



## **Cisco MDS 9000 Fabric Manager Quick Configuration Guide**

May 2006

### **Corporate Headquarters**

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

Text Part Number: OL-7765-02



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

*Cisco MDS 9000 Fabric Manager Quick Configuration Guide*

Copyright © 2004-2006, Cisco Systems, Inc.

All rights reserved.



<b>Preface</b>	<b>vii</b>
Audience	<b>vii</b>
Organization	<b>vii</b>
Document Conventions	<b>viii</b>
Related Documentation	<b>ix</b>
Release Notes	<b>ix</b>
Compatibility Information	<b>ix</b>
Regulatory Compliance and Safety Information	<b>ix</b>
Hardware Installation	<b>ix</b>
Cisco Fabric Manager	<b>x</b>
Command-Line Interface	<b>x</b>
Troubleshooting and Reference	<b>x</b>
Installation and Configuration Note	<b>x</b>
Obtaining Documentation	<b>x</b>
Cisco.com	<b>xi</b>
Product Documentation DVD	<b>xi</b>
Ordering Documentation	<b>xi</b>
Documentation Feedback	<b>xi</b>
Cisco Product Security Overview	<b>xii</b>
Reporting Security Problems in Cisco Products	<b>xii</b>
Obtaining Technical Assistance	<b>xiii</b>
Cisco Technical Support & Documentation Website	<b>xiii</b>
Submitting a Service Request	<b>xiii</b>
Definitions of Service Request Severity	<b>xiv</b>
Obtaining Additional Publications and Information	<b>xiv</b>
<b>CHAPTER 1</b>	<b>Overview 1-1</b>
	Overview of Fabric Manager <b>1-2</b>
	Overview of VSANs, Interfaces, Zones, and Zone Sets <b>1-2</b>
<b>CHAPTER 2</b>	<b>Initial Switch Configuration 2-1</b>
	Preparing for Network Connections <b>2-1</b>
	Configuration Prerequisites <b>2-1</b>
	Connecting the Console Port <b>2-2</b>

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

- Connecting the Console Port to a PC 2-4
- Connecting the 10/100 Ethernet Management Port 2-4
- Connecting to the MGMT 10/100/1000 Ethernet Port 2-5
- Using the Switch Setup Utility 2-5
- Verifying the Module Status 2-10

---

**CHAPTER 3**

**Installing and Launching Fabric Manager 3-1**

- Installing Cisco Fabric Manager 3-1
- Launching Cisco Fabric Manager 3-3

---

**CHAPTER 4**

**Configuring VSANs and Interfaces 4-1**

- Creating VSANs 4-2
  - Default VSAN 4-2
- Configuring Interfaces 4-4
  - Adding Interfaces to VSANs 4-4

---

**CHAPTER 5**

**Configuring Zones and Zone Sets 5-1**

- Configuring Zones 5-2
- Creating Zone Sets 5-4
- What's Next? 5-6

---

**APPENDIX A**

**Fabric Manager Client 1**

- Fabric Manager Client Quick Tour 2
  - Multiple Fabrics in the Fabric Pane 3
  - Contents Panes 4
  - Main Menu 6
  - Toolbar 6
  - Information Pane 8
  - Logical Domains Pane 9
  - Physical Attributes Pane 9
  - Status Bar 10
  - Context Menus 10
  - Filtering 10
  - Detachable Tables 11
- Fabric Manager Wizards 11

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

---

**APPENDIX B**      **Configuring Static Domain IDs and Persistent  
FC IDs**      B-1

---

**APPENDIX C**      **Configuration Files**      C-1  
                    Saving the Configuration File      C-1

---

**INDEX**

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***



## Preface

---

This preface describes the audience, organization, and conventions of the *Cisco MDS 9000 Family Fabric Manager 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	<a href="#">Overview</a>	Describes the flow of the <i>Cisco MDS 9000 Fabric Manager Quick Configuration Guide</i> and gives a brief overview of Fabric Manager components and their capabilities.
Chapter 2	<a href="#">Initial Switch Configuration</a>	Explains how to install the hardware and set up the switch.
Chapter 3	<a href="#">Installing and Launching Fabric Manager</a>	Provides detailed steps for installing Cisco Fabric Manager.
Chapter 4	<a href="#">Configuring VSANs and Interfaces</a>	Describes how to configure VSANs and interfaces.
Chapter 5	<a href="#">Configuring Zones and Zone Sets</a>	Provides basic configuration information for zones and zone sets.
Appendix A	<a href="#">Fabric Manager Client</a>	Provides an in-depth description of the GUI and the capabilities of the Fabric Manager Client.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

Chapter	Title	Description
Appendix B	<a href="#">Configuring Static Domain IDs and Persistent FC IDs</a>	Provides the procedure for configuring static domain IDs and persistent FC IDs.
Appendix C	<a href="#">Configuration Files</a>	Describes how to save and copy configuration files that contain the parameters required to configure a switch.

## Document Conventions

Command descriptions use these conventions:

<b>boldface font</b>	Commands and keywords are in boldface.
<i>italic font</i>	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:

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

This document uses the following conventions:



### Note

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



### Caution

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



***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

## Related Documentation

The documentation set for the Cisco MDS 9000 Family includes the following documents. To find a document online, use the Cisco MDS SAN-OS Documentation Locator at:

[http://www.cisco.com/en/US/products/ps5989/products\\_documentation\\_roadmap09186a00804500c1.html](http://www.cisco.com/en/US/products/ps5989/products_documentation_roadmap09186a00804500c1.html).

For information on IBM TotalStorage SAN Volume Controller Storage Software for the Cisco MDS 9000 Family, refer to the IBM TotalStorage Support website:

<http://www.ibm.com/storage/support/2062-2300/>

## Release Notes

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

## Compatibility Information

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

## Regulatory Compliance and Safety Information

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

## Hardware Installation

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

**[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

## Cisco Fabric Manager

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

## Command-Line Interface

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

## Troubleshooting and Reference

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

## Installation and Configuration Note

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

## Obtaining Documentation

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

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

## Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](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 Cisco Marketplace at this URL:

<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/>

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

## Documentation Feedback

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

## ***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

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

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

We appreciate your comments.

## **Cisco Product Security Overview**

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

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](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](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](mailto: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](mailto: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

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

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

---

## Obtaining Technical Assistance

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

## Cisco Technical Support & Documentation Website

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

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

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

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



### Note

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

---

## Submitting a Service Request

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

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

## Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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>

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

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

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

or view the digital edition at this URL:

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

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

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

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

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

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

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

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

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

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***





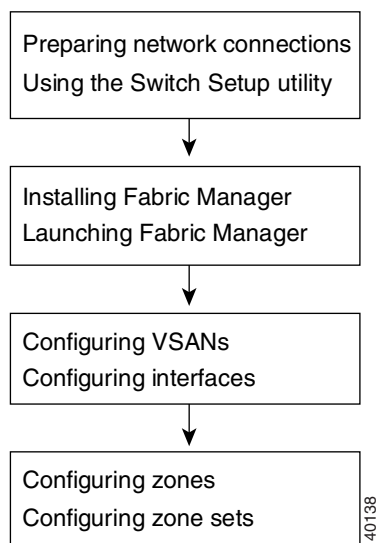
## Overview

---

The primary objective of the *Cisco MDS 9000 Family Fabric Manager Quick Configuration Guide* is to get you started with configuring your Cisco MDS 9000 Family switch using the Cisco Fabric Manager graphical user interface (GUI).

[Figure 1-1](#) outlines the organization of the guide and it also serves as a flowchart describing the major steps used in the installation and configuration of the fabric.

**Figure 1-1**      **Installation and Configuration Flowchart**



140138

## Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Start the process by setting up the hardware and performing the initial switch setup using the CLI. Then install Cisco Fabric Manager, and use it to configure VSANs, interfaces, zones, and zone sets, which are the minimum requirements for creating a fabric.

**Note**

After setting up the switch, if you choose to perform further configuration tasks using the CLI, refer to the *Cisco MDS 9000 Family Configuration Guide*.

This chapter includes the following sections:

- [Overview of Fabric Manager, page 1-2](#)
- [Overview of VSANs, Interfaces, Zones, and Zone Sets, page 1-2](#)

## Overview of Fabric Manager

Fabric Manager provides a graphical user interface (GUI) that displays real-time views of your network fabrics and lets you manage the configuration of Cisco MDS 9000 Family devices and third-party switches. It provides an alternative to the CLI for most switch configuration commands.

Fabric Manager includes management applications, such as Fabric Manager Client, Fabric Manager Server, Device Manager, Performance Manager, and Fabric Manager Web Services. For further details regarding the various management components of Fabric Manager, refer to the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.

Fabric Manager Server must be started before running Fabric Manager. On a Windows PC, Fabric Manager Server is installed as a service. This service can then be administered using the Windows Services applet in the control panel. Fabric Manager Server discovers the physical and logical fabric, and listens for SNMP traps, syslog messages, and Performance Manager threshold events.

See [Chapter 3, “Installing and Launching Fabric Manager,”](#) for instructions on installing Fabric Manager. [Appendix A, “Fabric Manager Client,”](#) has further details on using the Fabric Manager Client.

## Overview of VSANs, Interfaces, Zones, and Zone Sets

VSANs, interfaces, zones, and zone sets comprise the minimum configuration required for a Cisco MDS 9000 Family switch to be up and running.

Virtual SANs can scale SANs beyond current limitations in a resilient, secure, cost-effective, and manageable fashion. Using VSANs, you can build larger consolidated fabrics and still maintain the required security and isolation between applications beyond what is currently offered through zoning. A VSAN can create separate virtual fabrics on top of the same redundant physical infrastructure.

Interfaces enable a switch to relay frames from one data link to another. You must define the characteristics of the interfaces through which the frames are sent and received. The configured interfaces can be Fibre Channel interfaces, the management interface (mgmt0), or VSAN interfaces.

The zoning service within a Fibre Channel fabric can provide security between devices sharing the same fabric. The primary goal is to prevent certain devices from accessing other devices within the fabric. With many different types of servers and storage devices on the network, the need for security is critical. For example, if a host was to gain access to a disk being used by another host, potentially with a different operating system, the data on this disk could get corrupted. To avoid any compromise of critical data within the SAN, zoning allows you to overlay a security map dictating which devices, namely hosts, can communicate with which targets, reducing the risk of data loss.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

VSANs and zoning within the MDS 9000 Family of products aid the SAN designer in building secure and manageable networking environments while optimizing the use and cost of switching hardware. VSANs are used to divide a redundant physical SAN infrastructure into separate virtual SAN islands, each with its own set of Fibre Channel fabric services. By each VSAN supporting an independent set of Fibre Channel services, a VSAN-enabled infrastructure can house numerous applications without concern for fabric resource or event conflicts between these virtual environments. Once the physical fabric has been divided, zoning is then used to implement a security layout within each VSAN that is tuned to the needs of each application within each VSAN.

VSANs are first created as isolated fabrics within a common physical topology. Once VSANs have been created, individual unique zone sets can then be applied as necessary within each VSAN.

See [Chapter 4, “Configuring VSANs and Interfaces,”](#) and [Chapter 5, “Configuring Zones and Zone Sets,”](#) for details on configuring VSANs, interfaces, zones, and zone sets.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***



## Initial Switch Configuration

---

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

This chapter includes the following sections:

- [Preparing for Network Connections, page 2-1](#)
- [Connecting the Console Port, page 2-2](#)
- [Connecting the 10/100 Ethernet Management Port, page 2-4](#)
- [Using the Switch Setup Utility, page 2-5](#)
- [Verifying the Module Status, page 2-10](#)

## Preparing for Network Connections

When preparing your site for network connections to the Cisco MDS 9000 switch, consider the following:

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

Before installing a 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 name 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.

*Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)*

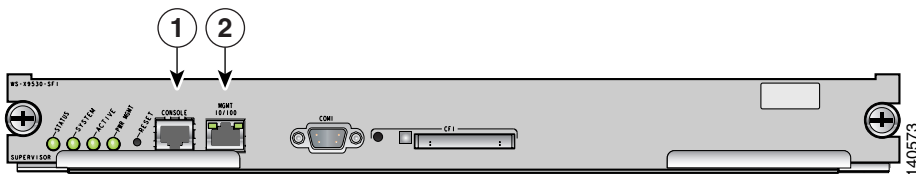
## Connecting the Console Port

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 Flash memory software images to attached devices.

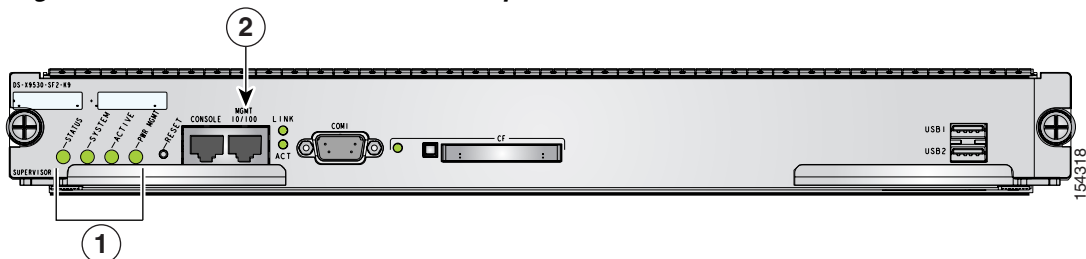
Figure 2-1, Figure 2-3, Figure 2-4 and Figure 2-4 show the console port and management port located on a Cisco MDS 9500 series supervisor-1 module, Cisco MDS 9500 series supervisor-2 module, a Cisco MDS 9200 series supervisor module, and Cisco MDS 9100 series supervisor module.

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



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

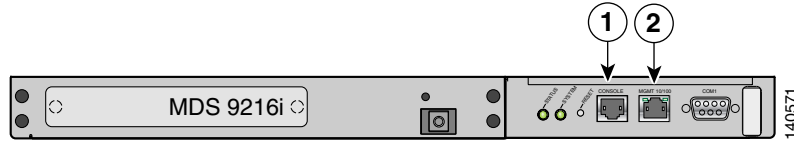
**Figure 2-2 Cisco MDS 9500 Series Supervisor-2 Module**



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

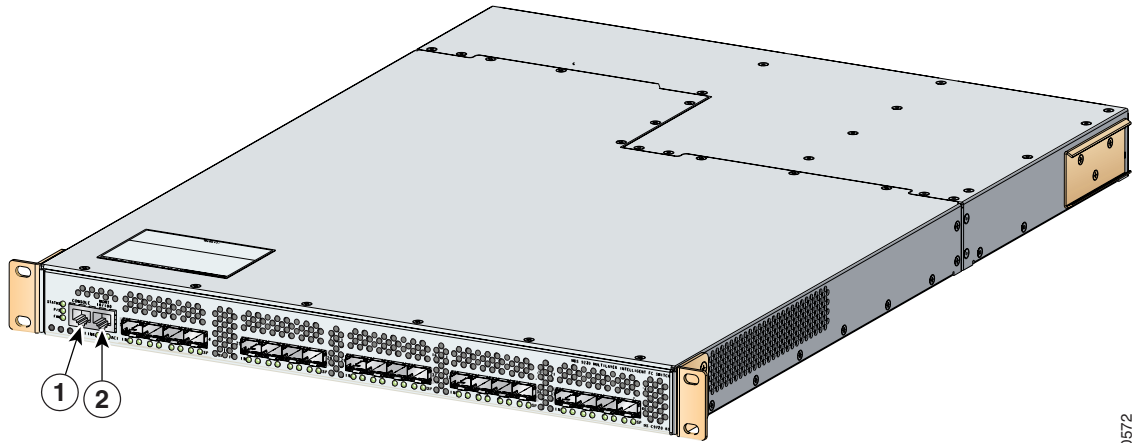
**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

**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)

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

## Connecting the Console Port to a PC

You can connect the console port to a PC serial port for local administrative access to the Cisco MDS 9000 Family 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 Cisco MDS 9000 Family 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
- 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 module. 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 2-3](#), 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 a MDS 9500 Series switch. Even though there are two Ethernet connections, only one management IP address is required for a switch with dual supervisor modules.



### Tip

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



***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

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 module reboots and the standby supervisor module becomes the active supervisor module.

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 through the CLI. 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 management 10/100 Ethernet 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 parameters 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)** prompt, contact your storage vendor support organization for technical assistance.

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

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

```
Firmware initialized.
```

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

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

```

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-sflek9-kickstart-mz.2.1.1a.bin bootflash:/m9500-s
flek9-mz.2.1.1a.bin...
Booting kickstart image:
bootflash:/m9500-sflek9-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-sflek9-mz.2.1.1a.bin
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
INIT: Entering runlevel: 3

```

**Step 4** Make sure you enter the password you wish to assign for the admin username.

```

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

```



**Tip** If you create a password that is short and easy to decipher, then your password 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 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 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.

## Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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**

**Step 12** Enter the default gateway IP address.

IP address of the default-gateway: *default\_gateway*

**Step 13** 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 14** Enter **yes** (yes is the default) to enable Telnet service.

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

**Step 15** Enter **no** (no is the default) to not enable the SSH service.

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

**Step 16** Enter **no** (no is the default) to not configure the NTP server.

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

**Step 17** 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**

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

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

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

**Step 19** Enter **deny** (deny is the default) to configure a default zone policy configuration.

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

This step denies traffic flow for all members of the default zone.

**Step 20** Enter **yes** (no is the default) to enable a full zone set distribution (refer to the *Cisco MDS 9000 Family 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.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

**Step 21** 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 22** Enter **yes** (yes is the 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, your changes will not be updated the next time that the switch is rebooted. Type yes to save the new configuration to ensure that the kickstart and system images are also automatically configured.

---

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

## Verifying the Module Status

Before you proceed with further configuration of 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. 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, contact your storage vendor support organization for further assistance.



## Installing and Launching Fabric Manager

---

Before installing Fabric Manager, make sure that the hardware setup and initial configuration using the CLI is completed. See [Chapter 2, “Initial Switch Configuration,”](#) for details.

The Cisco Fabric Manager software executable files reside on every supervisor module of each Cisco MDS 9000 Family switch in your network. The supervisor module provides an HTTP server that responds to browser requests and distributes the software to Windows or UNIX network management stations.

This chapter includes the following sections:

- [Installing Cisco Fabric Manager, page 3-1](#)
- [Launching Cisco Fabric Manager, page 3-3](#)

### Installing Cisco Fabric Manager

The Cisco Fabric Manager management software is compatible with the following software:

- Operating Systems
  - Windows 2000, Windows Server 2003, Windows XP
  - Solaris 2.8
  - Redhat Linux 7.2
- Java
  - Sun JRE and JDK 1.4.0, 1.4.1, 1.4.2, and 1.5.0



---

**Note** Sun JRE and JDK 1.5.0 is supported only for Cisco SAN-OS Release 2.1(2) or later.

IPv6 needs Java 1.5.0 to work with Fabric Manager.

---

- Java Web Start 1.2 and 1.0.1
- Browsers
  - Internet Explorer 5.5 or later
  - Netscape 6 or later
  - Mozilla 1.0 or later

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

To install Fabric Manager for the first time, or to update or reinstall the software, follow these steps:

**Step 1** Enter the mgmt0 IP address or host name of the supervisor module in the Address or Location field of your browser.

Click the **Cisco Fabric Manager** link on the Cisco Fabric Manager home page shown in [Figure 3-1](#).

**Figure 3-1 Cisco Fabric Manager Home Page**

**Installation 2.1(1a):**

The Cisco Fabric and Device Manager are separate applications. You can install or update them by clicking on the links below. Please remember to close older running applications before doing this. Once you install a 2.0 or newer version of the Fabric and Device Manager downgrade is not supported through the installer. Please uninstall the 2.0 or newer instance and install from scratch the older version.

[Cisco Fabric Manager](#)      [Cisco Device Manager](#)      [Cisco Fabric Manager Web Services and Performance Manager](#)      [Release Notes](#)

**Product Overview:**

<ul style="list-style-type: none"> <li>• Fabric discovery and topology mapping</li> <li>• Multiple switch configuration</li> <li>• VSAN and Zone management</li> <li>• Fabric Checker, Switch Health and Zone Merge Analysis</li> <li>• End-to-End Connectivity and Traceroute Analysis</li> </ul>	<p><b>Fabric Management</b></p>  <p>Fabric View</p>	<ul style="list-style-type: none"> <li>• Device level status at a glance</li> <li>• Intuitive single device configuration</li> <li>• Summary view of key port statistics</li> <li>• Drill-down for detailed information</li> <li>• Charting and printing</li> </ul>	<p><b>Device Management</b></p>  <p>Device &amp; Summary Views</p>
--	--	---	---

140042



**Note** Installation options include upgrading, downgrading, and uninstalling Fabric Manager. For details on these procedures, refer to the *Cisco MDS 9000 Family Fabric Manager Configuration Guide* or the *Cisco MDS 9000 Family CLI Configuration Guide*.

**Step 2** Click the link to the Sun Java Virtual Machine software (if required) and install the software.

When you connect to the server for the first time, it checks to see if you have the correct Sun Java Virtual Machine version installed on your workstation. If not, a link is provided to the appropriate Sun Microsystems web page so you can install it.

The supervisor module HTTP server displays the installation window.

**Step 3** Select an installation folder for Fabric Manager on your workstation.. The default location is C:\Program Files\Cisco Systems\MDS 9000 for Windows. On a Solaris or Linux machine, the installation path name is /usr/local/cisco\_mds9000 or \$HOME/cisco\_mds9000, depending on the permissions of the user performing the installation.



**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**



---

**Note** The Fabric Manager Server and the Fabric Manager Client must be able to communicate with each other at all times. They can be installed on different workstations or the same workstation.

---

- Step 4** Check the **Use Global Device Aliases in place of FC Aliases** check box if you want to use global device aliases or replace existing per VSAN FC aliases with global device aliases.
- Step 5** Check the **Don't install and run FM Server** check box if you are installing just the Fabric Manager Client on a remote workstation.
- 

During installation, a Cisco MDS 9000 program group is created under **Start > Programs** on Windows. This program group contains shortcuts to batch files in the install directory. Three services are also started: Fabric Manager Server, Fabric Manager Database, and Fabric Manager Web Server. The Performance Manager server is installed but the service is not started upon installation, because more setup must be completed first.

On a Solaris or Linux machine, shell scripts are created in the install directory. The shell scripts that run the programs equivalent to the Windows services are: FMServer.sh, FMPersist.sh, PMCollector.sh, and FMWebClient.sh. All server-side data and Performance Manager data are stored under the install directory.

Fabric Manager Client cannot run without the server component, Fabric Manager Server. The server component is downloaded and installed when you download and install Fabric Manager. On a Windows machine, Fabric Manager Server is a service. This service can be administered using the Services applet in the Microsoft Windows control panel. The default for Fabric Manager Server service is that the server is automatically started when the machine is rebooted. You can change this behavior by modifying the properties in Services.

When you install Fabric Manager, the basic unlicensed version of Fabric Manager Server is installed. To get licensed features, such as Performance Manager, remote client support, and continuously monitored fabrics, buy and install the Fabric Manager Server package.

Trial versions of licensed features are also available. To enable the trial version of a feature, run the feature as if you had purchased the license. You see a dialog box explaining that this is a trial version of the feature and how long the feature will be enabled.

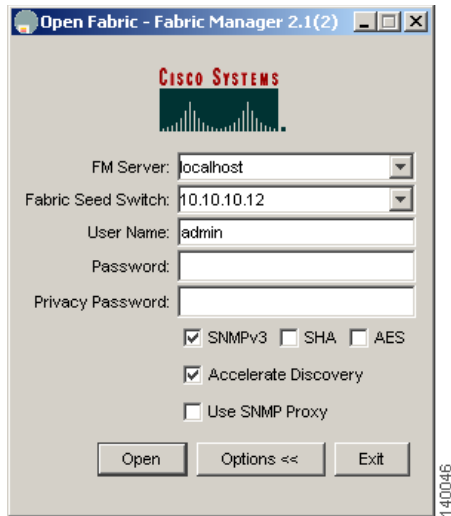
## Launching Cisco Fabric Manager

To launch Fabric Manager, follow these steps:

- 
- Step 1** Double-click the **Fabric Manager** icon on your desktop or select the option from the Windows Start menu.
- When you start Fabric Manager, the Fabric Manager Server loads. You see a login screen for Fabric Manager. A command-line window is briefly displayed.
- Step 2** Click **Options** to expand the login screen, if necessary, to select the seed switch and SNMP configuration. (See [Figure 3-2](#).)

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

**Figure 3-2 Fabric Manager Login Screen**



- Step 3** Enter the IP address or host name in the Fabric Seed Switch field, or select an IP address from the list of previously accessed devices in the drop-down menu.
- Step 4** Enter a user name and password in the appropriate fields.
- Step 5** Leave the **SNMPv3** check box checked to select SNMP version 3.
- Step 6** Click **Open**. You see Cisco Fabric Manager.
-



## Configuring VSANs and Interfaces

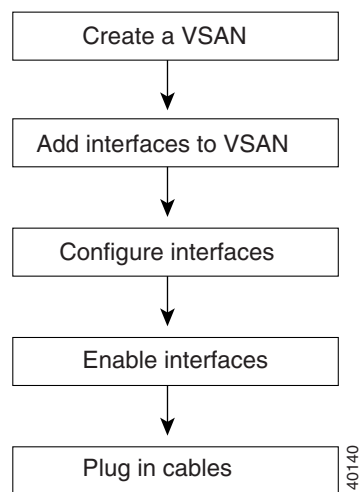
Before configuring VSANs and interfaces, make sure that you have launched and logged into Fabric Manager from your workstation. See [Chapter 3, “Installing and Launching Fabric Manager,”](#) for details.

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 4-1](#) describes the steps involved in configuring VSANs and interfaces.

**Figure 4-1** VSANs and Interfaces



This chapter includes the following sections:

- [Creating VSANs, page 4-2](#)
- [Configuring Interfaces, page 4-4](#)

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

## 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.



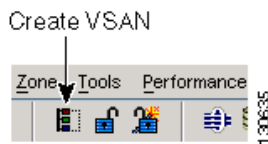
#### Note

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

To add and configure a VSAN, follow these steps.

**Step 1** Click the **Create VSAN** icon. (See [Figure 4-2](#).)

**Figure 4-2** Create VSAN Icon



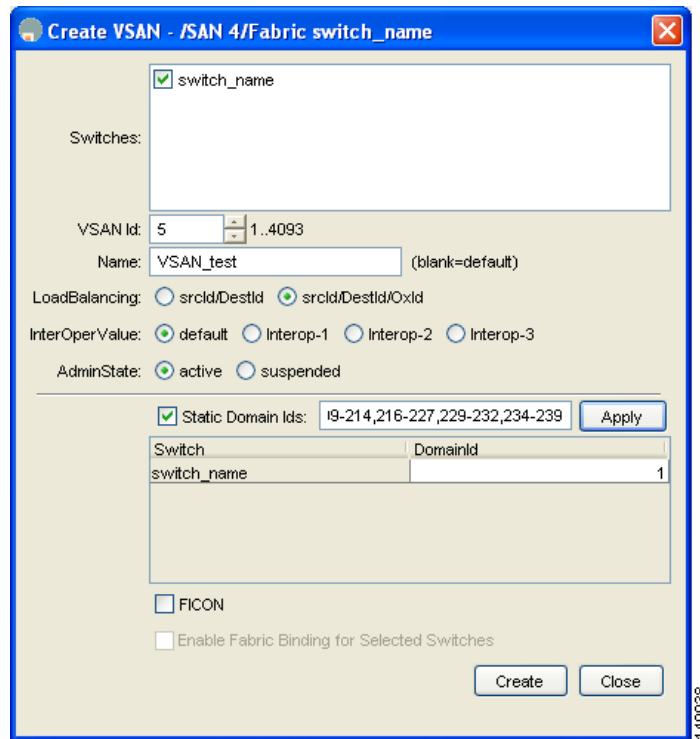
#### Note

For details about the icons and buttons used in Fabric Manager, see [Appendix A, “Fabric Manager Client.”](#)

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

You see the Create VSAN dialog box. (See [Figure 4-3](#).)

**Figure 4-3** Create VSAN



**Step 2** Complete the fields in the Create VSAN dialog box.

- Select the switches that you wish to assign to the VSAN. For example, in [Figure 4-3](#), switch\_name is the switch selected to be assigned to a VSAN.
- Select a VSAN ID for the VSAN.
- Assign a name to the VSAN. For example, in [Figure 4-3](#), VSAN\_test is the assigned VSAN name.
- Select the type of load balancing used on this VSAN. We recommend that, for this setup, you select the **srcdst Ox-Id** option, which is the default option.
  - **srcdst**—Use source and destination ID for path selection.
  - **srcdst Ox-Id**—Use source, destination, and exchange IDs.
- Select the interoperability value configured for the local switch on this VSAN. We recommend that, for this setup, you select the **default** option.
- Select the Admin State for the VSAN. We recommend that, for this setup, you select the **active** option, which is selected by default.
- Check the **Static Domain IDs** check box to assign a persistent domain ID to the VSAN. For example, in [Figure 4-3](#), the domain ID for the switch is 1; this ID is the domain ID assigned to the switch on VSAN\_test.

See [Appendix B, “Configuring Static Domain IDs and Persistent FC IDs,”](#) for details.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

**Note**

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.

- Check the **FICON** check box if the VSAN is FICON-enabled.

**Step 3** Click **Create** to add the VSAN.

---

## Configuring Interfaces

The main function of a switch 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.

The following procedures are used to move the ports on a switch of a previously created VSAN, configure the interfaces, and add them to the VSAN.

## Adding Interfaces to VSANs

To configure Fibre Channel interfaces, follow these steps:

- 
- Step 1** In the Physical Attributes pane, expand **Switches > Interfaces** then choose **FC Physical**.  
You see the interface configuration in the Information pane.
- Step 2** From the **General** tab, set the values for Mode Admin, Port VSAN membership, and Status Admin.
- Step 3** Optionally, set other configuration parameters using the other tabs.
- Step 4** Click **Apply Changes**.
- Step 5** Click **Yes**.
-

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

## Enabling or Disabling Interfaces



### Note

You are not required to enable interfaces if the default state of the ports in the setup script is set to **noshut**. See the “Using the Switch Setup Utility” section on page 2-5.

To enable an interface using Fabric Manager, follow these steps:

- Step 1** In the Physical Attributes pane, expand **Switches > Interfaces** and then select **FC Physical**.
- Step 2** From the **General** tab, set the value for **Status > Admin** to up (for enable) or down (for disable).
- Step 3** Optionally, set other configuration parameters using the other tabs.
- Step 4** Click **Apply Changes**.

After enabling the interfaces, be sure to plug in the cables. If the cables are not plugged in, the hosts cannot communicate with the storage device. In the example below, the message **linkFailure** indicates that a cable may not be plugged in (see [Figure 4-4](#)).

**Figure 4-4 Failed Switches**

Switch	Interface	Mode Admin	Mode Oper	Dynamic VSAN	VSAN	Description	Speed Admin	Speed Oper	Rate Mode	Status Service	Status Admin	Status Oper	FailureCause	Was Enabled	LastChange
v184	fc2/f	FX	auto	1	n/a		auto	n/a	shared	in	down	down	adminDown	false	n/a
v185-test	fc1/f	E	auto	55	n/a		auto	n/a	shared	in	up	down	linkFailure	false	n/a
c-186	fc1/f	E	auto	1	n/a		2Gb	n/a	dedicated	in	up	down	initializing	true	n/a
v184	fc2/2	FX	auto	1	n/a		auto	n/a	shared	in	down	down	isNotPresent	false	n/a

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***





## Configuring Zones and Zone Sets

Before setting up zones and zone sets make sure you have configured VSANs and interfaces. See [Chapter 4, “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. You can configure up to 8K zones in a VSAN.

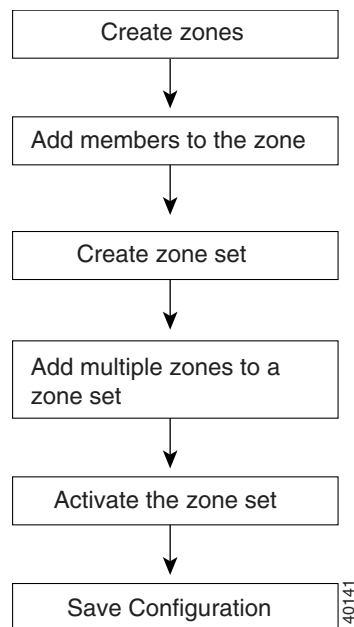


**Note**

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

[Figure 5-1](#) describes the steps for configuring zones and zone sets. See [Appendix C, “Configuration Files,”](#) for details on saving configuration files.

**Figure 5-1** Zones and Zone Sets



140141

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

This chapter includes the following sections:

- [Configuring Zones, page 5-2](#)
- [Creating Zone Sets, page 5-4](#)
- [What's Next?, page 5-6](#)

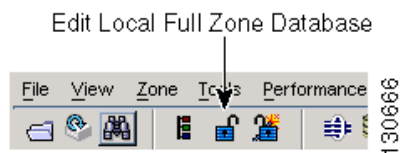
## Configuring Zones

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. You can configure up to 8K zones in a VSAN.

To configure pWWN-based zones using the Zone configuration tool, follow these steps:

- 
- Step 1** Click the **Edit Local Full Zone Database** icon as shown in [Figure 5-2](#).

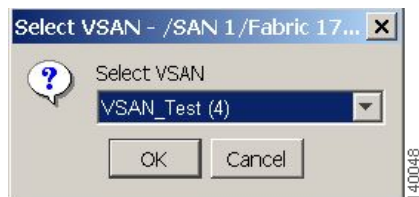
**Figure 5-2** *Edit Local Full Zone Database*



**Note** For details about the icons and buttons used in Fabric Manager, see [Appendix A, “Fabric Manager Client.”](#)

You see the Select VSAN dialog box. (See [Figure 5-3](#).)

**Figure 5-3** *Select VSAN*

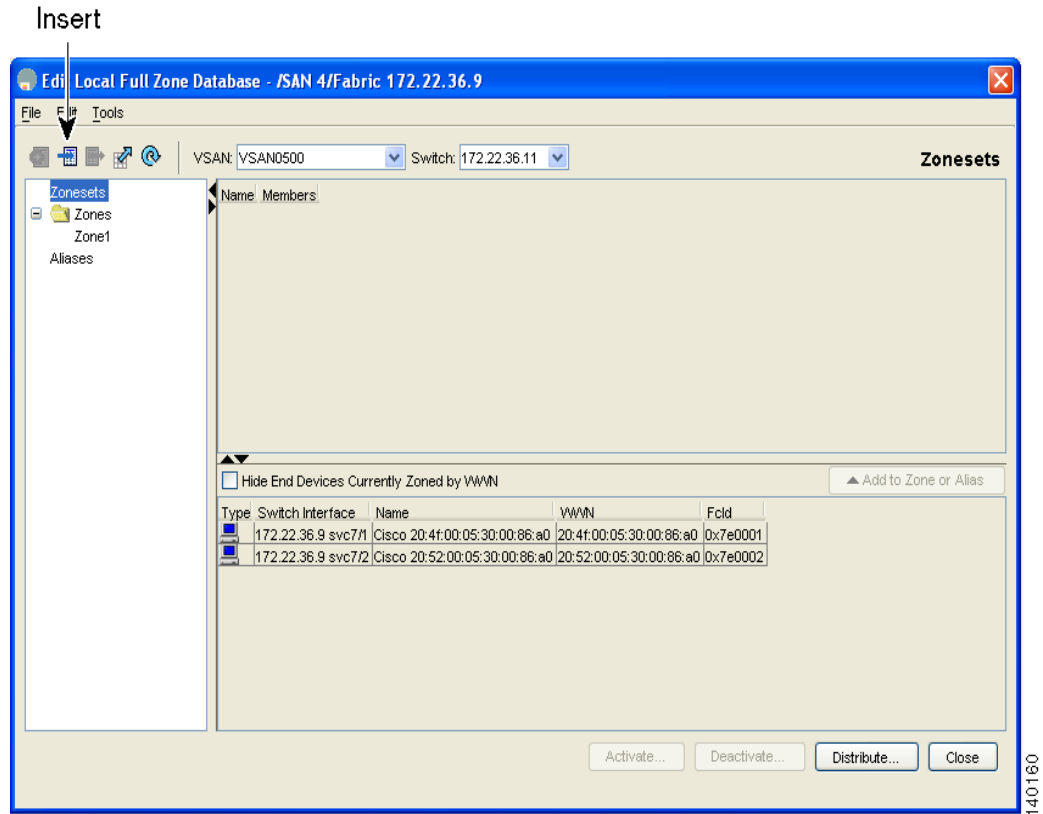


- Step 2** Select the VSAN where you want to configure zones or zone sets, or add members to a zone. (See [Figure 5-3](#).) Click **OK**.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

- Step 3** Click **Zones** then click **Insert** icon to make a new zone. We recommend that you use meaningful names for a zone. For example, you could use email05\_HBA2\_EMCA\_FA11a. (See [Figure 5-4](#).)

**Figure 5-4** Edit Local Full Zone Database



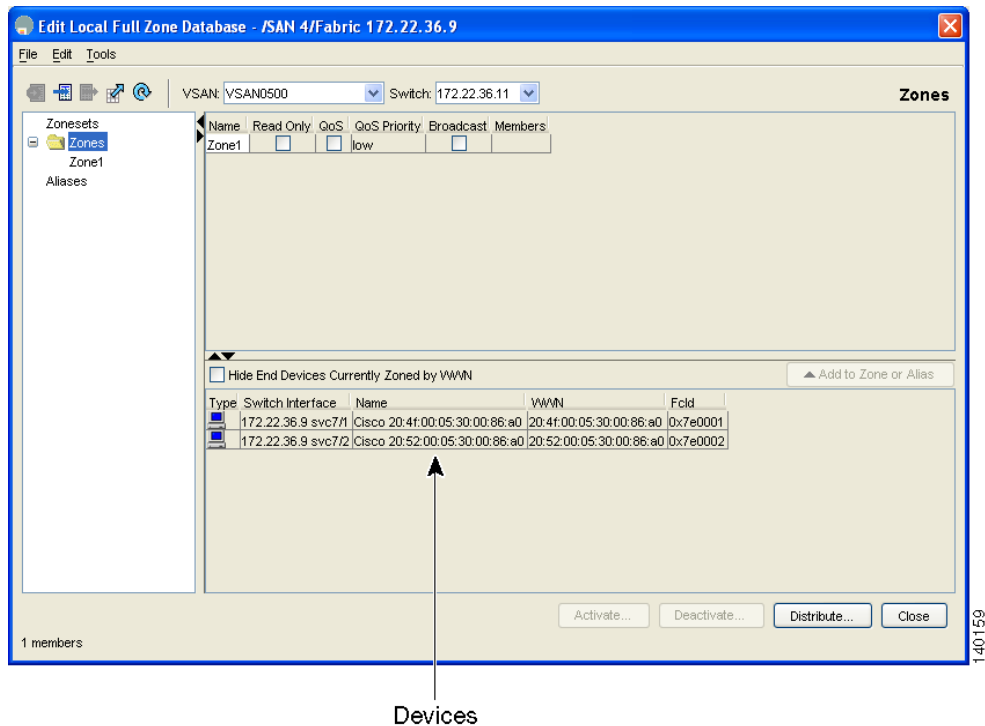
**Tip**

Instead of configuring zones using pWWNs, you can use device aliases as zone members. Device aliases are a distributed, fabric-wide database consisting of unique mappings of plain text names for pWWN mappings. For details on configuring device aliases, refer to the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

- Step 4** Drag and drop devices into the zone. Once the zone is populated with the devices, the name of the zone is displayed in italics. Click **Add to zone or alias** to move devices up or down by alias or by zone. (See [Figure 5-5](#).)

**Figure 5-5 Adding Devices to a Zone Set**



## 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**

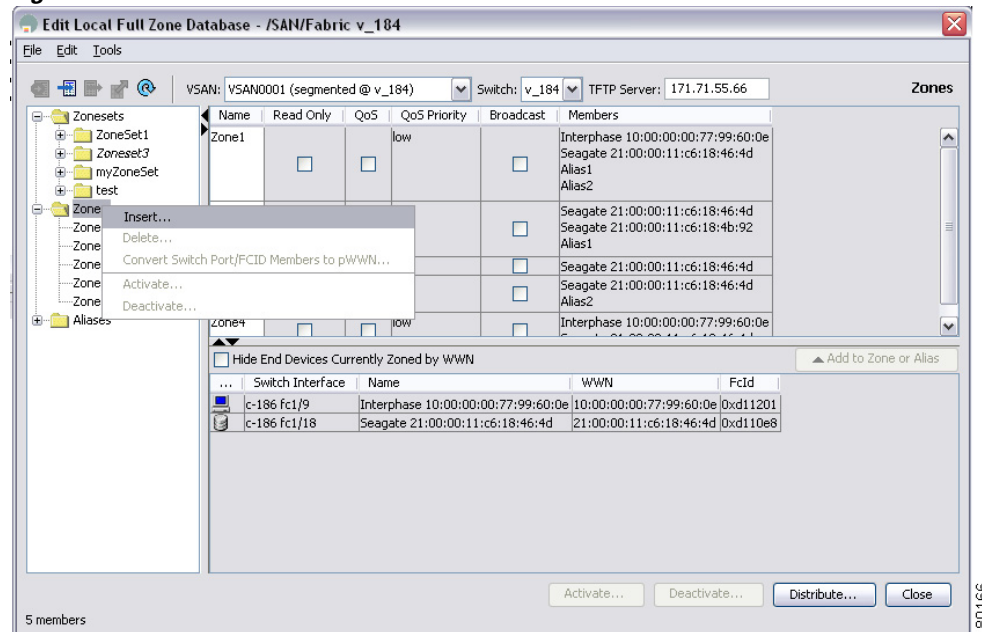
Zone sets are configured with the names of the member zones. If the zone set is in a configured VSAN, you must also specify the VSAN.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

To create zone sets, follow these steps:

- Step 1** Click **Zone > Edit Local Full Zone Database** from the Zone menu or right-click a VSAN folder in the **Logical** tab and choose **Edit Local Full Zone Database** from the pop-up menu.
- Step 2** Select a VSAN and click **OK**.  
You see the VSAN you selected in the Edit Local Full Zone Database window.
- Step 3** Right-click the **Zonesets** folder in the Edit Local Full Zone Database dialog box for that VSAN and select **Insert** to add a zone set (see [Figure 5-6](#)).

**Figure 5-6** Insert a new zone set



- Step 4** Assign a name to the new zone set.
- Step 5** In the left pane, drag and drop zones into the zone set.
- Step 6** After creating a zone set, you must activate it to take effect. Click a zone set to activate it or right-click the zone set and select **Activate**. This configuration is distributed to the other switches in the network fabric.



**Note** When you confirm the activate operation, the current running configuration is saved to the startup configuration. This permanently saves any changes made to the running configuration (not just zoning changes).

- Step 7** After creating a zone set and activating it, make sure you save the configuration file. See [Appendix C, "Configuration Files,"](#) for details about copying and saving configuration files.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

## 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 user names for each user.
- Create and assign roles for users that do not include 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

- If licensed, configure Fabric Manager Server to provide historical and performance trending.
- Configure Call Home.



## Fabric Manager Client

---

The Cisco Fabric Manager Client is a Java-based GUI application that provides easy access to Fabric Manager applications from a remote workstation.

This appendix contains the following sections:

- [Fabric Manager Client Quick Tour, page A-2](#)
- [Fabric Manager Wizards, page A-11](#)

In addition to complete configuration and status monitoring capabilities for Cisco MDS 9000 switches, Fabric Manager Client provides powerful Fibre Channel troubleshooting tools. These in-depth health and configuration analysis tools leverage unique MDS 9000 switch capabilities including Fibre Channel ping and traceroute.



**Note**

---

You must have the same release of Fabric Manager Client and Fabric Manager Server.

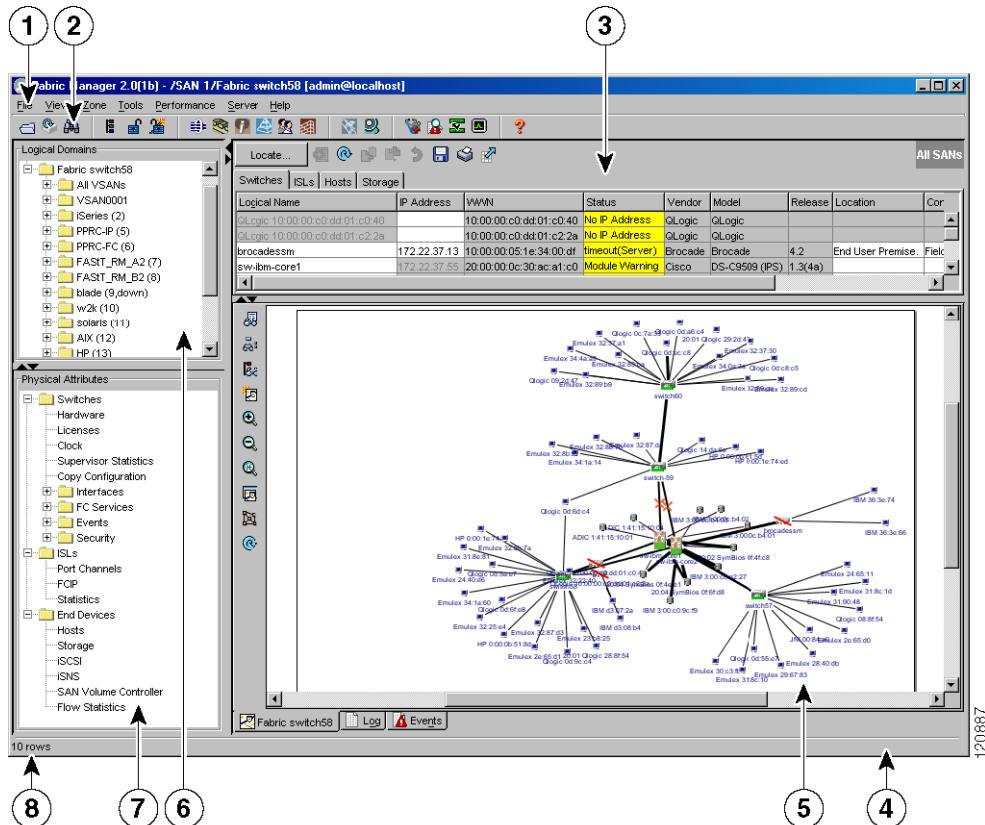
---

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

# Fabric Manager Client Quick Tour

This section helps you get familiar with the various icons and sections that enable navigation in the Fabric Manager Client interface, as shown in Figure A-1.

**Figure A-1 Fabric Manager Main Window**



1	Menu bar—Provides access to options that are organized by menus.
2	Toolbar—Provides icons to access the most commonly used options on the File, Tools, and Help menus.
3	Information pane—Displays information about whatever option is selected in the menu tree.
4	Status bar (right side)—Shows the last entry displayed by the discovery process, and the possible error message.
5	Fabric pane—Displays a map of the network fabric, including switches, hosts, and storage. It also provides tabs for displaying log and event data.
6	Logical domains—Displays a tree of configured SANs, fabrics, VSANs, and zones.
7	Physical attributes—Displays a tree of available configuration tasks depending on the SAN, fabric, VSAN, or zone selected above. Lists the switches and end devices in the logical selection.
8	Status Bar (left side)—Shows short-term transient messages, such as the number of rows displayed in a table.



**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

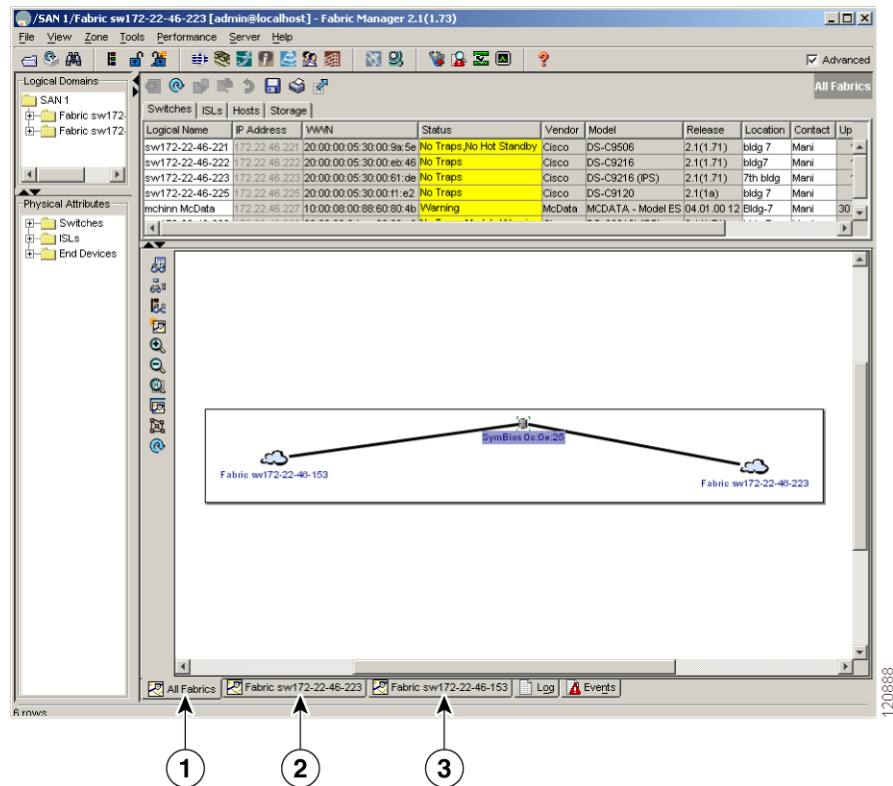
**Note**

As of Cisco MDS SAN-OS Release 2.1(1a), advanced mode is enabled by default and provides the full suite of Fabric Manager features, including security, IVR, iSCSI, and FICON. Uncheck the **Advanced** check box in the upper right corner of Fabric Manager Client to simplify the user interface. In this mode, you can access the basic MDS 9000 features like VSANs, zones, and interfaces.

## Multiple Fabrics in the Fabric Pane

You can display multiple fabrics in the same fabric pane (see [Figure A-2](#)). The tabs displayed at the bottom of the screen represent the various fabrics in your setup. You can access the fabrics by clicking the cloud icon.

**Figure A-2** *Displaying Multiple Fabrics*



1	All Fabrics tab (selected), showing two fabrics.
2	The Fabric view tab for fabric sw172-22-46-223.
3	The Fabric view tab for fabric sw172-22-46-153.

**Note**

The same username and password must be used to log into multiple fabrics.

## Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

The information for both fabrics is displayed, with no need to select a seed switch. To see details of a fabric, select the tab for that fabric at the bottom of the Fabric pane, or double-click the cloud icon for the fabric in the All Fabrics tab.










## Contents Panes

The following sections describe the panes in the Fabric Manager view. You can resize each pane by dragging the boundaries between each region or by clicking the **Minimize** or **Maximize** controls.

### Fabric Pane










The Fabric pane shows the graphical representation of your fabric. [Table A-1](#) explains the graphics you may see displayed, depending on which devices you have in your fabric.

**Table A-1** Fabric Manager Graphics

Icon or Graphic	Description
	Director class MDS 9000 switch.
	Non-director class MDS 9000 switch.
	Generic Fibre Channel switch.
	Cisco SN5428.
	An orange line through a device indicates that the device is manageable but there are operational problems.
	An orange X through a device or link indicates that the device or ISL is not working properly.
	A red line through a device indicates that the device is not manageable.
	A red X through a device or link indicates that the device is down or that the ISL is down.
	Fibre Channel HBA (or enclosure).

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

**Table A-1 Fabric Manager Graphics (continued)**

Icon or Graphic	Description
	Fibre Channel target (or enclosure).
	iSCSI host.
	Fibre Channel ISL and edge connection.
	Fibre Channel PortChannel.
	IP ISL and edge connection.
	IP PortChannel.
	Fibre Channel loop (storage).
	IP cloud (iSCSI hosts). This icon is also used to represent a fabric when viewing a SAN (multiple fabrics) in the Fabric pane.
	Any device, cloud, or loop with a box around it means that there are hidden links attached.

If a switch or director is dimmed, Fabric Manager can no longer communicate with it.

There are multiple tabs on the bottom of the Fabric pane:

- Fabric—Displays multiple fabrics; each fabric has its own tab. You can switch between fabrics by clicking on their respective tabs.
- Log—Displays messages that describe Fabric Manager operations, such as fabric discovery.
- Events—Displays information about the SNMP traps received by the management station, including combination events as detected by discovery and important traps such as license, SNMP, and FICON.

When viewing large fabrics in the Fabric pane, it is helpful to:

- Turn off end device labels.
- Collapse loops.
- Collapse expanded multiple links (collapsed multiple links are shown as very thick single lines).
- Dim or hide portions of your fabric by VSAN.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**



**Note** When a VSAN, zone, or zone member is selected in the VSAN tree, the map highlighting changes to identify the selected objects. To remove this highlighting, click **Clear Highlight** on the Fabric pane toolbar or choose **Clear Highlight** from the pop-up menu.

## Main Menu






The menu bar at the top of the Fabric Manager Client main window provides options for managing and troubleshooting the current fabric and for controlling the display of information on the Fabric pane. The menu bar provides the following menus:

- **File**—Opens a new fabric, rediscovers the current fabric, locates switches, sets preferences, prints the map, and clears (right-click on log) or exports the Fabric pane log.
- **View**—Changes the appearance of the map (these options are duplicated on the Fabric pane toolbar).
- **Zone**—Manages zones, zone sets, and inter-VSAN routing (IVR).
- **Tools**—Verifies and troubleshoots connectivity and configuration.
- **Performance**—Runs and configures Performance Manager and Cisco Traffic Analyzer and generates reports.
- **Server**—Runs administrative tasks on clients and fabrics. Provides Fabric Manager Server management and a purge command. Lists the switches that are being managed.
- **Help**—Displays online help topics for specific dialog boxes in the Information pane.

## Toolbar





The Fabric Manager Client main toolbar provides buttons for accessing the most commonly used menu bar options as shown in [Table A-2](#).

**Table A-2 Fabric Manager Client Main Toolbar**

Icon	Description
	Opens switch fabric.
	Rediscovers current fabric.
	Finds in the map.
	Creates VSAN.
	Launches DPVM wizard.



***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

**Table A-2 Fabric Manager Client Main Toolbar (continued)**

Icon	Description
	Edits full zone database.
	Launches IVR zone wizard.
	Launches PortChannel wizard.
	Launches FCIP wizard.
	Launches iSCSI wizard.
	Launches QoS wizard.
	Configures users and roles.
	Launches IP-ACL wizard.
	Launches License Install wizard.
	Launches Software Install wizard.
	Performs switch health analysis.
	Performs fabric configuration analysis.
	Performs end-to-end connectivity analysis.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***









**Table A-2 Fabric Manager Client Main Toolbar (continued)**

Icon	Description
	Monitor ISL performance.
	Show online help.

## Information Pane



The Information pane displays tables of information associated with the option selected from the menu tree in the Logical Domains or Physical Attributes panes. The Information pane toolbar provides buttons for performing one or more of the operations shown in [Table A-3](#).

**Table A-3 Information Pane Toolbar**

Icon	Description
 Apply Changes	Applies configuration changes.
 Refresh Values	Refreshes table values.
 Create Row	Opens the appropriate dialog box to create a row in the table.
 Delete Row	Deletes the currently highlighted rows from the table.
 Copy/Ctrl+C	Copies data from one row to another.
 Paste/Ctrl +V	Pastes the data from one row to another.
 Undo Changes/Ctrl-Z	Undoes the most recent change.
 Export	Exports and saves information to a file.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

**Table A-3 Information Pane Toolbar (continued)**

Icon	Description
 Print Table	Prints the contents of the Information pane.
 Detach Table	Displays a non-editable copy of the table in the Information pane in its own window, which you can move around the screen.



**Note**

After making changes, you must save the configuration or the changes are lost when the device is restarted.



**Note**

The buttons that appear on the toolbar vary according to the option that you select. They are activated or deactivated (dimmed) according to the field or other object that you select in the Information pane.

## Logical Domains Pane

Use the Logical Domains pane to manage attributes for SANs, fabrics, VSANs, and zones.

To manage these things, right-click one of the folders in the tree and click a menu item from the pop-up menu. You see the appropriate configuration dialog box.

The default name for the fabric is the name, IP address, or WWN for the principal switch in VSAN 1. If VSAN 1 is segmented, the default name is chosen from a principal switch with the smallest WWN. In order, you might see the following fabric names:

- Fabric <sysname>
- Fabric <ipAddress>
- Fabric <sWWN>

## Physical Attributes Pane

Use the Physical Attributes pane to display a tree of the options available for managing the switches in the currently discovered SAN, fabric, VSAN, or zone.

To select an option, click a folder to display the options available and then click the option. You see the table with information for the selected option in the Information pane. The Physical Attributes pane provides the following main folders:

- Switches—View and configure hardware, system, licensing, and configuration files.
- Interfaces—View and configure FC Physical, FC Logical, Ethernet, SVC, and PortChannel interfaces.
- FC Services—View and configure Fibre Channel network configurations.
- IP—View and configure IP storage and IP services.
- Events—View and configure events, alarms, thresholds, notifications, and informs.

## Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

- Security—View and configure MDS management and FC-SP security.
- ISLs—View and configure Inter-Switch Links.
- End Devices—View and configure end devices.

## Status Bar

The status bar at the bottom of the Fabric Manager window shows the last entry displayed by the discovery process, and the possible error message on the right side. The status bar displays a message stating that something has changed in the fabric and a new discovery is needed. The status bar shows both short-term, transient messages (such as the number of rows displayed in the table) and long-term discovery issues.

## Context Menus

When you right-click an icon in the Fabric pane, you see a pop-up menu with options that vary depending on the type of icon selected. The various options available for different objects include the following:

- Open an instance of Device Manager for the selected switch.
- Open a CLI session for the selected switch.
- Copy the display name of the selected object.
- Execute a **ping** or **tracert** command for the device.
- Show or hide end devices.
- View attributes.
- Quiesce and disable members for PortChannels.
- Set the trunking mode for an ISL.
- Create or add to a PortChannel for selected ISLs.

The Fabric pane has its own toolbar with options for saving, printing, and changing the appearance of the map. When you right-click on the map, a pop-up menu appears that provides options (duplicated on the toolbar) for changing the appearance of the map.



### Note

You can launch web-based or non-web-based applications from the Fabric pane. Assign an IP address to the storage port or enclosure, and then right-click to bring up the pop-up menu, and select **Device Manager**.

## Filtering

Fabric Manager has a built-in filtering mechanism that displays only the data that you are interested in. To filter, first select the SAN, fabric, and VSAN from the Logical Domains pane to narrow the scope of what is displayed in the Fabric pane. Any information that does not belong to the selected items is dimmed. Also, any information that does not belong to the selected items is not displayed in the tables in the Information pane.

To further narrow the scope, select attributes from the Physical Attributes pane. The Fabric Manager tables, display, and filter criteria change accordingly.



***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

## Detachable Tables

As of Cisco MDS SAN-OS Release 2.0(2b), Fabric Manager Client has detachable tables. You can detach tables and move them to different areas on your desktop so that you can compare similar tables from different VSANs, or you can keep informational tables open from one view while you examine a different area in Fabric Manager. To detach tables, click the **Detach Table** icon in the Information pane in Fabric Manager.

## Fabric Manager Wizards

Fabric Manager Client provides a series of wizards to facilitate common configuration tasks. These wizards are as follows:

- VSAN—Creates VSANs on multiple switches in the fabric and sets VSAN attributes including interop mode, load balancing, and FICON.
- Zone Edit Tool—Creates zone sets, zones, and aliases. Adds members to zone and edits the zone database.
- IVR Zone—Creates IVR zone sets, zones, and aliases. Enables IVR NAT and auto-topology. Adds members to IVR zones and edits the IVR zone database.
- PortChannel—Creates PortChannels from selected ISLs either manually or automatically. Sets PortChannel attributes such as channel ID and trunking mode.
- FCIP —Creates FCIP links between Gigabit Ethernet ports. Enables Fibre Channel Write Acceleration and IP compression
- DPVM—Establishes dynamic port VSAN membership, enables autolearning, and activates the DPVM database.
- iSCSI—Zones iSCSI initiators and adds VSAN to the target allowed VSAN list.
- QoS—Sets QoS attributes for zones in the selected VSAN.
- IP ACL—Creates ordered IP access control lists and distributes to selected switches in the fabric.
- License Install—Facilitates download and installation of licenses in selected switches in the fabric.
- Software Install—Verifies image compatibility and installs software images on selected switches in the fabric.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***



## 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 assigns 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).



---

**Note** 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.

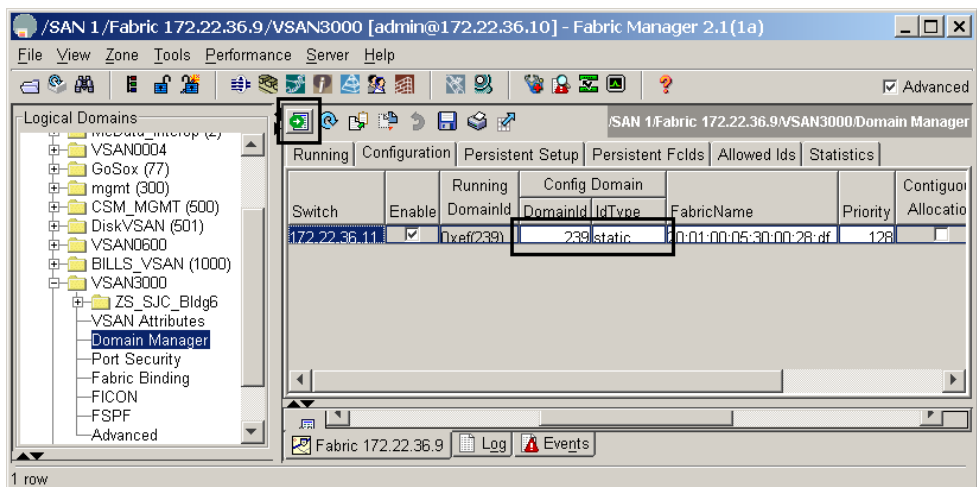
**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).**

In the following procedure, the existing VSAN has a switch C-186 with a domain ID of 209. In Fabric Manager, the VSAN is statically configured and a persistent FC ID is enabled. This procedure does not alter the running domain ID.

To configure a static domain ID for an existing VSAN and enable a persistent FC ID for the same VSAN using Fabric Manager, follow these steps:

- Step 1** In the Logical Domains pane, expand the VSAN to be modified and then choose **Domain Manager**. See [Figure B-1](#).
- Step 2** Click the **Configuration** tab.
- Step 3** Enter the domain ID that is in the Running DomainID (in [Figure B-1](#), it is 209) field in the Config Domain Id field.
- Step 4** Change the Config Domain IdType field to **static**.
- Step 5** Click the green **Apply Changes...** icon .

**Figure B-1 Enabling Static Domain ID**



- Step 6** Click the **Persistent Setup** tab.
- Step 7** Check the **Enable** check box.
- Step 8** Click **Apply Changes**.

At this point, the domain ID has been statically set and FC IDs will remain persistent across reboots for VSAN 3000 on the switch C-186. The persistent FC ID database can be viewed in the **Persistent Fcids** tab.



## 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 option 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 copy command will keep the existing startup configuration. This command does not affect the other switches in the fabric.

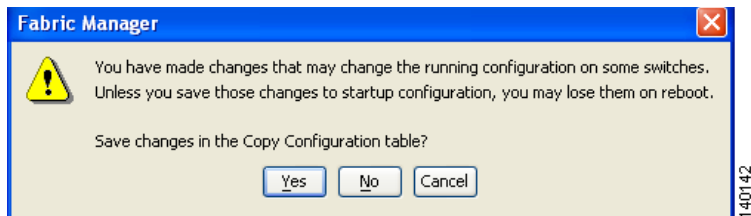
**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).**

To copy the configuration file, follow these steps:

- 
- Step 1** In the Physical Attributes pane, expand **Switches > Copy Configuration**.
  - Step 2** Check the check box for each switch configuration that you want to save. Set the From and To fields for each switch.
  - Step 3** Click **Apply**.

You are also prompted when exiting Fabric Manager to save changes in the Configuration file. (See [Figure C-1](#).) You see this dialog box only when any of the parameters of the Configuration file change when running a Fabric Manager session.

**Figure C-1 Save Configuration File**





---

## Numerics

10/100 Ethernet port [2-5](#)

10/100 MGMT [2-4](#)

---

## A

activate [5-5](#)

activating a zone set [5-5](#)

active supervisor [2-4](#)

active zone [5-4](#)

adapter [2-4](#)

    RJ-45 to DB-25 [2-4](#)

    RJ-45 to DB-9 [2-4](#)

additional accounts [2-7](#)

AIX [4-4, B-1](#)

aliases [5-3](#)

All Fabrics tab [3](#)

Apply Changes icon [8, B-2](#)

audience [vii](#)

---

## B

backing up MDS switch configuration [5-6](#)

basic MDS 9000 features [3](#)

baud rate [2-4](#)

---

## C

cables [4-5](#)

    recommended [2-5](#)

    RJ-45 to RJ-25 [2-4](#)

    RJ-45 to RJ-45 [2-4](#)

character format [2-4](#)

Cisco MDS 9000 program group

    installing on Linux [3-3](#)

    installing on Solaris [3-3](#)

    installing on Windows [3-3](#)

Cisco MDS 9500 series supervisor - 2 module  
    illustration [2-2](#)

Cisco SN5428 icon [4](#)

clear highlight [6](#)

Client main toolbar icons [6](#)

Cloud icon [3](#)

compatibility [ix](#)

Config Domain IdType [B-2](#)

configuration files

    copying [C-2](#)

    overview [C-1](#)

    running [5-5](#)

    saving [5-5, C-1](#)

    startup [5-5](#)

configuration flowchart [1-1](#)

Configure Users and Roles icon [7](#)

configuring a syslog server [5-6](#)

configuring Call Home [5-6](#)

configuring device aliases [5-6](#)

configuring DNS servers [5-6](#)

configuring switch

    CLI [2-5](#)

    Switch Setup Utility [2-5](#)

configuring TACACS+/RADIUS for centralized user  
    management [5-6](#)

configuring time/date/timezone and additionally NTP [5-6](#)

connecting to the console port [2-1](#)

connect to the server [3-2](#)

console port [2-1](#)

**REVIEW DRAFT – CISCO CONFIDENTIAL**

Cisco MDS 9100 Series switch (figure 2-3) [2-3](#)  
 Cisco MDS 9200 Series switch (figure 2-2) [2-3](#)  
 Cisco MDS 9500 Series Supervisor-2 Module (figure 2-1) [2-2](#)  
 Cisco MDS 9500 Series switch (figure 2-1) [2-2](#)  
   connecting the RS-232 cable [2-2](#)  
   connecting to a PC [2-4](#)  
 Copy/Ctrl+C icon [8](#)  
 Create Row icon [8](#)  
 Create VSAN icon [6](#)  
 creating unique user names for each user [5-6](#)

**D**

default network [2-7](#)  
 Delete Row icon [8](#)  
 detach tables [11](#)  
 device aliases as zone members [5-3](#)  
 device is not manageable [4](#)  
 Device Manager [10](#)  
 device or ISL is not working properly [4](#)  
 Director Class MDS 9000 Switch icon [4](#)  
 disabling Telnet [5-6](#)  
 DNS [2-7](#)  
 documentation  
   additional publications [ix](#)  
   related documents [ix](#)  
 Documentation Feedback [xi](#)  
 domain ID [B-1](#)  
 domain manager [B-1](#)  
 domain name [2-7](#)  
 downgrading [3-2](#)  
 DPVM wizard [11](#)  
 DVD [xi](#)

**E**

Edit Full Zone Database icon [7](#)  
 enabling SSH [5-6](#)

End Devices folder [10](#)  
 Events folder [9](#)  
 Events tab [5](#)  
 Export icon [8](#)

**F**

Fabric Manager  
   advanced mode [3](#)  
   browsers [3-1](#)  
   displaying multiple fabrics [3](#)  
   filtering [10](#)  
   graphics (table) [4](#)  
   icons (table) [4](#)  
   installing [3-1](#)  
   Java [3-1](#)  
   launching [3-3](#)  
   Login screen (figure) [3-4](#)  
   main menu [6](#)  
   operating systems [3-1](#)  
   overview [1-2](#)  
   quick tour [2](#)  
   reinstalling [3-2](#)  
   software executable files [3-1](#)  
   updating [3-2](#)  
   using interface (figure) [2](#)  
 Fabric Manager can no longer communicate [5](#)  
 Fabric Manager Client  
   Contents pane [4](#)  
   context menus [10](#)  
   detachable tables [11](#)  
   filtering [10](#)  
   Logical Domains pane [9](#)  
   overview [1](#)  
   Physical Attributes pane [9](#)  
   status bar [10](#)  
   toolbar [6](#)  
 Fabric Manager Server [1-2](#)  
 Fabric Manager Wizards [11](#)



## REVIEW DRAFT – CISCO CONFIDENTIAL

Fabric pane [2,10](#)

Fabric tab [5](#)

Fabric View tab [3](#)

FC IDs [B-1](#)

    configuring FC IDs and domain IDs (tip) [B-1](#)

    Fibre Channel IDs. [B-1](#)

    overview [B-1](#)

FCIP wizard [11](#)

FC Services folder [9](#)

Fibre Channel HBA icon [4](#)

Fibre Channel ISL and Edge Connection icon [5](#)

Fibre Channel Loop icon [5](#)

Fibre Channel PortChannel icon [5](#)

Fibre Channel Target icon [5](#)

FICON [4-4,3](#)

    traps [5](#)

Find in the Map icon [6](#)

FLOGI [B-1](#)

FMPersist.sh [3-3](#)

FMServer.sh [3-3](#)

FMWebClient.sh [3-3](#)

full zone set distribution [2-8](#)

## G

gateway IP address [2-7](#)

Generic Fibre Channel Switch icon [4](#)

global device aliases [3-3](#)

## H

hardware [2-1](#)

hardware installation [ix](#)

Hidden Links icon [5](#)

historical and performance trending [5-6](#)

HP-UX [4-4](#)

HTTP server [3-1,3-2](#)

hubs [2-5](#)

HyperTerminal Plus [2-4](#)

icons

    Fabric pane [4](#)

    Information pane [8](#)

    toolbar [6](#)

in-band management [2-7](#)

Information pane [2](#)

installation and configuration flowchart (figure) [1-1](#)

installation folder [3-2](#)

interfaces [4-5](#)

    adding [4-4](#)

    configuring [4-4](#)

    enabling or disabling [4-5](#)

    Fibre Channel [1-2](#)

    mgmt 0 [1-2](#)

    overview [1-2,4-1](#)

Interfaces folder [9](#)

Internet Explorer [3-1](#)

interoperability value [4-3](#)

IP ACL wizard [11](#)

IP Cloud icon [5](#)

IP folder [9](#)

IP ISL and Edge Connection icon [5](#)

IP PortChannel icon [5](#)

IPv6 [3-1](#)

iSCSI [3](#)

iSCSI Host icon [5](#)

iSCSI Hosts icon [5](#)

iSCSI wizard [11](#)

ISLs folder [10](#)

IVR [3](#)

IVR Zone wizard [11](#)

**REVIEW DRAFT – CISCO CONFIDENTIAL****J**

J 2-4  
 Java 1

**L**

LAN switch 2-4  
 large fabrics, viewing 5  
 Launch DPVM Wizard icon 6  
 Launch FCIP Wizard icon 7  
 Launch IP-ACL Wizard icon 7  
 Launch iSCSI Wizard icon 7  
 Launch IVR Zone Wizard icon 7  
 Launch License Install Wizard icon 7  
 Launch PortChannel Wizard icon 7  
 Launch QoS Wizard icon 7  
 Launch Software Install Wizard icon 7  
 LED 2-4  
 License Install wizard 11  
 linkFailure message 4-5  
 Linux 3-2  
 load balancing 4-3  
 loader> prompt 2-5  
 logical domains 2  
 Logical Domains pane 10  
   overview 9  
 Log tab 5

**M**

management port default characteristics 2-4  
 menu bar 2,6  
 mgmt0 2-5,3-2  
   connecting 2-4  
   IP address 2-7  
   netmask address 2-7  
 minimum configuration 1-2  
 Mode Admin 4-4

modules  
   verifying status 2-10  
 monitored fabrics 3-3  
 Monitor ISL Performance icon 8  
 Mozilla 3-1  
 multiple fabrics 3

**N**

Netscape 3-1  
 network connections  
   preparing 2-1  
 Non-director Class MDS 9000 Switch icon 4  
 noshut state 2-7  
 nstallation 1-1  
 NTP server 2-7

**O**

Open Switch Fabric icon 6  
 operational problems icon 4  
 orange line through a device 4  
 orange X through a device 4  
 ordering documentation xi  
 out-of-band management 2-7  
   10/100 ethernet management port 2-4

**P**

password  
   setting a strong password (tip) 2-6  
 Paste/Ctrl +V icon 8  
 PC serial port 2-4  
 Performance Manager 3-3  
 Perform End-to-end Connectivity Analysis icon 7  
 Perform Fabric Configuration Analysis icon 7  
 Perform Switch Health Analysis icon 7  
 persistent FC IDs B-1

**REVIEW DRAFT – CISCO CONFIDENTIAL**

enabling [B-2](#)  
 Physical Attributes pane [2, 10](#)  
   overview [9](#)  
 physical connections [2-5](#)  
 ping command [10](#)  
 PMCollector.sh [3-3](#)  
 PortChannels [10](#)  
 PortChannel wizard [11](#)  
 Port VSAN membership [4-4](#)  
 prerequisites for initial configuration [2-1](#)  
 principal switch [B-1](#)  
 pWWN mappings [5-3](#)

**Q**

QoS wizard [11](#)  
 quiesce [10](#)

**R**

Redhat Linux [3-1](#)  
 Rediscover Current Fabric icon [6](#)  
 red line through a device [4](#)  
 red X through a device [4](#)  
 reference [x](#)  
 Refresh Values icon [8](#)  
 Release Notes [ix](#)  
 remote client support [3-3](#)  
 remote workstation [1](#)  
 request a specific domain ID [B-1](#)  
 RJ-45 to DB-25 adapter [2-4](#)  
 RJ-45 to DB-9 adapter [2-4](#)  
 RJ-45 to RJ-45 cable [2-4](#)  
 roles  
   creating roles without network admin privileges [5-6](#)  
 Running DomainID [B-2](#)

**S**

scripts [3-3](#)  
 security [3](#)  
 Security folder [10](#)  
 serial port [2-4](#)  
 service [3-3](#)  
 service for Fabric Manager Server [1-2](#)  
 shell scripts [3-3](#)  
 show module command [2-10](#)  
 Show Online Help icon [8](#)  
 SNMP  
   community [2-7](#)  
   community strings [2-7](#)  
   connecting the console port [2-2](#)  
   logging into Fabric Manager [3-3](#)  
   traps [5](#)  
   version 3 [3-4](#)  
 Software Install wizard [11](#)  
 Solaris [3-1, 3-2](#)  
 srodst load balancing [4-3](#)  
 srodst Ox-ld load balancing [4-3](#)  
 SSH service [2-7](#)  
 static domain IDs  
   configuring [B-2](#)  
   Logical Domains pane [B-2](#)  
 static domain IDs and persistent FC IDs  
   HP-UX and AIX (tip) [4-4](#)  
   overview [B-1](#)  
 static routes [2-7](#)  
 Status Admin [4-4](#)  
 status bar [2, 10](#)  
 Sun Java Virtual Machine [3-2](#)  
 Sun JDK [3-1](#)  
 Sun JRE [3-1](#)  
 Sun Microsystems [3-2](#)  
 supervisor module [3-2](#)  
 switch  
   add to VSAN [4-4](#)

**REVIEW DRAFT – CISCO CONFIDENTIAL**

configure the interfaces [4-4](#)  
 minimum configuration [1-2](#)  
 move ports [4-4](#)  
 switch(boot) prompt [2-5](#)  
 switch configuration commands  
     CLI and Fabric Manager [1-2](#)  
 Switches folder [9](#)  
 Switch Setup Utility [2-5](#)  
     advanced IP options [2-7](#)  
     default gateway [2-7](#)  
     default switch port interface [2-7](#)  
     default zone policy [2-8](#)  
     ending the configuration [2-7](#)  
     entering the setup mode [2-6](#)  
     first-time configuration [2-6](#)  
     full zone set distribution [2-8](#)  
     host ID [2-5](#)  
     mgmt0  
         IP address [2-7](#)  
     NTP server [2-7](#)  
     out-of-band management [2-7](#)  
     SNMP community [2-7](#)  
     SSH service [2-7](#)  
     switch port trunk mode [2-8](#)  
     Telnet service [2-7](#)  
     user accounts  
         creating additional [2-7](#)

**T**

Telnet service [2-7](#)  
 threshold events [1-2](#)  
 toolbar [2](#)  
 traceroute command [10](#)  
 traps [5](#)  
 trial version [3-3](#)  
 troubleshooting [x](#)  
 trunking mode [2-8, 10](#)

**U**

uninstalling Fabric Manager [3-2](#)  
 upgrading [3-2](#)

**V**

VSANs  
     adding [4-2](#)  
     configuring [4-2](#)  
     Create VSAN dialog box (figure) [4-3](#)  
     overview [4-2](#)  
     static domain IDs [4-3](#)  
 VSANs and interfaces  
     steps for configuring (figure) [4-1](#)  
 VSAN wizard [11](#)  
 VT100 terminal emulation [2-4](#)

**W**

Windows 2000 [3-1](#)  
 Windows Server 2003 [3-1](#)  
 Windows Services applet [1-2](#)  
 Windows XP [3-1](#)  
 wizards [11](#)

**Z**

Zone Edit Tool wizard [11](#)  
 zone policy configuration [2-8](#)  
 zones  
     configuring [5-2](#)  
     configuring (flowchart) [5-1](#)  
     overview [5-2](#)  
     using device aliases (tip) [5-3](#)  
 zone sets  
     creating [5-4, 5-5](#)  
     overview [5-4](#)

***REVIEW DRAFT – CISCO CONFIDENTIAL***

rules 5-4

***REVIEW DRAFT – CISCO CONFIDENTIAL***