables, the front mounting rails of the cabinet should be offset from the front door by a minimum of 3 inches (7.6 cm), and a minimum of 5 inches (12.7 cm) if cable management brackets are installed on the front of the chassis.

- To ensure the minimum bend radius for fiber optic cables, the front mounting rails of the cabinet should be offset from the front door by a minimum of 3 inches (7.6 cm), and a minimum of 5 inches (12.7 cm) if cable management brackets are installed on the front of the chassis.
- To allow for rear bracket installation, the distance between the outside face of the front mounting rail and the outside face of the back mounting rail should be 23.5 to 34.0 inches (59.7 to 86.4 cm).
- To ensure adequate spacing, there should be a minimum of 2.5 inches (6.4 cm) clear space between the side edge of the chassis and the side wall of the cabinet. No sizeable flow obstructions should be immediately in the way of the chassis air intake or exhaust vents.

Note The Telco and EIA Shelf Bracket Kit is optional and is not provided with the switch. To order the kit, contact your switch provider.

Step 3 Connect the power cords to the switch and the power source using the appropriate power connectors.

Figure 2-1 and Figure 2-2 show the power connectors available for the Cisco MDS 9000 Family switches.

Figure 2-1 Power Connectors for the Cisco MDS 9100 Series Switches and Cisco MDS 9216 Switch

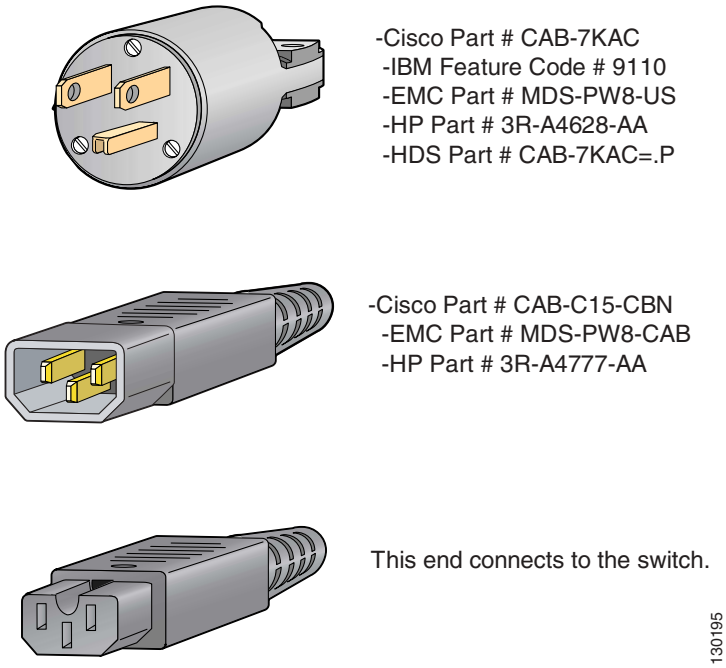
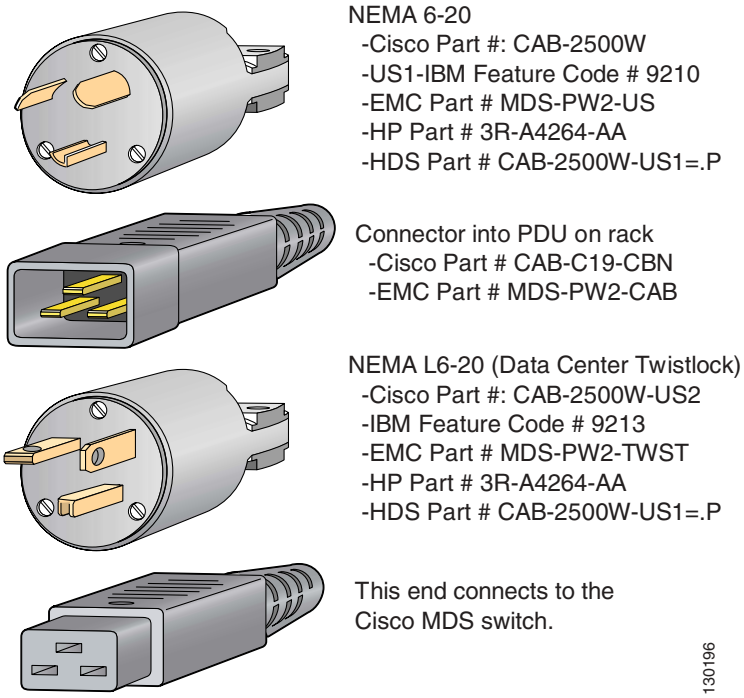


Figure 2-2 Power Connectors for the Cisco MDS 9500 Series Switches



Step 4 Connect the included rolled cable to the console port. Figure 2-3 shows how to connect the console port on a Cisco MDS 9100 Series switch.

Figure 2-3 Connecting the Console Port on a Cisco MDS 9100 Series Switch

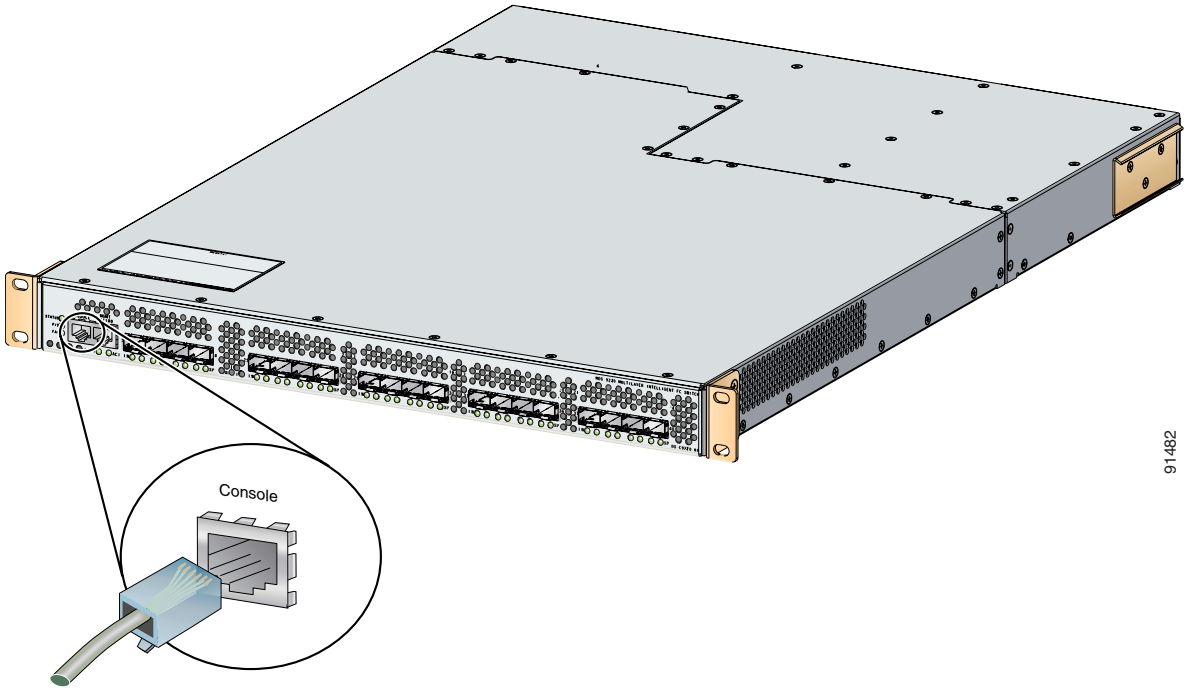


Figure 2-4 shows how to connect the console port on a Cisco MDS 9200 Series switch.

Figure 2-4 Connecting the Console Port on a Cisco MDS 9200 Series Switch

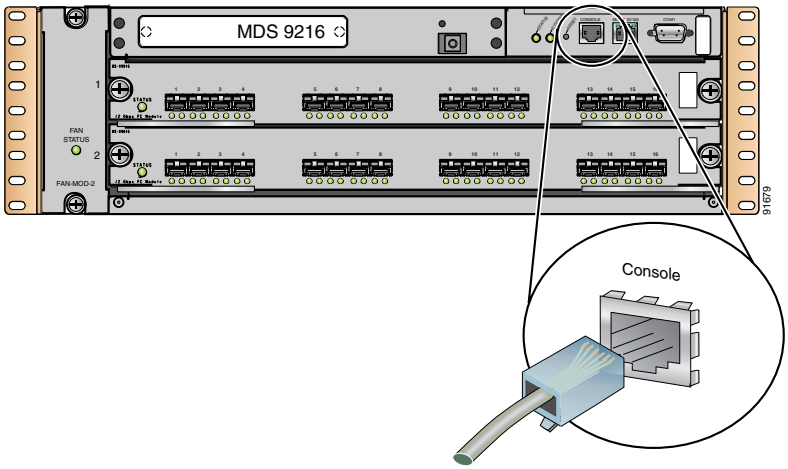
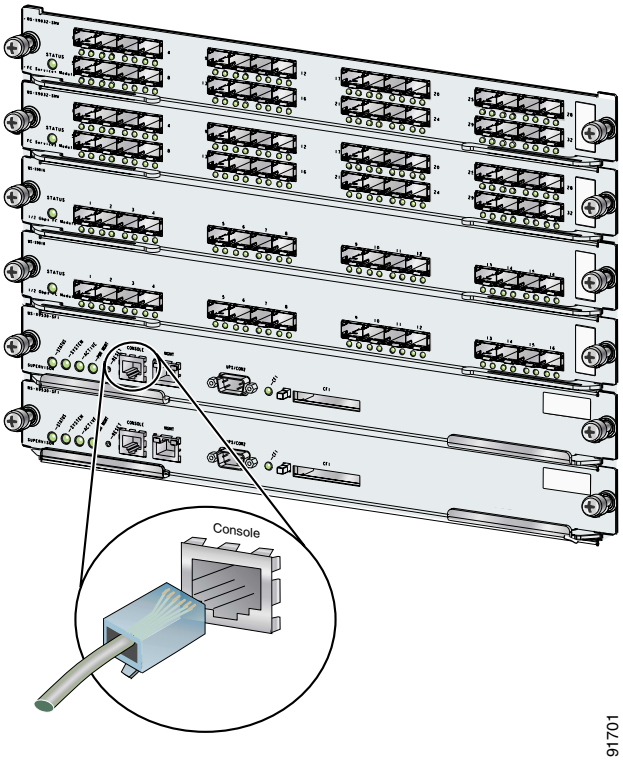


Figure 2-5 shows how to connect the console port on a Cisco MDS 9500 Series switch.

Figure 2-5 Connecting the Console Port on a Cisco MDS 9500 Series Switch



Step 5 Connect the other end of the rolled cable to a PC that is running HyperTerminal.

Note For information about how to turn off hardware flow control, refer to the following website for the latest Cisco MDS 9000 Family configuration guides: http://www.cisco.com/univercd/cc/td/doc/product/sn5000/mds9000/index.htm.

Step 6 Connect the 10/100 copper Ethernet cable to the 10/100 Ethernet management port on the Cisco MDS 9000 Family switch.

Figure 2-6 shows how to connect the 10/100 Ethernet management port on a Cisco MDS 9200 Series switch.

Figure 2-6 Connecting the 10/100 Ethernet Management Port on a Cisco MDS 9200 Series Switch

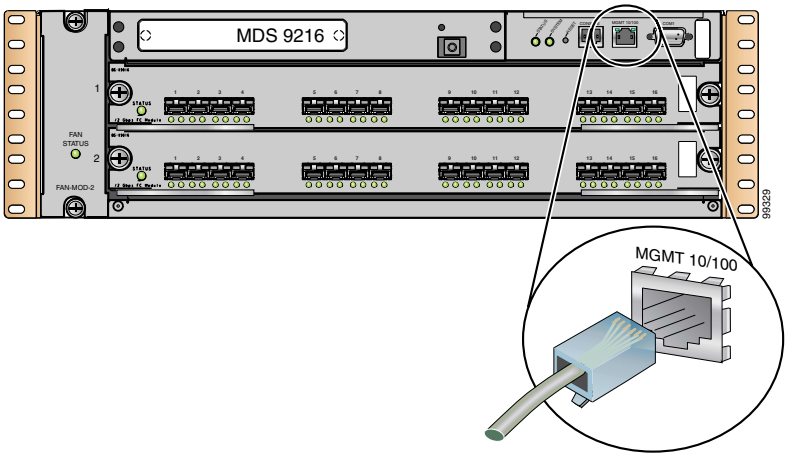
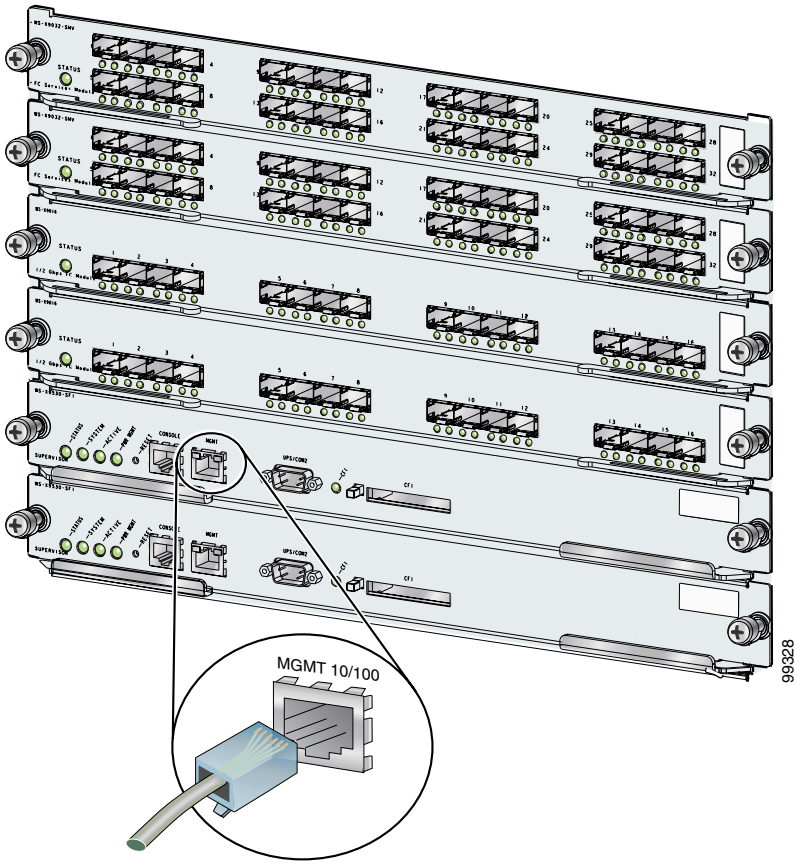


Figure 2-7 shows how to connect the 10/100 Ethernet management port on a Cisco MDS 9500 Series switch.

Figure 2-7 Connecting the 10/100 Ethernet Management Port on a Cisco MDS 9500 Series Switch



Step 7 Continue to Chapter 3, "Initial Configuration" for an explanation of the setup script prompts and other basic configurations.

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 Switch in the Cisco MDS 9000 Family

The following procedure reviews 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. See Chapter 2, “Quick Installation” for information on hardware installation.

Before you can configure a switch, follow these steps:

Step 1 Verify that the following physical connections are present on the new Cisco MDS 9000 Family 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.

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 Verify that the switch is powered. The switch boots automatically and the `switch#` prompt appears in your terminal window.

Initial Setup Routine

The first time that you access a switch in the Cisco MDS 9000 Family, it runs a setup program that prompts you for the IP address and other configuration information necessary for the switch to communicate over the supervisor module Ethernet interface. This information is required to configure and manage the switch.

Note The IP address can only be configured from the CLI. When you power up the switch for the first time assign the IP address. After you perform this step, the Cisco MDS 9000 Family Fabric Manager can reach the switch.

Preparing to Configure the Switch

Before you configure a switch in the Cisco MDS 9000 Family for the first time, you need the following information:

- Administrator password, including:
  - Changing the default password (admin) for the administrator.
  - Creating an additional login account and password.
- SNMPv3 user name and authentication password.
- SNMP community string.
- Switch name—This is your switch prompt.

- IP address for the switch's management interface—The management interface can be an out-of-band Ethernet interface or an in-band Fibre Channel interface.
- Subnet mask for the switch's management interface.
- 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.
  - Otherwise, provide an IP address of the default gateway.
- DNS IP address (optional).
- Default domain name (optional).
- SSH service on the switch—To enable this service, select the type of SSH key (dsa/rsa/rsa1) and number of key bits (768 to 2048).
- NTP server IP address (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 User

All Cisco MDS 9000 Family switches have the network administrator as a default user (admin) and a default password (admin). You can change the default password, if required, during the initial setup process. You cannot change the default user at any time.

During the initial setup process, you have the option to configure one additional user in the network administrator role. If you change the administrator password during the initial setup process and subsequently forget this new password, you have the option to recover this password.

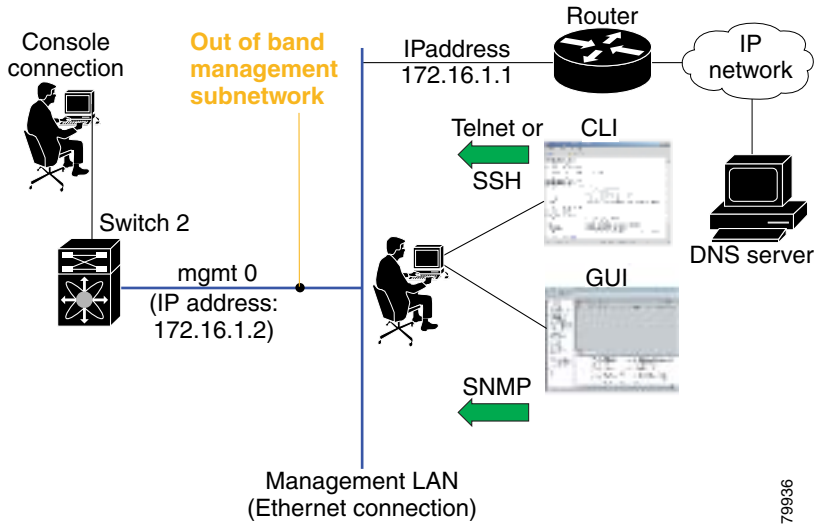
Refer to the *Cisco MDS 9000 Family Configuration Guide* for more information on the default login.

Setup Options

The setup scenario differs based on the subnet to which you are adding the new switch. The Cisco MDS 9000 Family supports two types of network management access:

- Out-of-band management—This feature provides a connection to the network through a supervisor module front panel Ethernet port.
- In-band management—This feature provides IP over Fibre Channel (IPFC) to manage the switches. The in-band management feature is transparent to the network management system (NMS). Instead of conventional Ethernet physical media, switches in the Cisco MDS 9000 Family use IPFC as the transport mechanism (see Figure 3-1).

Figure 3-1 Management Access to Switches



Configuring Out-of-Band Management

Note You can configure both in-band and out-of-band configuration together by entering **Yes** in both Step 11c. and Step 11d. in the following procedure.

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

Step 1 Power on the switch. Switches in the Cisco MDS 9000 Family boot automatically.

Step 2 Enter the new password for the administrator.

```
Enter the password for admin: 2004asdf*lkjh18
```

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. As of Cisco SAN-OS Release 2.0(1b), **admin** is not the default password for any switch in the Cisco MDS 9000 Family. You must explicitly configure a password that meets the requirements listed in this tip.

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

```
This setup utility will guide you through the basic configuration of the system. Setup
configures only enough connectivity for management of the system.

Please register Cisco MDS 9000 Family devices promptly with your supplier. Failure to
register may affect response times for initial service calls. MDS devices must be
registered to receive entitled support services.

Press Enter incase you want to skip any dialog. Use ctrl-c at anytime to skip away
remaining dialogs.

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

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

Step 4 Enter the new password for the administrator (admin is the default).

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

Step 5 Enter **yes** (no is the default) to create additional 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.

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
```

Step 6 Enter **yes** (yes is the default) to create an SNMPv3 account.

```
Configure SNMPv3 Management parameters (yes/no) [y]: yes
```

a. Enter the user name (admin is the default).

```
SNMPv3 user name [admin]: admin
```

b. Enter the SNMPv3 password (minimum of eight characters). The default is **admin123**.

```
SNMPv3 user authentication password: admin_pass
```

Note By default, if the admin password is at least eight characters, then the SNMP authentication password is the same as the admin password (at least eight characters). If the admin password is less than eight characters, then you need to provide a new password for SNMP.
The admin password can have a minimum of one character, but the SNMP authentication password must have a minimum of eight characters.

Step 7 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 8 Enter a name for the switch.

Note The switch name is limited to 32 alphanumeric characters. The default is **switch**.

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

Step 9 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 10 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 11 Enter **yes** (**no** is the default) to configure advanced IP options such as inband management, static routes, default network, DNS and domain name.

```
Configure Advanced IP options (yes/no)? [n]: yes
```

a. Enter **no** (no is the default) at the in-band management configuration prompt.

```
Continue with in-band (VSAN1) management configuration? (yes/no) [no]: no
```

Note In-band management is used for IPFC (not FCIP). It is easier to configure through the Fabric Manager GUI and configure for a specific dedicated VSAN.

b. Enter **yes** (yes is the default) to enable IP routing capabilities.

```
Enable the ip routing? (yes/no) [y]: yes
```

c. Enter **yes** (yes is the default) to configure a static route (recommended).

```
Configure static route: (yes/no) [y]: yes
```

Enter the destination prefix.

```
Destination prefix: dest_prefix
```

Type the destination prefix mask.

```
Destination prefix mask: dest_mask
```

Type the next hop IP address.

```
Next hop ip address: next_hop_address
```

Note This should be configured later if you have an IPS module to differentiate IP traffic out of the Gigabyte Ethernet ports versus the management ports.

Note Be sure to configure the IP route, the default network IP address, and the default gateway IP 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.

d. Enter **yes** (yes is the default) to configure the default network (recommended).

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

Enter the default network IP address.

Note The default network IP address is the destination prefix provided in Step 11c .

```
Default network IP address [dest_prefix]: dest_prefix
```

e. Enter **yes** (yes is the default) to configure the DNS IP address.

```
Configure the DNS IP address? (yes/no) [y]: yes
```

Enter the DNS IP address.

```
DNS IP address: name_server
```

f. Enter **yes** (default is no) to configure the default domain name.

```
Configure the default domain name? (yes/no) [n]: yes
```

Enter the default domain name.

```
Default domain name: domain_name
```

Step 12 Enter **yes** (yes is the default) to enable Telnet service.

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

Step 13 Enter **yes** (no is the default) to enable the SSH service.

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

Step 14 Enter the SSH key type that you would like to generate.

```
Type the SSH key you would like to generate (dsa/rsa/rsa1)? dsa
```

Step 15 Enter the number of key bits within the specified range.

```
Enter the number of key bits? (768 to 2048): 768
```

Step 16 Enter **yes** (no is the default) to configure the NTP server.

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

a. Enter the NTP server IP address.

```
NTP server IP address: ntp_server_IP_address
```

Step 17 Enter **shut** (shut is the default) to configure the default switchport interface to the shut state.

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

Note The management ethernet interface is not shut down at this point—only the Fibre Channel, iSCSI, FCIP, and Gigabit Ethernet interfaces are shut down.

Note We recommend that you lock things down so the device does not accidentally log into the wrong fabric.

Step 18 Enter **on** (on is the default) to configure the switchport trunk mode.

```
Configure default switchport trunk mode (on/off/auto) [on]: on
```

Note Set this at ON because you can always scale back the allowed VSAN traffic to a single VSAN.

Step 19 Enter **on** (off is the default) to configure the PortChannel auto-create state.

```
Configure default port-channel auto-create state (on/off) [off]: on
```

Step 20 Enter **permit** (deny is the default) to deny a default zone policy configuration.

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

Permits traffic flow to all members of the default zone.

Step 21 Enter **yes** (no is the default) to disable a full zone set distribution.

```
Enable full zoneset distribution (yes/no) [n]: yes
```

Disables the switch-wide default for the full zone set distribution feature.

Note Enabling full zone set distribution ensures that all zoning information is propagated to all of the switches that contain the same VSAN in the fabric.

Step 22 Review and edit the configuration that you have just entered.

Step 23 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
  username user_name password user_pass role network-admin
  snmp-server community snmp_community ro
  switchname switch
  interface mgmt0
    ip address ip_address subnet_mask
    no shutdown
  ip routing
  ip route dest_prefix dest_mask dest_address
  ip default-network dest_prefix
  ip default-gateway default_gateway
  ip name-server name_server
  ip domain-name domain_name
  telnet server enable
  ssh key dsa 768 force
  ssh server enable
  ntp server ipaddr ntp_server
  system default switchport shutdown
  system default switchport trunk mode on
  system default port-channel auto-create
  zone default-zone permit vsan 1-4093
  zoneset distribute full vsan 1-4093

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

Step 24 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** in order to save the new configuration. This ensures that the kickstart and system images are also automatically configured.

In-Band Management Configuration

The in-band management logical interface is VSAN 1. This management interface uses the Fibre Channel infrastructure to transport IP traffic. An interface for VSAN 1 is created on every switch in the fabric. Each switch should have its VSAN 1 interface configured with an IP address in the same subnetwork. A default route that points to the switch providing access to the IP network should be configured on every switch in the Fibre Channel fabric (see Chapter 4, “Configuring VSANs, Interfaces, and Zones”).

Note You can configure both in-band and out-of-band configuration together by entering **Yes** in both Step 9c. and Step 9d. in the following procedure.

To configure a switch for first time in-band access, follow these steps:

Step 1 Power on the switch. Switches in the Cisco MDS 9000 Family boot automatically.

Step 2 Enter the new password for the administrator.

```
Enter the password for admin: 2004asdf*lkjh18
```

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. As of Cisco SAN-OS Release 2.0(1b), **admin** is not the default password for any switch in the Cisco MDS 9000 Family. You must explicitly configure a password that meets the requirements listed in this tip.

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

```
This setup utility will guide you through the basic configuration of the system. Setup
configures only enough connectivity for management of the system.

Please register Cisco MDS 9000 Family devices promptly with your supplier. Failure to
register may affect response times for initial service calls. MDS devices must be
registered to receive entitled support services.

Press Enter incase you want to skip any dialog. Use ctrl-c at anytime to skip away
remaining dialogs.

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

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

Step 4 Enter **no** (no is the default) if you do not wish to create additional accounts.

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

Step 5 Configure the read-only or read-write SNMP community string.

a. Enter **no** (no is the default) to avoid configuring the read-only SNMP community string.

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

b. Enter **no** (no is the default) to configure the read-only SNMP community string.

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

c. 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. The default is **switch**.

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

Step 7 Enter **no** (yes is the default) at the configuration prompt to configure out-of-band management.

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

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

```
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** (**no** is the default) to configure advanced IP options such as Inband management, static routes, default network, dns and domain name.

```
Configure Advanced IP options (yes/no)? [n]: yes
```

a. Enter **yes** (no is the default) at the in-band management configuration prompt.

```
Continue with in-band (VSAN1) management configuration? (yes/no) [no]: yes
```

Enter the VSAN 1 IP address.

```
VSAN1 IP address: ip_address
```

Enter the subnet mask.

```
VSAN1 IP net mask: subnet_mask
```

b. Enter **no** (yes is the default) to enable IP routing capabilities.

```
Enable ip routing capabilities? (yes/no) [y]: no
```

c. Enter **no** (yes is the default) to configure a static route.

```
Configure static route: (yes/no) [y]: no
```

d. Enter **no** (yes is the default) to configure the default network.

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

e. Enter **no** (yes is the default) to configure the DNS IP address.

```
Configure the DNS IP address? (yes/no) [y]: no
```

f. Enter **no** (no is the default) to skip the default domain name configuration.

```
Configure the default domain name? (yes/no) [n]: no
```

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

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

Step 11 Enter **yes** (no is the default) to enable the SSH service.

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

Step 12 Enter the SSH key type that you would like to generate.

```
Type the SSH key you would like to generate (dsa/rsa/rsa1)? rsa
```

Step 13 Enter the number of key bits within the specified range.

```
Enter the number of key bits? (768 to 1024): 1024
```

Step 14 Enter **no** (no is the default) to configure the NTP server.

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

Step 15 Enter **shut** (shut is the default) to configure the default switchport interface to the shut state.

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

Note The management Ethernet interface is not shut down at this point—only the Fibre Channel, iSCSI, FCIP, and Gigabit Ethernet interfaces are shut down.

Step 16 Enter **auto** (off is the default) to configure the switchport trunk mode.

```
Configure default switchport trunk mode (on/off/auto) [off]: auto
```

Step 17 Enter **off** (off is the default) to configure the PortChannel auto-create state.

```
Configure default port-channel auto-create state (on/off) [off]: off
```

Step 18 Enter **deny** (deny is the default) to deny a default zone policy configuration.

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

Denies traffic flow to all members of the default zone.

Step 19 Enter **no** (no is the default) to disable a full zone set distribution.

```
Enable full zoneset distribution (yes/no) [n]: no
```

Disables the switch-wide default for the full zone set distribution feature.

You see the new configuration. Review and edit the configuration that you have just entered.

Step 20 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
  snmp-server community snmp_community rw
  switchname switch
  interface vsan1
    ip address ip_address subnet_mask
    no shutdown
  ip default-gateway default_gateway
  no telnet server enable
  ssh key rsa 1024 force
  ssh server enable
  no system default switchport shutdown
  system default switchport trunk mode auto
  no zone default-zone permit vsan 1-4093
  no zoneset distribute full vsan 1-4093

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

Step 21 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** in order to save the new configuration. This ensures that the kickstart and system images are also automatically configured.

Accessing the Switch

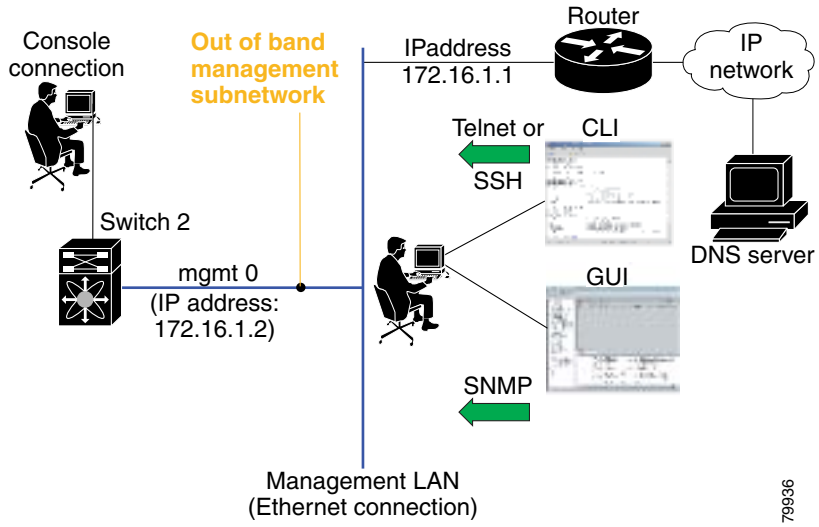
After initial configuration, you can access the switch in one of three ways (see Figure 3-2):

- In-band IP (IPFC) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use SNMP to connect to a Cisco MDS 9000 Fabric Manager GUI.
- Out-of-band (10/100BASE-T Ethernet) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use SNMP to connect to a Cisco MDS 9000 Fabric Manager GUI.

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

- Serial console access—You can use a serial port connection to access the CLI.

Figure 3-2 Switch Access Options



Obtaining and Installing License Key Files

The licensing functionality is available in all switches in the Cisco MDS 9000 Family. This functionality allows you to access specified premium features on the switch after you install the appropriate license for that feature. Licenses are sold, supported, and enforced as of Cisco MDS SAN-OS Release 1.3(1).

The license key file is a switch-specific unique file that specifies the licensed features. Each file contains digital signatures to prevent tampering and modification. License keys are required to use a licensed feature. License keys are enforced within a specified time span.

- License keys are required if your switch is running Cisco MDS SAN-OS Release 1.3(x) or later.

- License keys are not required to use licensed features in Cisco MDS SAN-OS Release 1.(x) and 1.2(x).

To obtain and install new or updated license key files, follow these steps:

Step 1 Log into the switch through the console port of the active supervisor.

Step 2 Use the **show license host-id** command to obtain the serial number for your switch. The host ID is also referred to as the switch serial number.

```
switch# show license host-id
License hostid: VDH=FOX064317SQ
```

Tip Use the entire ID that appears after the colon (:) sign. In this example, the host ID is `VDH=FOX064317SQ`.

Step 3 Obtain either your claim certificate or your proof of purchase document. This document accompanies every Cisco MDS switch.

Step 4 Get the product authorization key (PAK) from either the claim certificate or the proof of purchase document.

Step 5 Locate the website URL from either the claim certificate or the proof of purchase document.

Step 6 Access the specified URL that applies to your switch and enter the switch serial number and the PAK.

The license key file is sent to you by e-mail. The license key file is digitally signed to only authorize use on the requested switch. The requested features are also enabled once the SAN-OS software on the specified switch accesses the license key file.

Caution Install the license key file in the specified MDS switch without making any modifications.

A license is either permanent or it expires on a fixed date. If you do not have a license, the grace period for using that license starts from the first time you start using a feature offered by that license.

Step 7 Download the license key file to the switch using the **copy** command.

```
switch# copy <scheme>://<url> bootflash:license_file.lic
```

Tip If you need to install multiple licenses in any switch in the Cisco MDS 9000 Family, be sure to provide unique file names for each license key file.

Step 8 Install the license by issuing the **install license** command on the active supervisor module from the switch console.

```
switch# install license bootflash:license_file.lic
Installing license ..done
```

Note If you provide a target name for the license key file, the file is installed with the specified name. Otherwise, the file name specified in the license key file is used to install the license.

Step 9 Exit the switch console and open a new terminal session to view all license files installed on the switch using the **show license** command.

```
switch# show license
Permanent.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT MAINFRAME_PKG cisco 1.0 permanent uncounted \
        HOSTID=VDH=FOX0646S017 \
        NOTICE="<LicFileID></LicFileID><LicLineID>0</LicLineID> \
        <PAK>dummyPak</PAK>" SIGN=EE9F91EA4B64
```

Note If the license meets all guidelines when the **install license** command is issued, all features and modules continue functioning as configured. This is true for any switch in the Cisco MDS 9000 Family.

Displaying License Information

Use the **show license** commands to display all license information configured on this switch. Table 3-1 lists the **show** commands and the information they display.

Table 3-1 show license Commands

show Command	Description
show license usage	Displays information about current license usage.
show license host-id	Displays the Host ID for the license.
show license	Displays all installed license key files and their contents.
show license brief	Displays a list of installed license key files.

Verifying the Module Status

Before you begin configuring the switch, you need to ensure that the modules in the chassis are functioning as designed. To verify the status of a module at any time, issue 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
---  -----  -------------------------------- ------------------ ------------
2    8      IP Storage Services Module       DS-X9308-SMIP      ok
5    0      Supervisor/Fabric-1              DS-X9530-SF1-K9    active *
6    0      Supervisor/Fabric-1              DS-X9530-SF1-K9    ha-standby
8    0      Caching Services Module          DS-X9560-SMAP      ok
9    32     1/2 Gbps FC Module               DS-X9032           ok

Mod  Sw           Hw      World-Wide-Name(s) (WWN)
---  -----------  ------  --------------------------------------------------
2    1.3(0.106a)  0.206   20:41:00:05:30:00:00:00 to 20:48:00:05:30:00:00:00
5    1.3(0.106a)  0.602   --
6    1.3(0.106a)) 0.602   --
8    1.3(0.106a)  0.702   --
9    1.3(0.106a)  0.3     22:01:00:05:30:00:00:00 to 22:20:00:05:30:00:00:00


Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
2    00-05-30-00-9d-d2 to 00-05-30-00-9d-de  JAB064605a2
```

```
5    00-05-30-00-64-be to 00-05-30-00-64-c2  JAB06350B1R
6    00-d0-97-38-b3-f9 to 00-d0-97-38-b3-fd  JAB06350B1R
8    00-05-30-01-37-7a to 00-05-30-01-37-fe  JAB072705ja
9    00-05-30-00-2d-e2 to 00-05-30-00-2d-e6  JAB06280ae9

* this terminal session
```

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

Configuring Date and Time

Switches in the Cisco MDS 9000 Family use Coordinated Universal Time (UTC), which is the same as Greenwich Mean Time (GMT). To change the default time on the switch, issue the **clock** command from EXEC mode.

You can also specify a time zone for the switch and adjust for daylight saving time.

Configuring Default Time and Date, Time Zone, and Daylight Saving Time

To specify the default time and date, local time zone, and daylight savings adjustment, follow these steps:

	Command	Purpose
Step 1	`switch# clock set 12:07:50 23 September 2002` `Mon Sep 23 12:07:50 UTC 2002`	Changes the default time and date on the switch based on Coordinated Universal Time (UTC), which is the same as Greenwich Mean Time (GMT). **Note** The **clock** command changes are saved across system resets.
Step 2	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 3	`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 4	`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 set the Pacific standard offset time as negative 8 hours and 0 minutes.

	Command	Purpose

Step 5	`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*
	
	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.

Step 6	`switch(config)# exit` `switch#`	Returns to EXEC mode.
Step 7	`switch# show clock`	Verifies the time zone configuration.
Step 8	`switch# show run`	Displays changes made to the time zone configuration along with other configuration information.

Configuring NTP

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.

To configure NTP in a server association, follow these steps:

	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)# ntp peer 10.20.10.0` `switch(config)#`	Forms a peer association with a peer. You can specify multiple associations.
Step 4	`switch(config)# exit` `switch#`	Returns to EXEC mode.

	Command	Purpose
Step 5	`switch# copy running-config startup-config`	Saves your configuration changes to NVRAM. **Tip** This is one instance where you can save the configuration as a result of an NTP configuration change. You can issue this command at any time.

Step 6	`switch# show ntp peers`
	`----------`
	`Peer IP Address Serv/Peer`
	`----------`
	`10.20.10.2 Server`
	`10.20.10.0 Peer`
		Displays the configured server and peer associations.
		Note A domain name is resolved only when you have a DNS server configured.

Configuring the Management Interface

On director class switches, a single IP address is used to manage the switch. The active supervisor module's management (mgmt0) interface uses this IP address. The mgmt0 interface on the standby supervisor module remains in an inactive state and cannot be accessed until a switchover happens. After a switchover, the mgmt0 interface on the standby supervisor module becomes active and assumes the same IP address as the previously active supervisor module.

The management interface on the switch allows multiple simultaneous Telnet or SNMP sessions.

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.

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.

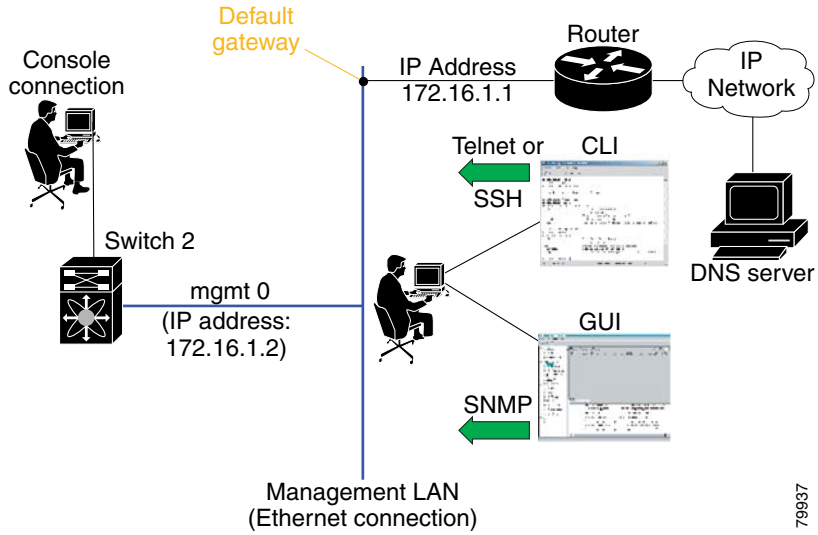
To configure remote management access, follow these steps:

	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 1.1.1.0 255.255.255.0`	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 1.1.1.1`	Configures the default gateway address.

Configuring the Default Gateway

The supervisor module sends IP packets with unresolved destination IP addresses to the default gateway (see Figure 3-3).

Figure 3-3 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.

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 following **show** commands to view the configuration file. Table 3-2 lists the show commands and the information they display.

Table 3-2 Show Config Commands

Show Command	Description
show running-config	Displays the running configuration file.
show startup-config	Displays the startup configuration file.

Downloading Configuration Files to the Switch

You can configure a switch in the Cisco MDS 9000 Family by using configuration files you create or download from another switch. In addition, you can configure the switch using a configuration stored on an external CompactFlash disk.

Before you begin downloading a configuration file using a remote server, do the following:

- Ensure 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 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.

To configure NTP in a server association, follow these steps:

	Command	Purpose
Step 1	switch# **copy** *<scheme>***://***<url>* **system:running-config**	Downloads a running configuration file from a remote server, where *scheme* is TFTP, FTP, SCP, or SFTP.
Step 2	switch **copy slot0:dns-config.cfg system:running-config**	Downloads a configuration file stored on an external CompactFlash disk.

Saving the Configuration

After you have created a configuration, you save the configuration using the following **copy** command:

```
switch# copy system:running-config nvram:startup-config
```

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

Downgrading to an Earlier Release

Use the **install all** command to gracefully reload the switch and handle configuration conversions. When downgrading any switch in the Cisco MDS 9000 Family, avoid using the **reload** command.

For example, to revert to Cisco MDS SAN-OS Release 1.4(4) or 1.4(3a) from a later release, follow these steps:

Step 1 Save the configuration using the **copy running-config startup-config** command.

Step 2 Issue the **install all** command to downgrade the software.

Accessing Standby Supervisor File Systems

To access contents of the standby supervisor module (remote), follow these steps:

Step 1 Verify if the standby supervisor module has sufficient space for new image files.

```
switch# dir bootflash://sup-remote
   12198912     Aug 27 17:21:10 2003  bootflash:boot-39a
   12198912     Aug 27 16:29:18 2003  bootflash:m9500-sf1ek9-kickstart-mzg.1.3.0.39a.bin
    1921922     Sep 14 19:58:12 2003  aOldImage
    1864931     Apr 29 12:41:50 2003  bOldImage
    1864931     Apr 29 12:41:59 2003  dplug2
      12288     Apr 18 20:23:11 2003  lost+found/
   12097024     Nov 21 16:34:18 2003  m9500-sf1ek9-kickstart-mz.1.3.1.1.bin
   41574014     Nov 21 16:34:47 2003  m9500-sf1ek9-mz.1.3.1.1.bin
       1024     Oct 28 20:24:59 2003  newer-fs/
    2021518     Oct 11 15:49:41 2003  plugin-69a
Usage for bootflash://sup-remote
  102081536 bytes used
   82478080 bytes free
  184559616 bytes total
```

Step 2 Delete files, if required, to make more space for the new image files.

```
switch# del aOldImage
```

Managing Files

This section describes how to work with files on the switch file systems.

Copying Files

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

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

Table 3-3 copy Command Syntax

Scheme	Server	File Name
bootflash	sup-active sup-standby sup-1 or module-5 sup-2 or module-6 sup-local sup-remote	User-specified
slot0	—	User-specified
volatile	—	User-specified
nvram	—	startup-config or snapshot-config
system	—	running-config
tftp[1]	IP address or DNS name	User-specified
ftp		
scp (secure copy)		
sftp		
core	*slot-numbe*r	Process identifier number

1. When downloading and uploading files, a TFTP limitation restricts a TFTP client to a 32-MB file size and some TFTP servers to a 16-MB file size.

Use the **copy** command as follows:

- This example shows how to copy a file from the active supervisor module's (sup-1 in slot 5) bootflash to the standby supervisor module's (sup-2 in slot 6) bootflash.

```
switch# copy bootflash:system_image bootflash://sup-2/system_image
```

- This example shows how to overwrite the contents of an existing configuration in NVRAM.

```
switch# copy nvram:snapshot-config nvram:startup-config
Warning: this command is going to overwrite your current startup-config.
Do you wish to continue? {y/n} [y] y
```

- This example shows how to copy a running configuration to the bootflash: directory.

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

- This example shows how to copy a system image file from the SCP server to bootflash.

```
switch# copy scp://user@10.1.7.2/system-image bootflash:system-image
```

- This example shows how to copy a script file from the SFTP server to the volatile: directory.

```
switch# copy sftp://172.16.10.100/myscript.txt volatile:myscript.txt
```

Note Use the **show version image** command to verify if the downloaded images are valid.

Deleting Files

Assuming you are already in the bootflash: directory, use the **delete** command as follows:

- This example shows how to delete a file from the bootflash: directory.

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

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

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

- This example shows how to delete the file named test from the Flash card inserted in slot 0.

```
switch# delete slot0:test
Delete slot0:test? [confirm]
```

- This example shows how to delete the entire `my-dir` directory and all its contents.

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

Configuring Console Port Settings

A console port is an asynchronous serial port that enables switches in the Cisco MDS 9000 Family to be set up for initial configuration through a standard RS-232 port with an RJ-45 connector. Any device connected to this port must be capable of asynchronous transmission. Connection to a terminal requires a terminal emulator to be configured as 9600 baud, 8 data bits, 1 stop bit, no parity.

Caution The console baud rate automatically reverts to the default rate (9600) after any BIOS upgrade.

To configure the console port parameters from the console terminal, follow these steps:

	Command	Command
Step 1	`switch# config terminal` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# line console` `switch(config-console)#`	Enters the line console configuration mode.
Step 3	`switch(config-console)# speed 9600`	Configures the port speed for the serial console. The default console baud rate is 9600 baud. The valid range is between 110 and 115,200 bps (110, 150, 300, 600, 1200, 2400, 4800, 9600, 19200, 28800, 38400, 57600, 115200). Be sure to specify one of these exact values.
Step 4	`switch(config-console)# databits 8`	Configures the data bits for the console connection. The default is 8 data bits and the valid range is between 5 and 8 data bits.
Step 5	`switch(config-console)# stopbits 1`	Configures the stop bits for the console connection. The default is 1 stop bit and the valid values are 1 or 2 stop bits.
Step 6	`switch(config-console)# parity none`	Configures the parity for the console connection. The default is no parity and the valid values are even or odd parity.

Use the **show line console** command to verify the configured console settings. This command also displays problems that may have occurred along with the other registration statistics.

Configuring COM1 Port Settings

A COM1 port is a RS-232 port with a DB-9 interface that enables you to connect to an external serial communication device such as a modem. Connection to a terminal requires the terminal emulator to be configured as 9600 baud, 8 data bits, 1 stop bit, no parity.

To configure the COM1 port parameters, follow these steps:

	Command	Command
Step 1	`switch# config terminal` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# line com1` `switch(config-com1)#`	Enters the COM1 port configuration mode.
Step 3	`switch(config-com1)# speed 9600`	Configures the port speed for the COM1 connection. The default console baud rate is 9600 baud. The valid range is between 110 and 115,200 bps (110, 150, 300, 600, 1200, 2400, 4800, 9600, 19200, 28800, 38400, 57600, 115200). Be sure to specify one of these exact values. **Note** This configuration depends on the incoming speed of the modem connected to COM1.
Step 4	`switch(config-com1)# databits 8`	Configures the data bits for the COM1 connection. The default is 8 data bits and the valid range is between 5 and 8 data bits.
Step 5	`switch(config-com1)# stopbits 1`	Configures the stop bits for the COM1 connection. The default is 1 stop bits and the valid values are 1 or 2 stop bits.
Step 6	`switch(config-com1)# parity none`	Configures the parity for the COM1 connection. The default is no parity and the valid values are even or odd parity.
Step 7	`switch(config-com1)# no flowcontrol hardware`	Disables hardware flow control. By default, hardware flow control is enabled on all switches in the Cisco 9000 Family. When enabled, this option is useful in protecting data loss at higher baud rates. **Note** This option is only available through the COM1 port.

Use the **show line com1** command to verify the configured COM1 settings. This command also displays problems that may have occurred along with the other registration statistics.

Configuring Modem Connections

Modems can only be configured if they are connected to the console or COM1 ports. A modem connection to a switch in the Cisco MDS 9000 Family does not affect switch functionality.

Guidelines to Configure Modems

Tip We recommend you use the COM1 port to connect the modem from a Cisco MDS 9216 switch or from any director in the Cisco MDS 9500 Series.

The following guidelines apply to modem configurations:

- The following Cisco modems were tested to work in the SAN-OS environment:
  - MultiTech MT2834BA (http://www.multitech.com/PRODUCTS/Families/MultiModemII/)
  - Hayes Accura V.92 (http://www.hayesmicro.com/Products/accura-prod-v92.htm)
- Connect the modem before attempting to configure the modem.
- Do not connect a modem to the console port while the system is booting.

  Follow the procedure specified in the "Initializing a Modem in a Powered-On Switch" section on page 3-28.

Enabling Modem Connections

To configure a modem connection through the COM1 port, follow these steps:

	Command	Command
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# line com1` `switch(config-com1)#`	Enters the COM1 port configuration mode.
Step 3	`switch(config-com1)# modem in`	Enables the COM1 port to only connect to a modem.
	`switch(config-com1)# no modem in`	Disables (default) the current modem from executing its functions.

To configure a modem connection through the console port, follow these steps:

	Command	Command
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# line console` `switch(config-console)#`	Enters the console port configuration mode.
Step 3	`switch(config-console)# modem in`	Enables the console port to only connect to a modem.
	`switch(config-console)# no modem in`	Disables (default) the current modem from executing its functions.

Configuring the Initialization String

Switches in the Cisco MDS 9500 Series and the Cisco MDS 9216 switch have a default initialization string (`ATE0Q1&D2&C1S0=1\015`) to detect connected modems. The default string only detects connected modems that are supported by Cisco systems. The default string contents are as follows:

- AT—Attention
- E0 (required)—No echo
- Q1—Result code on
- &D2—Normal data terminal ready (DTR) option
- &C1—Enable tracking the state of the data carrier
- S0=1—Pick up after one ring
- \015 (required)—Carriage return in octal

You may retain the default string or change it to another string (80 character limit) if you prefer to use a modem that is not supported or tested by Cisco systems.

Tip We recommend you use the default initialization string. If the required options are not provided in the user-input string, the initialization string is not processed.

The modem initialization string usage depends on the modem state when the switch boots:

- If the modem is already attached to the switch during bootup, the default initialization string is written to the modem (see the "Configuring the Default Initialization String" section on page 3-26).
- If the modem is not attached to the switch during bootup, then attach the modem as outlined in the *Cisco MDS 9000 Family Hardware Installation Guide* (depending on the product), and follow the procedure provided in this section (see the "Configuring a User-Specified Initialization String" section on page 3-27).

Note You can perform the configuration specified in this section only if you are connected to the console port or the COM1 port.

Configuring the Default Initialization String

To configure the default initialization string through the COM1 port, follow these steps:

	Command	Command
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# line com1` `switch(config-com1)#`	Enters the COM1 port configuration mode.
Step 3	`switch(config-com1)# modem init-string default`	Writes the default initialization string to the modem.

To configure the default initialization string through the console port, follow these steps:

	Command	Command
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# line com1` `switch(config-console)#`	Enters the console port configuration mode.
Step 3	`switch(config-console)# modem init-string default`	Writes the default initialization string to the modem.

Configuring a User-Specified Initialization String

To configure a user-specified initialization string through the COM1 port, follow these steps:

	Command	Command
Step 1	`switch# config terminal` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# line com1` `switch(config-com1)#`	Enters the COM1 port configuration mode.
Step 3	`switch(config-com1)# modem set-string user-input ATE0Q1&D2&C1S0=3\015`	Assigns the user-specified initialization string to its corresponding profile. **Note** You must first set the user-input string, before initializing the string.
	`switch(config-com1)# no modem set-string`	Reverts the configured initialization string to the factory default string.
Step 4	`switch(config-com1)# modem init-string user-input`	Writes the user-specified initialization string to the modem.

To configure a user-specified initialization string through the console port, follow these steps:

	Command	Command
Step 1	`switch# config terminal` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# line console` `switch(config-console)#`	Enters the console port configuration mode.
Step 3	`switch(config-console)# modem set-string user-input ATE0Q1&D2&C1S0=3\015`	Assigns the user-specified initialization string to its corresponding profile. **Note** You must first set the user-input string, before initializing the string.
	`switch(config-console)# no modem set-string`	Reverts the configured initialization string to the factory default string.
Step 4	`switch(config-console)# modem init-string user-input`	Writes the user-specified initialization string to the modem.

Initializing a Modem in a Powered-On Switch

When a switch is already powered on and the modem is later connected to either the console port or the COM1 port, you can initialize the modem using the **modem connect line** command in EXEC mode. You can specify the **com1** option if the modem is connected to the COM1 port, or the **console** option if the modem is connected to the console.

To connect a modem to a switch that is already powered on, follow these steps.

Step 1 Wait until the system has completed the boot sequence and the system image is running.

Step 2 Connect the modem to the switch as specified in the *Cisco MDS 9216 Switch Hardware Guide* or the *Cisco MDS 9500 Series Hardware Installation Guide*.

Step 3 Initialize the modem using the **modem connect line** command in EXEC mode.

Verifying the Modem Configuration

Use the following **show** commands to verify the configured modem settings. Table 3-4 lists the **show** commands and the information they display.

Table 3-4 show line Commands

show Command	Description
`show line console`	Displays the configured modem settings.
`show line com1`	Displays the configured modem settings for a specific port.

Configuring VSANs, Interfaces, and Zones

This chapter describes how to configure VSANs, interfaces, and zones. This chapter includes the following sections:

Configuring VSANs

You can achieve higher security and greater stability in Fibre Channel fabrics by using virtual SANs (VSANs). VSANs provide isolation among devices that are physically connected to the same fabric. With VSANs you can create multiple logical SANs over a common physical infrastructure. Each VSAN can contain up to 239 switches and has an independent address space that allows identical Fibre Channel IDs (FCIDs) to be used simultaneously in different VSANs.

Creating and Configuring VSANs

You cannot configure any application-specific parameters for a VSAN before creating the VSAN.

To create and configure VSANs, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# vsan database` `switch(config-vsan-db)#`	Configures the database for a VSAN. Application specific VSAN parameters cannot be configured from this prompt.
Step 3	`switch(config-vsan-db)# vsan 2` `switch(config-vsan-db)#`	Creates a VSAN with the specified ID (2) if that VSAN does not exist already.

	`switch(config-vsan-db)# vsan 2 name TechDoc`
	`updated vsan 2`
	`switch(config-vsan-db)#`
		Updates the VSAN with the assigned name (TechDoc).

	Command	Purpose
Step 4	`switch(config-vsan-db)# vsan 2 loadbalancing src-dst-id` `switch(config-vsan-db)#`	Enables the load balancing guarantee for the selected VSAN and directs the switch to use the source and destination ID for its path selection process.
	`switch(config-vsan-db)# no vsan 2 loadbalancing src-dst-id` `switch(config-vsan-db)#`	Negates the command issued in the previous step and reverts to the default values of the load-balancing parameters.
	`switch(config-vsan-db)# vsan 2 loadbalancing src-dst-ox-id` `switch(config-vsan-db)#`	Changes the path selection setting to use the source ID, the destination ID, and the OX ID (default).
Step 5	`switch(config-vsan-db)# vsan 2 suspend` `switch(config-vsan-db)#`	Suspends the selected VSAN.
	`switch(config-vsan-db)# no vsan 2 suspend` `vs.-config-vsan-db#`	Negates the **suspend** command issued in the previous step.
Step 6	`switch(config-vsan-db)# end` `switch#`	Returns you to EXEC mode.

Assigning VSAN Membership

To assign VSAN membership, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# vsan database` `switch(config-vsan-db)#`	Configures the database for a VSAN.
Step 3	`switch(config-vsan-db)# vsan 2` `switch(config-vsan-db)#`	Creates a VSAN with the specified ID (2) if that VSAN does not exist already.
Step 4	`switch(config-vsan-db)# vsan 2 interface fc1/8` `switch(config-vsan-db)#`	Assigns the membership of the fc1/8 interface to the specified VSAN (VSAN 2).
Step 5	`switch(config-vsan-db)# vsan 7` `switch(config-vsan-db)#`	Creates another VSAN with the specified ID (7) if that VSAN does not exist already.
Step 6	`switch(config-vsan-db)# vsan 7 interface fc1/8` `switch(config-vsan-db)#`	Updates the membership information of the interface to reflect the changed VSAN.

Displaying VSAN Information

The **show vsan** command is invoked from the EXEC mode and displays the VSAN configurations. Table 4-1 lists the **show** commands and the information they display.

Table 4-1 show interface Commands

show Command	Description
`show vsan`	Displays all VSANs.
`show vsan 100`	Displays a specific VSAN.
`show vsan usage`	Displays VSAN usage.

Table 4-1 show interface Commands (continued)

show Command	Description
`show vsan 100 membership`	Displays a VSAN membership information for a specified VSAN.
`show vsan membership`	Displays static membership information for all VSANs.
`show vsan membership interface fc1/1`	Displays static membership information for a specified interface.

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, the management interface (mgmt0), or VSAN interfaces.

Tip Before you begin configuring the switch, ensure that the modules in the chassis are functioning as designed. To verify the status of a module at any time, issue the **show module** command in EXEC mode.

Configuring Fibre Channel Interfaces

Each physical Fibre Channel interface in a switch may operate in one of several modes: E port, F port, FL port, TL port, TE port, SD port, ST port, and B port. Besides these modes, each interface may be configured in auto or Fx port mode. These two modes determine the port type during interface initialization.

To configure a Fibre Channel interface, follow these steps:

	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).

Configuring a Range of Interfaces

To configure a range of interfaces, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# interface fc1/1 - 4 , fc2/1 - 3`	Configures the range of specified interfaces. **Note** In this command, provide a space before and after the comma.

Enabling Interfaces

Interfaces on a port are shut down by default (unless you modified the initial configuration).

To enable traffic flow, follow these steps:

	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).
	`switch(config-if)# shutdown`	Shuts down the interface and administratively disables traffic flow (default).

Configuring Interface Modes

To configure the interface mode, follow these steps:

	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 operational state to auto, E, F, FL, Fx, TL, or SD 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 auto-negotiate an E, F, FL, or TE port mode (not TL or SD port modes) of operation. **Note** TL ports and SD ports cannot be configured automatically. They must be administratively configured.

Configuring the Management Interface

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, follow these steps:

	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 1.1.1.4` `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 issue 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.

Configuring VSAN Interfaces

VSANs apply to Fibre Channel fabrics and enable you to configure multiple isolated SAN topologies within the same physical infrastructure. You can create an IP interface on top of a VSAN and then use this interface to send frames to this VSAN. To use this feature, you must configure the IP address for this VSAN. VSAN interfaces cannot be created for nonexisting VSANs.

Follow these guidelines when creating or deleting VSAN interfaces:

- Create a VSAN before creating the interface for that VSAN. If a VSAN does not exist, the interface cannot be created.
- Create the interface using the **interface vsan** command. This is not done automatically.
- If you delete the VSAN, the attached interface is automatically deleted.
- Configure each interface only in one VSAN.

Tip After configuring the VSAN interface, you can configure an IP address or Virtual Router Redundancy Protocol (VRRP) features (refer to the).

To create a VSAN interface, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# interface vsan 5` `switch(config-if)#`	Configures a VSAN with the ID 5.

Configuring Common Information Models

Common Information Model (CIM) is an object-oriented information model that extends the existing standards for describing management information in a network/enterprise environment. CIM messages are independent of platform and implementation because they are encoded in an Extensible Markup Language (XML).

For more information about CIM, refer to the specification available through the Distributed Management Task Force (DMTF) website at the following URL: http://www.dmtf.org/

For more information about Cisco MDS 9000 Family support for CIM servers, refer to the *Cisco MDS 9000 Family CIM Programming Reference Guide*.

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

Configuring a CIM Server

For added security, you can install an SSL certificate to encrypt the login information and enable the HTTPS server before enabling the CIM server. The CIM server is disabled by default. If you do not enable the HTTPS server, the standard HTTP server is enabled (default).

To configure a CIM server using the HTTPS protocol, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# cimserver certificateName bootflash:simserver.pem`	Installs a Secure Socket Layer (SSL) certificate specified in the file named with a .pem extension.
	`switch(config)# cimserver clearCertificateName bootflash:simserver.pem`	(Optional) Clears the specified SSL certificate.
Step 3	`switch(config)# cimserver enableHttps`	Enables HTTPS (secure protocol).
	`switch(config)# no cimserver enableHttps`	(Optional) Disables HTTPS (default).
Step 4	`switch(config)# cimserver enable`	Enables the CIM server.
	`switch(config)# no cimserver enable`	(Optional) Disables the CIM server (default).

To configure a CIM server using the HTTP protocol, follow these steps:

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

	Command	Purpose
Step 2	`switch(config)# cimserver enable`	Enables the CIM server using the default HTTP (non-secure) protocol.
	`switch(config)# no cimserver enable`	(Optional) Disables the CIM server (default).
	`switch(config)# no cimserver enableHttp`	(Optional) Disables HTTP.
	`switch(config)# cimserver enableHttp`	(Optional) Enables HTTP and reverts to the switch default.

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. Table 4-2 lists the **show** commands and the information they display.

Table 4-2 show interface Commands

show Command	Description
`show interface`	Displays all interfaces.
`show interface fc2/2`	Displays a specified interface.
`show interface fc3/13 , fc3/16`	Displays multiple, specified interfaces.
`show interface vsan 2`	Displays a specified VSAN interface.
`show cimserver certificateName`	Displays CIM server certificate files.
`show cimserver`	Displays the CIM server configuration.
`show cimserver httpsstatus`	Displays the CIM server HTTPS status.
`show interface description`	Displays port description.
`show interface brief`	Displays interface information in a brief format.
`show interface counters`	Displays interface counters.
`show interface counters brief`	Displays interface counters in brief format.
`show interface bbcredit`	Displays BB_credit information.
`show interface fc2/31 bbcredit`	Displays BB_credit information for a specific Fibre Channel interface.
`show interface transceiver`	Displays transceiver information.
`show running-config interface fc1/1`	Displays the running configuration for a specific interface.

Configuring 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.

Configuring a Zone

To configure a zone and assign a zone name, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zone name Zone1 vsan 3` `switch(config-zone)#`	Configures a zone called Zone 1 for the VSAN called vsan3.

Step 3	`switch(config-zone)# member <type> <value>`
	`pWWN example:`
	`sswitch(config-zone)# member pwwn 10:00:00:23:45:67:89:ab`
	`Fabric pWWN example:`
	`switch(config-zone)# member fwwn 10:01:10:01:10:ab:cd:ef`
	`FC ID example:`
	`switch(config-zone)# member fcid 0xce00d1`
	`FC alias example:`
	`switch(config-zone)# member fcalias Payroll`
	`Domain ID example:`
	`switch(config-zone)# member domain-id 2 portnumber 23`
	`FC alias example:`
	`switch(config-zone)# member ipaddress 10.15.0.0 255.255.0.0`
	`Local sWWN interface example:`
	`switch(config-zone)# member interface fc 2/1`
	`Remote sWWN interface example:`
	`switch(config-zone)# member interface fc2/1 swwn`
	`20:00:00:05:30:00:4a:de`
	`Domain ID interface example:`
	`switch(config-zone)# member interface fc2/1 domain-id 25`
		Configures a member for the specified zone (Zone1) based on the type (pWWN, fabric pWWN, FC ID, FC alias, domain ID, IP address, or interface) 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.	

Note Interface-based zoning only works with Cisco MDS 9000 Family switches. Interface-based zoning does not work if **interop** mode is configured in that VSAN.

Tip Use the **show wwn switch** command to retrieve the sWWN. If you do not provide a sWWN, the software automatically uses the local sWWN.

You can assign an alias name and configure an alias member using either the FC ID, fabric port WWN (fWWN), or pWWN values.

Tip As of Cisco MDS SAN-OS Release 1.3(4), the Cisco SAN-OS software supports a maximum of 2048 aliases per VSAN.

Configuring an Alias

To create an alias using the **fcalias** command, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# fcalias name AliasSample vsan 3` `switch-config-fcalias#`	Configures an alias name (AliasSample).
Step 3	`switch-config-fcalias# member fcid 0x222222`	Configures alias members based on the specified FC ID type and value (0x222222).
	`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).
	`switch-config-fcalias# member fwwn 10:01:10:01:10:ab:cd:ef`	Configures alias members based on the specified fWWN type and value (fWWN 10:01:10:01:10:ab:cd:ef).
Note	Multiple members can be specified on multiple lines.	

Creating a Zone Set

Tip Zone sets are configured with the names of the member zones. If the zone set is in a configured VSAN, you must also specify the VSAN.

To create a zone set to include several zones, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zoneset name Zoneset1 vsan 3` `switch(config-zoneset)#`	Configures a zone set called Zoneset1. **Tip** To activate a zone set, you must first create the zone and a 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.

	Command	Purpose
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.
Step 5	`switch(config-zoneset-zone)# member fcid 0x111112` `switch(config-zoneset-zone)#`	Adds a new member (FC ID 0x111112) to the newly created zone (InlineZone1). **Tip** Execute this step only if you need to add a member to a zone from a zone set prompt.

Configuring the Default Zone Policy

The default zone members are explicitly listed when the default policy is configured as **permit** or when a zone set is active. When the default policy is configured as **deny**, the members of this zone are not explicitly enumerated when you issue the **show zoneset active** command.

To permit or deny traffic in the default zone, follow these steps:

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

Configuring a LUN-Based Zone

Logical unit number (LUN) zoning is a feature specific to switches in the Cisco MDS 9000 Family.

Caution LUN zoning can only be implemented in Cisco MDS 9000 Family switches. If LUN zoning is implemented in a switch, you cannot configure the interop mode in that switch.

To configure a LUN-based zone, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# zone name LunSample vsan 2` `switch(config-zone)#`	Configures a zone called LunSample for the specified VSAN (vsan 2).
Step 3	`switch(config-zone)# member pwwn 10:00:00:23:45:67:89:ab lun 64`	Configures a zone member based on the specified pWWN and LUN value. **Note** LUN x64 in hex format corresponds to 100 in decimal format.
	`switch(config-zone)# member fcid 0x12465 lun 64`	Configures a zone member based on the FC ID and LUN value.

Assigning LUNs to Storage Subsystems

LUN masking and mapping restricts server access to specific LUNs. If LUN masking is enabled on a storage subsystem and if you want to perform additional LUN zoning in a Cisco MDS 9000 Family switch, obtain the LUN number for each Host Bus Adapter (HBA) from the storage subsystem and then configure the LUN-based zone procedure provided earlier.

Note Refer to the relevant user manuals to obtain the LUN number for each HBA.

Caution If you make any errors when configuring this scenario, you are prone to loose data.

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, VSAN, alias, 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. Table 4-3 lists the **show** commands and the information they display.

Table 4-3 show zone and show zoneset Commands

show Command	Description
`show zone`	Displays zone information for all VSANs.
`show zone vsan 1`	Displays zone information for a specific VSAN.
`show zoneset vsan 1`	Displays information for the configured zone set.
`show zoneset vsan 2-3`	Displays configured zone set information for a range of VSANs.
`show zone name Zone1`	Displays members of a zone.
`show fcalias vsan 1`	Displays fcalias configuration.
`show zone member pwwn 21:00:00:20:37:9c:48:e5`	Displays membership status.
`show zone statistics`	Displays zone statistics.
`show zone statistics lun-zoning`	Displays LUN-based zone statistics.
`show zone statistics read-only-zoning`	Displays read-only zoning statistics.
`show zoneset active`	Displays active zone sets.
`show zoneset brief`	Displays brief descriptions of zone sets.
`show zone active`	Displays active zones.
`show zone status`	Displays zone status.
`show zone`	Displays zone statistics.
`show running`	Displays the interface-based zones.

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. The domains are configured on a per VSAN basis. If you do not configure a domain ID, the local switch uses a random ID.

This chapter includes the following sections:

Configuring Domain IDs

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 principal switch assigns the requested domain ID if available. Otherwise, it assigns another available domain ID.

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

If you change the configured domain ID, the change is only accepted if the new domain ID is included in all the allowed domain ID lists currently configured in the VSAN. Alternatively, you can also configure a 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.

Tip When the FICON feature is enabled in a given VSAN, the domain ID for that VSAN remains in the static state. You can change the static ID value but you cannot change it to the preferred option.

To specify a **preferred** or a **static** domain ID, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# fcdomain domain 3 preferred vsan 8`	Configures the switch in VSAN 8 to request a preferred domain ID 3 and accepts any value assigned by the principal switch.
	`switch(config)# no fcdomain domain 3 preferred vsan 8`	Resets the configured domain ID to 0 (default) in VSAN 8. The configured domain ID becomes 0 preferred.
Step 3	`switch(config)# fcdomain domain 2 static vsan 237`	Configures the switch in VSAN 237 to accept only a specific value and moves the local interfaces in VSAN 237 to an isolated state if the requested domain ID is not granted.
	`switch(config)# no fcdomain domain 18 static vsan 237`	Resets the configured domain ID to factory defaults in VSAN 237. The configured domain ID becomes 0 preferred.

Setting 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.

To configure the priority for the principal switch, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# fcdomain priority 25 VSAN 99`	Configures a priority of 25 for the local switch in VSAN 99.
	`switch(config)# no fcdomain priority 25 VSAN 99`	Reverts the priority to the factory default (128) in VSAN 99.

Configuring Allowed Domain ID Lists

By default, the valid range for an assigned domain ID list is from 1 to 239. You can specify a list of ranges to be in the allowed domain ID list and separate each range with a comma. The principal switch ensures that the domain requested by any switch in the fabric is specified in the allowed list.

Tip If you configure an allowed list on one switch in the fabric, we recommend you configure the same list in all other switches in the fabric to ensure consistency.

To configure the allowed domain ID list, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# fcdomain allowed 50-110 vsan 4`	Configures the list to allow switches with the domain ID 50 through 110 in VSAN 4.
	`switch(config)# no fcdomain allowed 50-110 vsan 5`	Reverts to the factory default of allowing domain IDs from 1 through 239 in VSAN 5.

Setting the Fabric Name

By default the configured fabric name is 20:01:00:05:30:00:28:df.

- When the fcdomain feature is disabled, the runtime fabric name is the same as the configured fabric name.
- When the fcdomain feature is enabled, the runtime fabric name is the same as the principal switch's WWN.

To set the fabric name value for a disabled fcdomain, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan 3`	Assigns the configured fabric name value in VSAN 3.
	`switch(config)# no fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan 3010`	Changes the fabric name value to the factory default (20:01:00:05:30:00:28:df) in VSAN 3010.

The fabric name is applied to runtime through a disruptive restart when the fcdomain is configured as disabled.

Stopping Incoming RCF Request Frames

The **rcf-reject** option is configured on a per-interface, per-VSAN basis. By default, the **rcf-reject** option is disabled (that is, reconfigure fabric (RCF) request frames are not automatically rejected).

To stop incoming RCF request frames, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# int fc1/1` `switch(config-if)#`	Configures the specified interface.
Step 3	`switch(config-if)# fcdomain rcf-reject vsan 1`	Enables the RCF filter on the specified interface in VSAN 1.
	`switch(config-if)# no fcdomain rcf-reject vsan 1`	Disables the RCF filter on the specified interface in VSAN 1.

The **rcf-reject** option takes immediate effect to runtime through a disruptive restart.

Enabling Persistent FC IDs

Persistent FC IDs are disabled by default. You can enable this option globally or for each VSAN. If you choose to enable it globally, you can do so at any time using the initial setup routine or the setup command (see the "Initial Setup Routine" section on page 3-2). When you enable this option globally, the switch remains in this state until you change the global configuration.

Note If you enable this option during the initial switch setup, this option is automatically enabled in all configured VSANs. If you enable this option at a later stage, this option is automatically enabled in all VSANs configured after that stage. VSANs configured before that stage remain unchanged.

Note Persistent FC IDs with loop-attached devices (FL ports) need to remain connected to the same port in which they were configured.

To enable the persistent FC ID feature, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# fcdomain fcid persistent vsan 1000` `FCID(s) persistent feature is enabled.`	Activates persistency of FC IDs in VSAN 1000.
	`switch(config)# no fcdomain fcid persistent vsan 20`	Disables the FC ID persistency feature in VSAN 20.

Configuring Persistent FC IDs Manually

Once the persistent FC ID feature is enabled, you can enter the persistent FC ID submode and add static or dynamic entries in the FC ID database. By default, all added entries are static. Persistent FC IDs are configured on a per-VSAN basis.

Note You cannot configure persistent FC IDs in FICON-enabled VSANs.

To configure persistent FC IDs, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# fcdomain fcid database`	Activates persistency of FC IDs in the specified VSAN.
Step 3	`switch(config-fcid-db)# vsan 1000 wwn 33:e8:00:05:30:00:16:df fcid 0x070128`	Configures a device WWN (33:e8:00:05:30:00:16:df) with the FC ID 0x070128 in VSAN 1000.
	`switch(config-fcid-db)# vsan 1000 wwn 11:22:11:22:33:44:33:44 fcid 0x070123 dynamic`	Configures a device WWN (11:22:11:22:33:44:33:44) with the FC ID 0x070123 in VSAN 1000 in dynamic mode.
	`switch(config-fcid-db)# vsan 1000 wwn 11:22:11:22:33:44:33:44 fcid 0x070100 area`	Configures a device WWN (11:22:11:22:33:44:33:44) with the FC IDs 0x070100 through 0x701FF in VSAN 1000. **Note** To secure the entire area for this fcdomain, assign 00 as the last two characters of the FC ID.

Displaying fcdomain Information

Use the **show fcdomain** command to display global information about fcdomain configurations. Table 5-1 lists the **show** commands and the information they display.

Table 5-1 show fcdomain Commands

show Command	Description
`show fcdomain`	Displays the global fcdomain information
`show fcdomain domain-list`	Displays the list of domain IDs of all switches belonging to a specified VSAN.
`show fcdomain allowed vsan`	Displays the list of allowed domain IDs configured on this switch.
`show fcdomain fcid persistent`	Displays all existing, persistent FC IDs for a specified VSAN. You can also specify the **unused** option to view only persistent FC IDs that are still not in use.

Table 5-1 show fcdomain Commands (continued)

show Command	Description
`show fcdomain statistics`	Displays frame and other fcdomain statistics for a specified VSAN or PortChannel.
`show fcdomain address-allocation`	Displays FC ID allocation statistics including a list of assigned and free FC IDs.

CHAPTER 6

Configuring Trunking and PortChannels

This chapter describes how to configure the trunking and PortChannel features provided in Cisco MDS 9000 switches. This chapter includes the following sections:

Configuring Trunking

Trunking, also known as VSAN trunking, is a feature specific to switches in the Cisco MDS 9000 Family. Trunking enables interconnect ports to transmit and receive frames in more than one VSAN, over the same physical link, using Extended ISL (EISL) frame format.

The trunking protocol is important for E-port and TE-port operations. It supports the following:

- Dynamic negotiation of operational trunk mode.
- Selection of a common set of trunk-allowed VSANs.
- Detection of a VSAN mismatch across an ISL.

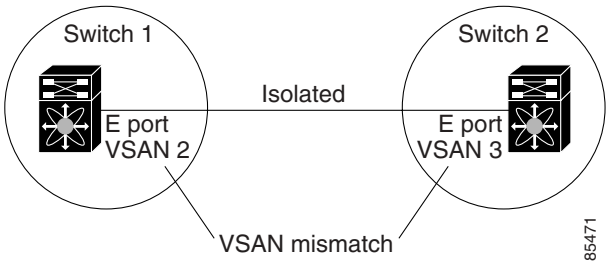
By default, the trunking protocol is enabled. If the trunking protocol is disabled on a switch, no port on that switch can apply new trunk configurations. Existing trunk configurations are not affected—the TE port continues to function in trunk mode, but only supports traffic in VSANs that it negotiated with previously (when the trunking protocol was enabled). Also, other switches that are directly connected to this switch are similarly affected on the connected interfaces. In some cases, you may need to merge traffic from different port VSANs across a non-trunking ISL. If so, disable the trunking protocol.

Tip To avoid inconsistent configurations, shut all E ports before enabling or disabling the trunking protocol.

Trunking Configuration Guidelines

If you misconfigure VSAN configurations across E ports, you could face consequences such as merging the traffic in two VSANs (thus causing both VSANs to mismatch). The trunking protocol validates the VSAN interfaces at both ends of an ISL to avoid VSANs merging (see Figure 6-1).

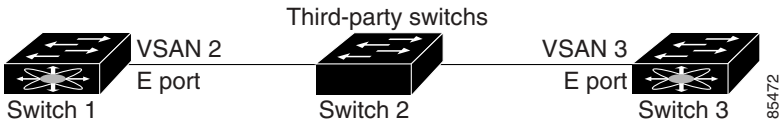
Figure 6-1 VSAN Mismatch



In this example, the trunking protocol detects potential VSAN merging and isolates the ports involved.

The trunking protocol cannot detect merging of VSANs when a third-party switch is placed in between two Cisco MDS 9000 Family switches (see Figure 6-2).

Figure 6-2 Third-Party Switch VSAN Mismatch



VSANs 2 and 3 get effectively merged with overlapping entries in the name server and the zone applications. The Cisco MDS 9000 Fabric Manager helps detect such topologies (refer to the *Cisco MDS 9000 Family Fabric Manager Configuration Guide)*.

Enabling or Disabling Trunking Protocol

To enable or disable the trunking protocol, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# no trunk protocol enable` `switch(config)#`	Disables the trunking protocol.
	`switch(config)# trunk protocol enable` `switch(config)#`	Enables trunking protocol (default).

Configuring Trunk Mode

To configure the trunk mode, follow these steps:

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

	Command	Purpose
Step 3	`switch(config-if)# switchport trunk mode on`	Enables the trunk mode for the specified interface.
	`switch(config-if)# switchport trunk mode off`	Disables the trunk mode for the specified interface.
	`switch(config-if)# switchport trunk mode auto`	Configures the trunk mode for the specified interface. The **auto** option provides automatic sensing for the interface.

Configuring an Allowed List of VSANs

To configure an allowed-active list of VSANs for an interface, follow these steps:

	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 trunk allowed vsan 2-4`	Changes the allowed list for the specified VSANs.
	`switch(config-if)# switchport trunk allowed vsan add 5` `updated trunking membership`	Expands the specified VSAN (5) to the new allowed list.
	`switch(config-if)# no switchport trunk allowed vsan 2-4`	Deletes VSANs 2, 3, and 4.
	`switch(config-if)# no switchport trunk allowed vsan add 5`	Deletes the expanded allowed list.

Displaying Trunking Information

The **show interface** command is invoked from the EXEC mode and displays trunking configurations for a TE port. Without any arguments, this command displays the information for all of the configured interfaces in the switch. Table 6-1 lists the **show** commands and the information they display.

Table 6-1 show trunking Commands

show Command	Description
`show interface fc1/13`	Displays a trunked Fibre Channel interface.
`show trunk protocol`	Displays the trunking protocol.
`show interface trunk vsan 1-1000`	Displays per VSAN information on trunk ports.

Configuring PortChannel

PortChannels refer to the aggregation of multiple physical interfaces into one logical interface to provide higher aggregated bandwidth, load balancing, and link redundancy. PortChannels can connect to interfaces across switching modules, so a failure of a switching module cannot bring down the PortChannel link.

PortChannel Configuration Guidelines

Before configuring a PortChannel, consider the following guidelines

- Configure the PortChannel across switching modules to prevent redundancy on switching module reboots or upgrades.
- Ensure that one PortChannel is not connected to two switches. PortChannels require point-to-point connections.

Creating PortChannels

You can create PortChannels using the **interface port-channel** command. PortChannels are created with default values. You can change the default configuration just like any other physical interface.

To create a PortChannel, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# interface port-channel 1` `switch(config-if)#`	Configures the specified PortChannel (1).

Note All interfaces added to PortChannels are administratively shut down, and the PortChannel remains administratively up.

Deleting PortChannels

To delete the PortChannel, you must explicitly issue the **no interface port-channel** command. When you delete the PortChannel, the corresponding channel membership is also deleted. All interfaces in the deleted PortChannel convert to individual physical links. To avoid inconsistent states across switches, and to maintain consistency across switches, the ports shut down. They continue to use the configured values of the physical port.

To delete a PortChannel, follow these steps:

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

Step 2	`switch(config)# no interface port-channel 1`
	`port-channel 1 deleted and all its members disabled`
	`please do the same operation on the switch at the other end of the port-channel`
	`switch(config)#`
		Deletes the specified PortChannel (1), its associated interface mappings, and the hardware associations for this PortChannel.

Adding Interfaces to a PortChannel

You can add a physical interface (or a range of interfaces) to a nonexistent or an existing PortChannel and the PortChannel is automatically created. If the PortChannel does not exist, it is created. The compatible parameters on the configuration are mapped to the PortChannel.

To add an interface (or a range of interfaces) to a PortChannel, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# interface fc1/15` `switch(config-if)#`	Configures the specified port interface (fc1/15).
	`switch(config)# interface fc1/1 - 5` `switch(config-if)#`	Configures the specified range of interfaces. In this example, interfaces from 1/1 to 1/5 are configured.

Step 3	`switch(config-if)# channel-group 15`
	`fc1/15 added to port-channel 15 and disabled`
	`please do the same operation on the switch at the other end of the port-channel, then do "no shutdown" at both ends to bring them up`
	`switch(config-if)#`
		Adds physical Fibre Channel port 1/15 to channel group 15. If channel group 15 does not exist, it is created. The port is shut down.

	`switch(config-if)# channel-group 2`
	`fc1/1 fc1/2 fc1/3 fc1/4 fc1/5 added to port-channel 2 and disabled`
	`please do the same operation on the switch at the other end of the port-channel, then do "no shutdown" at both ends to bring them up`
	`switch(config-if)#`
		Adds physical interfaces 1/1, 1/2, 1/3, 1/4, and 1/5 to channel group 2. If channel group 2 does not exist, it is created.
		If the compatibility check is successful, the interfaces are operational and the corresponding states apply to these interfaces.

Deleting Interfaces from a PortChannel

To delete a physical interface (or a range of physical interfaces), you must explicitly issue the **no channel-group** command at the physical interface level. When a physical interface is deleted from the PortChannel, the channel membership is automatically updated. If the deleted interface is the last operational interface, then the PortChannel status is changed to a down state. Deleting an interface from a PortChannel decreases the channel size and bandwidth of the PortChannel.

Note When an interface is deleted, it is shut down but the physical configuration is retained. The inherited PortChannel configuration information is not deleted.

To delete a physical interface (or a range of physical interfaces), follow these steps:

	Command	Purpose
Step 1	`switch(config)# interface fc1/1` `switch(config-if)#`	Enters the selected physical interface level.
	`switch(config)# interface fc1/1 - 5` `switch(config-if)#`	Enters the selected range of physical interfaces.

Step 2	`switch(config-if)# no channel-group 2`
	`fc1/1 fc1/2 fc1/3 fc1/4 fc1/5 removed from port-channel 2 and disabled. Please do the same operation on the switch at the other end of the port-channel`
	`switch(config-if)#`
		Deletes the physical Fibre Channel interfaces in channel group 2.

Displaying PortChannel Information

You can view specific information about existing PortChannels at any time from EXEC mode. The following **show** commands provide further details on existing PortChannels. You can force all screen output to go to a printer or save it to a file. Table 6-2 lists the **show** commands and the information they display.

Table 6-2 show port-channel Commands

show Command	Description
`show port-channel summary`	Displays PortChannel summary.
`show port-channel database`	Displays PortChannel database.
`show port-channel consistency`	Displays the command without details.
`show port-channel consistency detail`	Displays the command with details.
`show port-channel usage`	Displays PortChannel usage.
`show port-channel compatibility-parameters`	Displays PortChannel compatibility.

Configuring Security

Management security in any switch in the Cisco MDS 9000 Family is implemented using the command-line interface (CLI) or Simple Network Management Protocol (SNMP).

This chapter includes the following sections:

Configuring Switch Security

The authentication, authorization, and accounting (AAA) strategy verifies the identity of, grants access to, and tracks the actions of remote users in all switches in the Cisco MDS 9000 Family. The Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) provide AAA solutions.

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

Configuring AAA Accounting

Accounting refers to the log that is kept for each management session in a switch. This information may be used to generate reports for troubleshooting purposes and user accountability. Accounting can be implemented locally and remotely.

You can view the local accounting log using the **show accounting log** command. Table 7-1 lists the **show** commands and the information they display.

Table 7-1 show aaa Commands

show Command	Description
`show accounting log`	Displays the accounting log information.
`show aaa authentication`	Displays authentication information.

Configuring RADIUS

Cisco MDS 9000 Family switches use the RADIUS protocol to communicate with remote AAA servers. You can configure multiple RADIUS servers and set timeout and retry counts.

You can set the RADIUS server address, the RADIUS preshared key, the RADIUS server timeout interval, iterations of the RADIUS server, define vendor-specific attributes, and display RADIUS server details.

Use the **show radius-server** command to display configured RADIUS parameters.

Note Only administrators can view the RADIUS preshared key.

Table 7-2 lists the **show** commands and the information they display.

Table 7-2 show radius-server Commands

show Command	Description
`show radius-server`	Displays configured RADIUS information.
`show radius-server groups`	Displays configured RADIUS server-group order.

Setting the RADIUS Server Address

You can add up to 64 RADIUS servers using the **radius-server host** command. RADIUS keys are always stored in encrypted form in persistent storage. The running configuration also displays encrypted keys.

To specify the RADIUS server address and the options, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius-server host 10.10.0.0 key HostKey`	Specifies a key for the selected RADIUS server. This key overrides the key assigned using the **radius-server key** command. In this example, the host is 10.10.0.0 and the key is HostKey.
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 65366.
Step 4	`switch(config)# radius-server host 10.10.0.0 acct-port 2004`	Specifies the destination UDP port number to which RADIUS accounting messages should be sent. The default accounting port is 1813, and the valid range is 0 to 65366.
Step 5	`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.

	Command	Purpose
Step 6	`switch(config)# radius-server host radius2 key 0 abcd`	Specifies a clear text key for the specified server. The key is restricted to 65 characters.
	`switch(config)# radius-server host radius3 key 7 1234`	Specifies a reversible encrypted key for the specified server. The key is restricted to 65 characters.

Setting the RADIUS Preshared Key

You need to configure the RADIUS preshared key to authenticate the switch to the RADIUS server. The length of the key is restricted to 65 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all RADIUS server configurations on the switch. You can override this global key assignment by explicitly using the **key** option in the **radius-server host** command.

To set the RADIUS preshared key, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius-server key AnyWord`	Configures a preshared key (AnyWord) to authenticate communication between the RADIUS client and server. The default is clear text.
	`switch(config)# radius-server key 0 AnyWord`	Configures a preshared key (AnyWord) specified in clear text (indicated by 0) to authenticate communication between the RADIUS client and server.
	`switch(config)# radius-server key 7 public`	Configures a preshared key (public) specified in encrypted text (indicated by 7) to authenticate communication between the RADIUS client and server.

Setting the RADIUS Server Time-Out Interval

To specify the time between retransmissions to the RADIUS servers, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius-server timeout 30`	Specifies the time (in seconds) between retransmissions to the RADIUS server. The default timeout is one (1) second. The time range in seconds is 1 to 60.

You can revert the retransmission time to its default by issuing the **no radius-server timeout** command.

Setting Iterations of the RADIUS Server

By default, a switch retries a RADIUS server connection only once. This number can be configured. The maximum is five retries per server. You can revert the retry number to its default by issuing the **no radius-server retransmit** command.

To specify the number of times that RADIUS servers should try to authenticate a user, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius-server retransmit 3`	Configures the number of times (3) the switch tries to connect to a RADIUS server(s) before reverting to local authentication.

Configuring TACACS+

A Cisco MDS switch uses the Terminal Access Controller Access Control System Plus (TACACS+) protocol to communicate with remote AAA servers. You can configure multiple TACACS+ servers and set timeout values. TACACS+ is a client/server protocol that uses TCP (TCP port 49) for transport requirements. All switches in the Cisco MDS 9000 Family provide centralized authentication using the TACACS+ protocol.

Use the **show tacacs+** commands to display configurations for the TACACS+ protocol configuration in all switches in the Cisco MDS 9000 Family. Table 7-3 lists the **show** commands and the information they display.

Table 7-3 show tacacs-server Details Commands

show Command	Description
`show tacacs-server`	Displays configured TACACS+ server information.
`show aaa authentication`	Displays AAA authentication information.
`show tacacs-server groups`	Displays configured TACACS server groups.
`show aaa groups`	Displays all AAA server groups.

Enabling TACACS+

By default, the TACACS+ feature is disabled in all Cisco MDS 9000 Family switches. You must explicitly enable the TACACS+ feature to access the configuration and verification commands for fabric authentication. When you disable this feature, all related configurations are automatically discarded.

To enable TACACS+ for a Cisco MDS switch, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs+ enable`	Enables the TACACS+ in this switch.
	`switch(config)# no tacacs+ enable`	Disables (default) the TACACS+ in this switch.

Setting the TACACS+ Server Address

Use the **tacacs-server** command to configure the communication parameters for the required TACACS+ server.

If a secret key is not configured for a configured server, a warning message is issued and the global secret encryption key is automatically used (see the "Setting the Secret Key" section on page 7-5).

To configure the TACACS+ server option, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs-server host 171.71.58.91` `warning: no key is configured for the host`	Configures the TACACS+ server identified by the specified IP address.
	`switch(config)# no tacacs-server host 10.10.1.0`	Deletes the specified TACACS+ server identified by the IP address. By default, no server is configured.
Step 3	`switch(config)# tacacs-server host 171.71.58.91 port 2`	Configures the TCP port for all TACACS+ requests.
	`switch(config)# no tacacs-server host 171.71.58.91 port 2`	Reverts to the factory default of using Port 49 for server access.
Step 4	`switch(config)# tacacs-server host host1.cisco.com key MyKey`	Configures the TACACS+ server identified by the specified domain name and assigns a special key.
Step 5	`switch(config)# tacacs-server host host100.cisco.com timeout 25`	Configures the timeout period for the switch to wait for a response from the specified server before it declares a timeout failure.

Setting the Secret Key

Use the **tacacs-server** command to configure global values for the **key** for all TACACS+ servers.

Note Secret keys configured for individual servers override the globally configured values.

To set the secret key for TACACS+ servers, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs-server key 7 tacacsPword`	Assigns the global secret key to access the TACACS+ server. This example specifies **7** to indicate encryption. If this global key and the individual server keys are not configured, clear text messages are sent to the TACACS+ server(s). **Note** If secret keys are configured for individual servers, those keys override this global key.
	`switch(config)# no tacacs-server key oldPword`	Deletes the configured secret key to access the TACACS+ server and reverts to the factory default of allowing access to all configured servers.

Setting the Server Timeout Value

Use the **tacacs-server** command to configure global **timeout** values for all TACACS+ servers.

Note Timeout values configured for individual servers override the globally configured values.

To set the share password for TACACS+ servers, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs-server timeout 30`	Configures the global timeout period for the switch to wait for a response from all servers before it declares a timeout failure.
	`switch(config)# no tacacs-server timeout 30`	Deletes the configured timeout period and reverts to the factory default of 5 seconds. **Note** If the timeout value is configured for individual servers, that value overrides this global timeout value.

Configuring Server Groups

You can specify one or more remote AAA servers to authenticate users using server groups. All members of a group must belong to the same protocol: either RADIUS or TACACS+. The servers are tried in the same order in which you configure them.

You can configure these server groups at any time but they only take effect when you apply them to an AAA service using the **aaa authentication login** command. You can specify one or more remote AAA servers to authenticate users using server groups.

To specify the TACACS+ server order within a group, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# aaa group server tacacs+ TacacsServer1` `switch(config-tacacs+)#`	Configures a TacacsServer1 group and enters the submode for that group.
	`switch(config)# no aaa group server tacacs+ TacacsServer19`	Deletes the group called TacacsServer19 from the authentication list.
Step 3	`switch(config-tacacs+)# server ServerA`	Configures ServerA to be tried first within TacacsServer1. **Tip** If the specified TACACS+ server is not found, configure it using the **tacacs-server host** command and retry this command.
Step 4	`switch(config-tacacs+)# server ServerB`	Configures ServerB to be tried second within TacacsServer1.
	`switch(config-tacacs+)# no server ServerZ`	Deletes ServerZ within the TacacsServer1 list of servers.

Configuring Role-Based CLI Authorization

Switches in the Cisco MDS 9000 Family perform authentication based on roles. Role-based authorization limits access to switch operations by assigning users to roles. This kind of authentication restricts you to management operations based on the roles to which you have been added.

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.

Each role can contain multiple users and each user can be part of multiple roles. For example, if role1 users are only allowed access to configuration commands, and role2 users are only allowed access to debug commands, then if Joe belongs to both role1 and role2, he can access configuration as well as debug commands.

Note If you belong to multiple roles, you can execute a superset of all the commands permitted by these roles. Access to a command takes priority over being denied access to a command. For example, suppose you belong to a TechDocs group and you were denied access to configuration commands. However, you also belong to the engineering group and have access to configuration commands. In this case, you will have access to configuration commands.

Tip Any role, when created, does not allow access to the required commands immediately. The administrator must configure appropriate rules for each role to allow access to the required commands.

Configuring CLI User Profiles

Every Cisco MDS 9000 Family switch user has related NMS 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 CLI commands explained in this section enable you to create users and modify the profile of an existing user.These commands are restricted to privileged users as determined by your administrator.

Cisco MDS 9000 Family switches use the same command (**username**) to create a user and to update an existing user. The **expire** option determines the date on which the user account is disabled. The date is specified in the YYYY-MM-DD format. By default, the user account does not expire unless you explicitly configure it to expire.

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.

To configure a new user or to modify the profile of an existing user, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# username usam password abcd expire 2003-05-31`	Creates or updates the user account (usam) along with a password (abcd) that is set to expire on 2003-05-31. The password is limited to 64 characters.
	`switch(config)# username msam password 0 abcd role network-operator`	Creates or updates the user account (msam) along with a password (abcd) specified in clear text (indicated by 0). The password is limited to 64 characters.
	`switch(config)# username user1 password 5 !@*asdsfsdfjh!@df`	Specifies an encrypted (specified by 5) password (!@*asdsfsdfjh!@df) for the user account (user1).
Step 3	`switch(config)# username usam role network-admin`	Adds the specified user (usam) to the network-admin role.
	`switch(config)# no username usam role vsan-admin`	Deletes the specified user (usam) from the vsan-admin role.
Step 4	`switch(config)# username usam sshkey fsafsd2344234234ffgsdfg`	Specifies the SSH key for the user account (usam).
	`switch(config)# no username usam sshkey fsafsd2344234234ffgsdfgffsdfsfsfssf`	Deletes the SSH key for the user account (usam).

Note If the **update-snmpv3** option is used, specify the clear text and old SNMP password.

Recovering Administrator Password

An administrator can recover a password from a local console connection. The password recovery procedure must be performed on the supervisor module that becomes the active supervisor module after the recovery procedure is completed. To ensure the other supervisor module does not become the active module, you have two options:

- Physically remove the other supervisor module from the chassis, or
- For the duration of this procedure, change the other supervisor module's console prompt to the `loader>` or `switch(boot)#` prompt.

Note Password recovery is not possible from a Telnet or SSH session.

To recover a administrator's password, follow these steps:

Step 1 Reboot the switch.

```
switch# reload
The supervisor is going down for reboot NOW!
```

Step 2 Press the **Ctrl-]** key sequence (when the switch begins its Cisco SAN-OS software boot sequence) to enter the `switch(boot)#` prompt.

```
Ctrl-]
switch(boot)#
```

Step 3 Change to configuration mode.

```
switch(boot)# config terminal
```

Step 4 Enter the **admin-password** command to reset the administrator password.

```
switch(boot-config)# admin-password password
```

Step 5 Exit to the EXEC mode.

```
switch(boot-config)# exit
switchboot#
```

Step 6 Enter the **load** command to load the Cisco SAN-OS software.

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

Step 7 Save the software configuration.

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

Configuring SSH Services

The Telnet service is enabled by default on all Cisco MDS 9000 Family switches. Before enabling the SSH service, generate a host key pair. To generate a host key, use the **ssh key** command.

By default, the SSH service is disabled. To enable or disable the SSH service, follow these steps:

	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 issued the **aaa authentication login default none** command, you must enter one or more key strokes to log in. If you press the **Enter** key without entering at least one keystroke, your log in will be rejected.

Configuring SNMP Security

SNMP is an application layer protocol that facilitates the exchange of management information between network devices. In all Cisco MDS 9000 Family switches, three SNMP versions are available: SNMPv1, SNMPv2c, and SNMPv3.

Note Users and roles configured through the CLI are different from users and roles configured through SNMP. These configurations do not directly correspond with each other. However, you can configure both CLI and SNMP identically, if required.

SNMP users are different from CLI users. SNMP users also have role-based authentication for roles and authorization purposes.

To create or modify SNMP users from the CLI, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# snmp-server user joe network-admin auth sha abcd1234`	Creates or modifies the settings for a user (joe) in the network-admin role using the HMAC-SHA-96 authentication password (abcd1234).
	`switch(config)# snmp-server user sam network-admin auth md5 abcdefgh` `switch(config)#`	Creates or modifies the settings for a user (sam) in the network-admin role using the HMAC-MD5-96 authentication password (abcdefgh).
	`switch(config)# snmp-server user Bill network-admin auth sha abcd1234 priv abcdefgh`	Creates or modifies the settings for a user (network-admin) in the network-admin role using the HMAC-SHA-96 authentication level and privacy encryption parameters.
	`switch(config)# no snmp-server user usernameA`	Deletes the user (usernameA) and all associated parameters.
	`switch(config)# snmp-server user user1 network-admin auth md5 0xab0211gh priv 0x45abf342 localizedkey`	Specifies the password to be in localized key format (see RFC 2574). The localized key is provided in the hex format (for example, 0xacbdef).

Note Avoid using the **localizedkey** option when configuring an SNMP user from the CLI. The localized keys are not portable across devices as they contain device engine ID information. If a configuration file is copied to the device, the passwords may not be set correctly if the configuration file was generated at a different device. Explicitly configure the desired passwords after copying the configuration into the device.

Configuring Fabric Security

Fibre Channel Security Protocol (FC-SP) capabilities in Cisco MDS SAN-OS Release 1.3(x) provides switch-switch and host-switch authentication to overcome security challenges for enterprise-wide fabrics. Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP) is an FC-SP protocol implemented in this release to provide authentication between Cisco MDS 9000 Family switches and other devices. It consists of the CHAP protocol combined with the Diffie-Hellman exchange.

Configuring DHCHAP Authentication

The DHCHAP authentication process is outlined below and explained in the following sections.

To configure DHCHAP authentication using the local password database, follow these steps:

Step 1 Enable DHCHAP.

Step 2 Identify and configure the DHCHAP authentication modes.

Step 3 Configure the hash algorithm and DH group.

Step 4 Configure the DHCHAP password for the local switch and other switches in the fabric.

Step 5 Configure the DHCHAP timeout value for reauthentication.

Step 6 Verify the DHCHAP configuration.

Configuring DH Group Settings

All switches in the Cisco MDS Family support all DHCHAP groups specified in the standard: 0 (null DH group which does not perform the Diffie-Hellman exchange), 1, 2, 3, or 4.

Tip If you change the DH group configuration, make sure you change it globally for all switches in the fabric.

To change the DH group settings, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# fcsp dhchap group 2 3 4`	Prioritizes the use of DH group 2, 3, and 4 in the configured order.
	`switch(config)# no fcsp dhchap group 0`	Reverts to the DHCHAP factory default order of 0, 4, 1, 2, and 3.

Configuring the DHCHAP Password for the Local Switch

To configure the DHCHAP password for the local switch, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# fcsp dhchap password 0 mypassword`	Configures a clear text password for the local switch.
	`switch(config)# fcsp dhchap password 0 mypassword 30:11:bb:cc:dd:33:11:22`	Configures a clear text password for the local switch to be used for the device with the specified WWN.
	`switch(config)# no fcsp dhchap password 0 mypassword 30:11:bb:cc:dd:33:11:22`	Removes the clear text password for the local switch to be used for the device with the specified WWN.
	`switch(config)# fcsp dhchap password 7 sfsfdf`	Configures a password entered in an encrypted format for the local switch.
	`switch(config)# fcsp dhchap password 7 sfsfdf 29:11:bb:cc:dd:33:11:22`	Configures a password entered in an encrypted format for the local switch to be used for the device with the specified WWN.
	`switch(config)# no fcsp dhchap password 7 sfsfdf 29:11:bb:cc:dd:33:11:22`	Removes the password entered in an encrypted format for the local switch to be used for the device with the specified WWN.
	`switch(config)# fcsp dhchap password mypassword1`	Configures a clear text password for the local switch to be used with any connecting device.

Configuring Password for Other Devices

You can configure passwords in the local authentication database for other devices in a fabric. The other devices are identified by their device name, which is also known as the switch WWN or device WWN. The password is restricted to 64 characters and can be specified in clear text (0) or in encrypted text (7).

Note The switch WWN identifies the physical switch. This WWN is used to authenticate the switch and is different from the VSAN node WWN.

Configuring the Timeout Value

During the DHCHAP protocol exchange, if the MDS switch does not receive the expected DHCHAP message within a specified time interval, authentication failure is assumed. The time ranges from 20 (no authentication is performed) to 1000 seconds. The default is 30 seconds.

When changing the timeout value, consider the following factors:

- The existing RADIUS and TACACS+ timeout values.
- The same value must also be configured on all switches in the fabric.

To configure the DHCHAP timeout value, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# fcsp timeout 60`	Configures the reauthentication timeout to be 60 seconds.
	`switch(config)# no fcsp timeout 60`	Reverts to the factory default of 30 seconds.

Configuring DHCHAP AAA Authentication

You can individually set authentication options using the **aaa authentication dhchap** command. If authentication is not configured, local authentication is used by default.

To configure the AAA authentication, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# aaa authentication dhchap default group TacacsServer1`	Enables DHCHAP to use the TACACS+ server group (in this example, TacacsServer1) for authentication.
	`switch(config)# aaa authentication dhchap default local`	Enables DHCHAP for local authentication.
	`switch(config)# aaa authentication dhchap default group RadiusServer1`	Enables DHCHAP to use the RADIUS server group (in this example, RadiusServer1) for authentication.

Configuring Port Security

All switches in the Cisco MDS 9000 Family provide port security features that reject intrusion attempts and report these intrusions to the administrator.

Note Port security is only supported for Fibre Channel ports.

Configuring Auto-Learning

The state of the auto-learning configuration depends on the state of the port security feature:

- If the port security feature is not activated, the **auto-learn** option is disabled by default.
- If the port security feature is activated, the **auto-learn** option is enabled by default (unless it is turned off using the **port-security activate vsan** *number* **no-auto-learn** command).

To enable the **auto-learn** option, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# port-security auto-learn vsan 1`	Enables auto-learn so the switch can learn about any device that is allowed to access VSAN 1. These devices are logged in the port security active database.
	`switch(config)# no port-security auto-learn vsan 1`	Disables auto-learn and stops the switch from learning about new devices accessing the switch. Enforces the database contents based on the devices learned up to this point.

Tip If the **auto-learn** option is enabled on a VSAN, you cannot activate the database for that VSAN without the **force** option.

Manually Configuring Port Security

To configure port security on any switch in the Cisco MDS 9000 Family, follow these steps:

Step 1 Identify the WWN of the ports that need to be secured.

Step 2 Secure the fWWN to an authorized nWWN or pWWN.

Step 3 Activate the port security database.

Step 4 Verify your configuration.

Securing Authorized Ports

After identifying the WWN pairs that need to be bound, add those pairs to the port security database.

To configure port security, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# port-security database vsan 1` `switch(config-port-security)#`	Enters the port security database mode for the specified VSAN.
	`switch(config)# no port-security database vsan 1` `switch(config)#`	Deletes the port security configuration database from the specified VSAN.

	Command	Purpose
Step 3	`switch(config-port-security)# swwn 20:01:33:11:00:2a:4a:66 interface port-channel 5`	Configures the specified sWWN to only log in through PortChannel 5.
	`switch(config-port-security)# any-wwn interface fc1/1 - fc1/8`	Configures any WWN to log in through the specified interfaces.
	`switch(config-port-security)# pwwn 20:11:00:33:11:00:2a:4a fwwn 20:81:00:44:22:00:4a:9e`	Configures the specified pWWN to only log in through the specified fWWN.
	`switch(config-port-security)# no pwwn 20:11:00:33:11:00:2a:4a fwwn 20:81:00:44:22:00:4a:9e`	Deletes the specified pWWN configured in the previous step.
	`switch(config-port-security)# nwwn 26:33:22:00:55:05:3d:4c fwwn 20:81:00:44:22:00:4a:9e`	Configures the specified nWWN to log in through the specified fWWN.
	`switch(config-port-security)# pwwn 20:11:33:11:00:2a:4a:66`	Configures the specified pWWN to log in through any port on the local switch.
	`switch(config-port-security)# any-wwn interface fc3/1`	Configures any WWN to log in through the specified interface.
	`switch(config-port-security)# no any-wwn interface fc2/1`	Deletes the wildcard configured in the previous step.

Activating the Port Security Database

When you activate the port security database, all entries in the configured database are copied to the active database. After the database is activated, subsequent device login is subject to the activated port bound WWN pairs. Additionally, all devices that have already logged into the VSAN at the time of activation are also learned and added to the active database. If the auto-learn feature is already enabled in a VSAN, you will not be allowed to activate the database.

To activate the port database, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# port-security activate vsan 1` `switch(config-port-security)#`	Activates the port security database for the specified VSAN, and automatically turns on the auto-learn feature.
	`switch(config)# no port-security activate vsan 1`	Deactivates port security, deletes the active database, and disables auto-learn.

CHAPTER 8

Configuring Call Home

Call Home provides e-mail-based notification of critical system events. A versatile range of message formats are available for optimal compatibility with pager services, standard e-mail, or XML-based automated parsing applications.

This chapter provides configuration and messaging details on the Call Home feature. It includes the following sections:

Entering the Call Home Configuration Submode

To enter the Call Home submode, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# callhome` `switch(config-callhome)#`	Enters Call Home submode.

Step 3	`switch(config-callhome)# ?`
	`  contract-id  Service contract id of the customer`
	`  customer-id  Customer id`
	`  destination-profile  Configure destination profiles`
	`  disable  Disable callhome`
	`  email-contact  Email address of the contact person`
	`  enable  Enable callhome`
	`  exit  Exit from this submode`
	`  no  Negate a command or set its defaults`
	`  phone-contact  Contact person's phone number`
	`  site-id  Site id of the network where switch is deployed`
	`  streetaddress  Configure replacement part shipping address.`
	`  switch-priority  Priority of the switch(0-highest 7-lowest)`
	`  transport  Configure transport related configuration`
		Displays the options available at this prompt.

Assigning Contact Information

It is mandatory for each switch to include e-mail, phone, and street address information. It's optional to include the contract ID, customer ID, site ID, and switch priority information.

To assign the contact information, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch# snmp-server contact personname@companyname.com`	Configures the SNMP contact e-mail address to receive a test message reply from Cisco.
Step 3	`switch(config)# callhome` `switch(config-callhome)#`	Enters the Call Home submode.

Step 4	`switch(config-callhome)# email-contact username@company.com`
	`successfully updated the information`
	`switch(config-callhome)#`
		Assigns the customer's e-mail address. Up to 128 alphanumeric characters are accepted in e-mail address format.
		Note You can use any valid e-mail address. You cannot use spaces.

Step 5	`switch(config-callhome)# phone-contact +1-800-123-4567`
	`successfully updated the information`
	`switch(config-callhome)#`
		Assigns the customer's phone number. Up to 20 alphanumeric characters are accepted in international format.
		Note You cannot use spaces. Be sure to use the + prefix before the number.

Step 6	`switch(config-callhome)# streetaddress 1234 Picaboo Street, Any city, Any state, 12345`
	`successfully updated the information`
	`switch(config-callhome)#`
		Assigns the customer's street address where the equipment is located. Up to 256 alphanumeric characters are accepted in free format.

	Command	Purpose

Step 7	`switch(config-callhome)# switch-priority 0`
	`successfully updated the information`
	`switch(config-callhome)#`
		Assigns the switch priority, with 0 being the highest priority and 7 the lowest.
		Tip Use this field to create a hierarchical management structure.

Step 8	`switch(config-callhome)# customer-id Customer1234`
	`successfully updated the information`
	`switch(config-callhome)#`
		(Optional) Identifies the customer ID. Up to 256 alphanumeric characters are accepted in free format.

Step 9	`switch(config-callhome)# site-id Site1ManhattanNY`
	`successfully updated the information`
	`switch(config-callhome)#`
		(Optional) Identifies the customer site ID. Up to 256 alphanumeric characters are accepted in free format.

Step 10	`switch(config-callhome)# contract-id Company1234`
	`successfully updated the information`
	`switch(config-callhome)#`
		Assigns the customer ID for the switch. Up to 64 alphanumeric characters are accepted in free format.

Configuring Destination Profiles

A destination profile contains the required delivery information for an alert notification. Destination profiles are typically configured by the network administrator. At least one destination profile is required. You can configure multiple destination profiles of one or more types.

You can use one of the predefined destination profiles or define a desired profile. If you define a new profile, you must assign a profile name.

Note If you use the Cisco AutoNotify service, the XML destination profile is required (see http://www.cisco.com/warp/customer/cc/serv/mkt/sup/tsssv/opmsup/smton/anoti_ds.htm).

To configure predefined destination profile messaging options, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# callhome` `switch(config-callhome)#`	Enters the Call Home submode.
Step 3	`switch(config-callhome)# destination-profile full-txt-destination email-addr person@place.com`	Configures a predefined destination e-mail address for a message sent in full text format. This text provides the complete, detailed explanation of the failure. **Tip** Use a standard e-mail address that does not have any text size restrictions.
	`switch(config-callhome)# destination-profile full-txt-destination message-size 1000000`	Configures a predefined destination message size for a message sent in full text format. The valid range is 0 to 1,000,000 bytes and the default is 500,000. A value of 0 implies that a message of any size can be sent.

	Command	Purpose
Step 4	`switch(config-callhome)# destination-profile short-txt-destination email-addr person@place.com`	Configures a predefined destination e-mail address for a message sent in short text format. This text provides the basic explanation of the failure. **Tip** Use a pager-related e-mail address for this option.
	`switch(config-callhome)# destination-profile short-txt-destination message-size 100000`	Configures a predefined destination message size for a message sent in short text format. The valid range is 0 to 1,000,000 bytes and the default is 4000. A value of 0 implies that a message of any size can be sent.
Step 5	`switch(config-callhome)# destination-profile XML-destination email-addr findout@.cisco.com`	Configures a predefined destination e-mail address for a message sent in XML format. This option provides the full information that is compatible with Cisco Systems TAC support. **Tip** Do not add a pager-related e-mail address to this destination profile because of the large message size.
	`switch(config-callhome)# destination-profile XML-destination message-size 100000`	Configures a predefined destination message size for a message sent in XML format. The valid range is 0 to 1,000,000 bytes and the default is 500,000. A value of 0 implies that a message of any size can be sent.

Note Steps 3, 4, and 5 in this procedure can be skipped or configured in any order.

To configure new destination profile messaging options, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# callhome` `switch(config-callhome)#`	Enters the Call Home submode.
Step 3	`switch(config-callhome)# destination-profile test`	Configures a new destination profile called test.
Step 4	`switch(config-callhome)# destination-profile test email-addr person@place.com`	Configures the e-mail address for the user-defined destination message (test) sent in default XML format.
Step 5	`switch(config-callhome)# destination-profile test message-size 1000000`	Configures a message size for the user-defined destination message (test) sent in default XML format. The valid range is 0 to 1,000,000 bytes and the default is 500,000. A value of 0 implies that a message of any size can be sent.
Step 6	`switch(config-callhome)# destination-profile test format full-txt`	Configures a user-defined destination message (test) sent in full text format.
	`switch(config-callhome)# destination-profile test format short-txt`	Configures a user-defined destination message (test) sent in short text format.

Note Steps 4, 5, and 6 in this procedure can be skipped or configured in any order.

Configuring Alert Groups

You can associate one or more alert groups to each profile as required by your network. By default, all alert groups are associated with each profile. The **alert-group** option allows you to select predefined types of Call Home alert notifications for destination profiles (predefined and user-defined). Destination profiles can be associated with multiple alert groups.

To configure alert group options, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# callhome` `switch(config-callhome)#`	Enters Call Home submode.
Step 3	`switch(config-callhome)# destination-profile test1 alert-group test`	(Optional) Configures user-defined destination message profile (test1) to send Call Home notifications for all user-generated test events.
	`switch(config-callhome)# destination-profile short-txt-destination alert-group test`	(Optional) Configures predefined short-text destination message profile to send Call Home notifications for all user-generated test events.
Step 4	`switch(config-callhome)# destination-profile test1 alert-group all`	(Optional) Configures user-defined destination message profile (test1) to send Call Home notifications for all events.
	`switch(config-callhome)# destination-profile short-txt-destination alert-group all`	(Optional) Configures predefined short-text destination message profile to send Call Home notifications for all (default) events.
Step 5	`switch(config-callhome)# destination-profile test1 alert-group Cisco-TAC`	(Optional) Configures user-defined destination message profile (test1) to send Call Home notifications for events that are meant only for Cisco TAC or the auto-notify service.
	`switch(config-callhome)# destination-profile xml-destination alert-group Cisco-TAC`	(Optional) Configures predefined XML destination message profile to send Call Home notifications for events that are meant only for Cisco TAC or the auto-notify service.
Step 6	`switch(config-callhome)# destination-profile test1 alert-group environmental`	(Optional) Configures user-defined destination message profile (test1) to send Call Home notifications for power, fan, and temperature-related events.
	`switch(config-callhome)# destination-profile short-txt-destination alert-group environmental`	(Optional) Configures predefined short-text destination message profile to send Call Home notifications for power, fan, and temperature-related events.

	Command	Purpose
Step 7	`switch(config-callhome)# destination-profile test1 alert-group inventory`	(Optional) Configures user-defined destination message profile (test1) to send Call Home notifications for inventory status events.
	`switch(config-callhome)# destination-profile short-txt-destination alert-group inventory`	(Optional) Configures predefined short-text destination message profile to send Call Home notifications for inventory status events.
Step 8	`switch(config-callhome)# destination-profile test1 alert-group linecard-hardware`	(Optional) Configures user-defined destination message profile (test1) to send Call Home notifications for module-related events.
	`switch(config-callhome)# destination-profile short-txt-destination alert-group linecard-hardware`	(Optional) Configures predefined short-text destination message profile to send Call Home notifications for module-related events.
Step 9	`switch(config-callhome)# destination-profile test1 alert-group supervisor-hardware`	(Optional) Configures user-defined destination message profile (test1) to send Call Home notifications for supervisor-related events.
	`switch(config-callhome)# destination-profile short-txt-destination alert-group supervisor-hardware`	(Optional) Configures predefined short-text destination message profile to send Call Home notifications for supervisor-related events.
Step 10	`switch(config-callhome)# destination-profile test1 alert-group system`	(Optional) Configures user-defined destination message profile (test1) to send Call Home notifications for software-related events.
	`switch(config-callhome)# destination-profile short-txt-destination alert-group system`	(Optional) Configures predefined short-text destination message profile to send Call Home notifications for software-related events.

Configuring Message Levels

The **message-level** option allows you to filter messages based on their level of urgency. Each destination profile (predefined and user-defined) is associated with a Call Home message level threshold. Any message with a value lower that the urgency threshold is not sent. The urgency level ranges from 0 (lowest level of urgency) to 9 (highest level of urgency), and the default is 0 (all messages are sent).

To configure message level options, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# callhome` `switch(config-callhome)#`	Enters Call Home submode.
Step 3	`switch(config-callhome)# destination-profile test message-level 5`	(Optional) Configures the message level urgency as 5 and above for the user-defined profile (test1).
	`switch(config-callhome)# no destination-profile oldtest message-level 7`	Removes a previously configured urgency level and reverts it to the default of 0 (all messages are sent).

Configuring E-Mail Options

You can configure the from, reply-to, and return-receipt e-mail addresses. While most e-mail address configurations are optional, you must configure the SMTP server address and port number for the Call Home functionality to work.

To configure general e-mail options, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# callhome` `switch(config-callhome)#`	Enters Call Home submode.
Step 3	`switch(config-callhome)# transport email from user@company1.com`	(Optional) Configures the from e-mail address.
Step 4	`switch(config-callhome)# transport email reply-to person@place.com`	(Optional) Configures the reply-to e-mail address to which all responses should be sent.

To configure the SMTP server and port, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# callhome` `switch(config-callhome)#`	Enters Call Home submode.

Step 3	`switch(config-callhome)# transport email smtp-server 192.168.1.1`
	`successfully updated the information`
	`switch(config-callhome)#`
		Configures the DNS or IP address of the SMTP server to reach the server. The port usage defaults to 25 if no port is specified.
		Note The port number is optional and, if required, may be changed depending on the server location.

	`switch(config-callhome)# transport email smtp-server 192.168.1.1 port 30`
	`successfully updated the information`
	`switch(config-callhome)#`	

Enabling or Disabling Call Home

Once you have configured the contact information, you must enable the Call Home function. The **enable** command is required for the Call Home function to start operating.

To enable the Call Home function, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# callhome` `switch(config-callhome)#`	Enters Call Home submode.

Step 3	`switch(config-callhome)# enable`
	`callhome enabled successfully`
	`switch(config-callhome)#`
		Enables the Call Home function.

	`switch(config-callhome)# disable` `switch(config-callhome)#`	Disables the Call Home function. When you disable the Call Home function, all input events are ignored. **Note** Even if Call Home is disabled, basic information for each Call Home event is sent to syslog.

Configuring System Message Logging

This chapter describes how to configure system message logging on Cisco MDS 9000 Family switches. It includes the following sections:

Enabling System Message Logging

You can disable logging to the console or enable logging to a given Telnet or SSH session.

- When you disable or enable logging to a console session, that state is applied to all future console sessions. If you exit and log in again to a new session, the state is preserved.
- When you enable or disable logging to a Telnet or SSH session, that state is applied only to that session. If you exit and log in again to a new session, the state is not preserved.

To enable or disable the logging state for a Telnet or SSH session, follow these steps:

	Command	Purpose
Step 1	`switch# terminal monitor`	Enables logging for a Telnet or SSH session. **Note** A console session is enabled by default.
Step 2	`switch# terminal no monitor`	Disables logging for a Telnet or SSH session. **Note** A Telnet or SSH session is disabled by default.

Configuring Console Severity Level

When logging is enabled for a console session (default), you can configure the severity levels of messages that appear on the console. The default severity for console logging is 2 (critical).

To configure the severity level for a logging facility, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# logging console 3`	Configures console logging at level 3 (error). Logging messages with a severity level of 3 or above are displayed on the console.
	`switch(config)# logging console`	Reverts console logging to the factory set default severity level of 2 (critical). Logging messages with a severity level of 2 or above are displayed on the console.

Tip The current critical (default) logging level is maintained if the console baud speed is 9600 baud (default). All attempts to change the console logging level generates an error message. To increase the logging level (above critical), you must change the console baud speed to 38400 baud.

Configuring Module Logging

By default, logging is enabled at level 7 for all modules. You can enable or disable logging for each module at a specified level.

To configure the severity level for a logging facility, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# logging module 1`	Configures module logging at level 1 (alerts).
	`switch(config)# logging module`	Configures module logging for all modules in the switch.
	`switch(config)# no logging module`	Reverts module logging to the factory set default of not configuring logging for all modules.

Configuring Facility Severity Level

To configure the severity level for a logging facility, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# logging level kernel 4`	Configures Telnet or SSH logging for the kernel facility at level 4 (warning). As a result, logging messages with a severity level of 4 or above are displayed.

Configuring Log Files

Logging messages may be saved to a separate log file. You can configure the name of this file and restrict its size as required. The default log file name is `messages`. You can rename this file using the **logging logfile** command. The file name can have up to 80 characters and the file size ranges from 4096 bytes to 4194304 bytes.

To send log messages to file, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# logging logfile ManagerLog 3 size 3000000`	Configures logging information for errors or events above severity level 3 to be logged in a file named ManagerLog. By configuring a size, you are restricting the file size to 3000000 bytes. The maximum upper limit is 4194304 (default).

The configured log file is saved in the /var/log/external directory. The location of the log file cannot be changed. You can use the **show logging logfile** *filename* and **clear logging logfile** *filename* commands to view and delete this file. It is not accessible using the **dir** command.

Configuring Syslog Servers

To configure system message logging servers, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch#`	Enters configuration mode.
Step 2	`switch(config)# logging server 172.22.00.00` `switch(config)#`	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). **Note** You can configure a maximum of three system message logging servers.
	`switch(config)# logging server 172.22.00.00 facility local1` `switch(config)#`	Configures the switch to forward log messages according to the specified facility (local1) for the server IP address (172.22.00.00). The default outgoing facility is local7.
	`switch(config)# no logging server 172.11.00.00` `switch(config)#`	Removes the specified server (172.11.00.00) and reverts to factory default. **Note** You can configure a maximum of three system message logging servers.

A

B

C

D

E

F

I

L

M

N

O

P

R

S

T

U

V

Z