Cisco Systems

Send documentation comments to mdsfeedback-doc@cisco.com

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

Text Part Number: OL-8251-01

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	Initial Switch Configuration	Describes how to initially configure switches so they can be accessed by other devices.
Chapter 3	Configuring VSANs and Interfaces	Describes how to configure VSANs, interfaces, and zones.
Chapter 4	Configuring Zones and Zone Sets	Provides basic configuration information for zones and zone sets.
Appendix A	Configuring Static Domain IDs and Persistent FC IDs	Provides the procedure for configuring static domain IDs and persistent FC IDs.
Appendix B	Configuration Files	Describes how to save and copy configuration files that contain the parameters required to configure a switch.

Document Conventions

Command descriptions use these conventions:

boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Screen examples use these conventions:

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

This document uses the following conventions:

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

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

Related Documentation

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

- *Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Releases*
- Cisco MDS 9000 Family Interoperability Support Matrix
- Cisco MDS SAN-OS Release Compatibility Matrix for IBM SAN Volume Controller Software for Cisco MDS 9000
- Cisco MDS SAN-OS Release Compatibility Matrix for VERITAS Storage Foundation for Networks Software
- Cisco MDS SAN-OS Release Compatibility Matrix for Storage Service Interface Images
- Cisco MDS 9000 Family SSM Configuration Note
- Cisco MDS 9000 Family ASM Configuration Note
- *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*

- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9216 Switch Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- Cisco MDS 9020 Fabric Switch Hardware Installation Guide
- Cisco MDS 9000 Family Software Upgrade and Downgrade Guide
- *Cisco MDS 9000 Family Configuration Guide*
- *Cisco MDS 9000 Family Command Reference*
- Cisco MDS 9020 Fabric Switch Configuration Guide and Command Reference
- *Cisco MDS 9000 Family Fabric Manager Configuration Guide*
- Cisco MDS 9000 Family Fabric and Device Manager Online Help
- *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide*
- Cisco MDS 9000 Family Quick Configuration Guide
- Cisco MDS 9000 Family Fabric Manager Quick Configuration Guide
- *Cisco MDS 9000 Family MIB Quick Reference*
- Cisco MDS 9020 Fabric Switch MIB Quick Reference
- *Cisco MDS 9000 Family CIM Programming Reference*
- *Cisco MDS 9000 Family System Messages Reference*
- Cisco MDS 9020 Fabric Switch System Messages Reference
- *Cisco MDS 9000 Family Troubleshooting Guide*
- *Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note*
- *Cisco MDS 9000 Family Port Analyzer Adapter Installation and Configuration Note*

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/techsupport

Send documentation comments to mdsfeedback-doc@cisco.com

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

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

Cisco Marketplace:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

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

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

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

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

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

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

Documentation Feedback

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

Send documentation comments to mdsfeedback-doc@cisco.com

You can send comments about Cisco documentation to mdsfeedback-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

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

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

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

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

http://www.cisco.com/techsupport

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

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

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

Submitting a Service Request

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

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

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

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

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

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

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

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

  or view the digital edition at this URL:

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

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

  http://www.cisco.com/ipj

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

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

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

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

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

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

CHAPTER 1

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

Initial Switch Configuration

This chapter provides instructions for setting up the hardware, connecting to the console port, and initially configuring the switch.

This chapter includes the following sections:

Preparing for Network Connections

When preparing your site for network connections to the Andiamo 9500 switch, consider the following for each type of interface:

- Cabling required for each interface type
- Distance limitations for each signal type
- Additional interface equipment needed

Before installing the device, have all additional external equipment and cables available.

Configuration Prerequisites

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

- Administrator password.
- Switch name—This is also used as your switch prompt.
- IP address for the switch's management interface.
- Subnet mask for the switch's management interface.
- IP address of the default gateway.

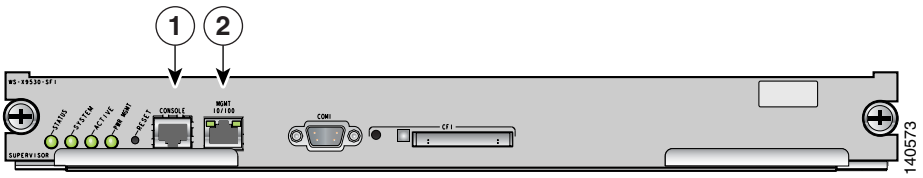
Connecting the Console Port

This section describes how to connect the RS-232 console port to a PC. The console port allows you to perform the following functions:

- Configure the switch from the CLI.
- Monitor network statistics and errors.
- Configure SNMP agent parameters.
- Manage downloading software updates (through the Ethernet management interface) or distributing software images residing in Flash memory to attached devices.

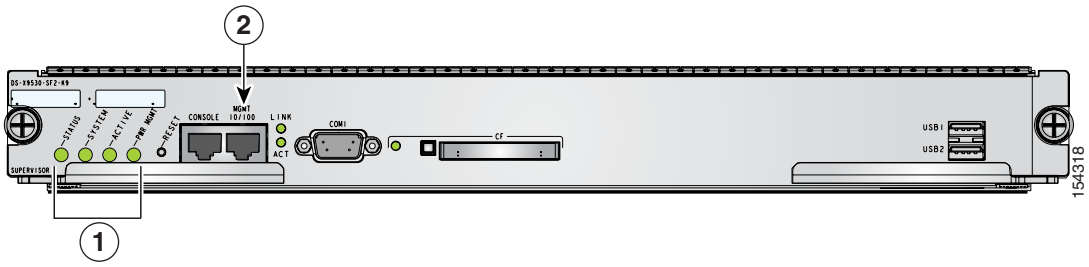
Figure 2-1, Figure 2-3, Figure 2-4, and Figure 2-4 show the console port and the management port, located on a Cisco MDS 9500 series supervisor-1 module, Cisco MDS 9500 series supervisor-2 module, a Cisco MDS 9200 Series supervisor module, and Cisco MDS 9100 Series supervisor module.

Figure 2-1 Cisco MDS 9500 Series Supervisor-1 Module



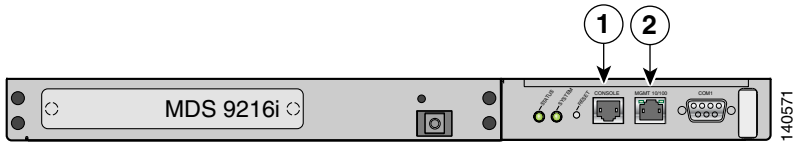
1	Console port
2	MGMT 10/100 Ethernet port (with integrated link and activity LEDs)

Figure 2-2 Cisco MDS 9500 Series Supervisor-2 Module



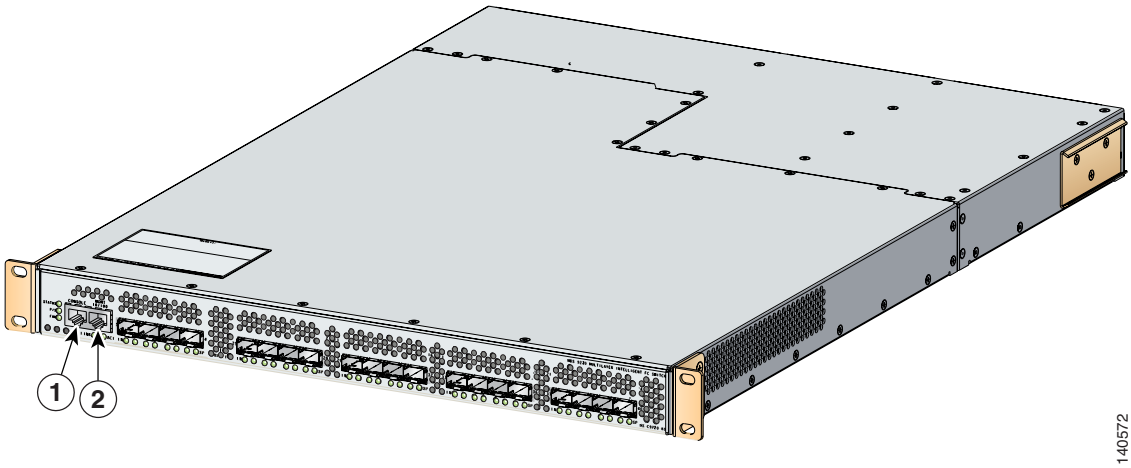
1	Status, System, Active, and Pwr Mgmt LEDs
4	MGMT 10/100/1000 Ethernet port (with integrated Link and Activity LEDs)

Figure 2-3 Connecting the Console Cable to a Cisco MDS 9200 Series Switch



1	Console port
2	MGMT 10/100 Ethernet port (with integrated link and activity LEDs)

Figure 2-4 Connecting the Console Cable to a Cisco MDS 9100 Series Switch



1	Console port
2	MGMT 10/100 Ethernet port (with integrated link and activity LEDs)

Connecting the Console Port to a PC

You can connect the console port to a PC serial port for local administrative access to the Andiamo 9500 switch.

Note The PC must support VT100 terminal emulation. The terminal emulation software—frequently a PC application such as HyperTerminal Plus—makes communication between the Andiamo 9500 switch and your PC possible during setup and configuration.

To connect the console port to a PC, follow these steps:

Step 1 Configure the baud rate and character format of the PC terminal emulation program to match the following management port default characteristics:

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

Note On Cisco terminal servers, issue the following commands starting in EXEC mode:

```
switch# config t
switch(config)# no flush-at-activation
switch(config)# exit
switch# copy running-config startup-config
```

This configuration ensures that the MDS switch does not receive random characters that might cause it to hang.

Step 2 Connect the supplied RJ-45 to DB-9 female adapter or RJ-45 to DB-25 female adapter (depending on your PC connection) to the PC serial port.

Step 3 Connect one end of the supplied console cable (a rollover RJ-45 to RJ-45 cable) to the console port. (See Figure 2-4.) Connect the other end to the RJ-45 to DB-9 (or RJ-45 to DB-25) adapter at the PC serial port.

Note If you are using a Cisco MDS 9500 Series switch that has multiple supervisor modules, connect the console port to the “active” supervisor. The active supervisor is the module with the green Active LED.

Connecting the 10/100 Ethernet Management Port

The autosensing 10/100 Ethernet management port is located on the left side of the front panel (labeled 10/100 MGMT), to the right of the Console port (see Figure 2-1, Figure 2-4, and Figure 2-4). This port is used for out-of-band management of the Cisco MDS 9000 Family switches.

Make sure to connect the Ethernet management ports of both supervisor modules on an MDS 9500 Series switch. Even though there are two Ethernet connections, only one management IP address is required for a switch with dual supervisors.

Tip The two Ethernet connections should be connected to ports in different slots on the same LAN switch, or should be split between two different LAN switches.

If only the active supervisor module is connected to the LAN and an event occurs that causes a system switchover (such as a software upgrade), the switch becomes unmanageable through the Ethernet port after the active supervisor reboots and the standby supervisor becomes the active supervisor.

Use modular, RJ-45 cables to connect the 10/100 Ethernet management port to external hubs and switches.

Connecting to the MGMT 10/100/1000 Ethernet Port

The Supervisor-2 module supports an autosensing MGMT 10/100/1000 Ethernet port (labeled "MGMT 10/100/1000") and has an RJ-45 interface. You can use this port to access and manage the switch by IP address, such as through Cisco Fabric Manager.

Use a modular, RJ-45, straight-through UTP cable to connect the MGMT 10/100/1000 Ethernet port to an Ethernet switch port or hub.

Using the Switch Setup Utility

The switch setup utility helps you configure the switch. To configure the switch, follow these steps:

Step 1 Verify the following physical connections for the new Cisco MDS 9000 Family switch (see Figure 2-4):

- The console port is physically connected to a computer terminal (or terminal server).
- The 10/100/1000 Ethernet management port (mgmt0) is connected to an external hub, switch, or router.

Refer to the hardware installation guide for your specific product.

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 (see the "Connecting the Console Port to a PC" section on page 2-4).

Step 3 Power on the switch. The switch boots automatically.

Note If the switch boots to the `loader>` or `switch(boot)` prompts, contact your storage vendor support organization for technical assistance.

After powering on the switch, you see the following output:

```
General Software Firmbase[r] SMM Kernel 1.1.1002 Aug  6 2003 22:19:14 Copyright (C) 2002
General Software, Inc.

Firmbase initialized.

00000589K Low Memory Passed
01042304K Ext Memory Passed
Wait.....

General Software Pentium III Embedded BIOS 2000 (tm) Revision 1.1.(0)
(C) 2002 General Software, Inc.ware, Inc.
Pentium III-1.1-6E69-AA6E
+------------------------------------------------------------------------------+
|          System BIOS Configuration, (C) 2002 General Software, Inc.          |
+---------------------------------------+--------------------------------------+
| System CPU            : Pentium III    | Low Memory            : 630KB        |
| Coprocessor           : Enabled        | Extended Memory       : 1018MB       |
| Embedded BIOS Date    : 10/24/03       | ROM Shadowing         : Enabled      |
+---------------------------------------+--------------------------------------+
Loader Loading stage1.5.

Loader loading, please wait...
Auto booting bootflash:/m9500-sf1ek9-kickstart-mz.2.1.1a.bin bootflash:/m9500-s
f1ek9-mz.2.1.1a.bin...
Booting kickstart image:
bootflash:/m9500-sf1ek9-kickstart-mz.2.1.1a.bin...................Image verification OK

Starting kernel...
INIT: version 2.78 booting
Checking all filesystems..... done.
Loading system software
Uncompressing system image: bootflash:/m9500-sf1ek9-mz.2.1.1a.bin
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
INIT: Entering runlevel: 3
```

Step 4 Make sure you enter the password you wish to assign for the admin user name.

```
---- System Admin Account Setup ----
  Enter the password for "admin":
```

Tip If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a strong password. Passwords are case-sensitive. You must explicitly configure a password that meets the requirements listed in the "Configuring User Accounts" section in the *Cisco MDS 9000 Family CLI Configuration Guide*.

Note If you are running the switch setup utility for the first-time, it starts automatically. If this is not the first-time configuration, you are required to enter **setup** at the system prompt.

Note If you do not wish to answer a previously configured question, or if you wish to skip answers to any questions, press **Enter**. If a default answer is not available (for example, the switch name), the switch uses what was previously configured and skips to the next question.

Step 5 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.
```

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

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

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

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

Step 6 Enter **no** (no is the default) to not create any additional accounts.

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

Step 7 Enter **no** (no is the default) to not configure any read-only SNMP community strings.

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

Step 8 Enter **no** (no is the default) to not configure any read-write SNMP community strings.

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

Step 9 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 10 Enter **yes** (yes is the default) to configure the out-of-band management configuration.

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

a. Enter the IP address for the mgmt0 interface.

```
Mgmt0 IP address : mgmt_IP_address
```

b. Enter the netmask for the mgmt0 interface in the xxx.xxx.xxx.xxx format.

```
Mgmt0 IP netmask : xxx.xxx.xxx.xxx
```

Step 11 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 12 Enter **no** (no is the default) to configure advanced IP options such as in-band management, static routes, default network, DNS, and domain name.

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

Step 13 Enter **yes** (yes is the default) to enable Telnet service.

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

Step 14 Enter **no** (no is the default) to not enable the SSH service.

```
Enable the ssh service? (yes/no) [n]: no
```

Step 15 Enter **no** (no is the default) to not configure the NTP server.

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

Step 16 Enter **noshut** (shut is the default) to configure the default switch port interface to the noshut state.

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

Step 17 Enter **on** (on is the default) to configure the switch port trunk mode.

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

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

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

Denies the traffic to flow for all members of the default zone.

Step 19 Enter **yes** (no is the default) to enable a full zone set distribution (refer to the *Cisco MDS 9000 Family CLI Configuration Guide*).

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

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:

switchname switch_name
  interface mgmt0
    ip address mgmt_IP_address
    subnetmask mgmt0_ip_netmask
    no shutdown
  ip default-gateway default_gateway
  telnet server enable
  no ssh server enable
  no system default switchport shutdown
  system default switchport trunk mode on
  no 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 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** to save the new configuration. This ensures that the kickstart and system images are also automatically configured.

Verifying the Module Status

Before you proceed with any further configuration of 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. All the hardware that was physically installed should be displayed.

A sample output of the **show module** command follows:

```
switch# show module
Mod  Ports  Module-Type                       Model              Status
---  -----  -------------------------------- ------------------ ------------
2    32     1/2 Gbps FC Module               DS-X9032           ok
3    16     1/2 Gbps FC Module               DS-X9016           ok
4    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
7    0      Caching Services Module          DS-X9560-SMAP      ok
9    32     Advanced Services Module         DS-X9032-SMV       ok

Mod  Sw           Hw      World-Wide-Name(s) (WWN)
---  -----------  ------  --------------------------------------------------
2    2.1(1a)      1.1     20:41:00:05:30:00:86:9e to 20:60:00:05:30:00:86:9e
3    2.1(1a)      3.0     20:81:00:05:30:00:86:9e to 20:90:00:05:30:00:86:9e
4    2.1(1a)      4.0     20:c1:00:05:30:00:86:9e to 20:c8:00:05:30:00:86:9e
5    2.1(1a)      4.0     --
6    2.1(1a)      4.0     --
7    2.1(1a)      0.702   --
9    2.1(1a)      0.502   22:01:00:05:30:00:86:9e to 22:20:00:05:30:00:86:9e

Mod      Application Image Description       Application Image Version
-------- ----------------------------       -------------------------
7        svc-node1                          1.3(5m)
7        svc-node2                          1.3(5m)
9        SSI linecard image                 2.1(1)

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
2    00-0c-30-d9-eb-60 to 00-0c-30-d9-eb-64  JAB074704EJ
3    00-0c-30-0d-27-54 to 00-0c-30-0d-27-58  JAB074004RR
4    00-0c-30-da-92-88 to 00-0c-30-da-92-94  JAB075204ZN
5    00-0c-30-d9-dc-d0 to 00-0c-30-d9-dc-d4  JAB074504RC
6    00-0c-30-d9-ef-80 to 00-0c-30-d9-ef-84  JAB0747055Y
7    00-0d-bc-2f-bc-b8 to 00-0d-bc-2f-bd-3c  JAB073907DK
9    00-05-30-00-ad-4e to 00-05-30-00-ad-52  JAB070605QV

* this terminal session
```

Note If you do not see all the installed hardware, call your storage vendor support organization for further assistance.

CHAPTER 3

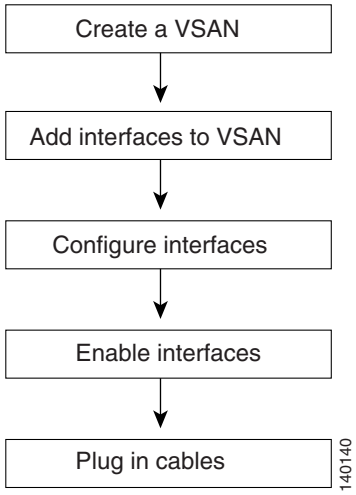
Configuring VSANs and Interfaces

You can achieve higher security and greater stability in Fibre Channel fabrics by using virtual storage area networks (VSANs). VSANs provide isolation among devices that are physically connected to the same fabric.

Interfaces are members of a VSAN. Interfaces enable communication between switches in a VSAN. Interfaces that are members of the same VSAN can communicate with each other; interfaces that are members of different VSANs cannot communicate with each other.

Figure 3-1 describes the steps involved in configuring VSANs and interfaces.

Figure 3-1 VSANs and Interfaces



This chapter includes the following sections:

Creating VSANs

VSANs help you 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 (FC IDs) to be used simultaneously in different VSANs.

Default VSAN

VSAN 1, also known as the default VSAN, is typically used for communication, management, or testing purposes. We recommend that you do not use VSAN 1 as your production environment VSAN. There are several features that, when configured, disrupt traffic on VSAN 1. If you use VSAN 1 as your production environment VSAN, you risk disrupting traffic when these features are configured.

Note By default, all Cisco MDS 9000 Family switches belong to VSAN 1. We recommend you create production environment VSANs and configure the switches to use those VSANs.

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

Creating and Configuring VSANs

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).

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).

	Command	Purpose
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.

See Appendix A, "Configuring Static Domain IDs and Persistent FC IDs," for details.

Warning **HP-UX and AIX are two operating systems that utilize the FC ID in the device path to the storage. For the switch to always assign the same FC ID to a device, persistent FC IDs and static Domain ID must be configured for the VSAN.**

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 3-1 lists the **show** commands and the information they display.

Table 3-1 show interface Commands

show Command	Description
`show vsan`	Displays information for all VSANs.
`show vsan 100`	Displays information for a specific VSAN.
`show vsan usage`	Displays information on VSAN usage.
`show vsan 100 membership`	Displays VSAN membership information for a specified VSAN.

Table 3-1 show interface Commands (continued)

show Command	Description
`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 sent and received must be defined. The configured interfaces can be Fibre Channel interfaces, the management interface (mgmt0), or VSAN interfaces.

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).

After enabling the interfaces, make sure you plug in the cables. If the cables are not plugged in, the hosts will not be able to communicate with the storage device.

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 refer 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 Ethernet mgmt0 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 Ethernet management 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.

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.

Creating 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.

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.

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 3-2 lists the **show** commands and the information they display.

Table 3-2 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.

CHAPTER 4

Configuring Zones and Zone Sets

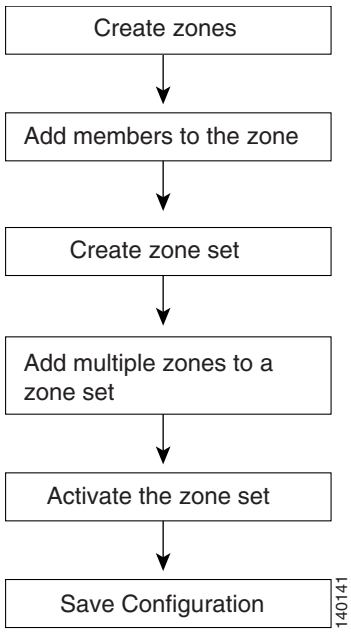
Before setting up zones and zone sets make sure you have configured VSANs and interfaces. See Chapter 3, "Configuring VSANs and Interfaces."

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.

Note Devices that do not belong to a zone follow the policy of the default zone.

Figure 4-1 describes the steps for configuring zones and zone sets. See Appendix B, "Configuration Files," for details on saving configuration files.

Figure 4-1 Zones and Zone Sets



This chapter includes the following sections:

Configuring Zones

Zones are configured within VSANs. The Logical tab displays the VSANs configured in the currently discovered fabric. Note that zone information must always be identical for all the switches in the network fabric.

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 Zone Sets

A zone set consists of one or more zones. A zone can be a member of more than one zone set and consists of multiple zone members. Members in a zone can access each other; members in different zones cannot access each other. Devices can belong to more than one zone.

A zone set can be activated or deactivated as a single entity across all switches in the fabric. Only one zone set can be activated at any time. If zoning is not activated, all devices are members of the default zone. If zoning is activated, any device that is not in an active zone (a zone that is part of an active zone set) is a member of the default zone.

Zoning can be administered from any switch in the fabric. When you activate a zone (from any switch), all switches in the fabric receive the active zone set. Additionally, full zone sets are distributed to all switches in the fabric, if this feature is enabled in the source switch.

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.

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.
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.

After creating a zone set and activating it make sure you save the configuration file. See Appendix B, "Configuration Files," for details about copying and saving configuration files.

Activating a Zone Set

Changes to a zone set do not take effect to a full zone set until you activate it.

To activate a zone set, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# zoneset activate name Zoneset1 vsan 3`	Activates the specified zone set.
	`switch(config)# no zoneset activate name Zoneset1 vsan 3`	Deactivates the specified zone set

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

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 4-1 lists the **show** commands and the information they display.

Table 4-1 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 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.

What's Next?

After completing the procedures in this book, your Cisco MDS 9000 Family switch can provide the basic, minimal Fibre Channel services necessary to enable hosts to access their storage. Beyond this, you will want to set up security, management, and monitoring for your network. These tasks are beyond the scope of this document. However, the following tasks should be performed to leverage the full abilities of the MDS switch.

Security

- Configure DNS servers.
- Enable SSH and disable Telnet.
- Create unique usernames for each user.
- Create and assign roles for users that do not require network administrative privileges.
- Configure TACACS+/Radius for centralized user management.

Management

- Configure a syslog server.
- Configure time/date/timezone and additionally NTP.
- Configure schedules and jobs to regularly back up the configuration of the MDS switch.
- Configure device aliases.

Monitoring

- Configure Call Home.

CHAPTER A

Configuring Static Domain IDs and Persistent FC IDs

The domain manager on the principal switch in a VSAN assigns a domain ID to a switch that is joining the fabric. When a switch boots up or joins a new fabric it can request a specific domain ID or take any available domain ID.

After obtaining the domain ID from the principal switch in the VSAN, the local switch will assign Fibre Channel Identifiers (FC IDs) to each end device as they are logged in to the fabric using a process known as FLOGI (Fabric Login).

Warning **HP-UX and AIX are two operating systems that utilize the FC ID in the device path to the storage. For a switch to always assign the same FC ID to a device, persistent FC IDs and static domain ID must be configured for the VSAN.**

By default, the switch assigns the same FC ID to a device. However, if the switch is rebooted, this database of pwwn/FC ID mapping is not maintained. Enabling persistent FC IDs makes this database persistent across reboots.

In the following procedure, the existing VSAN (3000) has a switch address of xx.xx.xx.xx and a domain ID of 239. This procedure configures a static Domain_ID for a VSAN and enables persistent FC_ID for the same VSAN.

Step 1 Display the current domain_ID for VSAN 3000 using the command show domain-list.

```
switch# show fcdomain domain-list vsan 3000
Number of domains: 2
Domain ID WWN
--------- -----------------------
0xef(239) 2b:b8:00:05:30:00:68:5f [Local] [Principal]
```

Step 2 Configure the static domain_ID with the domain static command.

```
switch# conf t

Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# fcdomain domain 239 static vsan 3000
```

Step 3 Enable persistent FC_ID with fcid persistent.

```
switch(config)# fcdomain fcid persistent vsan 3000
switch(config)# end
```

Step 4 Save the configuration.

```
switch# copy running-config startup-config
[########################################] 100%
```

Note If the domain ID of VSAN 200 is different than what is currently running (22 in this case) then the VSAN has to be restarted before configuration changes to the Domain_ID and FC_ID persistence take effect. Changing Domain_IDs and hence FC_IDs for a device is disruptive because an end device has to relogin to the fabric (FLOGI) to obtain a new FCID.

Caution Changing Domain_IDs and therefore FC_IDs for a device is disruptive, as an end device has to relogin to the fabric (FLOGI) to obtain a new FCID. However, making a Domain_ID static without changing its value is not disruptive.

CHAPTER B

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.

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 store configuration files on a bootflash: device on the supervisor module and 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.

Saving the Configuration File

Saving the configuration file refers to copying a running configuration file to a startup configuration file.

As of Cisco MDS SAN-OS Release 2.1(1a) or higher, you can copy the running configuration to the startup configuration across the entire fabric by using the Copy Configuration option. This triggers every switch in the fabric to copy its running configuration to its startup configuration.

Note If any switch fails during this fabric-wide copy, that switch and the switch that you used to initiate this command will keep the existing startup configuration. This does not affect the other switches in the fabric.

To copy the configuration file, follow these steps:

After you have created a running configuration in system memory, you can save it to the startup configuration in NVRAM.

Use the following **copy** command to save the configuration to NVRAM:

```
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.

To cancel the copy operation initiated by another switch, use the following command:

```
switch# system startup-config abort
```

To cancel the operation locally and throughout the fabric, enter **Ctrl-c** on the console or Telnet session of the initiator switch.

INDEX

A

B

C

D

E

F

T

V

Z