Cisco Fabric Manager Fabric Configuration Guide
Cisco Fabric Manager Release 4.2(3)
December 2009

Americas 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: 408 527-0883

Text Part Number: OL-19448-02
VSAN Configuration 2-5
  About VSAN Creation 2-6
  Creating VSANs Statically 2-6
  About Port VSAN Membership 2-7
  Assigning Static Port VSAN Membership 2-8
  About the Default VSAN 2-8
  About the Isolated VSAN 2-8
  Displaying Isolated VSAN Membership 2-9
  Operational State of a VSAN 2-9
  About Static VSAN Deletion 2-9
  Deleting Static VSANs 2-10
  About Load Balancing 2-11
  Configuring Load Balancing 2-11
  About Interop Mode 2-12
  About FICON VSANs 2-12
Host Provisioning Wizard 2-12
  Commissioning a Host 2-12
  Decommissioning a Host 2-16
Default Settings 2-18

CHAPTER 3
Configuring SAN Device Virtualization 3-1
  About SDV 3-1
    Key Concepts 3-3
    Automatic Failover and Fallback 3-4
  Configuring SDV 3-4
    Configuring a Virtual Device 3-4
    Linking a Virtual Device with a Physical Device 3-7
    Resolving Fabric Merge Conflicts 3-8
SDV Requirements and Guidelines 3-9
Default Settings 3-10

CHAPTER 4
Creating Dynamic VSANs 4-1
  DPVM 4-1
    About DPVM Configuration 4-2
    Configuring DPVM with the DPVM Wizard 4-2
    About DPVM Databases 4-5
    Configuring DPVM Config and Pending Databases 4-5
    Activating DPVM Config Databases 4-7
    Viewing the Pending Database 4-8
About Autolearned Entries 4-8
Enabling Autolearning 4-9
Clearing Learned Entries 4-9

DPVM Database Distribution 4-10
About DPVM Database Distribution 4-10
Disabling DPVM Database Distribution 4-11
About Locking the Fabric 4-11
Locking the Fabric 4-11
Committing Changes 4-12
Discarding Changes 4-13
Clearing a Locked Session 4-13

Database Merge Guidelines 4-13
About Copying DPVM Databases 4-14
Copying DPVM Databases 4-14
Comparing Database Differences 4-14

Default Settings 4-15

CHAPTER 5
Configuring and Managing Zones 5-1
About Zoning 5-1
Zoning Example 5-2
Zone Implementation 5-3
Zone Member Configuration Guidelines 5-4
Active and Full Zone Set Considerations 5-4

Using the Quick Config Wizard 5-7

Zone Configuration 5-10
About the Edit Local Full Zone Database Tool 5-11
Configuring a Zone Using the Zone Configuration Tool 5-12
Adding Zone Members 5-14
Filtering End Devices Based on Name, WWN or FC ID 5-15
Adding Multiple End Devices to Multiple Zones 5-16

Zone Sets 5-16
About Zone Set Creation 5-16
Activating a Zone Set 5-18
Deactivating a Zoneset 5-19
Displaying Zone Membership Information 5-21
About the Default Zone 5-21
Configuring the Default Zone 5-22
About FC Alias Creation 5-22
Creating FC Aliases 5-23
Contents

Send documentation comments to mdsfeedback-doc@cisco.com

Adding Members to Aliases 5-23
Converting Zone Members to pWWN-based Members 5-25
Filtering Zones, Zone Sets, and Device Aliases Based on Name 5-27
Adding Multiple Zones to Multiple Zone Sets 5-27
Zone Enforcement 5-27

Zone Set Distribution 5-28
   Enabling Full Zone Set Distribution 5-28
   Enabling a One-Time Distribution 5-29
   About Recovering from Link Isolation 5-29
   Importing and Exporting Zone Sets 5-30

Zone Set Duplication 5-31
   Copying Zone Sets 5-31
   About Backing Up and Restoring Zones 5-32
   Backing Up Zones 5-32
   Restoring Zones 5-34
   Renaming Zones, Zone Sets, and Aliases 5-35
   Cloning Zones, Zone Sets, FC Aliases, and Zone Attribute Groups 5-36
   Migrating a Non-MDS Database 5-37
   Clearing the Zone Server Database 5-37

Advanced Zone Attributes 5-37
   About Zone-Based Traffic Priority 5-38
   Configuring Zone-Based Traffic Priority 5-38
   Configuring Default Zone QoS Priority Attributes 5-39
   Configuring the Default Zone Policy 5-40
   About Broadcast Zoning 5-40
   Configuring Broadcast Zoning 5-41
   About LUN Zoning 5-41
   Configuring a LUN-Based Zone 5-42
   Assigning LUNs to Storage Subsystems 5-43
   About Read-Only Zones 5-43
   Configuring Read-Only Zones 5-44

Displaying Zone Information 5-44

Enhanced Zoning 5-45
   About Enhanced Zoning 5-45
   Changing from Basic Zoning to Enhanced Zoning 5-46
   Changing from Enhanced Zoning to Basic Zoning 5-46
   Enabling Enhanced Zoning 5-47
   Creating Attribute Groups 5-47
   Merging the Database 5-47
Analyzing a Zone Merge 5-48
Configuring Zone Merge Control Policies 5-49
Compacting the Zone Database for Downgrading 5-49
Default Settings 5-50

CHAPTER 6  
Distributing Device Alias Services 6-1
About Device Aliases 6-1
About Device Alias Modes 6-1
  Changing Mode Settings 6-2
  Device Alias Mode Distribution 6-2
  Merging Device Alias 6-2
  Resolving Merge and Device Alias Mode Mismatch 6-3
  Device Alias Features 6-3
  Device Alias Requirements 6-3
  Zone Aliases Versus Device Aliases 6-4
Device Alias Databases 6-4
  About Device Alias Distribution 6-5
  Distributing the Device Alias Database 6-5
About Creating a Device Alias 6-5
Creating a Device Alias 6-6
Committing Changes 6-6
Discarding Changes 6-7
About Legacy Zone Alias Configuration Conversion 6-7
Using Device Aliases or FC Aliases 6-8
Device Alias Statistics Cleanup 6-8
Database Merge Guidelines 6-8
Populating Device Alias to Interface Description 6-9
Default Settings 6-9

CHAPTER 7  
Configuring FCoE 7-1
About Fibre Channel over Ethernet 7-1
  FIP Initialization Protocol 7-1
Guidelines and Limitations 7-1
Configuring FCoE 7-1
  Enabling FCoE 7-2
  Configuring FCoE Using Fabric Manager 7-3
  Configuring FCoE Using Device Manager 7-4
CHAPTER 8
Configuring Fibre Channel Routing Services and Protocols 8-1

About FSPF 8-2

FSPF Examples 8-2

Fault Tolerant Fabric 8-2

Redundant Links 8-3

Failover Scenarios for PortChannels and FSPF Links 8-3

FSPF Global Configuration 8-4

About SPF Computational Hold Times 8-4

About Link State Records 8-4

Configuring FSPF on a VSAN 8-5

Resetting FSPF to the Default Configuration 8-5

Enabling or Disabling FSPF 8-6

FSPF Interface Configuration 8-6

About FSPF Link Cost 8-6

Configuring FSPF Link Cost 8-7

About Hello Time Intervals 8-7

Configuring Hello Time Intervals 8-8

About Dead Time Intervals 8-8

Configuring Dead Time Intervals 8-8

About Retransmitting Intervals 8-8

Configuring Retransmitting Intervals 8-9

About Disabling FSPF for Specific Interfaces 8-9

Disabling FSPF for Specific Interfaces 8-9

Displaying the FSPF Database 8-10

Viewing FSPF Statistics 8-11

FSPF Routes 8-12

About Fibre Channel Routes 8-12

Configuring Fibre Channel Routes 8-12

About Broadcast and Multicast Routing 8-14

About Multicast Root Switch 8-14

Setting the Multicast Root Switch 8-14

In-Order Delivery 8-15

About Reordering Network Frames 8-15

About Reordering PortChannel Frames 8-16

About Enabling In-Order Delivery 8-17

Enabling In-Order Delivery Globally 8-18

Enabling In-Order Delivery for a VSAN 8-18

Configuring the Drop Latency Time 8-18

Default Settings 8-19
Send documentation comments to mdsfeedback-doc@cisco.com

CHAPTER 9
Configuring Dense Wavelength Division Multiplexing  9-1
  About DWDM  9-1
  Viewing DWDM Links  9-1
  Configuring X2 DWDM Transceiver Frequency  9-4

CHAPTER 10
Managing FLOGI, Name Server, FDMI, and RSCN Databases  10-1
  About FLOGI  10-1
    Displaying FLOGI Details  10-1
  Name Server Proxy  10-2
    About Registering Name Server Proxies  10-2
    Registering Name Server Proxies  10-2
    About Rejecting Duplicate pWWN  10-3
    Rejecting Duplicate pWWNs  10-3
    To reject duplicate pWWNs, refer to the Cisco MDS 9000 Family CLI Configuration Guide. About
    Name Server Database Entries  10-3
    Viewing Name Server Database Entries  10-3
  FDMI  10-4
    Displaying FDMI  10-4
  RSCN  10-5
    About RSCN Information  10-5
    Displaying RSCN Information  10-5
    About the multi-pid Option  10-6
    Configuring the multi-pid Option  10-6
    Clearing RSCN Statistics  10-7
    RSCN Timer Configuration Distribution Using CFS  10-7
    Configuring the RSCN Timer with CFS  10-8
    Default Settings  10-8

CHAPTER 11
Discovering SCSI Targets  11-1
  About SCSI LUN Discovery  11-1
    About Starting SCSI LUN Discovery  11-1
    Starting SCSI LUN Discovery  11-2
    About Initiating Customized Discovery  11-2
    Initiating Customized Discovery  11-2
    Displaying SCSI LUN Information  11-3

CHAPTER 12
Configuring FICON  12-1
  About FICON  12-1
New and Changed Information

As of Cisco MDS NX-OS Release 4.2(1), software configuration information is available in new feature-specific configuration guides for the following information:

- System management
- Interfaces
- Fabric
- Quality of service
- Security
- IP services
- High availability and redundancy

The information in these new guides previously existed in the *Cisco MDS 9000 Family CLI Configuration Guide* and in the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*. Those configuration guides remain available on Cisco.com and should be used for all software releases prior to MDS NX-OS Release 4.2(1). Each guide addresses the features introduced in or available in a particular release. Select and view the configuration guide that pertains to the software installed in your switch.

For a complete list of document titles, see the list of Related Documentation in the “Preface.”

To find additional information about Cisco MDS NX-OS Release 4.2(x), see the *Cisco MDS 9000 Family Release Notes* available at the following Cisco Systems website:


About This Guide


Table 1 lists the New and Changed features for this guide, starting with MDS NX-OS Release 4.2(1).
### Table 1 New and Changed Features for Cisco Fabric Manager Release 4.2(x)

<table>
<thead>
<tr>
<th>Feature</th>
<th>GUI Change</th>
<th>Description</th>
<th>Changed in Release</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Provision</td>
<td>Host Provision Wizard</td>
<td>Added information about Host Provision Wizard</td>
<td>4.2(1)</td>
<td>Chapter 2, “Configuring and Managing VSANs”</td>
</tr>
<tr>
<td>Zones and Zonesets</td>
<td>Zone and Zoneset configuration windows</td>
<td>Added information about adding multiple end devices to zones and multiple zones to zonesets.</td>
<td>4.2(1)</td>
<td>Chapter 5, “Configuring and Managing Zones”</td>
</tr>
<tr>
<td>Device Alias</td>
<td>Interfaces configuration window</td>
<td>Added information about populating device alias to interface description.</td>
<td>4.2(1)</td>
<td>Chapter 6, “Distributing Device Alias Services”</td>
</tr>
<tr>
<td>X2 DWDM</td>
<td>Module configuration window</td>
<td>Added information about configuring X2 DWDM transceiver frequency.</td>
<td>4.2(1)</td>
<td>Chapter 9, “Configuring Dense Wavelength Division Multiplexing”</td>
</tr>
<tr>
<td>XRC Acceleration</td>
<td>Interfaces configuration window</td>
<td>Added information about configuring XRC Acceleration.</td>
<td>4.2(1)</td>
<td>Chapter 12, “Configuring FICON”</td>
</tr>
</tbody>
</table>
Preface

This preface describes the audience, organization, and conventions of the Cisco Fabric Manager Fabric 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

The Cisco Fabric Manager Fabric Configuration Guide is organized as follows:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1</td>
<td>Fabric Overview</td>
<td>Provides an overview of features described in this guide.</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>Configuring and Managing VSANs</td>
<td>Describes how virtual SANs (VSANs) work, explains the concept of default VSANs, isolated VSANs, VSAN IDs, and attributes, and provides details on how to create, delete, and view VSANs.</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>Configuring SAN Device Virtualization</td>
<td>Describes how to configure virtual devices to represent physical end devices for switches running Cisco MDS SAN-OS Release 3.1(2) and NX-OS Release 4.1(1a).</td>
</tr>
<tr>
<td>Chapter 4</td>
<td>Creating Dynamic VSANs</td>
<td>Defines the Dynamic Port VSAN Membership (DPVM) feature that is used to maintain fabric topology when a host or storage device connection is moved between two Cisco MDS switches.</td>
</tr>
<tr>
<td>Chapter 5</td>
<td>Configuring and Managing Zones</td>
<td>Defines various zoning concepts and provides details on configuring a zone set and zone management features.</td>
</tr>
</tbody>
</table>
Preface

Document Conventions

Command descriptions use these conventions:

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

Screen examples use these conventions:

- **screen font**: Terminal sessions and information the switch displays are in screen font.
- **boldface screen font**: Information you must enter is in boldface screen font.
- **italic screen font**: Arguments for which you supply values are in italic screen font.
This document uses the following conventions:

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; &gt;</td>
<td>Nonprinting characters, such as passwords, are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>! #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

Related Documentation

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


Release Notes

- Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Releases
- Cisco MDS 9000 Family Release Notes for Storage Services Interface Images
- Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images

Regulatory Compliance and Safety Information

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

Compatibility Information

- Cisco MDS 9000 NX-OS Hardware and Software Compatibility Information
- Cisco MDS NX-OS Release Compatibility Matrix for Storage Service Interface Images
- Cisco MDS 9000 Family Interoperability Support Matrix
- Cisco MDS NX-OS Release Compatibility Matrix for IBM SAN Volume Controller Software for Cisco MDS 9000
Send documentation comments to mdsfeedback-doc@cisco.com

Hardware Installation

- Cisco MDS 9500 Series Hardware Installation Guide
- Cisco MDS 9200 Series Hardware Installation Guide

Software Installation and Upgrade

- Cisco MDS 9000 Family Software Upgrade and Downgrade Guide - For Cisco NX-OS
- Cisco MDS 9000 Family Storage Services Interface Image Install and Upgrade Guide - For Cisco NX-OS
- Cisco MDS 9000 Family Port Analyzer Adapter Installation and Configuration Note

Cisco NX-OS

- Cisco NX-OS Fundamentals Configuration Guide
- Cisco NX-OS Family Licensing Guide
- Cisco MDS 9000 Family NX-OS System Management Configuration Guide
- Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide
- Cisco MDS 9000 Family NX-OS Fabric Configuration Guide
- Cisco MDS 9000 Family NX-OS Quality of Service Configuration Guide
- Cisco MDS 9000 Family NX-OS Security Configuration Guide
- Cisco MDS 9000 Family NX-OS IP Services Configuration Guide
- Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide

Cisco Fabric Manager

- Cisco MDS 9000 Family Fabric Manager Installation and Upgrade Guide
- Cisco MDS 9000 Family Fabric Manager Configuration Guide
- Cisco Fabric Manager Fundamentals Configuration Guide
- Cisco Fabric Manager System Management Configuration Guide
- Cisco Fabric Manager Interfaces Configuration Guide
- Cisco Fabric Manager Fabric Configuration Guide
- Cisco Fabric Manager Quality of Service Configuration Guide
- Cisco Fabric Manager Security Configuration Guide
- Cisco Fabric Manager IP Services Configuration Guide
- Cisco Fabric Manager Intelligent Storage Services Configuration Guide
- Cisco Fabric Manager High Availability and Redundancy Configuration Guide
- Cisco MDS 9000 Fabric Manager Online Help
Preface

Send documentation comments to mdsfeedback-doc@cisco.com

- Cisco MDS 9000 Fabric Manager Web Services Online Help
- Cisco Fabric Manager Web Services Programming Guide

Command-Line Interface

- Cisco MDS 9000 Family CLI Configuration Guide
- Cisco MDS 9000 Family Command Reference
- Cisco MDS 9000 Family SAN Volume Controller Configuration Guide

Intelligent Storage Networking Services Configuration Guides

- Cisco MDS 9000 Family NX-OS Intelligent Storage Services Configuration Guide
- Cisco MDS 9000 Family SANTap Deployment Guide
- Cisco MDS 9000 Family Data Mobility Manager Configuration Guide
- Cisco MDS 9000 Family Storage Media Encryption Configuration Guide
- Cisco MDS 9000 Family Secure Erase Configuration Guide - For Cisco MDS 9500 and 9200 Series

Troubleshooting and Reference

- Cisco MDS 9000 Family Troubleshooting Guide
- Cisco MDS 9000 Family MIB Quick Reference
- Cisco MDS 9000 Family SMI-S Programming Reference
- Cisco MDS 9000 Family System Messages Reference

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

Subscribe to the What’s New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.
CHAPTER 1

Fabric Overview

The Cisco MDS 9000 Family NX-OS command-line interface (CLI) can configure and manage features such as VSANs, SAN device virtualization, dynamic VSANs, zones, distributed device alias services, Fibre Channel routing services and protocols, FLOGI, name server, FDMI, RSCN database, SCSI targets, FICON, and other advanced features.

This chapter describes some of these features and includes the following topics:

- Virtual SANs, page 1-1
- Dynamic Port VSAN Membership, page 1-2
- SAN Device Virtualization, page 1-2
- Zoning, page 1-2
- Distributed Device Alias Services, page 1-3
- Fibre Channel over Ethernet, page 1-3
- Fibre Channel Routing Services and Protocols, page 1-3
- Multiprotocol Support, page 1-4

Virtual SANs

Virtual SAN (VSAN) technology partitions a single physical SAN into multiple VSANs. VSAN capabilities allow Cisco NX-OS software to logically divide a large physical fabric into separate, isolated environments to improve Fibre Channel SAN scalability, availability, manageability, and network security. For FICON, VSANs facilitate hardware-based separation of FICON and open systems.

Each VSAN is a logically and functionally separate SAN with its own set of Fibre Channel fabric services. This partitioning of fabric services greatly reduces network instability by containing fabric reconfigurations and error conditions within an individual VSAN. The strict traffic segregation provided by VSANs helps ensure that the control and data traffic of a specified VSAN are confined within the VSAN’s own domain, increasing SAN security. VSANs help reduce costs by facilitating consolidation of isolated SAN islands into a common infrastructure without compromising availability.

Users can create administrator roles that are limited in scope to certain VSANs. For example, a network administrator role can be set up to allow configuration of all platform-specific capabilities, while other roles can be set up to allow configuration and management only within specific VSANs. This approach improves the manageability of large SANs and reduces disruptions due to human error by isolating the effect of a user action to a specific VSAN whose membership can be assigned based on switch ports or the worldwide name (WWN) of attached devices.
Dynamic Port VSAN Membership

Port VSAN membership on the switch is assigned on a port-by-port basis. By default each port belongs to the default VSAN. You can dynamically assign VSAN membership to ports by assigning VSANs based on the device WWN. This method is referred to as Dynamic Port VSAN Membership (DPVM). DPVM offers flexibility and eliminates the need to reconfigure the port VSAN membership to maintain fabric topology when a host or storage device connection is moved between two Cisco MDS switches or two ports within a switch. DPVM retains the configured VSAN regardless of where a device is connected or moved.

SAN Device Virtualization

Cisco SAN device virtualization (SDV) allows virtual devices representing physical end devices to be used for SAN configuration. Virtualization of SAN devices significantly reduces the time needed to swap out hardware. For example, if a storage array was replaced without using SDV, server downtime would be required for SAN zoning changes and host operating system configuration updates. With SDV, only the mapping between virtual and physical devices needs to change after hardware is swapped, insulating the SAN and end devices from extensive configuration changes.

Zoning

Zoning provides access control for devices within a SAN. Cisco NX-OS software supports the following types of zoning:

- **N port zoning**—Defines zone members based on the end-device (host and storage) port.
  - WWN
  - Fibre Channel identifier (FC-ID)
- **Fx port zoning**—Defines zone members based on the switch port.
  - WWN
  - WWN plus interface index, or domain ID plus interface index
- **Domain ID and port number** (for Brocade interoperability)
- **iSCSI zoning**—Defines zone members based on the host zone.
  - iSCSI name
  - IP address
- **LUN zoning**—When combined with N port zoning, LUN zoning helps ensure that LUNs are accessible only by specific hosts, providing a single point of control for managing heterogeneous storage-subsystem access.
- **Read-only zones**—An attribute can be set to restrict I/O operations in any zone type to SCSI read-only commands. This feature is especially useful for sharing volumes across servers for backup, data warehousing, etc.
Broadcast zones—An attribute can be set for any zone type to restrict broadcast frames to members of the specific zone.

To provide strict network security, zoning is always enforced per frame using access control lists (ACLs) that are applied at the ingress switch. All zoning policies are enforced in hardware, and none of them cause performance degradation. Enhanced zoning session-management capabilities further enhance security by allowing only one user at a time to modify zones.

Distributed Device Alias Services

All switches in the Cisco MDS 9000 Family support Distributed Device Alias Services (device alias) on a per-VSAN basis and on a fabric-wide basis. Device alias distribution allows you to move host bus adapters (HBAs) between VSANs without manually reentering alias names.

Fibre Channel over Ethernet

Fibre Channel over Ethernet (FCoE) allows Fibre Channel traffic to be encapsulated over a physical Ethernet link. FCoE frames use a unique EtherType so that FCoE traffic and standard Ethernet traffic can be carried on the same link.

Classic Ethernet is a best-effort protocol. In the event of congestion, Ethernet will discard packets, relying on higher level protocols to provide retransmission and other reliability mechanisms. Fibre Channel traffic requires a lossless transport layer. As a data storage protocol, it is unacceptable to lose a single data packet. Native Fibre Channel implements a lossless service at the transport layer using a buffer-to-buffer credit system.

For FCoE traffic, the Ethernet link must provide a lossless service. Ethernet links on Cisco Nexus 5000 Series switches provide two mechanisms to ensure lossless transport for FCoE traffic: link-level flow control and priority flow control.

IEEE 802.3x link-level flow control allows a congested receiver to signal the far end to pause the data transmission for a short period of time. The pause functionality is applied to all the traffic on the link.

The priority flow control (PFC) feature applies pause functionality to specific classes of traffic on the Ethernet link. For example, PFC can provide lossless service for the FCoE traffic and best-effort service for the standard Ethernet traffic. PFC can provide different levels of service to specific classes of Ethernet traffic (using IEEE 802.1p traffic classes).

Fibre Channel Routing Services and Protocols

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

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

In addition to supporting Fibre Channel Protocol (FCP), Cisco NX-OS software supports IBM Fibre Connection (FICON), Small Computer System Interface over IP (iSCSI), and Fibre Channel over IP (FCIP) in a single platform. Native iSCSI support in the Cisco MDS 9000 Family switches helps customers consolidate storage for a wide range of servers into a common pool on the SAN.
Configuring and Managing VSANs

You can achieve higher security and greater stability in Fibre Channel fabrics by using virtual SANs (VSANs) on Cisco MDS 9000 Family switches and Cisco Nexus 5000 Series switches. VSANs provide isolation among devices that are physically connected to the same fabric. With VSANs you can create multiple logical SANs over a common physical infrastructure. Each VSAN can contain up to 239 switches and has an independent address space that allows identical Fibre Channel IDs (FC IDs) to be used simultaneously in different VSANs. This chapter includes the following sections:

- About VSANs, page 2-1
- VSAN Configuration, page 2-5
- Host Provisioning Wizard, page 2-12
- Default Settings, page 2-18

About VSANs

A VSAN is a virtual storage area network (SAN). A SAN is a dedicated network that interconnects hosts and storage devices primarily to exchange SCSI traffic. In SANs you use the physical links to make these interconnections. A set of protocols run over the SAN to handle routing, naming, and zoning. You can design multiple SANs with different topologies.

This section describes VSANs and includes the following topics:

- VSANs Topologies, page 2-1
- VSAN Advantages, page 2-3
- VSANs Versus Zones, page 2-4

VSANs Topologies

With the introduction of VSANs, the network administrator can build a single topology containing switches, links, and one or more VSANs. Each VSAN in this topology has the same behavior and property of a SAN. A VSAN has the following additional features:

- Multiple VSANs can share the same physical topology.
- The same Fibre Channel IDs (FC IDs) can be assigned to a host in another VSAN, thus increasing VSAN scalability.
- Every instance of a VSAN runs all required protocols such as FSPF, domain manager, and zoning.
About VSANs

- Fabric-related configurations in one VSAN do not affect the associated traffic in another VSAN.
- Events causing traffic disruptions in one VSAN are contained within that VSAN and are not propagated to other VSANs.

The switch icons shown in both Figure 2-1 and Figure 2-2 indicate that these features apply to any switch in the Cisco MDS 9000 Family.

Figure 2-1 shows a fabric with three switches, one on each floor. The geographic location of the switches and the attached devices is independent of their segmentation into logical VSANs. No communication between VSANs is possible. Within each VSAN, all members can talk to one another.

Figure 2-1 Logical VSAN Segmentation

Figure 2-2 shows a physical Fibre Channel switching infrastructure with two defined VSANs: VSAN 2 (dashed) and VSAN 7 (solid). VSAN 2 includes hosts H1 and H2, application servers AS2 and AS3, and storage arrays SA1 and SA4. VSAN 7 connects H3, AS1, SA2, and SA3.
About VSANs

The four switches in this network are interconnected by trunk links that carry both VSAN 2 and VSAN 7 traffic. The inter-switch topology of both VSAN 2 and VSAN 7 are identical. This is not a requirement and a network administrator can enable certain VSANs on certain links to create different VSAN topologies.

Without VSANs, a network administrator would need separate switches and links for separate SANs. By enabling VSANs, the same switches and links may be shared by multiple VSANs. VSANs allow SANs to be built on port granularity instead of switch granularity. Figure 2-2 illustrates that a VSAN is a group of hosts or storage devices that communicate with each other using a virtual topology defined on the physical SAN.

The criteria for creating such groups differ based on the VSAN topology:

- VSANs can separate traffic based on the following requirements:
  - Different customers in storage provider data centers
  - Production or test in an enterprise network
  - Low and high security requirements
  - Backup traffic on separate VSANs
  - Replicating data from user traffic
- VSANs can meet the needs of a particular department or application.

VSAN Advantages

VSANs offer the following advantages:

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

- Traffic isolation—Traffic is contained within VSAN boundaries and devices reside only in one VSAN ensuring absolute separation between user groups, if desired.
- Scalability—VSANs are overlaid on top of a single physical fabric. The ability to create several logical VSAN layers increases the scalability of the SAN.
- Per VSAN fabric services—Replication of fabric services on a per VSAN basis provides increased scalability and availability.
- Redundancy—Several VSANs created on the same physical SAN ensure redundancy. If one VSAN fails, redundant protection (to another VSAN in the same physical SAN) is configured using a backup path between the host and the device.
- Ease of configuration—Users can be added, moved, or changed between VSANs without changing the physical structure of a SAN. Moving a device from one VSAN to another only requires configuration at the port level, not at a physical level.

Up to 256 VSANs can be configured in a switch. Of these, one is a default VSAN (VSAN 1), and another is an isolated VSAN (VSAN 4094). User-specified VSAN IDs range from 2 to 4093.

VSANs Versus Zones

You can define multiple zones in a VSAN. Because two VSANs are equivalent to two unconnected SANs, zone A on VSAN 1 is different and separate from zone A in VSAN 2. Table 2-1 lists the differences between VSANs and zones.

Table 2-1  VSAN and Zone Comparison

<table>
<thead>
<tr>
<th>VSAN Characteristic</th>
<th>Zone Characteristic</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSANs equal SANs with routing, naming, and zoning protocols.</td>
<td>Routing, naming, and zoning protocols are not available on a per-zone basis.</td>
</tr>
<tr>
<td>VSANs limit unicast, multicast, and broadcast traffic.</td>
<td>Zones limit unicast traffic.</td>
</tr>
<tr>
<td>Membership is typically defined using the VSAN ID to Fx ports.</td>
<td>Membership is typically defined by the pWWN.</td>
</tr>
<tr>
<td>An HBA or a storage device can belong only to a single VSAN—the VSAN associated with the Fx port.</td>
<td>An HBA or storage device can belong to multiple zones.</td>
</tr>
<tr>
<td>VSANs enforce membership at each E port, source port, and destination port.</td>
<td>Zones enforce membership only at the source and destination ports.</td>
</tr>
<tr>
<td>VSANs are defined for larger environments (storage service providers).</td>
<td>Zones are defined for a set of initiators and targets not visible outside the zone.</td>
</tr>
<tr>
<td>VSANs encompass the entire fabric.</td>
<td>Zones are configured at the fabric edge.</td>
</tr>
</tbody>
</table>

Figure 2-3 shows the possible relationships between VSANs and zones. In VSAN 2, three zones are defined: zone A, zone B, and zone C. Zone C overlaps both zone A and zone B as permitted by Fibre Channel standards. In VSAN 7, two zones are defined: zone A and zone D. No zone crosses the VSAN boundary—they are completely contained within the VSAN. Zone A defined in VSAN 2 is different and separate from zone A defined in VSAN 7.
Chapter 2  Configuring and Managing VSANs

VSAN Configuration

VSANs have the following attributes:

- **VSAN ID**—The VSAN ID identifies the VSAN as the default VSAN (VSAN 1), user-defined VSANs (VSAN 2 to 4093), and the isolated VSAN (VSAN 4094).

- **State**—The administrative state of a VSAN can be configured to an active (default) or suspended state. Once VSANs are created, they may exist in various conditions or states.
  - The active state of a VSAN indicates that the VSAN is configured and enabled. By enabling a VSAN, you activate the services for that VSAN.
  - The suspended state of a VSAN indicates that the VSAN is configured but not enabled. If a port is configured in this VSAN, it is disabled. Use this state to deactivate a VSAN without losing the VSAN’s configuration. All ports in a suspended VSAN are disabled. By suspending a VSAN, you can preconfigure all the VSAN parameters for the whole fabric and activate the VSAN immediately.

- **VSAN name**—This text string identifies the VSAN for management purposes. The name can be from 1 to 32 characters long and it must be unique across all VSANs. By default, the VSAN name is a concatenation of VSAN and a four-digit string representing the VSAN ID. For example, the default name for VSAN 3 is VSAN0003.

  **Note** A VSAN name must be unique.

- **Load balancing attributes**—These attributes indicate the use of the source-destination ID (src-dst-id) or the originator exchange OX ID (src-dst-ox-id, the default) for load balancing path selection.
About VSAN Creation

A VSAN is in the operational state if the VSAN is active and at least one port is up. This state indicates that traffic can pass through this VSAN. This state cannot be configured.

Creating VSANs Statically

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

To create and configure VSANs using Fabric Manager, follow these steps:

Step 1
Click the Create VSAN icon (see Figure 2-4).

Figure 2-4 Create VSAN Icon

You see the Create VSAN dialog box in Figure 2-5.
Step 2  Check the switches that you want in this VSAN.

Step 3  Fill in the VSAN Name and VSAN ID fields.

Step 4  Set the LoadBalancing value and the InterOperValue.

Step 5  Set the Admin State to active or suspended.

Step 6  Check the Static Domain Ids check box to assign an unused static domain ID to the VSAN.

Step 7  (Optional) Select the FICON and Enable Fabric Binding for Selected Switches options if you want these features enabled.

See the “Configuring FICON” section on page 12-1 and refer to the Cisco MDS 9000 Family NX-OS Security Configuration Guide for details.

Step 8  Complete the fields in this dialog box and click Create to add the VSAN or click Close.

About Port VSAN Membership

Port VSAN membership on the switch is assigned on a port-by-port basis. By default, each port belongs to the default VSAN. You can assign VSAN membership to ports using one of two methods:

- Statically—By assigning VSANs to ports.
Assigning Static Port VSAN Membership

To statically assign VSAN membership for an interface using Fabric Manager, follow these steps:

Step 1  Choose Interfaces > FC Physical from the Physical Attributes pane. You see the interface configuration in the Information pane.

Step 2  Click the General tab.

You see the Fibre Channel general physical information. Double-click and complete the PortVSAN field.

Step 3  Click Apply Changes to save these changes, or click Undo Changes to discard any unsaved changes.

About the Default VSAN

The factory settings for switches in the Cisco MDS 9000 Family have only the default VSAN 1 enabled. We recommend that you do not use VSAN 1 as your production environment VSAN. If no VSANs are configured, all devices in the fabric are considered part of the default VSAN. By default, all ports are assigned to the default VSAN.

Note  VSAN 1 cannot be deleted, but it can be suspended.

Note  Up to 256 VSANs can be configured in a switch. Of these, one is a default VSAN (VSAN 1), and another is an isolated VSAN (VSAN 4094). User-specified VSAN IDs range from 2 to 4093.

About the Isolated VSAN

VSAN 4094 is an isolated VSAN. All non-trunking ports are transferred to this VSAN when the VSAN to which they belong is deleted. This avoids an implicit transfer of ports to the default VSAN or to another configured VSAN. All ports in the deleted VSAN are isolated (disabled).

Note  When you configure a port in VSAN 4094 or move a port to VSAN 4094, that port is immediately isolated.

Caution  Do not use an isolated VSAN to configure ports.
Displaying Isolated VSAN Membership

To display interfaces that exist in the isolated VSAN using Fabric Manager, follow these steps:

Step 1. Expand Fabricxx and then select All VSANs in the Logical Domains pane.
You see the VSAN configuration in the Information pane.

Step 2. Click the Isolated Interfaces tab.
You see the interfaces that are in the isolated VSAN.

Operational State of a VSAN

A VSAN is in the operational state if the VSAN is active and at least one port is up. This state indicates that traffic can pass through this VSAN. This state cannot be configured.

About Static VSAN Deletion

When an active VSAN is deleted, all of its attributes are removed from the running configuration. VSAN-related information is maintained by the system software as follows:

- VSAN attributes and port membership details are maintained by the VSAN manager. This feature is affected when you delete a VSAN from the configuration. When a VSAN is deleted, all the ports in that VSAN are made inactive and the ports are moved to the isolated VSAN. If the same VSAN is recreated, the ports do not automatically get assigned to that VSAN. You must explicitly reconfigure the port VSAN membership (see Figure 2-6).
VSAN Configuration

Send documentation comments to mdsfeedback-doc@cisco.com

Figure 2-6 VSAN Port Membership Details

VSAN-based runtime (name server), zoning, and configuration (static routes) information is removed when the VSAN is deleted.

Configured VSAN interface information is removed when the VSAN is deleted.

Note

The allowed VSAN list is not affected when a VSAN is deleted (refer to the Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide).

Any commands for a nonconfigured VSAN are rejected. For example, if VSAN 10 is not configured in the system, then a command request to move a port to VSAN 10 is rejected.

Deleting Static VSANs

To delete a VSAN and its attributes using Fabric Manager, follow these steps:

Step 1

Select All VSANs from the Logical Domains pane.

The VSANs in the fabric are listed in the Information pane.

Step 2

Right-click the VSAN that you want to delete and select Delete Row from the drop-down menu (see Figure 2-7).
You see a confirmation dialog box.

**Step 3** Click **Yes** to confirm the deletion or **No** to close the dialog box without deleting the VSAN.

---

### About Load Balancing

Load balancing attributes indicate the use of the source-destination ID (src-dst-id) or the originator exchange OX ID (src-dst-ox-id, the default) for load balancing path selection.

### Configuring Load Balancing

To configure load balancing on an existing VSAN using Fabric Manager, follow these steps:

**Step 1** Choose **Fabricxx > All VSANs** from the Logical Domains pane.

You see the VSAN configuration in the Information pane shown in Figure 2-8.

**Figure 2-8 All VSAN Attributes**

You see a confirmation dialog box.

**Step 3** Click **Yes** to confirm the deletion or **No** to close the dialog box without deleting the VSAN.

---

### About Load Balancing

Load balancing attributes indicate the use of the source-destination ID (src-dst-id) or the originator exchange OX ID (src-dst-ox-id, the default) for load balancing path selection.

### Configuring Load Balancing

To configure load balancing on an existing VSAN using Fabric Manager, follow these steps:

**Step 1** Choose **Fabricxx > All VSANs** from the Logical Domains pane.

You see the VSAN configuration in the Information pane shown in Figure 2-8.

**Figure 2-8 All VSAN Attributes**

**Step 2** Select a VSAN and complete the LoadBalancing field.
Click **Apply Changes** to save these changes, or click **Undo Changes** to discard any unsaved changes.

### About Interop Mode

Interoperability enables the products of multiple vendors to come into contact with each other. Fibre Channel standards guide vendors towards common external Fibre Channel interfaces. See the “Switch Interoperability” section on page 13-8.

### About FICON VSANs

You can enable FICON in up to eight VSANs. See the “FICON VSAN Prerequisites” section on page 12-7.

### Host Provisioning Wizard

The Host Provisioning wizard provides an intuitive way to commission a new host or decommission an existing host without having to use multiple tools and features. The wizard allows you to create a device alias, and configure DPVM, zoning, and flow creation.

This section includes the following topics:

- Commissioning a Host, page 2-12
- Decommissioning a Host, page 2-16

### Commissioning a Host

To commission a new host, follow these steps:

#### Step 1
From the Fabric Manager window, select **Tools > Host Provisioning**.

The Host Provisioning wizard window is displayed (Figure 2-9).
Step 2  Click the Commission radio button.

Step 3  Click [...] and select the host from the existing configurations or VSAN (see Figure 2-10), or enter the WWN of a host that is not in VSAN or not configured yet.
If the host configuration already exists, the switch, device alias, and VSAN information are populated in the window.

If the configuration does not exist already, enter a device alias for the WWN, enter a switch where the configuration will be initiated, and select a VSAN to which the host should belong. The entries are created and saved when you click Next in the Host Provisioning wizard window.

**Step 4** Uncheck the **Skip Zoning** check box.

The Select Targets (Figure 2-11) and the Select Zone (Figure 2-12) windows will after you click Next.

**Step 5** Uncheck the **Skip DPVM** check box.

The DPVM entries are created when you click Next.

**Step 6** Click **Next**.

The Select Targets window appears.
The Host Provisioning wizard requires that basic and enhanced device alias, DPVM, and CFS to be enabled in all switches in the selected VSAN.

**Step 7**
Select the target with which the host needs to communicate, and click **Add** (Figure 2-11).
The target entry is moved to the bottom of the window.

**Step 8**
Click **Next**.
The Select Zone window appears.
Step 9  Select a Zone, and check the **Create Flow after Activation** check box.

The host and storage are added to a zone and the zone is activated, and a flow between host and storage is created when you click Finish.

Step 10  Click **Finish**.

The device alias and DPVM entries are created, zone is created and activated, and the flow is created based on the check boxes you checked.

**Decommissioning a Host**

To decommission an existing host, follow these steps:

Step 1  From the Fabric Manager window, select **Tools > Host Provisioning**.

The Select Host window appears (Figure 2-13).
Step 2  Click the **Decommission** radio button.

Step 3  Click [...] and select the host from the existing configurations or VSAN, or enter the WWN of a host that is not in VSAN.

The device alias and DPVM state from all of the switches in the selected VSAN are populated if device alias with CFS and CFS DPVM are enabled, and the WWN is an eight-byte number. The device alias entry is removed when you click Finish.

Step 4  Uncheck the **Skip Zoning** check box.

The WWN zone member is removed from all zones. If the zones without a WWN member become single member zones, then, these zones are also removed. If there is a local active zonerset change due to removal of zones, then the appropriate zonerset is activated when you click Finish.

Step 5  Uncheck the **Skip DPVM** check box.

The DPVM entry is removed when you click Finish.

Step 6  Click **Next**
Step 7 Check the **Remove Flow after Deactivation** check box.
The flow entry associated with the host is removed when you click Finish.

Step 8 Click **Finish**.
The device alias and DPVM entries are deleted, the zone is deactivated and deleted if it has only one member after removing the host, and the flow is deleted depending on the check boxes you checked.

**Default Settings**

Table 2-2 lists the default settings for all configured VSANs.
### Default Settings

Table 2-2  Default VSAN Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default VSAN</td>
<td>VSAN 1.</td>
</tr>
<tr>
<td>State</td>
<td>Active state.</td>
</tr>
<tr>
<td>Name</td>
<td>Concatenation of VSAN and a four-digit string representing the VSAN ID. For example, VSAN 3 is VSAN0003.</td>
</tr>
<tr>
<td>Load-balancing attribute</td>
<td>OX ID (src-dst-ox-id).</td>
</tr>
</tbody>
</table>
Configuring SAN Device Virtualization

This chapter describes how to configure virtual devices to represent physical end devices for switches running Cisco MDS SAN-OS Release 3.1(2) and later, or NX-OS Release 4.1(1a) and later.

Cisco SAN device virtualization (SDV) is a licensed feature included in the Cisco MDS 9000 Family Enterprise package (ENTERPRISE_PKG). Refer to the Cisco NX-OS Family Licensing Guide for details about acquiring licenses.

This chapter includes the following sections:

- About SDV, page 3-1
- Configuring SDV, page 3-4
- Default Settings, page 3-10

About SDV

As of Cisco SAN-OS Release 3.1(2) and NX-OS Release 4.1(1a), you can use Cisco SDV to create virtual devices that represent physical end-devices. Virtualization of SAN devices accelerates swapout or failover to a replacement disk array, and it also minimizes downtime when replacing host bus adapters (HBAs) or when re-hosting an application on a different server.

SAN devices that are virtualized can be either initiators or targets. You can virtualize targets to create a virtual target, and also virtualize initiators to create a virtual initiator. Such configurations do not distinguish between virtual initiators and virtual targets (see Figure 3-1 and Figure 3-2).

Figure 3-1 Target Virtualization
About SDV

Note

While most of the examples in this chapter describe target virtualization, the initiator virtualization functions similarly.

Typically, today’s deployments for handling device failures are designed for high availability (HA), with redundancy being a key part of this design. Consider the situation where a target is designed to be redundant. Two arrays are deployed—a primary and secondary in this situation. Enterprises often use some type of consistency technology (such as EMF SRDF) between the primary and secondary arrays to ensure that the secondary is a mirrored copy of the production LUN. However, if the primary array fails, it must be replaced by the secondary because all I/O must occur on the secondary array. Problems can occur because the time required to bring the secondary array up and have it working often takes longer than most can afford (Figure 3-3 illustrates this dilemma).

If a storage array is replaced without using Cisco SDV, then it may require the following actions:

- Taking down a server to modify zoning and account for the new array.
- Changing the Cisco NX-OS configuration to accommodate Fibre Channel IDs (FC IDs) and pWWNs of the new array.
- Changing a server configuration to accommodate the new FC IDs and pWWNs.

More specifically, without SDV you might experience the following conditions:

- It can take a considerable amount of time to configure a secondary device for a typical production environment.
- In the zoning configuration, all the initiators must be rezoned with the secondary device, and certain initiators must also be reconfigured. For example, the WWN and FC ID of the secondary device are different, so driver files must be changed and the server must be rebooted.
Send documentation comments to mdsfeedback-doc@cisco.com

- Clustering (multiple initiators) compounds the problem, and the failover procedure must be repeated for each server of the cluster. Think of a server cluster as a set of HBAs—any storage array FC ID changes must be performed for each HBA.

SDV enables you to achieve the following performance targets:

- Reduce the amount of time it takes for data migration, and ultimately the overall amount of downtime.
- Easily scale to larger numbers of devices.

Figure 3-4 illustrates the benefits of SDV. In this configuration, disk array Y replaces disk array X. When disk array X was deployed, the user created virtual devices for all the Fibre Channel interfaces using SDV. After data replication from disk array X was completed, the user briefly pauses activity on the application server and relinked disk array Y to the virtual devices used by the server, completing the swapout of disk array X. No zoning changes or host operating system configuration changes were required during the time-critical period when the swap was performed; this significantly minimized application downtime.

The array administrator will likely have to perform actions on array Y for it to become a primary device and accept server logins before linking the virtual device to the array Y pWWN.

Figure 3-4 SDV Example

Key Concepts

The following terms are used throughout this chapter:

- Virtual device—The virtualized or proxy representation of the real device, which is registered with the name server and has a pWWN and FC ID. A virtual device exists as long as its real (physical) counterpart is online. The virtual device pWWN and FC ID must be unique and cannot clash with any real device pWWNs and FC IDs.
- Virtual domain—Reserved by SDV to assign FC IDs to virtual devices. If the switch that reserved the domain goes down, another switch takes over its role using the same domain.
- Primary device—The device that is configured as primary. By default, the primary device becomes the active device if it is online.
Configuring SDV

SDV is a distributed service and uses Cisco Fabric Services (CFS) distribution to synchronize the databases. When you configure SDV, it starts a CFS session and locks the fabric. When a fabric is locked, Cisco NX-OS software does not allow any configuration changes from a switch other than the switch holding the lock—and issues a message to inform users about the locked status. Configuration changes are held in a pending database for the application. You must perform a commit operation to make the configuration active and to release the lock for all switches.

Refer to the Cisco MDS 9000 Family NX-OS System Management Configuration Guide for more details about CFS.

When you enable SDV, CFS distribution is also enabled; CFS distribution cannot be disabled for SDV.

The following sections describe how to configure SDV:
- Configuring a Virtual Device, page 3-4
- Linking a Virtual Device with a Physical Device, page 3-7
- Resolving Fabric Merge Conflicts, page 3-8

Configuring a Virtual Device

A virtual device is identified by an alphanumeric name of up to 32 characters and defines all the real devices (one primary and one or more secondary) that it represents. Upon the successful creation of a virtual device, the virtual device name is internally registered as the device alias name with the device alias database; the pWWN is automatically assigned by the system using Cisco Organizational Unique
Identifier (OUI). A virtual device appears as a real, physical device. You can enumerate up to 128 devices for a virtual device. There is a limit of 4095 on the number of virtual devices that you can create in a single VSAN.

Figure 3-5 shows a configuration that includes a new virtual device, vt1.

![Creating a Virtual Device](image)

As of MDS NX-OS Release 4.1(1a), the following conditions must be considered when configuring the virtual device failover attributes:

- The attribute configuration is supported only with MDS NX-OS Release 4.1(1a) and later. In a mixed mode fabric where earlier releases are combined, the attribute configuration will fail.
- When the failover attribute is configured, if the primary device is offline then the secondary device becomes active.
- When the failover attribute is deleted after the primary device failover to the secondary device, then the primary becomes active if the primary device is online. If the primary device is not online, then the SDV virtual device is shut down.

**Note**

The SDV attributes configuration is supported in MDS Fabric Manager Release 4.1(2) and later.

To configure a virtual target and commit it to the fabric configuration using Fabric Manager, follow these steps:

**Step 1** Expand SAN in the Logical Domains pane. Then expand the fabric in which your VSAN resides.

**Step 2** Expand the VSAN in which you wish to create the virtual target and select SDV. You see the switches in the VSAN that you selected listed in the Information pane.

**Step 3** In the Control tab, select **enable** from the drop-down menu in the Command column to enable SAN device virtualization for a particular switch in the VSAN (see Figure 3-6).
Step 4  Click the **Apply Changes** icon to commit the configuration change.

Step 5  Click the **CFS** tab. Confirm that the SAN device virtualization feature is enabled for the switch.

Step 6  Click the **Virtual Devices** tab and then click the **Create Row** icon.

You see the Create Virtual Devices dialog box (see Figure 3-7).

**Figure 3-7  Create Virtual Devices Dialog Box**

Step 7  Select the Virtual Device ID from the drop-down list (ranges from 1 to 4096).

Step 8  Enter a Name for the Virtual Device. Select the Virtual Domain and enter a Virtual FC ID for the virtual target.

Step 9  Check only the autoFailover check box, or check the autoFailover and primFallback check boxes. For more information, see the “Automatic Failover and Fallback” section on page 3-4. You can also change the option in the Option column of the Virtual Devices tab. (See Figure 3-8).
Configuring SDV

Send documentation comments to mdsfeedback-doc@cisco.com

Figure 3-8  Virtual Devices tab

<table>
<thead>
<tr>
<th>Control</th>
<th>CFS</th>
<th>Virtual Devices</th>
<th>Root Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master</td>
<td>VISAN Id, Id</td>
<td>Name</td>
<td>Virtual Domain</td>
</tr>
<tr>
<td>172.22.47.24 1, 1</td>
<td>abc</td>
<td>0x0000000000000000000000000000000000000000000000000</td>
<td>0x0000000000000000000000000000000000000000000000000</td>
</tr>
<tr>
<td>172.22.47.24 1, 2</td>
<td>efg</td>
<td>0x0000000000000000000000000000000000000000000000000</td>
<td>0x0000000000000000000000000000000000000000000000000</td>
</tr>
</tbody>
</table>

Step 10  Click Create to create the virtual target.

Step 11  Click the CFS icon to commit and distribute the configuration changes.

The pWWN of the virtual target does not appear in the zoning end devices database in Fabric Manager. If you want to zone the virtual device with a pWWN, you must enter it in the Add Member to Zone dialog box when creating a zone. However, if the device alias is in enhanced mode, the virtual device names appear in the device alias database in the Fabric Manager zoning window. In this case, users can choose to select either the device alias name or enter the pWWN in the Add Member to Zone dialog box.

For more information, see the “Adding Zone Members” section on page 5-14.

Set the device alias mode to enhanced when using SDV (because the pWWN of a virtual device could change).

For example, SDV is enabled on a switch and a virtual device is defined. SDV assigns a pWWN for the virtual device, and it is zoned based on the pWWN in a zone. If you later disable SDV, this configuration is lost. If you reenable SDV and create the virtual device using the same name, there is no guarantee that it will get the same pWWN again. You would have to rezone the pWWN-based zone. However, if you perform zoning based on the device-alias name, there are no configuration changes required if or when the pWWN changes.

Be sure you understand how device alias modes work before enabling them. Refer to Chapter 6, “Distributing the Device Alias Database” for details and requirements about device alias modes.

Linking a Virtual Device with a Physical Device

After creating a virtual device and configuring it as part of a zone, you can define the primary device for it using the link command, which is also used to fail over to the secondary device.

Note  When a link operation fails over to the secondary device, the virtual device is taken offline, and then brought online.

As of MDS NX-OS Release 4.1(1a), the following conditions must be considered before linking a device:

- If you link to the secondary device which is currently active because of failover, the primary tag is moved to the secondary device and the secondary device becomes the primary device.
- When the secondary device is active, if you link to a third device, and if the fallback attribute was not configured, the third device becomes the primary device but the secondary device continues to be the active device.
When the secondary device is active, if you link to a third device, and if the fallback attribute was configured, then the third device becomes the primary device as well as the active device.

To link a virtual target with a physical target using Fabric Manager, follow these steps:

**Step 1** Click the Real Devices tab and then click the Create Row icon.

**Step 2** Select the Virtual Device ID from the pull-down list or enter an existing ID for the virtual target that you are linking with a physical target (see Figure 3-9).

**Step 3** Select the Real Device ID of the physical target that you are linking with the virtual target.

**Step 4** Choose either the pWWN or device Alias radio button, and select the appropriate pWWN or device alias from the pull-down menu. Note that the Name field is automatically populated when you select the pWWN or device alias.

**Step 5** Choose either the primary or secondary radio button for the Map Type.

**Step 6** Click the CFS icon to save and distribute these changes, or click Close to discard any unsaved changes.

### Resolving Fabric Merge Conflicts

Whenever two fabrics merge SDV merges its database. A merge conflict can occur when there is a run-time information conflict or configuration mismatch. Run-time conflicts can occur due to:

- Identical pWWNs being assigned to different virtual devices
- The same virtual devices are assigned different pWWNs.
- The virtual device and virtual FC ID are mismatched.
A blank commit is a commit operation that does not contain configuration changes, and enforces the SDV configuration of the committing switch fabric-wide. A blank commit operation resolves merge conflicts by pushing the configuration from the committing switch throughout the fabric, which reinitializes the conflicting virtual devices. Exercise caution while performing this operation, as it can easily take some virtual devices offline.

Merge failures resulting from a pWWN conflict can cause a failure with the device alias as well. A blank commit operation on a merge-failed VSAN within SDV should resolve the merge failure in the device alias.

You can avoid merge conflicts due to configuration mismatch by ensuring that:

- The pWWN and device alias entries for a virtual device are identical (in terms of primary and secondary).
- There are no virtual device name conflicts across VSANs in fabrics.

**SDV Requirements and Guidelines**

Be aware of the following requirements and guidelines as you plan and configure SDV:

- SDV should be enabled on switches where devices that are part of SDV zones are connected.
- SDV does not work for devices connected to non-MDS switches.
- Broadcast zoning is not supported for a zone with a virtual device.
- IVR and SDV cannot be used for the same device. A SDV-virtualized device cannot be part of a IVR zone or zoneset.
- Virtual device names should be unique across VSANs because they are registered with the device alias server, which is unaware of VSANs. For example, if you have enabled SDV and have registered a name, vt1 in both VSAN 1 and VSAN 2, then the device alias server cannot store both entries because they have the same name.
- You cannot specify the same primary device for different virtual devices.
- SDV does not work with soft zoning (Soft zoning means that zoning restrictions are applied only during interaction between the name server and the end device. If an end device somehow knows the FC ID of a device outside its zone, it can access that device), nor does it work with the zone default-zone permit vsan operation (which would otherwise permit or deny traffic to members in the default zone).
- If devices are not already zoned with the initiators, then you can configure SDV virtual device zones with no negative impact. If they are already zoned, then zoning changes are required.
- The real device-virtual device zone cannot coexist with the real device-real device zone. If the real devices are not already zoned together, then you can configure the real device-virtual device zone with no negative impact. If these devices are already zoned, then adding the real device-virtual device zone may cause the zone activation to fail. If this occurs, then you must delete one of the zones before activation.

For example, a user attempts to create a configuration with zone A, which consists of I, the initiator, and T, the target (I,T), and zone B, which consists of a virtual initiator, VI, and real target, T (zone VI, T). Such a configuration would fail. Likewise, an attempt to configure zone C, which consists of an initiator, I, and target T, with zone D, which consists of an initiator, I, and virtual target, VT (zone I, VT), would also fail.
There must be at least one SDV-enabled switch that is not a Cisco MDS 9124 Switch between the server and the device that are being virtualized. SDV does not work when initiators and primary devices are connected to the same Cisco MDS 9124 Switch.

**Default Settings**

Table 3-1 lists the default settings for SDV parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disabled</td>
</tr>
</tbody>
</table>
Creating Dynamic VSANs

Port VSAN membership on the switch is assigned on a port-by-port basis. By default each port belongs to the default VSAN.

You can dynamically assign VSAN membership to ports by assigning VSANs based on the device WWN. This method is referred to as Dynamic Port VSAN Membership (DPVM). DPVM offers flexibility and eliminates the need to reconfigure the port VSAN membership to maintain fabric topology when a host or storage device connection is moved between two Cisco MDS switches or two ports within a switch. It retains the configured VSAN regardless of where a device is connected or moved. To assign VSANs statically, see Chapter 2, “Configuring and Managing VSANs.”

This chapter includes the following sections:

- DPVM, page 4-1
- DPVM Database Distribution, page 4-10
- Database Merge Guidelines, page 4-13
- Default Settings, page 4-15

DPVM

DPVM configurations are based on port world wide name (pWWN) and node world wide name (nWWN) assignments. A DPVM database contains mapping information for each device pWWN/nWWN assignment and the corresponding VSAN. The Cisco NX-OS software checks the database during a device FLOGI and obtains the required VSAN details.

The pWWN identifies the host or device and the nWWN identifies a node consisting of multiple devices. You can assign any one of these identifiers or any combination of these identifiers to configure DPVM mapping. If you assign a combination, then preference is given to the pWWN.

DPVM uses the Cisco Fabric Services (CFS) infrastructure to allow efficient database management and distribution. DPVM uses the application driven, coordinated distribution mode and the fabric-wide distribution scope (for information about CFS, refer to the Cisco MDS 9000 Family NX-OS System Management Configuration Guide).

Note

DPVM does not cause any changes to device addressing. DPVM only pertains to the VSAN membership of the device, ensuring that the host gets the same VSAN membership on any port on the switch. For example, if a port on the switch has a hardware failure, you can move the host connection to another port on the switch and you do not need to update the VSAN membership manually.
This section describes DPVM and includes the following topics:

- About DPVM Configuration, page 4-2
- Configuring DPVM with the DPVM Wizard, page 4-2
- Figure 4-2DPVM Setup Wizard: Select Master Switch, page 4-3
- Configuring DPVM Config and Pending Databases, page 4-5
- Activating DPVM Config Databases, page 4-7
- Viewing the Pending Database, page 4-8
- About Autolearned Entries, page 4-8
- Enabling Autolearning, page 4-9
- Clearing Learned Entries, page 4-9

### About DPVM Configuration

To use the DPVM feature as designed, be sure to verify the following requirements:

- The interface through which the dynamic device connects to the Cisco MDS 9000 Family switch must be configured as an F port.
- The static port VSAN of the F port should be valid (not isolated, not suspended, and in existence).
- The dynamic VSAN configured for the device in the DPVM database should be valid (not isolated, not suspended, and in existence).

**Note**

The DPVM feature overrides any existing static port VSAN membership configuration. If the VSAN corresponding to the dynamic port is deleted or suspended, the port is shut down.

To begin configuring DPVM, you must explicitly enable DPVM on the required switches in the fabric. By default, this feature is disabled in all switches in the Cisco MDS 9000 Family.

### Configuring DPVM with the DPVM Wizard

To use the DPVM Setup Wizard in Fabric Manager to set up dynamic port VSAN membership, follow these steps:

**Step 1**

Click the **DPVM Setup Wizard** icon in the Fabric Manager toolbar (See Figure 4-1).
Send documentation comments to mdsfeedback-doc@cisco.com

Figure 4-1 DPVM Wizard Icon

Step 2 Click the switch you want to be the master switch. This switch controls the distribution of the DPVM database to other switches in the fabric.

Step 3 Click Next.

You see the AutoLearn Current End Devices page.

Step 4 (Optional) Click the Create Configuration From Currently Logged In End Devices check box if you want to turn on autolearning.

Step 5 Click Next.

You see the Edit and Activate Configuration page.

Step 6 Verify the current or autolearned configuration. Optionally, click Insert to add more entries into the DPVM config database.

Step 7 Click Finish to update the DPVM config database, distribute the changes using CFS, and activate the database, or click Cancel to exit the DPVM Setup Wizard without saving changes.

Figure 4-2 DPVM Setup Wizard: Select Master Switch

Step 8 Select the switch you want to be the master switch. This switch controls the distribution of the DPVM database to other switches in the fabric.

Step 9 Click Next.

You see the AutoLearn Current End Devices page as shown in Figure 4-3.
Figure 4-3  DPVM Setup Wizard: AutoLearn Current End Devices

Step 10  (Optional) Check the Create Configuration From Currently Logged In End Devices check box if you want to enable autolearning.

Step 11  Click Next.

You see the Edit and Activate Configuration page as shown in Figure 4-4.

Figure 4-4  DPVM Setup Wizard: Edit and Activate Configuration

Step 12  Verify the current or autolearned configuration. Optionally, click Insert to add more entries into the DPVM config database.
Step 13  Click **Finish** to update the DPVM config database, distribute the changes using CFS, and activate the database, or click **Cancel** to exit the DPVM Setup Wizard without saving changes.

**About DPVM Databases**

The DPVM database consists of a series of device mapping entries. Each entry consists of a device pWWN or nWWN assignment along with the dynamic VSAN to be assigned. You can configure a maximum of 16,000 DPVM entries in the DPVM database. This database is global to the whole switch (and fabric) and is not maintained for each VSAN.

The DPVM feature uses three databases to accept and implement configurations.

- **Configuration (config) database**—All configuration changes are stored in the configuration database when distribution is disabled.
- **Active database**—The database currently enforced by the fabric.
- **Pending database**—All configuration changes are stored in the DPVM pending database when distribution is enabled (see the “DPVM Database Distribution” section on page 4-10).

Changes to the DPVM config database are not reflected in the active DPVM database until you activate the DPVM config database. Changes to the DPVM pending database are not reflected in the config or active DPVM database until you commit the DPVM pending database. This database structure allows you to create multiple entries, review changes, and let the DPVM config and pending databases take effect.

Figure 4-5 shows an example of the DPVM databases in the Information pane in Fabric Manager.

**Figure 4-5   DPVM Configuration in Fabric Manager**

![Fabric Manager 3.1(2b) [admin@localhost] /SAN/Fabric sw172-22-46-220](image)

**Configuring DPVM Config and Pending Databases**

To create and populate the config and pending databases using Fabric Manager, follow these steps:

**Step 1**  Expand **Fabricxx > All VSANs** and then select **DPVM** in the Logical Attributes pane.
You see the DPVM configuration in the Information pane.

**Step 2**  Click the **CFS** tab and select a master switch by checking a check box in the Master column.
**Note** You must click on the CFS tab inorder to activate the other tabs.

**Step 3** Click the **Config Database** tab and then click the **Create Row** to insert a new entry.

You see the Create Config Database dialog box shown in Figure 4-6.

![Create Config Database](image)

**Figure 4-6 Create Config Database**

**Step 4** Choose an available WWN and VSAN combination or fill in the pWWN and Login VSAN fields.

**Step 5** Click **Create** to save these changes in the config or pending database or click **Close** to discard any unsaved changes.

**Step 6** Click the **CFS** tab and select the Config Action drop-down menu for the master database.

You see the options shown in Figure 4-7.

![Config Action Drop-down Menu](image)

**Figure 4-7 Config Action Drop-down Menu**

**Step 7** Select **commit** from the drop-down menu to distribute these changes or **abort** to discard the changes.
Activating DPVM Config Databases

When you explicitly activate the DPVM config database, the DPVM config database becomes the active DPVM database. Activation may fail if conflicting entries are found between the DPVM config database and the currently active DPVM database. However, you can force activation to override conflicting entries.

To activate the DPVM config database using Fabric Manager, follow these steps:

**Step 1**
Expand Fabricxx > All VSANs and then select DPVM from the Logical Attributes pane.

You see the DPVM configuration in the Information pane.

**Step 2**
Click the Action tab and set the Action drop-down menu to activate or forceActivate to activate the DPVM config database (see Figure 4-8).

**Figure 4-8 Activate a Configured Database**

**Step 3**
Click the CFS tab and select the Config Action drop-down menu for the master database.

You see the options shown in Figure 4-9.

**Figure 4-9 Config Action Drop-down Menu**

**Step 4**
Select commit from the drop-down menu to distribute these changes or abort to discard the changes.

**Note**
To disable DPVM, you must explicitly deactivate the currently active DPVM database.
Viewing the Pending Database

To view the pending database using Fabric Manager, follow these steps:

**Step 1** Expand **Fabricxxx > All VSANs** and then select **DPVM** from the Logical Attributes pane. You see the DPVM configuration in the Information pane.

**Step 2** Click the **CFS** tab and set the Config View drop-down menu to **pending** (see Figure 4-10).

**Figure 4-10  CFS Tab with Master Switch Checked**

**Step 3** Click **Apply Changes**.

**Step 4** Click the **Config Database** tab. You see the pending database entries.

### About Autolearned Entries

The DPVM database can be configured to automatically learn (autolearn) about new devices within each VSAN. The autolearn feature can be enabled or disabled at any time. Learned entries are created by populating device pWWNs and VSANs in the active DPVM database. The active DPVM database should already be available to enable autolearn.

You can delete any learned entry from the active DPVM database when you enable autolearn. These entries only become permanent in the active DPVM database when you disable autolearn.

**Note**

Autolearning is only supported for devices connected to F ports. Devices connected to FL ports are not entered into the DPVM database because DPVM is not supported on FL ports.

The following conditions apply to learned entries:

- If a device logs out while autolearn is enabled, that entry is automatically deleted from the active DPVM database.
- If the same device logs multiple times into the switch through different ports, then the VSAN corresponding to last login is remembered.
- Learned entries do not override previously configured and activated entries.
- Learning is a two-part process—Enabling autolearning followed by disabling autolearning. When the **auto-learn** option is enabled, the following applies:
  - Learning currently logged-in devices—Occurs from the time learning is enabled.
Enabling Autolearning

To enable autolearning using Fabric Manager, follow these steps:

---

**Step 1** Expand **Fabricxx > All VSANs** and then select **DPVM** from the Logical Attributes pane. You see the DPVM configuration in the Information pane.

**Step 2** Click the **Actions** tab and check the **Auto Learn Enable** check box to enable autolearning (see Figure 4-11).

**Figure 4-11 DPVM Actions Tab**

---

**Step 3** Click the **CFS** tab and select **commit** to distribute these changes or **abort** to discard the changes.

Clearing Learned Entries

You can clear DPVM entries from the active DPVM database (if autolearn is still enabled) using one of two methods.

To clear a single autolearn entry using Fabric Manager, follow these steps:

---

**Step 1** Expand **Fabricxx > All VSANs** and then select **DPVM** from the Logical Attributes pane. You see the DPVM configuration in the Information pane.

**Step 2** Click the **Actions** tab and select **clearOnWWN** from the Auto Learn Clear drop-down menu.

**Step 3** Check the **clear WWN** check box next to the WWN of the autolearned entry that you want to clear.

**Step 4** Click **CFS** and select **commit** to distribute these changes or **abort** to discard the changes.

To clear all autolearn entries using Fabric Manager, follow these steps:

---

**Step 1** Expand **Fabricxx > All VSANs** and then select **DPVM** from the Logical Attributes pane. You see the DPVM configuration in the Information pane.

**Step 2** Click the **Actions** tab. You see the DPVM Actions menu shown in Figure 4-12.
Step 3  Select clear from the Auto Learn Clear drop-down menu.

Step 4  Click the CFS tab and select commit to distribute these changes or abort to discard the changes.

Note  These two procedures do not start a session and can only be issued in the local switch.

**DPVM Database Distribution**

If the DPVM database is available on all switches in the fabric, devices can be moved anywhere and offer the greatest flexibility. To enable database distribution to the neighboring switches, the database should be consistently administered and distributed across all switches in the fabric. The Cisco NX-OS software uses the Cisco Fabric Services (CFS) infrastructure to achieve this requirement (refer to the *Cisco MDS 9000 Family NX-OS System Management Configuration Guide*).

This section describes how to distribute the DPVM database and includes the following topics:

- About DPVM Database Distribution, page 4-10
- Disabling DPVM Database Distribution, page 4-11
- About Locking the Fabric, page 4-11
- Locking the Fabric, page 4-11
- Committing Changes, page 4-12
- Discarding Changes, page 4-13
- Clearing a Locked Session, page 4-13

**About DPVM Database Distribution**

Using the CFS infrastructure, each DPVM server learns the DPVM database from each of its neighboring switches during the ISL bring-up process. If you change the database locally, the DPVM server notifies its neighboring switches, and that database is updated by all switches in the fabric.

If fabric distribution is enabled, all changes to the configuration database are stored in the DPVM pending database. These changes include the following tasks:

- Adding, deleting, or modifying database entries.
- Activating, deactivating, or deleting the configuration database.
- Enabling or disabling autolearning.
These changes are distributed to all switches in a fabric when you commit the changes. You can also discard (abort) the changes at this point.

**Tip**
See the “Viewing the Pending Database” section on page 4-8 to view the contents of the pending database.

### Disabling DPVM Database Distribution

These changes are distributed to all switches in a fabric when you commit the changes. You can also discard (abort) the changes at this point.

**Tip**
See the “Viewing the Pending Database” section on page 4-8 to view the contents of the pending database.

To disable DPVM database distribution to the neighboring switches using Fabric Manager, follow these steps:

1. Expand **Fabricxx > All VSANs** and then select **DPVM** from the Logical Attributes pane. You see the DPVM configuration in the Information pane.
2. Click the **CFS** tab and select **disable** from the Admin drop-down menu.
3. Click **Apply Changes** to save this change or click **Undo Changes** to discard the change.

### About Locking the Fabric

The first action that modifies the existing configuration creates the DPVM pending database and locks the feature in the fabric. Once you lock the fabric, the following conditions apply:

- No other user can make any configuration changes to this feature.
- A copy of the configuration database becomes the DPVM pending database. Modifications from this point on are made to the DPVM pending database. The DPVM pending database remains in effect until you commit the modifications to the DPVM pending database or discard (abort) the changes to the DPVM pending database.

### Locking the Fabric

To lock the fabric and apply changes to the DPVM pending database using Fabric Manager, follow these steps:

1. Expand **Fabricxx > All VSANs** and then select **DPVM** from the Logical Attributes pane. You see the DPVM configuration in the Information pane.
2. Click the **Config Database** tab and **Create Row**.
   You see the Create Config Database dialog box shown in Figure 4-13.
Step 3  Choose an available pWWN and login VSAN.

Step 4  Click **Create** to save this change to the pending database or click **Close** to discard any unsaved change.

---

**Committing Changes**

If you commit the changes made to the configuration, the configuration in the DPVM pending database are distributed to other switches. On a successful commit, the configuration change is applied throughout the fabric and the lock is released.

To commit the DPVM pending database using Fabric Manager, follow these steps:

Step 1  Expand **Fabric> All VSANs** and then select **DPVM** from the Logical Attributes pane.

Step 2  Click the **CFS** tab and select **commit from** the Config Action drop-down menu.

Step 3  Click **Apply Changes** to save this change or click **Undo Changes** to discard the change.
Discarding Changes

If you discard (abort) the changes made to the DPVM pending database, the configurations remain unaffected and the lock is released.

To discard the DPVM pending database using Fabric Manager, follow these steps:

Step 1: Expand Fabricxx > All VSANs and then select DPVM from the Logical Attributes pane. You see the DPVM configuration in the Information pane.

Step 2: Click the CFS tab and select abort from the Config Action drop-down menu.

Step 3: Click Apply Changes to save this change or click Undo Changes to discard the change.

Clearing a Locked Session

If you have performed a DPVM task and have forgotten to release the lock by either committing or discarding the changes, an administrator can release the lock from any switch in the fabric. If the administrator performs this task, your changes to the DPVM pending database are discarded and the fabric lock is released.

Tip: The DPVM pending database is only available in the volatile directory and is subject to being discarded if the switch is restarted.

To use administrative privileges and release a locked DPVM session using Fabric Manager, follow these steps:

Step 1: Expand Fabricxx > All VSANs and then select DPVM from the Logical Attributes pane. You see the DPVM configuration in the Information pane.

Step 2: Click the CFS tab and select clear from the Config Action drop-down menu.

Step 3: Click Apply Changes to save this change or click Undo Changes to discard the change.

Database Merge Guidelines

A database merge refers to a union of the configuration database and static (unlearned) entries in the active DPVM database. For information about CFS merge support, refer to the Cisco MDS 9000 Family NX-OS System Management Configuration Guide for detailed concepts.

When merging the DPVM database between two fabrics, follow these guidelines:

- Verify that the activation status and the auto-learn status is the same is both fabrics.
- Verify that the combined number of device entries in each database does not exceed 16 K.
Database Merge Guidelines

Caution
If you do not follow these two conditions, the merge will fail. The next distribution will forcefully synchronize the databases and the activation states in the fabric.

This section describes how to merge DPVM databases and includes the following topics:
- About Copying DPVM Databases, page 4-14
- Copying DPVM Databases, page 4-14
- Comparing Database Differences, page 4-14

About Copying DPVM Databases

The following circumstances may require the active DPVM database to be copied to the DPVM config database:
- If the learned entries are only added to the active DPVM database.
- If the DPVM config database or entries in the DPVM config database are accidently deleted.

Note
If you copy the DPVM database and fabric distribution is enabled, you must commit the changes.

Copying DPVM Databases

To copy the currently active DPVM database to the DPVM config database using Fabric Manager, follow these steps:

Step 1 Expand Fabricxx> All VSANs and then select DPVM in the Logical Attributes pane.
You see the DPVM configuration in the Information pane.

Step 2 Click the Actions tab and check the CopyActive to Config check box.

Step 3 Click the CFS tab and select commit from the Config Action drop-down menu.

Comparing Database Differences

To compare the currently active database entries to the DPVM config database using Fabric Manager, follow these steps:

Step 1 Expand Fabricxx> All VSANs and then select DPVM from the Logical Attributes pane.
You see the DPVM active database in the Information pane.

Step 2 Click the Active Database tab.
You see the DPVM active database in the Information pane.

Step 3 Select Config from the Compare With drop-down menu.
You see the comparison dialog box.
Step 4
Select Close to close the comparison dialog box.

Default Settings

Table 4-1 lists the default settings for DPVM parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPVM</td>
<td>Disabled.</td>
</tr>
<tr>
<td>DPVM distribution</td>
<td>Enabled.</td>
</tr>
<tr>
<td>Autolearning</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>
Configuring and Managing Zones

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

Advanced zoning capabilities specified in the FC-GS-4 and FC-SW-3 standards are provided. You can use either the existing basic zoning capabilities or the advanced, standards-compliant zoning capabilities.

This chapter includes the following sections:

- About Zoning, page 5-1
- Using the Quick Config Wizard, page 5-7
- Zone Configuration, page 5-10
- Zone Sets, page 5-16
- Zone Set Distribution, page 5-28
- Zone Set Duplication, page 5-31
- Advanced Zone Attributes, page 5-37
- Displaying Zone Information, page 5-44
- Enhanced Zoning, page 5-45
- Compacting the Zone Database for Downgrading, page 5-49
- Default Settings, page 5-50

Note

Table 2-1 on page 2-4 lists the differences between zones and VSANs.

About Zoning

Zoning has the following features:

- A zone consists of multiple zone members.
  - Members in a zone can access each other; members in different zones cannot access each other.
  - If zoning is not activated, all devices are members of the default zone.
  - If zoning is activated, any device that is not in an active zone (a zone that is part of an active zone set) is a member of the default zone.
About Zoning

- Zones can vary in size.
- Devices can belong to more than one zone.
- A physical fabric can have a maximum of 16,000 members. This includes all VSANs in the fabric.

- A zone set consists of one or more zones.
- A zone set can be activated or deactivated as a single entity across all switches in the fabric.
- Only one zone set can be activated at any time.
- A zone can be a member of more than one zone set.
- A zone switch can have a maximum of 500 zone sets.

- 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.
  - If a new switch is added to an existing fabric, zone sets are acquired by the new switch.

- Zone changes can be configured nondisruptively. New zones and zone sets can be activated without interrupting traffic on unaffected ports or devices.

- Zone membership criteria is based mainly on WWNs or FC IDs.
  - Port world wide name (pWWN)—Specifies the pWWN of an N port attached to the switch as a member of the zone.
  - Fabric pWWN—Specifies the WWN of the fabric port (switch port’s WWN). This membership is also referred to as port-based zoning.
  - FC ID—Specifies the FC ID of an N port attached to the switch as a member of the zone.
  - Interface and switch WWN (sWWN)—Specifies the interface of a switch identified by the sWWN. This membership is also referred to as interface-based zoning.
  - Interface and domain ID—Specifies the interface of a switch identified by the domain ID.
  - Domain ID and port number—Specifies the domain ID of an MDS domain and additionally specifies a port belonging to a non-Cisco switch.
  - IPv4 address—Specifies the IPv4 address (and optionally the subnet mask) of an attached device.
  - IPv6 address—The IPv6 address of an attached device in 128 bits in colon(:)-separated hexadecimal format.

- Default zone membership includes all ports or WWNs that do not have a specific membership association. Access between default zone members is controlled by the default zone policy.
- You can configure up to 8000 zones per VSAN and a maximum of 8000 zones for all VSANs on the switch.

Zoning Example

Figure 5-1 illustrates a zone set with two zones, zone 1 and zone 2, in a fabric. Zone 1 provides access from all three hosts (H1, H2, H3) to the data residing on storage systems S1 and S2. Zone 2 restricts the data on S3 to access only by H3. Note that H3 resides in both zones.
Chapter 5 Configuring and Managing Zones

Send documentation comments to mdsfeedback-doc@cisco.com

Figure 5-1 Fabric with Two Zones

![Fabric with Two Zones Diagram]

Of course, there are other ways to partition this fabric into zones. Figure 5-2 illustrates another possibility. Assume that there is a need to isolate storage system S2 for the purpose of testing new software. To achieve this, zone 3 is configured, which contains only host H2 and storage S2. You can restrict access to just H2 and S2 in zone 3, and to H1 and S1 in zone 1.

Figure 5-2 Fabric with Three Zones

![Fabric with Three Zones Diagram]

Zone Implementation

All switches in the Cisco MDS 9000 Family automatically support the following basic zone features (no additional configuration is required):

- Zones are contained in a VSAN.
- Hard zoning cannot be disabled.
- Name server queries are soft-zoned.
- Only active zone sets are distributed.
- Unzoned devices cannot access each other.
- A zone or zone set with the same name can exist in each VSAN.
Each VSAN has a full database and an active database.

Active zone sets cannot be changed, without activating a full zone database.

Active zone sets are preserved across switch reboots.

Changes to the full database must be explicitly saved.

Zone reactivation (a zone set is active and you activate another zone set) does not disrupt existing traffic.

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

- Propagate full zone sets to all switches on a per VSAN basis.
- Change the default policy for unzoned members.
- Interoperate with other vendors by configuring a VSAN in the interop mode. You can also configure one VSAN in the interop mode and another VSAN in the basic mode in the same switch without disrupting each other.
- Bring E ports out of isolation.

### Zone Member Configuration Guidelines

All members of a zone can communicate with each other. For a zone with N members, $N^N(N-1)$ access permissions need to be enabled. The best practice is to avoid configuring large numbers of targets or large numbers of initiators in a single zone. This type of configuration wastes switch resources by provisioning and managing many communicating pairs (initiator-to-initiator or target-to-target) that will never actually communicate with each other. For this reason, a single initiator with a single target is the most efficient approach to zoning.

The following guidelines must be considered when creating zone members:

- Configuring only one initiator and one target for a zone provides the most efficient use of the switch resources.
- Configuring the same initiator to multiple targets is accepted.
- Configuring multiple initiators to multiple targets is not recommended.

### Active and Full Zone Set Considerations

Before configuring a zone set, consider the following guidelines:

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

An FC ID or Nx port that is not part of the active zone set belongs to the default zone and the default zone information is not distributed to other switches.

Note

If one zone set is active and you activate another zone set, the currently active zone set is automatically deactivated. You do not need to explicitly deactivate the currently active zone set before activating a new zone set.

Figure 5-3 shows a zone being added to an activated zone set.
About Zoning

Figure 5-3  Active and Full Zone Sets

Full zone set

Zone set Z1
Zone A
Zone B
Zone C

Zone set Z2
Zone C
Zone D
Zone E

Zone set Z3
Zone A
Zone C
Zone D

Full zone set

No active Zone set

Zone set Z1
Zone A
Zone B
Zone C

Zone set Z2
Zone C
Zone D
Zone E

Zone set Z3
Zone A
Zone C
Zone D

Full zone set

Active zone set

Zone set Z1
Zone A
Zone B
Zone C

Zone set Z2
Zone C
Zone D
Zone E

Zone set Z3
Zone A
Zone C
Zone D

After activating Zone set Z1

Active zone set

Zone set Z1
Zone A
Zone B
Zone C

Zone set Z2
Zone C
Zone D
Zone E

Zone set Z3
Zone A
Zone C
Zone D

After adding Zone D to Zone set Z1

Active zone set

Zone set Z1
Zone A
Zone B
Zone C

Zone set Z2
Zone C
Zone D
Zone E

Zone set Z3
Zone A
Zone C
Zone D

After activating Zone set Z1 again

Full zone set

-zone-
Using the Quick Config Wizard

**Note**
The Quick Config Wizard supports only switch interface zone members.

As of Cisco SAN-OS Release 3.1(1) and NX-OS Release 4.1(2), you can use the Quick Config Wizard on the Cisco MDS 9124 Switch to add or remove zone members per VSAN. You can use the Quick Config Wizard to perform interface-based zoning and to assign zone members for multiple VSANs using Device Manager.

**Note**
The Quick Config Wizard is supported on the Cisco MDS 9124 Fabric Switch, the Cisco MDS 9134 Fabric Switch, the Cisco Fabric Switch for HP c-Class BladeSystem, and the Cisco Fabric Switch for IBM BladeCenter.

**Caution**
The Quick Config Wizard can only be used on stand-alone switches that do not have any existing zoning defined on the switch.

To add or remove ports from a zone and to zone only the devices within a specific VSAN using Device Manager on the Cisco MDS 9124 Switch, follow these steps:

**Step 1**
Choose **FC > Quick Config** or click the **Zone** icon in the toolbar.

You see the Quick Config Wizard (see Figure 5-5) with all controls disabled and the Discrepancies dialog box (see Figure 5-4), which shows all unsupported configurations.

**Note**
You will see the Discrepancies dialog box only if there are any discrepancies.
Step 2   Click **OK** to continue.

You see the Quick Config Wizard dialog box shown in Figure 5-5.

⚠️ **Caution** If there are discrepancies and you click **OK**, the affected VSANs in the zone databases are cleared. This may become disruptive if the switch is in use.
Step 3: Check the check box in the Ports Zoned To column for the port you want to add or remove from a zone. The check box for the matching port is similarly set. The selected port pair is added or removed from the zone, creating a two-device zone. The VSAN drop-down menu provides a filter that enables you to zone only those devices within a selected VSAN.

Step 4: Right-click any of the column names to show or hide a column.

Step 5: Click Next to verify the changes.

You see the Confirm Changes dialog box shown in Figure 5-6.
Chapter 5: Configuring and Managing Zones

Zone Configuration

This section describes how to configure zones and includes the following topics:

- About the Edit Local Full Zone Database Tool, page 5-11
- Configuring a Zone Using the Zone Configuration Tool, page 5-12
- Adding Zone Members, page 5-14

---

**Figure 5-6  Confirm Changes Dialog Box**

Step 6  If you want to see the CLI commands, right-click in the dialog box and click **CLI Commands** from the pop-up menu.

Step 7  Click **Finish** to save the configuration changes.
About the Edit Local Full Zone Database Tool

The Edit Local Full Zone Database tool allows you to zone across multiple switches and all zoning features are available through the Edit Local Full Zone Database dialog box (see Figure 5-7).

**Figure 5-7 Edit Local Full Zone Database Dialog Box**

1. You can display information by VSAN by using the drop-down menu without closing the dialog box, selecting a VSAN, and re-entering.

2. You can use the *Add to zone* button to move devices up or down by alias or by zone.

3. You can add zoning characteristics based on alias in different folders.

4. You can triple-click to rename zone sets, zones, or aliases in the tree.

**Note**

The Device Alias radio button is visible only if device alias is in enhanced mode. For more information, see “Creating a Device Alias” section on page 6-6.

**Tip**

Expand *Switches* from the Physical Attributes pane to retrieve the sWNN. If you do not provide a sWNN, the software automatically uses the local sWNN.
Note: Interface-based zoning only works with Cisco MDS 9000 Family switches. Interface-based zoning does not work if interop mode is configured in that VSAN.

Configuring a Zone Using the Zone Configuration Tool

To create a zone and move it into a zone set using Fabric Manager, follow these steps:

Step 1 Click the Zone icon in the toolbar (See Figure 5-8).

Figure 5-8 Zone Icon

You see the Select VSAN dialog box.

Step 2 Select the VSAN where you want to create a zone and click OK.

You see the Edit Local Full Zone Database dialog box shown in Figure 5-9.

Figure 5-9 Edit Local Full Zone Database Dialog Box

If you want to view zone membership information, right-click in the All Zone Membership(s) column, and then click Show Details for the current row or all rows from the pop-up menu.

Step 3 Click Zones in the left pane and click the Insert icon to create a zone.
You see the Create Zone dialog box shown in Figure 5-10.

**Figure 5-10 Create Zone Dialog Box**

Step 4 Enter a zone name.

Step 5 Check one of the following check boxes:
   a. **Read Only**—The zone permits read and denies write.
   b. **Permit QoS Traffic with Priority**—You set the priority from the drop-down menu.
   c. **Restrict Broadcast Frames to Zone Members**

Step 6 Click **OK** to create the zone.

If you want to move this zone into an existing zone set, skip to Step 8.

Step 7 Click **Zoneset** in the left pane and click the **Insert** icon to create a zone set.

You see the Zoneset Name dialog box shown in Figure 5-11.

**Figure 5-11 Zoneset Name Dialog Box**

Step 8 Enter a zone set name and click **OK**.

**Note** One of these symbols ($, -, ^, _) or all alphanumeric characters are supported. In interop mode 2 and 3, this symbol ( _) or all alphanumeric characters are supported.

Step 9 Select the zone set where you want to add a zone and click the **Insert** icon or you can drag and drop Zone3 over Zoneset1.

You see the Select Zone dialog box shown in Figure 5-12.
Adding Zone Members

Once you create a zone, you can add members to the zone. You can add members using multiple port identification types.

To add a member to a zone using Fabric Manager, follow these steps:

**Step 1** Choose Zone > Edit Local Full Zone Database.
You see the Select VSAN dialog box.

**Step 2** Select a VSAN and click OK.
You see the Edit Local Full Zone Database dialog box for the selected VSAN.

---

Figure 5-12 Select Zone Dialog Box

**Figure 5-13 Edit Local Full Zone Database Dialog Box**
Send documentation comments to mdsfeedback-doc@cisco.com

Step 3 Select the members you want to add from the Fabric pane (see Figure 5-13) and click Add to Zone or click the zone where you want to add members and click the Insert icon.

You see the Add Member to Zone dialog box shown in Figure 5-14.

Figure 5-14 Add Member to Zone Dialog Box

![Add Member to Zone Dialog Box](image)

**Note** The Device Alias radio button is visible only if device alias is in enhanced mode. For more information, see “Creating a Device Alias” section on page 6-6.

Step 4 Click the browse button and select a port name or check the LUN check box and click the browse button to configure LUNs.

Step 5 Click Add to add the member to the zone.

**Note** When configuring a zone member, you can specify that a single LUN has multiple IDs depending on the operating system. You can select from six different operating systems.

Filtering End Devices Based on Name, WWN or FC ID

To filter the end devices and device aliases, follow these steps:

Step 1 Click the Zone icon in the toolbar (See Figure 5-8).

Step 2 Select Name, WWN or FC ID from the With drop-down list.

Step 3 Enter a filter condition, such as *zo1*, in the Filter text box.

Step 4 Click Go.
Adding Multiple End Devices to Multiple Zones

To add multiple end devices to multiple zones, follow these steps:

1. Click the Zone icon in the toolbar (See Figure 5-8).
2. Use the Ctrl key to select multiple end devices.
3. Right-click and then select Add to Zone.
4. Use the Ctrl key to select multiple zones from the pop-up window displayed.
5. Click Add.

Selected end devices are added to the selected zones.

Zone Sets

Zones provide a mechanism for specifying access control, while zone sets are a grouping of zones to enforce access control in the fabric.

This section describes zone sets and includes the following topics:

- About Zone Set Creation, page 5-16
- Activating a Zone Set, page 5-18
- Displaying Zone Membership Information, page 5-21
- About the Default Zone, page 5-21
- Configuring the Default Zone, page 5-22
- About FC Alias Creation, page 5-22
- Creating FC Aliases, page 5-23
- Adding Members to Aliases, page 5-23
- Converting Zone Members to pWWN-based Members, page 5-25
- Zone Enforcement, page 5-27

About Zone Set Creation

In Figure 5-15, two separate sets are created, each with its own membership hierarchy and zone members.
Either zone set A or zone set B can be activated (but not together).

**Tip**

Zone sets are configured with the names of the member zones and the VSAN (if the zone set is in a configured VSAN).
Activating a Zone Set

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

To activate an existing zone set using Fabric Manager, follow these steps:

**Step 1** Choose Zone > Edit Local Full Zone Database.
You see the Select VSAN dialog box.

**Step 2** Select a VSAN and click OK.
You see the Edit Local Full Zone Database dialog box for the selected VSAN.

**Step 3** Click Activate to activate the zone set.
You see the pre-activation check dialog box shown in Figure 5-16.

**Figure 5-16 Pre-Activation Check Dialog Box**

![Pre-activation check dialog box](image)

**Step 4** Click Yes to review the differences.
You see the Local vs. Active Differences dialog box shown in Figure 5-17.

**Figure 5-17 Local vs Active Differences Dialog Box**

![Local vs Active Differences dialog box](image)

**Step 5** Click Close to close the dialog box.
You see the Save Configuration dialog box shown in Figure 5-18.
Send documentation comments to mdsfeedback-doc@cisco.com

Figure 5-18 Save Configuration Dialog Box

Step 6 Check the Save Running to Startup Configuration check box to save all changes to the startup configuration.

Step 7 Click Continue Activation to activate the zone set, or click Cancel to close the dialog box and discard any unsaved changes.

You see the Zone Log dialog box, which shows if the zone set activation was successful (see Figure 5-19).

Figure 5-19 Zone Log Dialog Box

Deactivating a Zoneset

To deactivate an existing zone set, follow these steps:

Step 1 Right-click the zone set you want to deactivate and then click Deactivate from the pop-up menu.

You see the Deactivate Zoneset dialog box as shown in Figure 5-20.
Step 2 Enter deactivate in the text box and then click **OK**.

You see the Input dialog box as shown in **Figure 5-21**.

**Figure 5-21 Input Dialog Box**

Step 3 Enter deactivate in the text box and then click **OK** to deactivate the zone set.

**Note**

To enable this option, you need to modify the server.properties file. Refer to the *Cisco Fabric Manager Fundamentals Configuration Guide* to know more about modifying server.properties file.
Displaying Zone Membership Information

To display zone membership information for members assigned to zones in Fabric Manager, follow these steps:

**Step 1** Choose **Zone > Edit Local Full Zone Database**.
You see the Select VSAN dialog box.

**Step 2** Select a VSAN and click **OK**.
You see the Edit Local Full Zone Database dialog box for the selected VSAN.

**Step 3** Click **Zones** in the left pane. The right pane lists the members for each zone.

**Note** The default zone members are explicitly listed only when the default zone policy is configured as **permit**. When the default zone policy is configured as **deny**, the members of this zone are not shown. See the “Displaying Zone Information” section on page 5-44.

About the Default Zone

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

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

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

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

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

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

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

You can change the default zone policy for any VSAN by choosing **VSCANxx > Default Zone** from the Fabric Manager menu tree and clicking the **Policies** tab. It is recommended that you establish connectivity among devices by assigning them to a non-default zone.
Configuring the Default Zone

To permit or deny traffic to members in the default zone using Fabric Manager, follow these steps:

**Step 1**
Expand a VSAN and then select **Default Zone** in the Fabric Manager Logical Domains pane.

**Step 2**
Click the **Policies** tab in the Information pane.

You see the zone policies information in the Information pane (see Figure 5-22).

**Figure 5-22 Default Zone Policies**

The active zone set is shown in italic type. After you make changes to the active zone set and before you activate the changes, the zone set is shown in boldface italic type.

**Step 3**
In the Default Zone Behaviour field, choose either **permit** or **deny** from the drop-down menu.

### About FC Alias Creation

You can assign an alias name and configure an alias member using the following values:

- **pWWN**—The WWN of the N or NL port is in hex format (for example, 10:00:00:23:45:67:89:ab).
- **fWWN**—The WWN of the fabric port name is in hex format (for example, 10:00:00:23:45:67:89:ab).
- **FC ID**—The N port ID is in 0xhhhhhh format (for example, 0xce00d1).
- **Domain ID**—The domain ID is an integer from 1 to 239. A mandatory port number of a non-Cisco switch is required to complete this membership configuration.
- **IPv4 address**—The IPv4 address of an attached device is in 32 bits in dotted decimal format along with an optional subnet mask. If a mask is specified, any device within the subnet becomes a member of the specified zone.
- **IPv6 address**—The IPv6 address of an attached device is in 128 bits in colon- (:) separated) hexadecimal format.
- **Interface**—Interface-based zoning is similar to port-based zoning because the switch interface is used to configure the zone. You can specify a switch interface as a zone member for both local and remote switches. To specify a remote switch, enter the remote switch WWN (sWWN) or the domain ID in the particular VSAN.

**Tip**

The Cisco NX-OS software supports a maximum of 2048 aliases per VSAN.
Creating FC Aliases

To create an FC alias using Fabric Manager, follow these steps:

1. Choose Zone > Edit Local Full Zone Database.
   You see the Select VSAN dialog box.
2. Select a VSAN and click OK.
   You see the Edit Local Full Zone Database dialog box for the selected VSAN.
3. Click Aliases in the lower left pane (see Figure 5-23). The right pane lists the existing aliases.
4. Click the Insert icon to create an alias.
   You see the Create Alias dialog box shown in Figure 5-24.
5. Set the Alias Name and the pWWN.
6. Click OK to create the alias.

Adding Members to Aliases

To add a member to an alias using Fabric Manager, follow these steps:
Step 1  Choose Zone > Edit Local Full Zone Database.
You see the Select VSAN dialog box.

Step 2  Select a VSAN and click OK.
You see the Edit Local Full Zone Database dialog box for the selected VSAN as shown in Figure 5-25.

Figure 5-25  Edit Local Full Zone Database Dialog Box

Step 3  Select the member(s) you want to add from the Fabric pane (see Figure 5-25) and click Add to Alias or click the alias where you want to add members and click the Insert icon.
You see the Add Member to Alias dialog box shown in Figure 5-26.


**Note**  The Device Alias radio button is visible only if device alias is in enhanced mode. For more information, see “Creating a Device Alias” section on page 6-6.

**Step 4**  Click the browse button and select a port name or check the LUN check box and click the browse button to configure LUNs.

**Step 5**  Click **Add** to add the member to the alias.

---

**Converting Zone Members to pWWN-based Members**

You can convert zone and alias members from switch port or FC ID based membership to pWWN-based membership. You can use this feature to convert to pWWN so that your zone configuration does not change if a card or switch is changed in your fabric.

To convert switch port and FC ID members to pWWN members using Fabric Manager, follow these steps:

**Step 1**  Choose **Zone > Edit Local Full Zone Database**.

You see the Select VSAN dialog box.

**Step 2**  Select a VSAN and click **OK**.

You see the Edit Local Full Zone Database dialog box for the selected VSAN.

**Step 3**  Click the zone you want to convert.

**Step 4**  Choose **Tools > Convert Switch Port/FCID members to By pWWN**.

You see the conversion dialog box, listing all members that will be converted.

**Step 5**  Verify the changes and click **Continue Conversion**.
Step 6  Click Yes in the confirmation dialog box to convert that member to pWWN-based membership.

Note  If one zone set is active and you activate another zone set, the currently active zone set is automatically deactivated.

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

Caution  If you deactivate the active zone set in a VSAN that is also configured for IVR, the active IVR zone set (IVZS) is also deactivated and all IVR traffic to and from the switch is stopped. This deactivation can disrupt traffic in more than one VSAN. Before deactivating the active zone set, check the active zone analysis for the VSAN. To reactivate the IVZS, you must reactivate the regular zone set (refer to the Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide).

Caution  If the currently active zone set contains IVR zones, activating the zone set from a switch where IVR is not enabled disrupts IVR traffic to and from that VSAN. We strongly recommend that you always activate the zone set from an IVR-enabled switch to avoid disrupting IVR traffic.

Note  The pWWN of the virtual target does not appear in the zoning end devices database in Fabric Manager. If you want to zone the virtual device with a pWWN, you must enter it in the Add Member to Zone dialog box when creating a zone. However, if the device alias is in enhanced mode, the virtual device names appear in the device alias database in the Fabric Manager zoning window. In this case, users can choose to select either the device alias name or enter the pWWN in the Add Member to Zone dialog box.

For more information, see the “Adding Zone Members” section on page 5-14.

Note  Set the device alias mode to enhanced when using SDV (because the pWWN of a virtual device could change).

For example, SDV is enabled on a switch and a virtual device is defined. SDV assigns a pWWN for the virtual device, and it is zoned based on the pWWN in a zone. If you later disable SDV, this configuration is lost. If you reenable SDV and create the virtual device using the same name, there is no guarantee that it will get the same pWWN again. Hence, you would have to rezone the pWWN-based zone. However, if you perform zoning based on the device-alias name, there are no configuration changes required if or when the pWWN changes.

Be sure you understand how device alias modes work before enabling them. Refer to Chapter 6, “Distributing Device Alias Services” for details and requirements about device alias modes.
Filtering Zones, Zone Sets, and Device Aliases Based on Name

To filter the zones, zone sets or device aliases, follow these steps:

- **Step 1** Click the Zone icon in the toolbar (See Figure 5-8).
- **Step 2** Enter a filter condition, such as *zo1*, in the Filter text box.
- **Step 3** Click Go.

Adding Multiple Zones to Multiple Zone Sets

To add multiple zones to multiple zone sets, follow these steps:

- **Step 1** Click the Zone icon in the toolbar (See Figure 5-8).
- **Step 2** From the tree view, select Zoneset.
- **Step 3** Use the Ctrl key to select multiple zones.
- **Step 4** Right-click and then select Add to Zoneset.
- **Step 5** Use the Ctrl key to select multiple zone sets from the pop-up window displayed.
- **Step 6** Click Add.

Selected zones are added to the selected zone sets.

Zone Enforcement

Zoning can be enforced in two ways: soft and hard. Each end device (N port or NL port) discovers other devices in the fabric by querying the name server. When a device logs in to the name server, the name server returns the list of other devices that can be accessed by the querying device. If an Nx port does not know about the FC IDs of other devices outside its zone, it cannot access those devices.

In soft zoning, zoning restrictions are applied only during interaction between the name server and the end device. If an end device somehow knows the FC ID of a device outside its zone, it can access that device.

Hard zoning is enforced by the hardware on each frame sent by an Nx port. As frames enter the switch, source-destination IDs are compared with permitted combinations to allow the frame at wirespeed. Hard zoning is applied to all forms of zoning.

**Note**

Hard zoning enforces zoning restrictions on every frame, and prevents unauthorized access.

Switches in the Cisco MDS 9000 Family support both hard and soft zoning.
Zone Set Distribution

You can distribute full zone sets using one of two methods: one-time distribution or full zone set distribution. Table 5-1 lists the differences between these distribution methods.

<table>
<thead>
<tr>
<th>Table 5-1 Zone Set Distribution Differences</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>One-Time Distribution</strong></td>
</tr>
<tr>
<td>Distributes the full zone set immediately.</td>
</tr>
<tr>
<td>Does not distribute the full zone set information along with the active zone set during activation, deactivation, or merge process.</td>
</tr>
</tbody>
</table>

This section describes zone set distribution and includes the following topics:

- Enabling Full Zone Set Distribution, page 5-28
- Enabling a One-Time Distribution, page 5-29
- About Recovering from Link Isolation, page 5-29
- Importing and Exporting Zone Sets, page 5-30

**Enabling Full Zone Set Distribution**

All switches in the Cisco MDS 9000 Family distribute active zone sets when new E port links come up or when a new zone set is activated in a VSAN. The zone set distribution takes effect while sending merge requests to the adjacent switch or while activating a zone set.

To enable full zone set and active zone set distribution to all switches on a per VSAN basis using Fabric Manager, follow these steps:

**Step 1**
Expand a VSAN and select a zone set in the Logical Domains pane.
You see the zone set configuration in the Information pane. The Active Zones tab is the default.

**Step 2**
Click the Policies tab.
You see the configured policies for the zone (see Figure 5-27).
Enabling a One-Time Distribution

You can perform a one-time distribution of inactive, unmodified zone sets throughout the fabric. To propagate a one-time distribution of the full zone set using Fabric Manager, follow these steps:

Step 1 Choose Zone > Edit Local Full Zone Database.

You see the Edit Local Full Zone Database dialog box.

Step 2 Click the appropriate zone from the list in the left pane.

Step 3 Click Distribute to distribute the full zone set across the fabric.

This procedure only distributes the full zone set information; it does not save the information to the startup configuration. You must explicitly save the running configuration to the startup configuration issue the to save the full zone set information to the startup configuration.

Note

The one-time distribution of the full zone set is supported in interop 2 and interop 3 modes, not in interop 1 mode.

About Recovering from Link Isolation

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

- Import the neighboring switch's active zone set database and replace the current active zone set (see Figure 5-28).
Zone Set Distribution

Send documentation comments to mdsfeedback-doc@cisco.com

- Export the current database to the neighboring switch.
- Manually resolve the conflict by editing the full zone set, activating the corrected zone set, and then bringing up the link.

Figure 5-28  Importing and Exporting the Database

Importing and Exporting Zone Sets

To import or export the zone set information from or to an adjacent switch using Fabric Manager, follow these steps:

Step 1  Choose Tools > Zone Merge Fail Recovery.
You see the Zone Merge Failure Recovery dialog box shown in Figure 5-29.

Figure 5-29  Zone Merge Failure Recovery Dialog Box

Step 2  Click the Import Active Zoneset or the Export Active Zoneset radio button.
Step 3  Select the switch from which to import or export the zone set information from the drop-down list.
Step 4  Select the VSAN from which to import or export the zone set information from the drop-down list.
Zone Set Duplication

You can make a copy and then edit it without altering the existing active zone set. You can copy an active zone set from the bootflash: directory, volatile: directory, or slot0, to one of the following areas:

- To the full zone set
- To a remote location (using FTP, SCP, SFTP, or TFTP)

The active zone set is not part of the full zone set. You cannot make changes to an existing zone set and activate it, if the full zone set is lost or is not propagated.

Caution

Copying an active zone set to a full zone set may overwrite a zone with the same name, if it already exists in the full zone set database.

This section includes the following topics:

- Copying Zone Sets, page 5-31
- About Backing Up and Restoring Zones, page 5-32
- Backing Up Zones, page 5-32
- Renaming Zones, Zone Sets, and Aliases, page 5-35
- Cloning Zones, Zone Sets, FC Aliases, and Zone Attribute Groups, page 5-36
- Migrating a Non-MDS Database, page 5-37
- Clearing the Zone Server Database, page 5-37

Copying Zone Sets

On the Cisco MDS Family switches, you cannot edit an active zone set. However, you can copy an active zone set to create a new zone set that you can edit.

To make a copy of a zone set using Fabric Manager, follow these steps:

Step 1

Choose Edit > Copy Full Zone Database.

You see the Copy Full Zone Database dialog box (Figure 5-30).
Zone Set Duplication

Send documentation comments to mdsfeedback-doc@cisco.com

Figure 5-30 Copy Full Zone Database Dialog Box

Step 2 Click the Active or the Full radio button, depending on which type of database you want to copy.
Step 3 Select the source VSAN from the drop-down list.
Step 4 If you selected Copy Full, select the source switch and the destination VSAN from those drop-down lists.
Step 5 Select the destination switch from the drop-down list.
Step 6 Click Copy to copy the database.

Caution
If the Inter-VSAN Routing (IVR) feature is enabled and if IVR zones exist in the active zone set, then a zone set copy operation copies all the IVR zones to the full zone database. To prevent copying to the IVR zones, you must explicitly remove them from the full zone set database before performing the copy operation. Refer to the Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide for more information on the IVR feature.

About Backing Up and Restoring Zones

You can back up the zone configuration to a workstation using TFTP. This zone backup file can then be used to restore the zone configuration on a switch. Restoring the zone configuration overwrites any existing zone configuration on a switch.

Back up Zones

To back up the full zone configuration using Fabric Manager, follow these steps:

Step 1 Choose Zone > Edit Local Full Zone Database.
You see the Select VSAN dialog box.
Step 2 Select a VSAN and click OK.
You see the Edit Local Full Zone Database dialog box for the selected VSAN as shown in Figure 5-31.
Step 3  Choose **File > Backup > This VSAN Zones** to back up the existing zone configuration to a workstation using TFTP, SFTP, SCP, or FTP.

You see the Backup Zone Configuration dialog box shown in Figure 5-32.

**Figure 5-32  Backup Zone Configuration Dialog Box**

You can edit this configuration before backing up the data to a remote server.

Step 4  Provide the following Remote Options information to back up data onto a remote server:

a. **Using**—Select the protocol.

b. **Server IP Address**—Enter the IP address of the server.
Zone Set Duplication

Send documentation comments to mdsfeedback-doc@cisco.com

c. **UserName**—Enter the name of the user.
d. **Password**—Enter the password for the user.
e. **File Name (Root Path)**—Enter the path and the filename.

**Step 5** Click **Backup** or click **Cancel** to close the dialog box without backing up.

---

### Restoring Zones

To restore the full zone configuration using Fabric Manager, follow these steps:

**Step 1** Choose **Zone > Edit Local Full Zone Database**.

You see the Select VSAN dialog box.

**Step 2** Select a VSAN and click **OK**.

You see the Edit Local Full Zone Database dialog box for the selected VSAN as shown in **Figure 5-33**.

**Figure 5-33**  **Edit Local Full Zone Database**

**Step 3** Choose **File > Restore** to restore a saved zone configuration using TFTP, SFTP, SCP or FTP.

You see the Restore Zone Configuration dialog box shown in **Figure 5-34**.
Step 4 Provide the following **Remote Options** information to restore data from a remote server:

a. **Using**—Select the protocol.

b. **Server IP Address**—Enter the IP address of the server.

c. **UserName**—Enter the name of the user.

d. **Password**—Enter the password for the user.

e. **File Name**—Enter the path and the filename.

Step 5 Click **Restore** to continue or click **Cancel** to close the dialog box without restoring.

**Note**

Click **View Config** to see information on how the zone configuration file from a remote server will be restored. When you click **Yes** in this dialog box, you will be presented with the CLI commands that are executed. To close the dialog box, click **Close**.

**Note**

Backup and Restore options are available to switches that run Cisco NX-OS Release 4.1(3) or later.

### Renaming Zones, Zone Sets, and Aliases

To rename a zone, zone set, or alias using Fabric Manager, follow these steps:

**Step 1** Choose **Zone > Edit Local Full Zone Database**.

You see the Select VSAN dialog box.

**Step 2** Select a VSAN and click **OK**.

You see the Edit Local Full Zone Database dialog box for the selected VSAN (see **Figure 5-35**).
Cloning Zones, Zone Sets, FC Aliases, and Zone Attribute Groups

To clone a zone, zone set, fcalias, or zone attribute group, follow these steps:

Step 1 Choose Zone > Edit Local Full Zone Database.
You see the Select VSAN dialog box.

Step 2 Select a VSAN and click OK.
You see the Edit Local Full Zone Database dialog box for the selected VSAN.

Step 3 Choose Edit > Clone.
You see the Clone Zoneset dialog box shown in Figure 5-36. The default name is the word Clone followed by the original name.
Figure 5-36  Clone Zoneset Dialog Box

Step 4  Change the name for the cloned entry.
Step 5  Click OK to save the new clone.

The cloned database now appears along with the original database.

Migrating a Non-MDS Database

To use the Zone Migration Wizard to migrate a non-MDS database using Fabric Manager, follow these steps:

Step 1  Choose Zone > Migrate Non-MDS Database.
You see the Zone Migration Wizard.
Step 2  Follow the prompts in the wizard to migrate the database.

Clearing the Zone Server Database

You can clear all configured information in the zone server database for the specified VSAN. To clear the zone server database, refer to the Cisco MDS 9000 Family CLI Configuration Guide.

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

Note  After clearing the zone server database, you must explicitly copy the running configuration to the startup configuration to ensure that the running configuration is used when the switch reboots.

Advanced Zone Attributes

This section describes advanced zone attributes and includes the following topics:

- About Zone-Based Traffic Priority, page 5-38
- Configuring Zone-Based Traffic Priority, page 5-38
- Configuring Default Zone QoS Priority Attributes, page 5-39
- Configuring the Default Zone Policy, page 5-40
About Zone-Based Traffic Priority

The zoning feature provides an additional segregation mechanism to prioritize select zones in a fabric and set up access control between devices. Using this feature, you can configure the quality of service (QoS) priority as a zone attribute. You can assign the QoS traffic priority attribute to be high, medium, or low. By default, zones with no specified priority are implicitly assigned a low priority. Refer to the *Cisco MDS 9000 NX-OS Family Quality of Service Configuration Guide* for more information.

To use this feature, you need to obtain the ENTERPRISE_PKG license (refer to the *Cisco NX-OS Family Licensing Guide*) and you must enable QoS in the switch (refer to the *Cisco MDS 9000 Family NX-OS Quality of Service Configuration Guide*).

This feature allows SAN administrators to configure QoS in terms of a familiar data flow identification paradigm. You can configure this attribute on a zone-wide basis rather than between zone members.

**Caution**

If zone-based QoS is implemented in a switch, you cannot configure the interop mode in that VSAN.

Configuring Zone-Based Traffic Priority

To configure the zone priority using Fabric Manager, follow these steps:

1. **Step 1** Expand a VSAN and then select a zone set in the Logical Domains pane.
2. **Step 2** Click the **Policies** tab in the Information pane.

   You see the Zone policy information in the Information pane (see *Figure 5-37*).
Step 3 Use the check boxes and drop-down menus to configure QoS on the default zone.

Step 4 Click Apply Changes to save the changes.

Configuring Default Zone QoS Priority Attributes

QoS priority attribute configuration changes take effect when you activate the zone set of the associated zone.

Note If a member is part of two zones with two different QoS priority attributes, the higher QoS value is implemented. This situation does not arise in the VSAN-based QoS as the first matching entry is implemented.

To configure the QoS priority attributes for a default zone using Fabric Manager, follow these steps:

Step 1 Choose Zone > Edit Local Full Zone Database. You see the Select VSAN dialog box.

Step 2 Select a VSAN and click OK. You see the Edit Local Full Zone Database dialog box for the selected VSAN.

Step 3 Choose Edit > Edit Default Zone Attributes to configure the default zone QoS priority attributes (see Figure 5-38).

Step 4 Check the Permit QoS Traffic with Priority check box and set the Qos Priority drop-down menu to low, medium, or high.
Configuring the Default Zone Policy

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

Step 1  Choose Zone > Edit Local Full Zone Database.
You see the Select VSAN dialog box.

Step 2  Select a VSAN and click OK.
You see the Edit Local Full Zone Database dialog box for the selected VSAN.

Step 3  Choose Edit > Edit Default Zone Attributes to configure the default zone QoS priority attributes.
You see the Modify Default Zone Properties dialog box shown in Figure 5-39.

Figure 5-39  Modify Default Zone Properties Dialog Box

Step 4  Set the Policy drop-down menu to permit to permit traffic in the default zone, or set it to deny to block traffic in the default zone.

Step 5  Click OK to save these changes.

About Broadcast Zoning

Note  Broadcast zoning is not supported on the Cisco Fabric Switch for HP c-Class BladeSystem and the Cisco Fabric Switch for IBM BladeCenter.

You can configure broadcast frames in the basic zoning mode. By default, broadcast zoning is disabled and broadcast frames are sent to all Nx ports in the VSAN. When enabled, broadcast frames are only sent to Nx ports in the same zone, or zones, as the sender. Enable broadcast zoning when a host or storage device uses this feature.

Table 5-2 identifies the rules for the delivery of broadcast frames.
Tip
If any NL port attached to an FL port shares a broadcast zone with the source of the broadcast frame, then the frames are broadcast to all devices in the loop.

Caution
If broadcast zoning is enabled on a switch, you cannot configure the interop mode in that VSAN.

### Configuring Broadcast Zoning

To broadcast frames in the basic zoning mode using Fabric Manager, follow these steps:

**Step 1** Expand a **VSAN** and then select a zone set in the Logical Domains pane.

**Step 2** Click the **Policies** tab in the Information pane.

You see the Zone policy information in the Information pane in **Figure 5-40**.

**Figure 5-40 Zone Policy Information**

![Zone Policy Information](image)

**Step 3** Check the **Broadcast** check box to enable broadcast frames on the default zone.

**Step 4** Click **Apply Changes** to save these changes.

### About LUN Zoning

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Broadcast to all Nx ports that share a broadcast zone with the source of broadcast frames.</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Broadcast to all Nx ports.</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Broadcasting is disabled.</td>
</tr>
</tbody>
</table>
Caution
LUN zoning can only be implemented in Cisco MDS 9000 Family switches. If LUN zoning is implemented in a switch, you cannot configure the interop mode in that switch.

A storage device can have multiple LUNs behind it. If the device port is part of a zone, a member of the zone can access any LUN in the device. With LUN zoning, you can restrict access to specific LUNs associated with a device.

Note
When LUN 0 is not included within a zone, then, as per standards requirements, control traffic to LUN 0 (for example, REPORT_LUNS, INQUIRY) is supported, but data traffic to LUN 0 (for example, READ, WRITE) is denied.

- Host H1 can access LUN 2 in S1 and LUN 0 in S2. It cannot access any other LUNs in S1 or S2.
- Host H2 can access LUNs 1 and 3 in S1 and only LUN 1 in S2. It cannot access any other LUNs in S1 or S2.

Note
Unzoned LUNs automatically become members of the default zone.

Figure 5-41 shows a LUN-based zone example.

**Figure 5-41  LUN Zoning Access**

Configuring a LUN-Based Zone

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

**Step 1** Choose Zone > Edit Local Full Zone Database.
You see the Select VSAN dialog box.

**Step 2** Select a VSAN and click OK.
You see the Edit Local Full Zone Database dialog box for the selected VSAN.

**Step 3** Click the zone where you want to add members and click the Insert icon.
You see the Add Member to Zone dialog box shown in Figure 5-42.
Assigning LUNs to Storage Subsystems

LUN masking and mapping restricts server access to specific LUNs. If LUN masking is enabled on a storage subsystem and if you want to perform additional LUN zoning in a Cisco MDS 9000 Family switch, obtain the LUN number for each host bus adapter (HBA) from the storage subsystem and then configure the LUN-based zone procedure provided in the “Configuring a LUN-Based Zone” section on page 5-42.

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

Caution
If you make any errors when assigning LUNs, you might lose data.

About Read-Only Zones

By default, an initiator has both read and write access to the target’s media when they are members of the same Fibre Channel zone. The read-only zone feature allows members to have only read access to the media within a read-only Fibre Channel zone.

You can also configure LUN zones as read-only zones.

Any zone can be identified as a read-only zone. By default all zones have read-write permission unless explicitly configured as a read-only zone.

Follow these guidelines when configuring read-only zones:

- If read-only zones are implemented, the switch prevents write access to user data within the zone.
- If two members belong to a read-only zone and to a read-write zone, the read-only zone takes priority and write access is denied.
- LUN zoning can only be implemented in Cisco MDS 9000 Family switches. If LUN zoning is implemented in a switch, you cannot configure interop mode in that switch.
- Read-only volumes are not supported by some operating system and file system combinations (for example, Windows NT or Windows 2000 and NTFS file system). Volumes within read-only zones are not available to such hosts. However, if these hosts are already booted when the read-only zones are activated, then read-only volumes are available to those hosts.

The read-only zone feature behaves as designed if either the FAT16 or FAT32 file system is used with the previously mentioned Windows operating systems.
Configuring Read-Only Zones

To configure read-only zones using Fabric Manager, follow these steps:

**Step 1** Choose **Zone > Edit Local Full Zone Database**.
You see the Select VSAN dialog box.

**Step 2** Select a VSAN and click **OK**.
You see the Edit Local Full Zone Database dialog box for the selected VSAN.

**Step 3** Click **Zones** in the left pane and click the **Insert** icon to add a zone.
You see the Create Zone Dialog Box as shown in **Figure 5-43**.

![Create Zone Dialog Box](image)

**Step 4** Check the **Read Only** check box to create a read-only zone.

**Step 5** Click **OK**.

---

**Note**
To configure the read-only option for a default zone, see “Configuring the Default Zone Policy” section on page 5-40.

Displaying Zone Information

To view zone information and statistics using Fabric Manager, follow these steps:

**Step 1** Expand a **VSAN** and select a zone set in the Logical Domains pane.
You see the zone configuration in the Information pane.

**Step 2** Click the **Read Only Violations, Statistics** tab, or **LUN Zoning Statistics** tab to view statistics for the selected zone.
Send documentation comments to mdsfeedback-doc@cisco.com

Enhanced Zoning

The zoning feature complies with the FC-GS-4 and FC-SW-3 standards. Both standards support the basic zoning functionalities explained in the previous section and the enhanced zoning functionalities described in this section.

This section includes the following topics:
- About Enhanced Zoning, page 5-45
- Changing from Basic Zoning to Enhanced Zoning, page 5-46
- Changing from Enhanced Zoning to Basic Zoning, page 5-46
- Enabling Enhanced Zoning, page 5-47
- Creating Attribute Groups, page 5-47
- Merging the Database, page 5-47
- Analyzing a Zone Merge, page 5-48
- Configuring Zone Merge Control Policies, page 5-49

About Enhanced Zoning

Table 5-3 lists the advantages of the enhanced zoning feature in all switches in the Cisco MDS 9000 Family.

<table>
<thead>
<tr>
<th>Basic Zoning</th>
<th>Enhanced Zoning</th>
<th>Enhanced Zoning Advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrators can make simultaneous configuration changes. Upon activation, one administrator can overwrite another administrator’s changes.</td>
<td>Performs all configurations within a single configuration session. When you begin a session, the switch locks the entire fabric to implement the change.</td>
<td>One configuration session for the entire fabric to ensure consistency within the fabric.</td>
</tr>
<tr>
<td>If a zone is part of multiple zone sets, you create an instance of this zone in each zone set.</td>
<td>References to the zone are used by the zone sets as required once you define the zone.</td>
<td>Reduced payload size as the zone is referenced. The size is more pronounced with bigger databases.</td>
</tr>
<tr>
<td>The default zone policy is defined per switch. To ensure smooth fabric operation, all switches in the fabric must have the same default zone setting.</td>
<td>Enforces and exchanges the default zone setting throughout the fabric.</td>
<td>Fabric-wide policy enforcement reduces troubleshooting time.</td>
</tr>
<tr>
<td>To retrieve the results of the activation on a per switch basis, the managing switch provides a combined status about the activation. It does not identify the failure switch.</td>
<td>Retrieves the activation results and the nature of the problem from each remote switch.</td>
<td>Enhanced error reporting eases the troubleshooting process.</td>
</tr>
<tr>
<td>To distribute the zoning database, you must reactivate the same zone set. The reactivation may affect hardware changes for hard zoning on the local switch and on remote switches.</td>
<td>Implements changes to the zoning database and distributes it without reactivation.</td>
<td>Distribution of zone sets without activation avoids hardware changes for hard zoning in the switches.</td>
</tr>
</tbody>
</table>
Changing from Basic Zoning to Enhanced Zoning

To change to the enhanced zoning mode from the basic mode, follow these steps:

Step 1
Verify that all switches in the fabric are capable of working in the enhanced mode.
If one or more switches are not capable of working in enhanced mode, then your request to move to enhanced mode is rejected.

Step 2
Set the operation mode to enhanced zoning mode. By doing so, you will automatically start a session, acquire a fabric wide lock, distribute the active and full zoning database using the enhanced zoning data structures, distribute zoning policies and then release the lock. All switches in the fabric then move to the enhanced zoning mode.

Tip
After moving from basic zoning to enhanced zoning, we recommend that you save the running configuration.

Changing from Enhanced Zoning to Basic Zoning

The standards do not allow you to move back to basic zoning. However, Cisco MDS switches allow this move to enable you to downgrade and upgrade to other Cisco SAN-OS or Cisco NX-OS releases.

To change to the basic zoning mode from the enhanced mode, follow these steps:

Step 1
Verify that the active and full zone set do not contain any configuration that is specific to the enhanced zoning mode.
If such configurations exist, delete them before proceeding with this procedure. If you do not delete the existing configuration, the Cisco NX-OS software automatically removes them.

Step 2
Set the operation mode to basic zoning mode. By doing so, you will automatically start a session, acquire a fabric wide lock, distribute the zoning information using the basic zoning data structure, apply the configuration changes and release the lock from all switches in the fabric. All switches in the fabric then move to basic zoning mode.
Enhanced Zoning

By default, the enhanced zoning feature is disabled in all switches in the Cisco MDS 9000 Family. To enable enhanced zoning in a VSAN using Fabric Manager, follow these steps:

1. Expand a VSAN and then select a zone set in the Logical Domains pane.
2. You see the zone set configuration in the Information pane.
3. Click the **Enhanced** tab.
4. You see the current enhanced zoning configuration.
5. From the Action drop-down menu, choose **enhanced** to enable enhanced zoning in this VSAN.
6. Click **Apply Changes** to save these changes.

Creating Attribute Groups

In enhanced mode, you can directly configure attributes using attribute groups.

To configure attribute groups, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

Merging the Database

The merge behavior depends on the fabric-wide merge control setting:

- **Restrict**—If the two databases are not identical, the ISLs between the switches are isolated.
- **Allow**—The two databases are merged using the merge rules specified in Table 5-4.

### Table 5-4 Database Zone Merge Status

<table>
<thead>
<tr>
<th>Local Database</th>
<th>Adjacent Database</th>
<th>Merge Status</th>
<th>Results of the Merge</th>
</tr>
</thead>
<tbody>
<tr>
<td>The databases contain zone sets with the same name¹ but different zones, aliases, and attributes groups.</td>
<td></td>
<td>Successful.</td>
<td>The union of the local and adjacent databases.</td>
</tr>
<tr>
<td>The databases contain a zone, zone alias, or zone attribute group object with same name¹ but different members.</td>
<td></td>
<td>Failed.</td>
<td>ISLs are isolated.</td>
</tr>
</tbody>
</table>

¹ The same name includes the zone set name and the zone name, or zone alias name, or zone attribute group object name.
Enhanced Zoning

Caution
Remove all non-pWWN-type zone entries on all MDS switches running Cisco SAN-OS prior to merging fabrics if there is a Cisco MDS 9020 switch running FabricWare in the adjacent fabric.

The merge process operates as follows:
1. The software compares the protocol versions. If the protocol versions differ, then the ISL is isolated.
2. If the protocol versions are the same, then the zone policies are compared. If the zone policies differ, then the ISL is isolated.
3. If the zone merge options are the same, then the comparison is implemented based on the merge control setting.
   a. If the setting is restrict, the active zone set and the full zone set should be identical. Otherwise the link is isolated.
   b. If the setting is allow, then the merge rules are used to perform the merge.

Analyzing a Zone Merge

To perform a zone merge analysis using Fabric Manager, follow these steps:

Step 1  Choose Zone > Merge Analysis.
You see the Zone Merge Analysis dialog box shown in Figure 5-44.

Send documentation comments to mdsfeedback-doc@cisco.com

Table 5-4 Database Zone Merge Status (continued)

<table>
<thead>
<tr>
<th>Local Database</th>
<th>Adjacent Database</th>
<th>Merge Status</th>
<th>Results of the Merge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Empty.</td>
<td>Contains data.</td>
<td>Successful.</td>
<td>The adjacent database information populates the local database.</td>
</tr>
<tr>
<td>Contains data.</td>
<td>Empty.</td>
<td>Successful.</td>
<td>The local database information populates the adjacent database.</td>
</tr>
</tbody>
</table>

1. In the enhanced zoning mode, the active zone set does not have a name in interop mode 1. The zone set names are only present for full zone sets.
Configuring Zone Merge Control Policies

To configure merge control policies, refer to the Cisco MDS 9000 Family CLI Configuration Guide. Zone generic service permission setting is used to control zoning operation through generic service (GS) interface. The zone generic service permission can be read-only, read-write or none (deny).

To configure generic service (GS) settings, follow these steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch# config t</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>switch(config)# zone gs read vsan 3000</td>
<td>Configures gs permission value as read only in the specified vsan.</td>
</tr>
<tr>
<td>switch(config)# zone gs read-write vsan 3000</td>
<td>Configures gs permission value as read-write in the specified vsan.</td>
</tr>
<tr>
<td>switch(config)# no zone gs read-write vsan 3000</td>
<td>Configures gs permission value as none(deny) in the specified vsan.</td>
</tr>
</tbody>
</table>

Compacting the Zone Database for Downgrading

Prior to Cisco SAN-OS Release 3.0(1), only 2000 zones are supported per VSAN. If you add more than 2000 zones to a VSAN, a configuration check is registered to indicate that downgrading to a previous release could cause you to lose the zones over the limit. To avoid the configuration check, delete the...
excess zones and compact the zone database for the VSAN. If there are 2000 zones or fewer after deleting the excess zones, the compacting process assigns new internal zone IDs and the configuration can be supported by Cisco SAN-OS Release 2.x or earlier. Perform this procedure for every VSAN on the switch with more than 2000 zones.

**Note**

A merge failure occurs when a switch supports more than 2000 zones per VSAN but its neighbor does not. Also, zone set activation can fail if the switch has more than 2000 zones per VSAN and not all switches in the fabric support more than 2000 zones per VSAN.

To compact the zone database for downgrading, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

### Default Settings

Table 5-5 lists the default settings for basic zone parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default zone policy</td>
<td>Denied to all members.</td>
</tr>
<tr>
<td>Full zone set distribute</td>
<td>The full zone set(s) is not distributed.</td>
</tr>
<tr>
<td>Zone based traffic priority</td>
<td>Low.</td>
</tr>
<tr>
<td>Read-only zones</td>
<td>Read-write attributes for all zones.</td>
</tr>
<tr>
<td>Broadcast frames</td>
<td>Sent to all Nx ports.</td>
</tr>
<tr>
<td>Broadcast zoning</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Enhanced zoning</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>
Distributing Device Alias Services

All switches in the Cisco MDS 9000 Family support Distributed Device Alias Services (device alias) on a per-VSAN basis and on a fabric-wide basis. Device alias distribution allows you to move host bus adapters (HBAs) between VSANs without manually reentering alias names.

This chapter includes the following sections:
- About Device Aliases, page 6-1
- About Device Alias Modes, page 6-1
- Device Alias Databases, page 6-4
- About Legacy Zone Alias Configuration Conversion, page 6-7
- Device Alias Statistics Cleanup, page 6-8
- Default Settings, page 6-9

About Device Aliases

When the port WWN (pWWN) of a device must be specified to configure different features (zoning, QoS, port security) in a Cisco MDS 9000 Family switch, you must assign the correct device name each time you configure these features. An incorrect device name may cause unexpected results. You can avoid this problem if you define a user-friendly name for a port WWN and use this name in all of the configuration commands as required. These user-friendly names are referred to as device aliases in this chapter.

About Device Alias Modes

Device alias supports two modes: basic and enhanced mode.
- When device alias runs in the basic mode, all applications function like the applications on the 3.0 switches. When you configure the basic mode using device aliases, the application immediately expands to pWWNs. This operation continues until the mode is changed to enhanced.
- When device alias runs in the enhanced mode, all applications accept the device-alias configuration in the native format. The applications store the device alias name in the configuration and distribute it in the device alias format instead of expanding to pWWN. The applications track the device alias database changes and take actions to enforce it.
About Device Alias Modes

A native device-alias configuration is not accepted in the interop mode VSAN. IVR zoneset activation will fail in interop mode VSANs if the corresponding twilight zones being injected are native device alias members.

Changing Mode Settings

When the device alias mode is changed from basic to enhanced mode, the applications are informed about the change. The applications start accepting the device alias-based configuration in the native format.

Note
Because the device alias was previously running in the basic mode, the applications do not have any prior native device alias configuration.

The applications check for an existing device alias configuration in the native format. If the device alias is in the native format, the applications reject the request and device alias mode cannot be changed to basic.

All native device alias configurations (both on local and remote switches) must be explicitly removed, or all device alias members must be replaced with the corresponding pWWN before changing the mode back to basic.

The process can be automated using the force option. Use the `no device-alias mode enhanced force` command to enable applications to automatically replace all device alias members with the corresponding pWWNs. If a device alias member does not have a corresponding pWWN mapping in the device alias database, the configuration will be removed.

Device Alias Mode Distribution

If the device alias distribution is turned on, it is distributed to the other switches in the network whenever there is a change in the mode. You cannot change the mode from basic to enhanced unless all the switches are upgraded to Release 3.1. The device alias enhancements will not apply unless the entire fabric is upgraded to Release 3.1.

Note
When all the switches are upgraded to Release 3.1, you cannot automatically convert to enhanced mode. You do not need to change to enhanced mode, you can continue working in the basic mode.

Merging Device Alias

If two fabrics are running different device alias modes and are joined together, the device alias merge will fail. There is no automatic conversion of one mode to the other during the merge process. You will need to resolve the issue.

Note
Release 3.0 switches run in basic mode.

At the application level, a merger takes place between the applications and the fabric. For example, zone merge occurs when the E port is up and the IVR/PSM/DPVM merge occurs due to CFS. This merge is completely independent of the device alias merge.
If the application running on an enhanced fabric has a native device alias configuration, the application must fail the merge. The application has to fail the merge even though the other fabric is can support the native device alias-based configuration, but is running in the basic mode. You will need to resolve the issue. Once the device alias merge issue is resolved, each application must be fixed accordingly.

Resolving Merge and Device Alias Mode Mismatch

If two fabrics are running in different modes and the device alias merge fails between the fabrics, the conflict can be resolved by selecting one mode or the other. If you choose the enhanced mode, ensure that all the switches are running at least the Release 3.1 version. Otherwise, the enhanced mode cannot be turned on. If you choose the basic mode, the applications running on the enhanced fabric have to comply with the device alias merge.

The device alias merge fails because of mode mismatch, but the application merge succeeds if it does not have any native device alias configurations.

If the native device alias configuration is attempted on an application from a Release 3.1 switch, the commit must be rejected because of device alias mode mismatch on some of the applications.

Note

The applications should not accept any native device alias configuration over SNMP if the device alias is running in the basic mode on that particular switch.

Note

Confcheck will be added when the enhanced mode is turned on and removed when it is turned off. Applications have to add confcheck if they have a device alias configuration in the native format. They have to remove confcheck once the configuration is removed.

Device Alias Features

Device aliases have the following features:

- The device alias information is independent of your VSAN configuration.
- The device alias configuration and distribution is independent of the zone server and the zone server database.
- You can import legacy zone alias configurations without losing data.
- The device alias application uses the Cisco Fabric Services (CFS) infrastructure to enable efficient database management and distribution. Device aliases use the coordinated distribution mode and the fabric-wide distribution scope (refer to the Cisco MDS 9000 Family NX-OS System Management Configuration Guide).
- When you configure zones, IVR zones, or QoS features using device aliases, and if you display these configurations, you will automatically see that the device aliases are displayed along with their respective pWWNs.

Device Alias Requirements

Device aliases have the following requirements:

- You can only assign device aliases to pWWNs.
Device Alias Databases

- The mapping between the pWWN and the device alias to which it is mapped must have a one-to-one relationship. A pWWN can be mapped to only one device alias and vice versa.
- A device alias name is restricted to 64 alphanumeric characters and may include one or more of the following characters:
  - a to z and A to Z
  - 1 to 9
  - - (hyphen) and _ (underscore)
  - $ (dollar sign) and ^ (up caret)

Zone Aliases Versus Device Aliases

Table 6-1 compares the configuration differences between zone-based alias configuration and device alias configuration.

<table>
<thead>
<tr>
<th>Zone-Based Aliases</th>
<th>Device Aliases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases are limited to the specified VSAN.</td>
<td>You can define device aliases without specifying the VSAN number. You can also use the same definition in one or more VSANs without any restrictions.</td>
</tr>
<tr>
<td>Zone aliases are part of the zoning configuration. The alias mapping cannot be used to configure other features.</td>
<td>Device aliases can be used with any feature that uses the pWWN.</td>
</tr>
<tr>
<td>You can use any zone member type to specify the end devices.</td>
<td>Only pWWNs are supported along with new device aliases such as IP addresses.</td>
</tr>
<tr>
<td>Configuration is contained within the Zone Server database and is not available to other features.</td>
<td>Device aliases are not restricted to zoning. Device alias configuration is available to the FCNS, zone, fcping, traceroute, and IVR applications.</td>
</tr>
</tbody>
</table>

Device Alias Databases

The device alias feature uses two databases to accept and implement device alias configurations.
- Effective database—The database currently used by the fabric.
- Pending database—Your subsequent device alias configuration changes are stored in the pending database.

If you modify the device alias configuration, you need to commit or discard the changes as the fabric remains locked during this period.

This section includes the following sections:
- About Device Alias Distribution, page 6-5
- Committing Changes, page 6-6
- Discarding Changes, page 6-7
- About Legacy Zone Alias Configuration Conversion, page 6-7
About Device Alias Distribution

By default, device alias distribution is enabled. The device alias feature uses the coordinated distribution mechanism to distribute the modifications to all switches in a fabric.

If you have not committed the changes and you disable distribution, then a commit task will fail.

Distributing the Device Alias Database

To enable the device alias distribution using Fabric Manager, follow these steps:

**Step 1** Expand **End Devices** and then select **Device Alias** in the Physical Attributes pane. You see the device alias configuration in the Information pane Figure 6-1.

**Figure 6-1 Device Aliases in Fabric Manager**

The CFS tab is the default tab.

**Step 2** Select **enable** from the Global drop-down menus to enabled switch aliases.

**Step 3** Select **commit** from the Config Action drop-down menu for the newly enabled switches.

**Step 4** Click **Apply Changes** to commit and distribute these changes or click **Undo Changes** to discard any unsaved changes.

About Creating a Device Alias

When you perform the first device alias task (regardless of which device alias task), the fabric is automatically locked for the device alias feature. Once you lock the fabric, the following situations apply:

- No other user can make any configuration changes to this feature.
A copy of the effective database is obtained and used as the pending database. Modifications from this point on are made to the pending database. The pending database remains in effect until you commit the modifications to the pending database or discard (abort) the changes to the pending database.

Creating a Device Alias

To lock the fabric and create a device alias in the pending database using Fabric Manager, follow these steps:

Step 1
Expand End Devices and then select Device Alias in the Physical Attributes pane. You see the device alias configuration in the Information pane.

Step 2
Click the Configuration tab and click the Create Row icon. You see the Device Alias Creation dialog box in Figure 6-2.

Figure 6-2 Create Device Alias Dialog Box

Step 3
Select a switch from the drop-down menu.

Step 4
Complete the Alias name and pWWN fields.

Step 5
Click Create to create this alias or click Close to discard any unsaved changes.

Committing Changes

If you commit the changes made to the pending database, the following events occur:

1. The pending database contents overwrites the effective database contents.
2. The pending database is emptied of its contents.
3. The fabric lock is released for this feature.

To commit the changes to the device alias database using Fabric Manager, follow these steps:

---

**Step 1**
Expand **End Devices** and then select **Device Alias** in the Physical Attributes pane.

You see the device alias configuration in the Information pane. The **CFS** tab is the default tab.

**Step 2**
Select **enable** from the Global drop-down menus to enabled switch aliases.

**Step 3**
Select **commit** from the Config Action drop-down menu for the newly enabled switches.

**Step 4**
Click **Apply Changes** to commit and distribute these changes or click **Undo Changes** to discard any unsaved changes.

---

**Discarding Changes**

If you discard the changes made to the pending database, the following events occur:

1. The effective database contents remain unaffected.
2. The pending database is emptied of its contents.
3. The fabric lock is released for this feature.

To discard the device alias session using Fabric Manager, follow these steps:

---

**Step 1**
Expand **End Devices** and then select **Device Alias** in the Physical Attributes pane.

You see the device alias configuration in the Information pane. The **CFS** tab is the default tab.

**Step 2**
Select **abort** from the Config Action drop-down menu.

**Step 3**
Click **Apply Changes** to discard the session.

---

**About Legacy Zone Alias Configuration Conversion**

You can import legacy zone alias configurations to use this feature without loosing data, if they satisfy the following restrictions:

- Each zone alias has only one member.
- The member type is pWWN.
- The name and definition of the zone alias should not be the same as any existing device alias name.

If any name conflict exists, the zone aliases are not imported.

---

**Tip**
Ensure to copy any required zone aliases to the device alias database as required by your configuration.
When an import operation is complete, the modified alias database is distributed to all other switches in the physical fabric when you perform the commit operation. At this time if you do not want to distribute the configuration to other switches in the fabric, you can perform the abort operation and the merge changes are completely discarded.

This section includes the following topics:

- Using Device Aliases or FC Aliases, page 6-8
- Device Alias Statistics Cleanup, page 6-8

### Using Device Aliases or FC Aliases

You can change whether Fabric Manager uses FC aliases or global device aliases from Fabric Manager client without restarting Fabric Manager Server.

To change whether Fabric Manager uses FC aliases or global device aliases, follow these steps:

**Step 1** Click Server > Admin.

You see the Admin dialog box in Figure 6-3.

**Figure 6-3 Server Admin Dialog Box**

![Server Admin Dialog Box](image)

**Step 2** For each fabric that you are monitoring with Fabric Manager Server, check the Device Alias check box to use global device aliases, or uncheck to use FC aliases.

**Step 3** Click Apply to save these changes or click Close to exit the dialog box without saving any changes.

### Device Alias Statistics Cleanup

To clear device alias statistics (for debugging purposes), refer to the Cisco MDS 9000 Family CLI Configuration Guide.

### Database Merge Guidelines

For information about CFS merge support, refer to the Cisco MDS 9000 Family NX-OS System Management Configuration Guide for detailed concepts.

When merging two device alias databases, follow these guidelines:

- Verify that two device aliases with different names are not mapped to the same pWWN.
Populating Device Alias to Interface Description

When an end device is not logged into the switch, the Device Alias is blank. To find out what device is supposed to connect to an FC port when the device is logged out, you can populate the interface description with the device alias when the devices are logged in.

To populate the interface description with the device alias, follow these steps:

1. From the Physical Attributes pane, expand End Devices.
2. From the right pane, click the General tab.
3. Select the rows of FC interfaces.
4. Click the Alias->Description button.
5. Click the commit button.

**Figure 6-4 Copy Device Alias to Interface Description**

### Default Settings

Table 6-2 lists the default settings for device alias parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database in use</td>
<td>Effective database.</td>
</tr>
</tbody>
</table>
### Table 6-2 Default Device Alias Parameters (continued)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database to accept changes</td>
<td>Pending database.</td>
</tr>
<tr>
<td>Device alias fabric lock state</td>
<td>Locked with the first device alias task.</td>
</tr>
</tbody>
</table>
Configuring FCoE

This chapter describes how to configure Fibre Channel over Ethernet (FCoE) on a Cisco Nexus 5000 Series switch.

This chapter includes the following sections:

- About Fibre Channel over Ethernet, page 7-1
- Guidelines and Limitations, page 7-1
- Configuring FCoE, page 7-1

About Fibre Channel over Ethernet

Cisco Nexus 5000 Series switches support Fibre Channel over Ethernet (FCoE), which allows Fibre Channel and Ethernet traffic to be carried on the same physical Ethernet connection between the switch and the servers. FCoE requires the underlying Ethernet to be full duplex and to provide lossless behavior for Fibre Channel traffic.

FIP Initialization Protocol

The FCoE Initialization Protocol (FIP) allows the switch to discover and initialize FCoE-capable entities that are connected to an Ethernet LAN.

Guidelines and Limitations

When configuring FCoE, note the following guidelines and limitations:

- FCoE is supported on 10-Gigabit Ethernet interfaces.
- FCoE is not supported on private VLANs.

Configuring FCoE

This section describes how to configure FCoE on a switch and includes the following topics:

- Enabling FCoE, page 7-2
- Configuring FCoE Using Fabric Manager, page 7-3
Enabling FCoE

Fibre Channel over Ethernet (FCoE) provides a method of transporting Fibre Channel traffic over a physical Ethernet connection. By default, each Ethernet interface attempts to enable FCoE by advertising that it has FCoE to the adapter. If the FCoE negotiation fails, you can configure the Cisco Nexus 5000 Series switch to disable FCoE for this interface.

**Note**
In Cisco Nexus 5000 Series switches, FCoE is supported on all 10-Gigabit Ethernet interfaces.

To enable, or disable, FCoE features on a switch using Device Manager, follow these steps:

**Step 1**
Launch Device Manager from the Cisco Nexus 5000 Series switch.

**Step 2**
Choose **Admin > Feature Control**.

You see the Feature Control dialog box shown in Figure 7-1.

**Figure 7-1 Feature Control Dialog Box**

![Feature Control Dialog Box](image)

**Step 3**
In the dialog box, in the table, click the **fcoe_mgr** row, and then click the **Action** cell in the fcoe_mgr row. From the drop-down list, choose **enable** to enable the FCoE feature in the switch.
Configuring FCoE

You can also disable the FCoE feature in the switch. To do so, from the drop-down list in the Action column, choose disable.

Note

Step 4
Click Apply.

Note
If the Cisco Nexus 5000 Series switch is running a Cisco NX–OS release prior to Release 4.2(1), you must do the following after you enable or disable FCoE on the switch:
- In the confirmation dialog box that appears, click Yes to enable the FCoE feature in the switch.
- Reboot the switch before you use the FCoE feature.

Configuring FCoE Using Fabric Manager

To configure FCoE on a switch using Fabric Manager, follow these steps:

Step 1
In the Physical Attributes pane, choose Switches > FCoE.
You see the FCoE information pane shown in Figure 7-2.
The Config tab displays the FCoE parameters for each Cisco Nexus 5000 Series switch that runs Cisco NX-OS Release 4.1(3) or later releases. Table 7-1 lists the FCoE parameters for a switch.
Configuring FCoE

Figure 7-2  FCoE Information Pane

Table 7-1  FCoE Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC Map</td>
<td>The FCoE Mac Address Prefix used to associate the FCoE Node (ENode). Default value is 0e:fc:00.</td>
</tr>
<tr>
<td>Default FCF Priority</td>
<td>The FCoE Initialization Protocol (FIP) priority value advertised by the FCF to ENodes by default. Default priority value is 128 seconds.</td>
</tr>
<tr>
<td>FKA Advertisement Period</td>
<td>The time interval at which FIP Keep Alive (FKA) messages are transmitted to the MAC address of the ENode. Default advertisement period is 8 seconds.</td>
</tr>
</tbody>
</table>

Step 2  Double-click the relevant FCoE parameter for a switch, and modify the value of the parameter.

Step 3  In the Information pane toolbar, click the Apply Changes icon to save the changes.

Configuring FCoE Using Device Manager

To configure FCoE on a switch using Device Manager, follow these steps:

Step 1  Launch Device Manager from the Cisco Nexus 5000 Series switch.

Step 2  Choose FCoE > Config.

You see the FCoE Config dialog box shown in Figure 7-3.
Chapter 7 Configuring FCoE

Send documentation comments to mdsfeedback-doc@cisco.com

The Config tab displays the FCoE parameters, such as FC Map, default FCF priority value, and FKA advertisement period, for each Cisco Nexus 5000 Series switch that runs Cisco NX-OS Release 4.1(3) or later releases. Table 7-1 lists the FCoE parameters for a switch.

Figure 7-3 FCoE Config Dialog Box

Step 3 Double-click the relevant FCoE parameter for a switch, and modify the value of the parameter.

Step 4 Click Apply to save the changes.
Configuring Fibre Channel Routing Services and Protocols

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

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

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

- About FSPF, page 8-2
- FSPF Global Configuration, page 8-4
- FSPF Interface Configuration, page 8-6
- FSPF Routes, page 8-12
- In-Order Delivery, page 8-15
- Default Settings, page 8-19
About FSPF

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

- Supports multipath routing.
- Bases path status on a link state protocol.
- Routes hop by hop, based only on the domain ID.
- Runs only on E ports or TE ports and provides a loop free topology.
- Runs on a per VSAN basis. Connectivity in a given VSAN in a fabric is guaranteed only for the switches configured in that VSAN.
- Uses a topology database to keep track of the state of the links on all switches in the fabric and associates a cost with each link.
- Guarantees a fast reconvergence time in case of a topology change. Uses the standard Dijkstra algorithm, but there is a static dynamic option for a more robust, efficient, and incremental Dijkstra algorithm. The reconvergence time is fast and efficient as the route computation is done on a per VSAN basis.

FSPF Examples

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

Note

The FSPF feature can be used on any topology.

Fault Tolerant Fabric

Figure 8-1 depicts a fault tolerant fabric using a partial mesh topology. If a link goes down anywhere in the fabric, any switch can still communicate with all others in the fabric. In the same way, if any switch goes down, the connectivity of the rest of the fabric is preserved.

Figure 8-1 Fault Tolerant Fabric

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

To further improve on the topology in Figure 8-1, each connection between any pair of switches can be replicated; two or more links can be present between a pair of switches. Figure 8-2 shows this arrangement. Because switches in the Cisco MDS 9000 Family support PortChanneling, each pair of physical links can appear to the FSPF protocol as one single logical link.

By bundling pairs of physical links, FSPF efficiency is considerably improved by the reduced database size and the frequency of link updates. Once physical links are aggregated, failures are not attached to a single link but to the entire PortChannel. This configuration also improves the resiliency of the network. The failure of a link in a PortChannel does not trigger a route change, thereby reducing the risks of routing loops, traffic loss, or fabric downtime for route reconfiguration.

**Figure 8-2**  **Fault Tolerant Fabric with Redundant Links**

For example, if all links are of equal speed and no PortChannels exist, the FSPF calculates four equal paths from A to C: A1-E-C, A2-E-C, A3-D-C, and A4-D-C. If PortChannels exist, these paths are reduced to two.

**Failover Scenarios for PortChannels and FSPF Links**

The SmartBits traffic generator was used to evaluate the scenarios displayed in Figure 8-3. Two links between switch 1 and switch 2 exist as either equal-cost ISLs or PortChannels. There is one flow from traffic generator 1 to traffic generator 2. The traffic was tested at 100 percent utilization at 1 Gbps in two scenarios:

- Disabling the traffic link by physically removing the cable (see Table 8-1).
- Shutting down either switch 1 or switch 2 (see Table 8-2).

**Figure 8-3**  **Failover Scenario Using Traffic Generators**

**Table 8-1**  **Physically Removing the Cable for the SmartBits Scenario**

<table>
<thead>
<tr>
<th>PortChannel Scenario</th>
<th>FSPF Scenario (Equal cost ISL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch 1</td>
<td>Switch 2</td>
</tr>
<tr>
<td>110 msec (~2K frame drops)</td>
<td>130+ msec (~4k frame drops)</td>
</tr>
<tr>
<td>100 msec (hold time when a signal loss is reported as mandated by the standard)</td>
<td></td>
</tr>
</tbody>
</table>
FSPF Global Configuration

By default, FSPF is enabled on switches in the Cisco MDS 9000 Family.

Some FSPF features can be globally configured in each VSAN. By configuring a feature for the entire VSAN, you do not have to specify the VSAN number for every command. This global configuration feature also reduces the chance of typing errors or other minor configuration errors.

Note

FSPF is enabled by default. Generally, you do not need to configure these advanced features.

Caution

The default for the backbone region is 0 (zero). You do not need to change this setting unless your region is different from the default. If you are operating with other vendors using the backbone region, you can change this default to be compatible with those settings.

This section includes the following topics:

- About SPF Computational Hold Times, page 8-4
- About Link State Records, page 8-4
- Configuring FSPF on a VSAN, page 8-5
- Resetting FSPF to the Default Configuration, page 8-5
- Enabling or Disabling FSPF, page 8-6

About SPF Computational Hold Times

The SPF computational hold time sets the minimum time between two consecutive SPF computations on the VSAN. Setting this to a small value means that FSPF reacts faster to any fabric changes by recomputing paths on the VSAN. A small SPF computational hold time uses more switch CPU time.

About Link State Records

Each time a new switch enters the fabric, a link state record (LSR) is sent to the neighboring switches, and then flooded throughout the fabric. Table 8-3 displays the default settings for switch responses.
The LSR minimum arrival time is the period between receiving LSR updates on this VSAN. Any LSR updates that arrive before the LSR minimum arrival time are discarded.

The LSR minimum interval time is the frequency at which this switch sends LSR updates on a VSAN.

### Configuring FSPF on a VSAN

To configure an FSPF feature for the entire VSAN using Fabric Manager, follow these steps:

**Step 1** Expand a Fabric, expand a VSAN and select **FSPF** for a VSAN that you want to configure for FSPF.

You see the FSPF configuration in the Information pane as shown in Figure 8-4.

**Figure 8-4 FSPF General Information**

<table>
<thead>
<tr>
<th>Switch</th>
<th>Status</th>
<th>Status Oper</th>
<th>SetTo</th>
<th>Default</th>
<th>RegStatus</th>
<th>Element</th>
<th>Spf Comp Holdtime</th>
<th>Spf Comp Dltem</th>
<th>LSR Min Arrival</th>
<th>LSR Min Interval</th>
<th>LSR Min Age</th>
<th>CreateTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>sn172-22-46-225</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sn172-22-46-226</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sn172-22-46-227</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sn172-22-46-228</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sn172-22-46-229</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sn172-22-46-230</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sn172-22-46-231</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sn172-22-46-232</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sn172-22-46-233</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sn172-22-46-234</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sn172-22-46-235</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sn172-22-46-236</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 2** The RegionID, Spf Comp Holdtime, LSR Min Arrival, and LSR Min Interval field values are applied across all interfaces on the VSAN. You can change them here or, if they do not exist create them here.

**Step 3** Click **Apply Changes** to save these changes, or click **Undo Changes** to discard any unsaved changes.

### Resetting FSPF to the Default Configuration

To return the FSPF VSAN global configuration to its factory default using Fabric Manager, follow these steps:

**Step 1** Expand a Fabric, expand a VSAN and select **FSPF** for a VSAN that you want to configure for FSPF.

You see the FSPF configuration in the Information pane as shown in Figure 8-4.

**Step 2** Check the **SetToDefault** check box for a switch.

### Table 8-3 LSR Default Settings

<table>
<thead>
<tr>
<th>LSR Option</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledgment interval (RxmtInterval)</td>
<td>5 seconds</td>
<td>The time a switch waits for an acknowledgment from the LSR before retransmission.</td>
</tr>
<tr>
<td>Refresh time (LSRefreshTime)</td>
<td>30 minutes</td>
<td>The time a switch waits before sending an LSR refresh transmission.</td>
</tr>
<tr>
<td>Maximum age (MaxAge)</td>
<td>60 minutes</td>
<td>The time a switch waits before dropping the LSR from the database.</td>
</tr>
</tbody>
</table>
Enabling or Disabling FSPF

To enable or disable FSPF using Fabric Manager, follow these steps:

Step 1 Expand a Fabric, expand a VSAN and select FSPF for a VSAN that you want to configure for FSPF. You see the FSPF configuration in the Information pane as shown in Figure 8-4.

Step 2 Set the Status Admin drop-down menu to up to enable FSPF or to down to disable FSPF.

Step 3 Click Apply Changes to save these changes, or click Undo Changes to discard any unsaved changes.

FSPF Interface Configuration

Several FSPF commands are available on a per-interface basis. These configuration procedures apply to an interface in a specific VSAN.

This section includes the following topics:

- About FSPF Link Cost, page 8-6
- Configuring FSPF Link Cost, page 8-7
- About Hello Time Intervals, page 8-7
- Configuring Hello Time Intervals, page 8-8
- About Dead Time Intervals, page 8-8
- Configuring Dead Time Intervals, page 8-8
- About Retransmitting Intervals, page 8-8
- Configuring Retransmitting Intervals, page 8-9
- About Disabling FSPF for Specific Interfaces, page 8-9
- Disabling FSPF for Specific Interfaces, page 8-9
- Displaying the FSPF Database, page 8-10
- Viewing FSPF Statistics, page 8-11

About FSPF Link Cost

FSPF tracks the state of links on all switches in the fabric, associates a cost with each link in its database, and then chooses the path with a minimal cost. The cost associated with an interface can be administratively changed to implement the FSPF route selection. The integer value to specify cost can range from 1 to 65,535. The default cost for 1 Gbps is 1000 and for 2 Gbps is 500.
Configuring FSPF Link Cost

To configure FSPF link cost using Fabric Manager, follow these steps:

**Step 1** Expand **Switches**, expand **Interfaces** and then select **FC Physical**. You see the interface configuration in the Information pane.

**Step 2** Click the **FSPF** tab. You see the FSPF interface configuration in the Information pane as shown in Figure 8-5.

**Step 3** Double-click in the Cost field of a switch and change the value.

**Step 4** Click **Apply Changes** to save these changes, or click **Undo Changes** to discard any unsaved changes.

### About Hello Time Intervals

You can set the FSPF Hello time interval to specify the interval between the periodic hello messages sent to verify the health of the link. The integer value can range from 1 to 65,535 seconds.

**Note** This value must be the same in the ports at both ends of the ISL.
Configuring Hello Time Intervals

To configure the FSPF Hello time interval using Fabric Manager, follow these steps:

1. Expand **Switches**, expand **Interfaces** and then select **FC Physical**.
   You see the interface configuration in the Information pane.
2. Click the **FSPF** tab.
   You see the FSPF interface configuration in the Information pane as shown in Figure 8-5.
3. Change the Hello Interval field for a switch.
4. Click **Apply Changes** to save these changes, or click **Undo Changes** to discard any unsaved changes.

About Dead Time Intervals

You can set the FSPF dead time interval to specify the maximum interval for which a hello message must be received before the neighbor is considered lost and removed from the database. The integer value can range from 1 to 65,535 seconds.

- **Note**
  This value must be the same in the ports at both ends of the ISL.

- **Caution**
  An error is reported at the command prompt if the configured dead time interval is less than the hello time interval.

Configuring Dead Time Intervals

To configure the FSPF dead time interval using Fabric Manager, follow these steps:

1. Expand **Switches**, expand **Interfaces** and then select **FC Physical**.
   You see the interface configuration in the Information pane.
2. Click the **FSPF** tab.
   You see the FSPF interface configuration in the Information pane as shown in Figure 8-5.
3. Double-click the Dead Interval field for a switch and provide a new value.
4. Click **Apply Changes** to save these changes, or click **Undo Changes** to discard any unsaved changes.

About Retransmitting Intervals

You can specify the time after which an unacknowledged link state update should be transmitted on the interface. The integer value to specify retransmit intervals can range from 1 to 65,535 seconds.
Configuring Retransmitting Intervals

To configure the FSPF retransmit time interval using Fabric Manager, follow these steps:

**Step 1** Expand **Switches**, expand **Interfaces**, and then select **FC Physical**.
You see the interface configuration in the Information pane.

**Step 2** Click the **FSPF** tab.
You see the FSPF interface configuration in the Information pane as shown in Figure 8-5.

**Step 3** Double-click the ReTx Interval field and enter a value.

**Step 4** Click **Apply Changes** to save these changes, or click **Undo Changes** to discard any unsaved changes.

About Disabling FSPF for Specific Interfaces

You can disable the FSPF protocol for selected interfaces. By default, FSPF is enabled on all E ports and TE ports. This default can be disabled by setting the interface as passive.

**Note**
FSPF must be enabled at both ends of the interface for the protocol to work.

Disabling FSPF for Specific Interfaces

You can disable the FSPF protocol for selected interfaces. By default, FSPF is enabled on all E ports and TE ports. This default can be disabled by setting the interface as passive.

To disable FSPF for a specific interface using Fabric Manager, follow these steps:

**Step 1** Expand **Switches**, expand **Interfaces** and then select **FC Physical**.
You see the interface configuration in the Information pane.

**Step 2** Click the **FSPF** tab.
You see the FSPF interface configuration in the Information pane shown in Figure 8-5.

**Step 3** Set a switch Admin Status drop-down menu to **down**.

**Step 4** Click **Apply Changes** to save these changes, or click **Undo Changes** to discard any unsaved changes.

You can disable the FSPF protocol for selected interfaces. By default, FSPF is enabled on all E ports and TE ports. This default can be disabled by setting the interface as passive.
Displaying the FSPF Database

The FSPF database for a specified VSAN includes the following information:

- Link State Record (LSR) type
- Domain ID of the LSR owner
- Domain ID of the advertising router
- LSR age
- LSR incarnation member
- Number of links

To display the FSPF database using Device Manager, follow these steps:

**Step 1**
Choose FC > Advanced > FSPF.

You see the FSPF dialog box shown in Figure 8-6.

**Figure 8-6  FSPF Dialog Box in Device Manager**

![FSPF Dialog Box in Device Manager](image)

**Step 2**
Click the LSDB LSRs tab.

You see the FSPF database information shown in Figure 8-7.
Step 3 Click Close to close the dialog box.

Viewing FSPF Statistics

To view FSPF statistics using Fabric Manager, follow these steps:

Step 1 Expand a Fabric, expand a VSAN, and then select FSPF in the Logical Domains pane.

You see the FSPF configuration dialog box.

Step 2 Click the Statistics tab.

You see the FSPF VSAN statistics in the Information pane (see Figure 8-8).

Step 3 Click the Interface Statistics tab.
FSPF Routes

FSPF routes traffic across the fabric, based on entries in the FSPF database. These routes can be learned dynamically, or configured statically.

This section includes the following topics:

- About Fibre Channel Routes, page 8-12
- Configuring Fibre Channel Routes, page 8-12
- About Broadcast and Multicast Routing, page 8-14
- About Multicast Root Switch, page 8-14
- Setting the Multicast Root Switch, page 8-14

About Fibre Channel Routes

Each port implements forwarding logic, which forwards frames based on its FC ID. Using the FC ID for the specified interface and domain, you can configure the specified route (for example FC ID 111211 and domain ID 3) in the switch with domain ID 1 (see Figure 8-9).

Note

Other than in VSANs, runtime checks are not performed on configured and suspended static routes.

Configuring Fibre Channel Routes

If you disable FSPF, you can manually configure a Fibre Channel route.

To configure a Fibre Channel route using Device Manager, follow these steps:

Step 1  Click **FC > Advanced > Routes**.

You see the FC Static Route Configuration dialog box shown in Figure 8-10.
Step 2  Click **Create** to create a static route.  
You see the Create Route dialog box shown in **Figure 8-11**.

**Figure 8-11**  
Create Fibre Channel Route Dialog Box  

---

**Step 3**  Select the VSAN ID that for which you are configuring this route.  
**Step 4**  Fill in the destination address and destination mask for the device you are configuring a route.  
**Step 5**  Select the interface that you want to use to reach this destination.  
**Step 6**  Select the next hop domain ID and route metric.  
**Step 7**  Select either the **local** or **remote** radio button.  
**Step 8**  Click **Create** to save these changes, or click **Close** to discard any unsaved changes.
About Broadcast and Multicast Routing

Broadcast and multicast in a Fibre Channel fabric uses the concept of a distribution tree to reach all switches in the fabric.

FSPF provides the topology information to compute the distribution tree. Fibre Channel defines 256 multicast groups and one broadcast address for each VSAN. Switches in the Cisco MDS 9000 Family only use broadcast routing. By default, they use the principal switch as the root node to derive a loop-free distribution tree for multicast and broadcast routing in a VSAN.

Caution

All switches in the fabric should run the same multicast and broadcast distribution tree algorithm to ensure the same distribution tree.

To interoperate with other vendor switches (following FC-SW3 guidelines), the SAN-OS and NX-OS 4.1(1b) and later software uses the lowest domain switch as the root to compute the multicast tree in interop mode.

About Multicast Root Switch

By default, the native (non-interop) mode uses the principal switch as the root. If you change the default, be sure to configure the same mode in all switches in the fabric. Otherwise, multicast traffic could encounter potential loop and frame-drop problems.

Note

The operational mode can be different from the configured interop mode. The interop mode always uses the lowest domain switch as the root.

Setting the Multicast Root Switch

To use the lowest domain switch for the multicast tree computation using Fabric Manager, follow these steps:

Step 1
Expand a fabric, expand a VSAN, and then select Advanced for the VSAN that you want to configure FSPF on.
You see the advanced Fibre Channel configuration in the Information pane.

Step 2
Select the Multicast Root tab.
You see the multicast root configuration in the Information pane as shown in Figure 8-12.
In-Order Delivery

In-Order Delivery (IOD) of data frames guarantees frame delivery to a destination in the same order that they were sent by the originator.

Some Fibre Channel protocols or applications cannot handle out-of-order frame delivery. In these cases, switches in the Cisco MDS 9000 Family preserve frame ordering in the frame flow. The source ID (SID), destination ID (DID), and optionally the originator exchange ID (OX ID) identify the flow of the frame.

On any given switch with IOD enabled, all frames received by a specific ingress port and destined to a certain egress port are always delivered in the same order in which they were received.

Use IOD only if your environment cannot support out-of-order frame delivery.

Tip

If you enable the in-order delivery feature, the graceful shutdown feature is not implemented.

This section includes the following topics:

- About Reordering Network Frames, page 8-15
- About Reordering PortChannel Frames, page 8-16
- About Enabling In-Order Delivery, page 8-17
- Enabling In-Order Delivery Globally, page 8-18
- Enabling In-Order Delivery for a VSAN, page 8-18
- Configuring the Drop Latency Time, page 8-18

About Reordering Network Frames

When you experience a route change in the network, the new selected path may be faster or less congested than the old route.

Step 3  Set the Config Mode drop-down menu to lowestDomainSwitch.
Step 4  Click Apply Changes to save these changes, or click Undo Changes to discard any unsaved changes.
In Figure 8-13, the new path from Switch 1 to Switch 4 is faster. In this scenario, Frame 3 and Frame 4 may be delivered before Frame 1 and Frame 2.

If the in-order guarantee feature is enabled, the frames within the network are treated as follows:

- Frames in the network are delivered in the order in which they are transmitted.
- Frames that cannot be delivered in order within the network latency drop period are dropped inside the network.

**About Reordering PortChannel Frames**

When a link change occurs in a PortChannel, the frames for the same exchange or the same flow can switch from one path to another faster path.

In Figure 8-14, the port of the old path (red dot) is congested. In this scenario, Frame 3 and Frame 4 can be delivered before Frame 1 and Frame 2.

The in-order delivery feature attempts to minimize the number of frames dropped during PortChannel link changes when the in-order delivery is enabled by sending a request to the remote switch on the PortChannel to flush all frames for this PortChannel.

| Note | Both switches on the PortChannel must be running Cisco SAN-OS Release 3.0(1) for this IOD enhancement. For earlier releases, IOD waits for the switch latency period before sending new frames. |

When the in-order delivery guarantee feature is enabled and a PortChannel link change occurs, the frames crossing the PortChannel are treated as follows:

- Frames using the old path are delivered before new frames are accepted.
In-Order Delivery

The new frames are delivered through the new path after the switch latency drop period has elapsed and all old frames are flushed. Frames that cannot be delivered in order through the old path within the switch latency drop period are dropped. See the “Configuring the Drop Latency Time” section on page 8-18.

About Enabling In-Order Delivery

You can enable the in-order delivery feature for a specific VSAN or for the entire switch. By default, in-order delivery is disabled on switches in the Cisco MDS 9000 Family.

Tip

We recommend that you only enable this feature when devices that cannot handle any out-of-order frames are present in the switch. Load-balancing algorithms within the Cisco MDS 9000 Family ensure that frames are delivered in order during normal fabric operation. The load-balancing algorithms based on source FC ID, destination FC ID, and exchange ID are enforced in hardware without any performance degradation. However, if the fabric encounters a failure and this feature is enabled, the recovery will be delayed because of an intentional pausing of fabric forwarding to purge the fabric of resident frames that could potentially be forwarded out-of-order.
Enabling In-Order Delivery Globally

To ensure that the in-order delivery parameters are uniform across all VSANs on an MDS switch, enable in-order delivery globally.

Only enable in-order delivery globally if this is a requirement across your entire fabric. Otherwise, enable IOD only for the VSANs that require this feature.

**Note**

Enable in-order delivery on the entire switch before performing a downgrade to Cisco MDS SAN-OS Release 1.3(3) or earlier.

Enabling In-Order Delivery for a VSAN

When you create a VSAN, that VSAN automatically inherits the global in-order-guarantee value. You can override this global value by enabling or disabling in-order-guarantee for the new VSAN.

To use the lowest domain switch for the multicast tree computation using Fabric Manager, follow these steps:

**Step 1** Expand a fabric and select **All VSANS**.

**Step 2** Select the **Attributes** tab.

You see the general VSAN attributes in the Information pane shown in **Figure 8-15**.

**Figure 8-15** General VSAN Attributes

**Step 3** Check the **InOrder Delivery** check box to enable IOD for the switch.

**Step 4** Click **Apply Changes** to save these changes, or click **Undo Changes** to discard any unsaved changes.

Configuring the Drop Latency Time

You can change the default latency time for either the entire switch or a specified VSAN in a switch.

To configure the drop latency time for a switch using Fabric Manager, follow these steps:
Step 1  Expand a fabric and select All VSANS.
You see the VSAN configuration in the Information pane.

Step 2  Select the Attributes tab.
You see the general VSAN attributes in the Information pane shown in Figure 8-16.

Figure 8-16  General VSAN Attributes

Step 3  Double-click the Network Latency field and change the value.

Step 4  Click Apply Changes to save these changes, or click Undo Changes to discard any unsaved changes.

Default Settings

Table 8-4 lists the default settings for FSPF features.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSPF</td>
<td>Enabled on all E ports and TE ports.</td>
</tr>
<tr>
<td>SPF computation</td>
<td>Dynamic.</td>
</tr>
<tr>
<td>SPF hold time</td>
<td>0.</td>
</tr>
<tr>
<td>Backbone region</td>
<td>0.</td>
</tr>
<tr>
<td>Acknowledgment interval (RxmtInterval)</td>
<td>5 seconds.</td>
</tr>
<tr>
<td>Refresh time (LSRefreshTime)</td>
<td>30 minutes.</td>
</tr>
<tr>
<td>Maximum age (MaxAge)</td>
<td>60 minutes.</td>
</tr>
<tr>
<td>Hello interval</td>
<td>20 seconds.</td>
</tr>
<tr>
<td>Dead interval</td>
<td>80 seconds.</td>
</tr>
<tr>
<td>Distribution tree information</td>
<td>Derived from the principal switch (root node).</td>
</tr>
</tbody>
</table>
Default Settings

Send documentation comments to mdsfeedback-doc@cisco.com

Table 8-4 Default FSPF Settings (continued)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing table</td>
<td>FSPF stores up to 16 equal cost paths to a given destination.</td>
</tr>
<tr>
<td>Load balancing</td>
<td>Based on destination ID and source ID on different, equal cost paths.</td>
</tr>
<tr>
<td>In-order delivery</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Drop latency</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Static route cost</td>
<td>If the cost (metric) of the route is not specified, the default is 10.</td>
</tr>
<tr>
<td>Remote destination switch</td>
<td>If the remote destination switch is not specified, the default is direct.</td>
</tr>
<tr>
<td>Multicast routing</td>
<td>Uses the principal switch to compute the multicast tree.</td>
</tr>
</tbody>
</table>
Configuring Dense Wavelength Division Multiplexing

This chapter includes the following topics:

- About DWDM, page 9-1
- Viewing DWDM Links, page 9-1
- Configuring X2 DWDM Transceiver Frequency, page 9-4

About DWDM

Dense Wavelength-Division Multiplexing (DWDM) multiplexes multiple optical carrier signals on a single optical fiber. DWDM uses different wavelengths to carry various signals.

To establish a DWDM link, both ends of an Inter Switch Link (ISL) need to be connected with DWDM SFPs (small form-factor pluggable) at each end of the link. To identify a DWDM link, Fabric Manager discovers the connector type on the Fiber Channel (FC) ports. If the ISL link is associated with the FC ports at each end, then the FC port uses DWDM SFP to connect the links.

Fabric Manager Server discovers FC ports with DWDM SFPs and the ISLs associated with the FC ports. The Fabric Manager Client displays ISL with DWDM attribute on the topology map.

Note

The Fabric Shortest Path First (FSPF) database only displays an ISL link, which is connected with DWDM SFPs at both ends.

Viewing DWDM Links

The Fabric Manager Client displays DWDM links with “dash-dash” pattern. The tooltip for the link displays “DWDM” to indicate its link type.

To view the DWDM link, follow these steps:

Step 1  Select the switch in the Logical Domain region.
Step 2  Select ISL in the Physical Attributes region.

The Information pane displays the ISL’s information.
Step 3  Click the Physical tab.

You see the ISL in the Information pane as shown in Figure 9-1.

Figure 9-1  Fabric Manager with ISL Link

Step 4  The ISL's Physical table displays the connector type as “sfpDwdm” as shown in Figure 9-2.
Step 5  Move the mouse over the link to see the tooltip as DWDM indicating the link type as shown in Figure 9-3.
Perform a Dump Discovery of ISL to list all ISLs. DWDM links are listed with “[DWDM]” as shown in Figure 9-4.

**Figure 9-4** ISL List Displayed in the Information Pane

---

### Configuring X2 DWDM Transceiver Frequency

**Note**
This feature is not supported in non-UROS modules. In the UROS modules, the 10-Gigabit Ethernet ports must be in down state when you configure the X2 transceiver frequency.

To configure the X2 DWDM transceiver frequency using Device Manager, follow these steps:

**Step 1**
From Device Manager menu bar, select **Physical > Modules**.
The module configuration window is displayed (Figure 9-5).
To configure the X2 DWDM transceiver frequency using Fabric Manager, follow these steps:

**Step 1**
From the Physical Attributes pane, select **Hardware**.

The module configuration window is displayed.

**Step 2**
Click the **Card Module Config** tab.
Configuring X2 DWDM Transceiver Frequency

Send documentation comments to mdsfeedback-doc@cisco.com

Step 3  In the X2 XcvrFrequencyConfig column, choose an option.
Step 4  Click Apply.
Managing FLOGI, Name Server, FDMI, and RSCN Databases

This chapter describes the fabric login (FLOGI) database, the name server features, the Fabric-Device Management Interface, and Registered State Change Notification (RSCN) information provided in the Cisco MDS 9000 Family. It includes the following sections:

- About FLOGI, page 10-1
- Displaying FLOGI Details, page 10-1
- Name Server Proxy, page 10-2
- FDMI, page 10-4
- Displaying FDMI, page 10-4
- RSCN, page 10-5
- Default Settings, page 10-8

About FLOGI

In a Fibre Channel fabric, each host or disk requires an FC ID. If the required device is displayed in the FLOGI table, the fabric login is successful. Examine the FLOGI database on a switch that is directly connected to the host HBA and connected ports. See the “Default Company ID List” section on page 13-8 and the “Switch Interoperability” section on page 13-8.

Displaying FLOGI Details

To verify that a storage device is in the fabric login (FLOGI) table using Fabric Manager, follow these steps:

**Step 1** Expand **Switches**, expand **Interfaces** and then select **FC Physical**.
You see the interface configuration in the Information pane.

**Step 2** Click the **FLOGI** tab.
You see all end devices that are logged into the fabric (see **Figure 10-1**).
Name Server Proxy

The name server functionality maintains a database containing the attributes for all hosts and storage devices in each VSAN. Name servers allow a database entry to be modified by a device that originally registered the information.

The proxy feature is useful when you want to modify (update or delete) the contents of a database entry that was previously registered by a different device.

This section includes the following topics:

- About Registering Name Server Proxies, page 10-2
- Registering Name Server Proxies, page 10-2
- About Rejecting Duplicate pWWN, page 10-3
- Rejecting Duplicate pWWNs, page 10-3
- To reject duplicate pWWNs, refer to the Cisco MDS 9000 Family CLI Configuration Guide. About Name Server Database Entries, page 10-3
- Viewing Name Server Database Entries, page 10-3

About Registering Name Server Proxies

All name server registration requests come from the same port whose parameter is registered or changed. If it does not, then the request is rejected.

This authorization enables WWNs to register specific parameters for another node.

Registering Name Server Proxies

To register the name server proxy using Fabric Manager, follow these steps:

1. **Step 1** Expand a fabric, expand a VSAN, and then select Advanced.
   You see the VSAN advanced configuration in the Information pane.

2. **Step 2** Click the NS Proxies tab.
   You see the existing name server proxy for the selected VSAN shown in Figure 10-2.
**Name Server Proxy**

**Figure 10-2** Name Server Proxies

Step 3 Double-click the PortName field to register a new name server proxy.

Step 4 Click **Apply Changes** to save these changes, or click **Undo Changes** to cancel any unsaved changes.

---

**About Rejecting Duplicate pWWN**

You can prevent a malicious or accidental login when using another device’s pWWN. These pWWNs are allowed to log in to the fabric and replace the first device in the name server database.

**Rejecting Duplicate pWWNs**

To reject duplicate pWWNs, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*. **About Name Server Database Entries**

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

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

**Viewing Name Server Database Entries**

To view the name server database using Device Manager, follow these steps:

**Step 1** Click FC > Name Server.

You see the Name Server dialog box as shown in **Figure 10-3**.
FDMI

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

Using the FDMI functionality, the NX-OS software can extract the following management information about attached HBAs and host operating systems without installing proprietary host agents:

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

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

Displaying FDMI

To display the FDMI database information using Device Manager, choose **FC > Advanced > FDMI**. You see the FDMI dialog box.

The General tab is the default tab; you see the name server database.

**Step 2**

Click the **Statistics** tab.

You see the name server statistics.

**Step 3**

Click **Close** to close the dialog box.
RSCN

The Registered State Change Notification (RSCN) is a Fibre Channel service that informs hosts about changes in the fabric. Hosts can receive this information by registering with the fabric controller (through SCR). These notifications provide a timely indication of one or more of the following events:

- Disks joining or leaving the fabric.
- A name server registration change.
- A new zone enforcement.
- IP address change.
- Any other similar event that affects the operation of the host.

This section includes the following topics:

- About RSCN Information, page 10-5
- Displaying RSCN Information, page 10-5
- About the multi-pid Option, page 10-6
- Configuring the multi-pid Option, page 10-6
- Clearing RSCN Statistics, page 10-7
- RSCN Timer Configuration Distribution Using CFS, page 10-7
- Configuring the RSCN Timer with CFS, page 10-8

About RSCN Information

Apart from sending these events to registered hosts, a switch RSCN (SW-RSCN) is sent to all reachable switches in the fabric.

**Note** The switch sends an RSCN to notify registered nodes that a change has occurred. It is up to the nodes to query the name server again to obtain the new information. The details of the changed information are not delivered by the switch in the RSCN sent to the nodes.

Displaying RSCN Information

To display RSCN information using Fabric Manager, follow these steps:

**Step 1** Expand a fabric, expand a VSAN and then select Advanced. You see the VSAN advanced configuration in the Information pane.

**Step 2** Select the RSCN Reg tab or the RSCN Statistics tab (see Figure 10-4).
About the multi-pid Option

If the RSCN multi-pid option is enabled, then RSCNs generated to the registered Nx ports may contain more than one affected port IDs. In this case, zoning rules are applied before putting the multiple affected port IDs together in a single RSCN. By enabling this option, you can reduce the number of RSCNs. For example: Suppose you have two disks (D1, D2) and a host (H) connected to switch 1. Host H is registered to receive RSCNs. D1, D2 and H belong to the same zone. If disks D1 and D2 are online at the same time, then one of the following applies:

- The multi-pid option is disabled on switch 1: two RSCNs are generated to host H—one for the disk D1 and another for disk D2.
- The multi-pid option is enabled on switch 1: a single RSCN is generated to host H, and the RSCN payload lists the affected port IDs (in this case, both D1 and D2).

**Note** Some Nx ports may not understand multi-pid RSCN payloads. If so, disable the RSCN multi-pid option.

Configuring the multi-pid Option

To configure the multi-pid option using Fabric Manager, follow these steps:

**Step 1** Expand a fabric, expand a VSAN and then select Advanced.
You see the VSAN advanced configuration in the Information pane.

**Step 2** Click the RSCN Multi-PID tab.
You see the screen shown in Figure 10-5.
Step 3 Check the Enable check box.
Step 4 Click Apply Changes to save these changes, or click Undo Changes to cancel any unsaved changes.

**Clearing RSCN Statistics**

You can clear the counters and later view the counters for a different set of events. For example, you can keep track of how many RSCNs or SW-RSCNs are generated on a particular event (such as ONLINE or OFFLINE events). You can use these statistics to monitor responses for each event in the VSAN.

To clear the RSCN statistics for the specified VSAN, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

**RSCN Timer Configuration Distribution Using CFS**

Because the timeout value for each switch is configured manually, a misconfiguration occurs when different switches time out at different times. This means different N-ports in a network can receive RSCNs at different times. Cisco Fabric Services (CFS) alleviates this situation by automatically distributing configuration information to all switches in a fabric. This also reduces the number of SW-RSCNs.

RSCN supports two modes, distributed and nondistributed. In distributed mode, RSCN uses CFS to distribute configuration to all switches in the fabric. In nondistributed mode, only the configuration commands on the local switch are affected.

*Note*

All configuration commands are not distributed. Only the `rscn event-tov tov vsan vsan` command is distributed.

The RSCN timer is registered with CFS during initialization and switchover. For high availability, if the RSCN timer distribution crashes and restarts or a switchover occurs, it resumes normal functionality from the state prior to the crash or switchover.
Before performing a downgrade, make sure that you revert the RCSN timer value in your network to the default value. Failure to do so will disable the links across your VSANs and other devices.

Compatibility across various Cisco MDS NX-OS releases during an upgrade or downgrade is supported by `conf-check` provided by CFS. If you attempt to downgrade from Cisco MDS SAN-OS Release 3.0, you are prompted with a `conf-check` warning. You are required to disable RSCN timer distribution support before you downgrade.

By default, the RSCN timer distribution capability is disabled and is therefore compatible when upgrading from any Cisco MDS SAN-OS release earlier than Release 3.0.

### Configuring the RSCN Timer with CFS

To configure the RSCN timer with CFS using Fabric Manager, follow these steps:

**Step 1** Expand a fabric, expand a VSAN and then select **Advanced** in the Logical Domains pane.

**Step 2** Select the **RSCN Event** tab.

You see the VSAN advanced configuration in the Information pane shown in Figure 10-6.

**Figure 10-6 VSAN Advanced Configuration**

![VSAN Advanced Configuration](image)

**Step 3** Double-click the **TimeOut** value to change the value (in milliseconds) for the selected VSAN.

**Step 4** Click **Apply Changes** to save these changes, or click **Undo Changes** to cancel any unsaved changes.

### Default Settings

Table 10-1 lists the default settings for RSCN.
### Table 10-1 Default RSCN Settings

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSCN timer value</td>
<td>2000 milliseconds for Fibre Channel VSANs</td>
</tr>
<tr>
<td></td>
<td>1000 milliseconds for FICON VSANs</td>
</tr>
<tr>
<td>RSCN timer configuration distribution</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
This chapter describes the SCSI LUN discovery feature provided in switches in the Cisco MDS 9000 Family. It includes the following sections:

- About SCSI LUN Discovery, page 11-1
- Displaying SCSI LUN Information, page 11-3

About SCSI LUN Discovery

Small Computer System Interface (SCSI) targets include disks, tapes, and other storage devices. These targets do not register logical unit numbers (LUNs) with the name server. The name server requires LUN information for the following reasons:

- To display LUN storage device information so an NMS can access this information.
- To report device capacity, serial number, and device ID information.
- To register the initiator and target features with the name server.

The SCSI LUN discovery feature uses the local domain controller Fibre Channel address. It uses the local domain controller as the source FC ID, and performs SCSI INQUIRY, REPORT LUNS, and READ CAPACITY commands on SCSI devices.

The SCSI LUN discovery feature is initiated on demand, through CLI or SNMP. This information is also synchronized with neighboring switches, if those switches belong to the Cisco MDS 9000 Family.

This section includes the following topics:

- About Starting SCSI LUN Discovery, page 11-1
- Starting SCSI LUN Discovery, page 11-2
- About Initiating Customized Discovery, page 11-2
- Initiating Customized Discovery, page 11-2

About Starting SCSI LUN Discovery

SCSI LUN discovery is done on demand.

Only Nx ports that are present in the name server database and that are registered as FC4 Type = SCSI_FCP are discovered.
Starting SCSI LUN Discovery

To begin SCSI LUN discovery using Device Manager, follow these steps:

**Step 1** Choose FC > Advanced > LUNs.
You see the LUN Configuration dialog box.

**Figure 11-1  LUN Configuration Dialog Box**

**Step 2** Set StartDiscovery to local, remote or both.
**Step 3** Choose the DiscoveryType and OS.
**Step 4** Click Apply to begin discovery.

About Initiating Customized Discovery

Customized discovery consists of a list of VSAN and domain pairs that are selectively configured to initiate a discovery. The domain ID is a number from 0 to 255 in decimal or a number from 0x0 to 0xFF in hex.

Initiating Customized Discovery

To initiate a customized discovery using Device Manager, follow these steps:

**Step 1** Click the VSAN drop-down menu and select the VSAN in which you want to initiate a customized discovery.
**Step 2** Click FC > Advanced > LUNs.
You see the LUN Configuration dialog box.
**Step 3** Set StartDiscovery to local, remote or both.
**Step 4** Fill in the DiscoveryType and OS fields.
Displaying SCSI LUN Information

To display the results of the discovery using Device Manager, follow these steps:

**Step 1** Click FC > Advanced > LUNs
You see the LUN Configuration dialog box.

**Step 2** Click the LUN tab or the Targets tab.
Fibre Connection (FICON) interface capabilities enhance the Cisco MDS 9000 Family by supporting both open systems and mainframe storage network environments. Inclusion of Control Unit Port (CUP) support further enhances the MDS offering by allowing in-band management of the switch from FICON processors.


The Registered Link Incident Report (RLIR) application provides a method for a switch port to send an LIR to a registered Nx port.

Note: Cisco Fabric Manager release 3.x does not support FICON management of Cisco MDS 9000 Family switches running SAN-OS release 2.(x).

This chapter includes the following sections:
- About FICON, page 12-1
- FICON Port Numbering, page 12-8
- Configuring FICON, page 12-15
- Configuring FICON Ports, page 12-24
- FICON Configuration Files, page 12-28
- Port Swapping, page 12-31
- FICON Tape Acceleration, page 12-33
- Configuring XRC Acceleration, page 12-37
- CUP In-Band Management, page 12-38
- Calculating FICON Flow Load Balance, page 12-40
- Displaying FICON Information, page 12-41
- Default Settings, page 12-43

About FICON

The FICON feature is not supported on:
- Cisco MDS 9120 switches
Cisco Fabric Manager Fabric Configuration Guide

Chapter 12 Configuring FICON

Send documentation comments to mdsfeedback-doc@cisco.com

About FICON

Cisco MDS 9124 switches
Cisco MDS 9140 switches
The 32-port Fibre Channel switching module
Cisco Fabric Switch for HP c-Class BladeSystem
Cisco Fabric Switch for IBM BladeSystem

The Cisco MDS 9000 Family supports the Fibre Channel Protocol (FCP), FICON, iSCSI, and FCIP capabilities within a single, high availability platform. This solution simplifies purchasing, reduces deployment and management costs, and reduces the complex evolution to shared mainframe and open systems storage networks (see Figure 12-1).

Figure 12-1 Shared System Storage Network

FCP and FICON are different FC4 protocols and their traffic is independent of each other. Devices using these protocols should be isolated using VSANs.

This section includes the following topics:

- FICON Requirements, page 12-2
- MDS-Specific FICON Advantages, page 12-3
- FICON Cascading, page 12-7
- FICON VSAN Prerequisites, page 12-7

FICON Requirements

The FICON feature has the following requirements:

- You can implement FICON features in the following switches:
  - Any switch in the Cisco MDS 9500 Series.
  - Any switch in the Cisco MDS 9200 Series (including the Cisco MDS 9222i Multiservice Modular Switch).
  - Cisco MDS 9134 Multilayer Fabric Switch.
  - MDS 9000 Family 18/4-Port Multiservice Module.
You need the MAINFRAME_PKG license to configure FICON parameters. To extend your FICON configuration over a WAN link using FCIP, you need the appropriate SAN_EXTN_OVER_IP license for the module you are using. For more information, refer to the Cisco NX-OS Family Licensing Guide.

MDS-Specific FICON Advantages

This section explains the additional FICON advantages in Cisco MDS switches and includes the following topics:

- Fabric Optimization with VSANs, page 12-3
- FCIP Support, page 12-5
- PortChannel Support, page 12-5
- VSANs for FICON and FCP Mixing, page 12-5
- Cisco MDS-Supported FICON Features, page 12-5

Fabric Optimization with VSANs

Generally, separate physical fabrics have a high level of switch management and have a higher implementation cost. The ports in each island also may be over-provisioned depending on the fabric configuration.

By using the Cisco MDS-specific VSAN technology, you can introduce greater efficiency between these physical fabrics by lowering the cost of over-provisioning and reducing the number of switches to be managed. VSANs also help you to move unused ports nondisruptively and provide a common redundant physical infrastructure (see Figure 12-2).
About FICON

VSANs enable global SAN consolidation by allowing you to convert existing SAN islands into virtual SAN islands on a single physical network. It provides hardware-enforced security and separation between applications or departments to allow coexistence on a single network. It also allows virtual rewiring to consolidate your storage infrastructure. You can move assets between departments or applications without the expense and disruption of physical relocation of equipment.

**Note**
While you can configure VSANs in any Cisco MDS switch, you can enable FICON in at most eight of these VSANs. The number of VSANs configured depends on the platform.

**Note**
Mainframe users can think of VSANs as being like FICON LPARs in the MDS SAN fabric. You can partition switch resources into FICON LPARs (VSANs) that are isolated from each other, in much the same way that you can partition resources on a zSeries or DS8000. Each VSAN has its own set of fabric services (such as fabric server and name server), FICON Control Unit Port, domain ID, Fabric Shortest Path First (FSPF) routing, operating mode, IP address, and security profile.

FICON LPARs can span line cards and are dynamic in size. For example, one FICON LPAR with 10 ports can span 10 different line cards. FICON LPARs can also include ports on more than one switch in a cascaded configuration. The consistent fairness of the Cisco MDS 9000 switching architecture means that “all ports are created equal,” simplifying provisioning by eliminating the “local switching” issues seen on other vendors’ platforms.
Addition of ports to a FICON LPAR is a nondisruptive process. The maximum number of ports for a FICON LPAR is 255 due to FICON addressing limitations.

**FCIP Support**

The multilayer architecture of the Cisco MDS 9000 Family enables a consistent feature set over a protocol-agnostic switch fabric. Cisco MDS 9500 Series and 9200 Series switches transparently integrate Fibre Channel, FICON, and Fibre Channel over IP (FCIP) in one system. The FICON over FCIP feature enables cost-effective access to remotely located mainframe resources. With the Cisco MDS 9000 Family platform, storage replication services such as IBM PPRC and XRC can be extended over metro to global distances using ubiquitous IP infrastructure which simplifies business continuance strategies.

Refer to the *Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*.

**PortChannel Support**

The Cisco MDS implementation of FICON provides support for efficient utilization and increased availability of Inter-Switch Links (ISLs) necessary to build stable large-scale SAN environments. PortChannels ensure an enhanced ISL availability and performance in Cisco MDS switches.

Refer to the *Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide* for more information on PortChannels.

**VSANs for FICON and FCP Mixing**

Cisco MDS 9000 Family FICON-enabled switches simplify deployment of even the most complex mixed environments. Multiple logical FICON, Z-Series Linux/FCP, and Open-Systems Fibre Channel Protocol (FCP) fabrics can be overlaid onto a single physical fabric by simply creating VSANs as required for each service. VSANs provide both hardware isolation and protocol specific fabric services, eliminating the complexity and potential instability of zone-based mixed schemes.

By default, the FICON feature is disabled in all switches in the Cisco MDS 9000 Family. When the FICON feature is disabled, FC IDs can be allocated seamlessly. Mixed environments are addressed by the Cisco NX-OS software. The challenge of mixing FCP and FICON protocols are addressed by Cisco MDS switches when implementing VSANs.

Switches and directors in the Cisco MDS 9000 Family support FCP and FICON protocol mixing at the port level. If these protocols are mixed in the same switch, you can use VSANs to isolate FCP and FICON ports.

**Tip**

When creating a mixed environment, place all FICON devices in one VSAN (other than the default VSAN) and segregate the FCP switch ports in a separate VSAN (other than the default VSAN). This isolation ensures proper communication for all connected devices.

**Cisco MDS-Supported FICON Features**

The Cisco MDS 9000 Family FICON features include:

- Flexibility and investment protection—The Cisco MDS 9000 Family shares common switching and service modules across the Cisco MDS 9500 Series and the 9200 Series.
About FICON

Refer to the Cisco MDS 9500 Series Hardware Installation Guide and the Cisco MDS 9200 Series Hardware Installation Guide.

- High-availability FICON-enabled director—The Cisco MDS 9500 Series combines nondisruptive software upgrades, stateful process restart and failover, and full redundancy of all major components for a new standard in director-class availability. It supports up to 528 autosensing, 4/2/1-Gbps, 10-Gbps, FICON or FCP ports in any combination in a single chassis. Refer to the Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide.

- Infrastructure protection—Common software releases provide infrastructure protection across all Cisco MDS 9000 platforms. Refer to the Cisco MDS 9000 Family NX-OS Software Upgrade and Downgrade Guide.

- VSAN technology—The Cisco MDS 9000 Family provides VSAN technology for hardware-enforced, isolated environments within a single physical fabric for secure sharing of physical infrastructure and enhanced FICON mixed support. See Chapter 2, “Configuring and Managing VSANs.”

- Port-level configurations—There are BB_credits, beacon mode, and port security for each port. Refer to the Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide for information about buffer-to-buffer credits, beacon LEDs, and trunking.

- Alias name configuration—Provides user-friendly aliases instead of the WWN for switches and attached node devices. See Chapter 5, “Configuring and Managing Zones.”


- Traffic encryption—IPSec is supported over FCIP. You can encrypt FICON and Fibre Channel traffic that is carried over FCIP. Refer to the Cisco MDS 9000 Family NX-OS Security Configuration Guide.

- Local accounting log—View the local accounting log to locate FICON events. For more information about MSCHAP authentication, and local AAA services, refer to the Cisco MDS 9000 Family NX-OS Security Configuration Guide.

- Unified storage management—Cisco MDS 9000 FICON-enabled switches are fully IBM CUP standard compliant for in-band management using the IBM S/A OS/390 I/O operations console. See the “CUP In-Band Management” section on page 12-38.

- Port address-based configurations—Configure port name, blocked or unblocked state, and the prohibit connectivity attributes. See the “Configuring FICON Ports” section on page 12-24.

- You can display the following information:
  - Individual Fibre Channel ports, such as the port name, port number, Fibre Channel address, operational state, type of port, and login data.
  - Nodes attached to ports.
  - Port performance and statistics.

  See the “Calculating FICON Flow Load Balance” section on page 12-40.

- Configuration files—Store and apply configuration files. See the “FICON Configuration Files” section on page 12-28.
Send documentation comments to mdsfeedback-doc@cisco.com

- FICON and Open Systems Management Server features if installed. —See the “VSANs for FICON and FCP Mixing” section on page 12-5.
- Enhanced cascading support—See the “CUP In-Band Management” section on page 12-38.
- Date and time—Set the date and time on the switch. See the “Allowing the Host to Control the Timestamp” section on page 12-22.
- Configure SNMP trap recipients and community names—See the “Configuring SNMP Control of FICON Parameters” section on page 12-22.
- Call Home configurations—Configure the director name, location, description, and contact person. Refer to the Cisco MDS 9000 Family NX-OS System Management Configuration Guide.
- Configure preferred domain ID, FC ID persistence, and principal switch priority—For information about configuring domain parameters, refer to the Cisco MDS 9000 Family NX-OS System Management Configuration Guide.
- Sophisticated SPAN diagnostics—The Cisco MDS 9000 Family provides industry-first intelligent diagnostics, protocol decoding, and network analysis tools as well as integrated Call Home capability for added reliability, faster problem resolution, and reduced service costs. For information about monitoring network traffic using SPAN, refer to the Cisco MDS 9000 Family NX-OS System Management Configuration Guide.
- Configure R_A_TOV, E_D_TOV — See the “Fibre Channel Time-Out Values” section on page 13-2.
- Director-level maintenance tasks—Perform maintenance tasks for the director including maintaining firmware levels, accessing the director logs, and collecting data to support failure analysis. For information about monitoring system processes and logs refer to the Cisco MDS 9000 Family NX-OS System Management Configuration Guide.

FICON Cascading

The Cisco MDS NX-OS software allows multiple switches in a FICON network. To configure multiple switches, you must enable and configure fabric binding in that switch (see the “Calculating FICON Flow Load Balance” section on page 12-40 and refer to the Cisco MDS 9000 Family NX-OS Security Configuration Guide).

FICON VSAN Prerequisites

To ensure that a FICON VSAN is operationally up, be sure to verify the following requirements:
- Set the default zone to permit, if you are not using the zoning feature. See the “About the Default Zone” section on page 5-21.
- Enable in-order delivery on the VSAN. See Chapter 8, “Configuring Fibre Channel Routing Services and Protocols.”
- Enable (and if required, configure) fabric binding on the VSAN. See the “Calculating FICON Flow Load Balance” section on page 12-40. For more information about Fabric Binding, refer to the Cisco MDS 9000 Family NX-OS Security Configuration Guide.
- Verify that conflicting persistent FC IDs do not exist in the switch. For information about configuring domain parameters, refer to the Cisco MDS 9000 Family NX-OS System Management Configuration Guide.
FICON Port Numbering

With reference to the FICON feature, ports in Cisco MDS switches are identified by a statically defined 8-bit value known as the *port number*. A maximum of 255 port numbers are available. You can use the following port numbering schemes:

- Default port numbers based on the chassis type
- Reserved port numbers

This section includes the following topics:

- Default FICON Port Numbering Scheme, page 12-8
- Port Addresses, page 12-11
- Implemented and Unimplemented Port Addresses, page 12-11
- About the Reserved FICON Port Numbering Scheme, page 12-11
- Installed and Uninstalled Ports, page 12-12
- FICON Port Numbering Guidelines, page 12-12
- Assigning FICON Port Numbers to Slots, page 12-13
- About Port Numbers for FCIP and PortChannel, page 12-13
- About the Reserved FICON Port Numbering Scheme, page 12-11
- FC ID Allocation, page 12-14

**Note** You must enable FICON on the switch before reserving FICON port number (see the “About Enabling FICON on a VSAN” section on page 12-15).

Default FICON Port Numbering Scheme

Default FICON port numbers are assigned by the Cisco MDS NX-OS software based on the module and the slot in the chassis. The first port in a switch always starts with a zero (0) (see Figure 12-3).
The default FICON port number is assigned based on the front panel location of the port and is specific to the slot in which the module resides. Thirty-two (32) port numbers are assigned to each slot on all Cisco MDS 9000 Family switches except for the Cisco MDS 9513 Director, which has 16 port numbers assigned for each slot. These default numbers are assigned regardless of the module’s physical presence in the chassis, the port status (up or down), or the number of ports on the module (4, 12, 16, 24, or 48). If a module has fewer ports than the number of port numbers assigned to the slot, then the excess port numbers are unused. If a module has more ports than the number of port numbers assigned to the slot, the excess ports cannot be used for FICON traffic unless you manually assign the port numbers.

Follow the steps in “Assigning FICON Port Numbers to Slots” section on page 12-13 to make use of excess ports by manually assigning more port numbers to the slot. Before doing this, however, we recommend that you review the default port number assignments for Cisco MDS 9000 switches shown in Table 12-3 on page 12-43, and that you read the following sections to gain a complete understanding of FICON port numbering: “About the Reserved FICON Port Numbering Scheme” section on page 12-11, “FICON Port Numbering Guidelines” section on page 12-12, and “Assigning FICON Port Numbers to Slots” section on page 12-13.

Note

Only Fibre Channel, PortChannel, and FCIP ports are mapped to FICON port numbers. Other types of interfaces do not have a corresponding port number.

Table 12-3 lists the default port number assignment for the Cisco MDS 9000 Family of switches and directors.
### Table 12-1  Default FICON Port Numbering in the Cisco MDS 9000 Family

<table>
<thead>
<tr>
<th>Product</th>
<th>Slot Number</th>
<th>Implemented Port Allocation</th>
<th>Unimplemented Ports</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco MDS 9200 Series</td>
<td>Slot 1</td>
<td>0 through 31</td>
<td>64 through 89</td>
<td>Similar to a switching module.</td>
</tr>
<tr>
<td></td>
<td>Slot 2</td>
<td>32 through 63</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco MDS 9222i Series</td>
<td>Slot 1</td>
<td>0 through 31</td>
<td>64 through 89</td>
<td>The first 4, 12, 16, or 24 port numbers in a 4-port, 12-port, 16-port, or 24-port module are used and the rest remain unused. Extra 16 ports on 48-port modules are not allocated numbers.</td>
</tr>
<tr>
<td></td>
<td>Slot 2</td>
<td>32 through 63</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco MDS 9506 Director</td>
<td>Slot 1</td>
<td>0 through 31</td>
<td>128 through 153</td>
<td>Supervisor modules are not allocated port numbers.</td>
</tr>
<tr>
<td></td>
<td>Slot 2</td>
<td>32 through 63</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 3</td>
<td>64 through 95</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 4</td>
<td>96 through 127</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 5</td>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 6</td>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco MDS 9134 Director</td>
<td>Slot 1</td>
<td>0 through 33</td>
<td>34 through 59</td>
<td>The first 4, 12, 16, or 24 port numbers in a 4-port, 12-port, 16-port, or 24-port module are used and the rest remain unused. Extra 16 ports on 48-port modules are not allocated port numbers.</td>
</tr>
<tr>
<td></td>
<td>Slot 2</td>
<td>32 through 63</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 3</td>
<td>64 through 95</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 4</td>
<td>96 through 127</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 5</td>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 6</td>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 7</td>
<td>128 through 159</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 8</td>
<td>160 through 191</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 9</td>
<td>192 through 223</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Send documentation comments to mdsfeedback-doc@cisco.com

Table 12-1  Default FICON Port Numbering in the Cisco MDS 9000 Family (continued)

<table>
<thead>
<tr>
<th>Product</th>
<th>Slot Number</th>
<th>Implemented Port Allocation To Ports</th>
<th>To PortChannel/FCIP</th>
<th>Unimplemented Ports</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco MDS 9513 Director</td>
<td>Slot 1</td>
<td>0 through 15</td>
<td>224 through 249</td>
<td>250 through 253 and port 255</td>
<td>The first 4, 12 or 16 port numbers are used for a 4-port, 12-port or 16-port module and the rest remain unused. Extra ports on 24-port, 32-port, and 48-port modules are not allocated port numbers.</td>
</tr>
<tr>
<td></td>
<td>Slot 2</td>
<td>16 through 31</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 3</td>
<td>32 through 47</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 4</td>
<td>48 through 63</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 5</td>
<td>64 through 79</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 6</td>
<td>80 through 95</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 7</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 8</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 9</td>
<td>96 through 111</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 10</td>
<td>112 through 127</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 11</td>
<td>128 through 143</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 12</td>
<td>144 through 159</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slot 13</td>
<td>160 through 175</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Port Addresses**

By default, port numbers are the same as port addresses. You can swap the port addresses (see the “Port Swapping” section on page 12-31).

**Implemented and Unimplemented Port Addresses**

An implemented port refers to any port address that is assigned by default to a slot in the chassis (see Table 12-3). An unimplemented port refers to any port address that is not assigned by default to a slot in the chassis (see Table 12-3).

**About the Reserved FICON Port Numbering Scheme**

A range of 250 port numbers are available for you to assign to all the ports on a switch. Table 12-3 shows that you can have more than 250 physical ports on a switch and the excess ports do not have port numbers in the default numbering scheme. When you have more than 250 physical ports on your switch, you can have ports without a port number assigned if they are not in a FICON VSAN, or you can assign duplicate port numbers if they are not used in the same FICON VSAN. For example, you can configure port number 1 on interface fc1/1 in FICON VSAN 10 and fc10/1 in FICON VSAN 20.

**Note**

A VSAN can have a maximum of 250 port numbers.
FICON Port Numbering

Note: FICON port numbers are not changed for ports that are active. You must first disable the interfaces using the `shutdown` command.

Note: You can configure port numbers even when no module is installed in the slot.

Installed and Uninstalled Ports

An installed port refers to a port for which all required hardware is present. A specified port number in a VSAN can be implemented, and yet not installed, if any of the following conditions apply:

- The module is not present—For example, if module 1 is not physically present in slot 1 in a Cisco MDS 9509 Director, ports 0 to 31 are considered uninstalled.
- The small form-factor pluggable (SFP) port is not present—For example, if a 16-port module is inserted in slot 2 in a Cisco MDS 9509 Director, ports 48 to 63 are considered uninstalled.
- For slot 1, ports 0 to 31, or 0 to 15 have been assigned. Only the physical port fc1/5 with port number 4 is in VSAN 2. The rest of the physical ports are not in VSAN 2. The port numbers 0 to 249 are considered implemented for any FICON-enabled VSAN. Therefore, VSAN 2 has port numbers 0 to 249 and one physical port, fc1/4. The corresponding physical ports 0 to 3, and 5 to 249 are not in VSAN 2. When the FICON VSAN port address is displayed, those port numbers with the physical ports not in VSAN 2 are not installed (for example, ports 0 to 3, or 5 to 249).
- The port is part of a PortChannel—For example, if interface fc1/1 is part of PortChannel 5, port address 0 is uninstalled in all FICON VSANs. See Table 12-3.

FICON Port Numbering Guidelines

The following guidelines apply to FICON port numbers:

- Supervisor modules do not have port number assignments.
- Port numbers do not change based on TE ports. Since TE ports appear in multiple VSANs, chassis-wide unique port numbers should be reserved for TE ports.
- Each PortChannel must be explicitly associated with a FICON port number.
- When the port number for a physical PortChannel becomes uninstalled, the relevant PortChannel configuration is applied to the physical port.
- Each FCIP tunnel must be explicitly associated with a FICON port number. If the port numbers are not assigned for PortChannels or for FCIP tunnels, then the associated ports will not come up.

See the “About Port Numbers for FCIP and PortChannel” section on page 12-13.
Assigning FICON Port Numbers to Slots

**Caution**

When you assign, change, or release a port number, the port reloads.

To assign FICON port numbers to slots using Device Manager, follow these steps:

**Step 1**
Click **FICON** and then select **Port Numbers**.

You see the FICON port numbers (see Figure 12-4).

**Figure 12-4  FICON Port Numbers**

**Step 2**
Enter the chassis slot port numbers in the Reserved Port Numbers field.

**Step 3**
Click **Apply**.

**About Port Numbers for FCIP and PortChannel**

FCIP and PortChannels cannot be used in a FICON-enabled VSAN unless they are explicitly bound to a port number.

See the “Configuring FICON Ports” section on page 12-24 and the “Reserving FICON Port Numbers for FCIP and PortChannel Interfaces” section on page 12-13.

You can use the default port numbers if they are available (see Table 12-1 on page 12-10) or if you reserve port numbers from the pool of port numbers that are not reserved for Fibre Channel interfaces (see the “FICON Port Numbering” section on page 12-8).

**Reserving FICON Port Numbers for FCIP and PortChannel Interfaces**

You must reserve port numbers for logical interfaces, such as FCIP and PortChannels, if you plan to use them.

To reserve FICON port numbers for FCIP and PortChannel interfaces using Device Manager, follow these steps:
FICON Port Numbering

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

**Step 1** Click FICON > Port Numbers.
You see the FICON port numbers dialog box (see Figure 12-4).

**Step 2** Click the Logical tab to see the reserved port numbers for the slot (see Figure 12-5).

**Figure 12-5 Reserved Port Numbers for the Selected Slot**

Step 3 Enter the chassis slot port numbers. These are the reserved port numbers for one chassis slot. There can be up to 64 port numbers reserved for each slot in the chassis.

Step 4 Click Apply.

### FC ID Allocation

FICON requires a predictable and static FC ID allocation scheme. When FICON is enabled, the FC ID allocated to a device is based on the port address of the port to which it is attached. The port address forms the middle byte of the fabric address. Additionally, the last byte of the fabric address should be the same for all devices in the fabric. By default, the last byte value is 0 and can be configured (see the "Assigning FC ID Last Byte" section on page 12-20).

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

Cisco MDS switches have a dynamic FC ID allocation scheme. When FICON is enabled or disabled on a VSAN, all the ports are shut down and restarted to switch from the dynamic to static FC IDs and vice versa (see Figure 12-6).

**Figure 12-6 Static FC ID Allocation for FICON**

Static FC ID allocation for interface fc3/5 includes the static domain ID (5), the port address (0x44), and the last byte value (0).
Configuring FICON

By default FICON is disabled in all switches in the Cisco MDS 9000 Family. You can enable FICON on a per VSAN basis by using the Device Manager.

This section includes the following topics:

- **About Enabling FICON on a VSAN**, page 12-15
- **Setting Up a Basic FICON Configuration**, page 12-16
- **Manually Enabling FICON on a VSAN**, page 12-18
- **Deleting FICON VSANs**, page 12-18
- **Suspending a FICON VSAN**, page 12-19
- **Configuring the code-page Option**, page 12-19
- **Assigning FC ID Last Byte**, page 12-20
- **Allowing the Host to Move the Switch Offline**, page 12-21
- **Allowing the Host to Change FICON Port Parameters**, page 12-22
- **Allowing the Host to Control the Timestamp**, page 12-22
- **Configuring SNMP Control of FICON Parameters**, page 12-22
- **FICON Information Refresh**, page 12-23
- **About FICON Device Allegiance**, page 12-23
- **Automatically Saving the Running Configuration**, page 12-23

**About Enabling FICON on a VSAN**

By default FICON is disabled in all VSANs on the switch.

You can enable FICON on a per VSAN basis in one of the following ways:

- Manually address each prerequisite.
  
  See the “About FICON” section on page 12-1.

- Use Device Manager.

When you enable the FICON feature in Cisco MDS switches, the following restrictions apply:

- You cannot disable in-order delivery for the FICON-enabled VSAN.
- You cannot disable fabric binding or static domain ID configurations for the FICON-enabled VSAN.
- The load balancing scheme is changed to Source ID (SID)—Destination ID (DID). You cannot change it back to SID—DID—OXID.
- The IPL configuration file is automatically created.

  See the “About FICON Configuration Files” section on page 12-29.
Tip
Using Device Manager, FICON auto-save can be invoked by multiple users logged on to the same FICON-enabled switch. Device Manager performs a periodic auto-save on any FICON-enabled switch causing increments in the FICON key counter. These increments highlight a change that has actually not occurred. To avoid this we recommend that only one instance of Device Manager monitor a FICON-enabled switch.

Setting Up a Basic FICON Configuration

This section steps you through the procedure to set up FICON on a specified VSAN in a Cisco MDS 9000 Family switch.

To create a FICON-enabled VSAN using Fabric Manager, follow these steps:

Step 1
Click the Create VSAN icon (see Figure 12-7).

Figure 12-7 Create VSAN Icon

You see the Create VSAN dialog box (see Figure 12-8).
Configuring FICON

Step 2 Select the switches you want to be in the VSAN.
Step 3 Enter a VSAN ID.
Step 4 Enter the name of the VSAN, if desired.
Step 5 Select the type of load balancing, the interop value, and the administrative state for this VSAN.
Step 6 Check the FICON check box.

Note You cannot enable interop modes on FICON-enabled VSANs.

Step 7 Check the option, if appropriate, to enable fabric binding for the selected switches.
Step 8 Check the All Ports Prohibited option if all ports in this VSAN are prohibited.
Step 9 Click Create to create the VSAN.
Step 10 Choose Tools > Device Manager to open Device Manager for each switch in the FICON VSAN.
Step 11 Click FC > VSANs.
You see the VSAN dialog box (see Figure 12-9).
Configuring FICON

Step 12 Enter the VSAN membership information.
Step 13 Click the VSAN you want to become a FICON VSAN and select Add from the FICON drop-down menu.
Step 14 Click Apply to save these changes.

Manually Enabling FICON on a VSAN

Note This section describes the procedure to manually enable FICON on a VSAN. If you have already enabled FICON on the required VSAN using the automated setup (recommended), skip to the “Automatically Saving the Running Configuration” section on page 12-23.

To manually enable FICON on a VSAN using Fabric Manager, follow these steps:

Step 1 Choose VSAN > FICON.
You see the FICON VSAN configuration information in the Information pane.
Step 2 Select the switch in the VSAN on which you want to enable FICON.
Step 3 Click enable from the Command drop-down menu.
Step 4 Click the Apply Changes icon to save these changes.

Deleting FICON VSANs

To delete a FICON VSAN using Fabric Manager, follow these steps:

Step 1 Select All VSANS.
You see the VSAN table in the Information pane (see Figure 12-10).
Configuring FICON

Send documentation comments to mdsfeedback-doc@cisco.com

Figure 12-10  All VSANs Table

Step 2  Click anywhere in the row of the VSAN that you want to delete.
Step 3  Click **Delete Row** to delete the VSAN.

Note  Deleting the VSAN will also delete the associated FICON configuration file, and the file cannot be recovered.

Suspending a FICON VSAN

To suspend a FICON VSAN using Fabric Manager, follow these steps:

Step 1  Click **All VSANs**.
You see all the VSANs listed in the Information pane.
Step 2  Select the VSAN that you want to suspend.
Step 3  Set the Admin drop-down menu for a VSAN to **suspended**.
Step 4  Click the **Apply Changes** icon to save these changes.

Note  This command can be issued by the host if the host is allowed to do so (see the “Allowing the Host to Move the Switch Offline” section on page 12-21).

Configuring the code-page Option

FICON strings are coded in Extended Binary-Coded Decimal Interchange Code (EBCDIC) format. Refer to your mainframe documentation for details on the code page options.

Cisco MDS switches support **international-5, france, brazil, germany, italy, japan, spain-latinamerica, uk, and us-canada** (default) EBCDIC format options.
Configuring FICON

Tip

This is an optional configuration. If you are not sure of the EBCDIC format to be used, we recommend retaining the **us-canada** (default) option.

To modify the code-page option using Device Manager, follow these steps:

**Step 1**

Choose **FICON > VSANs**.

You see the FICON VSAN configuration dialog box (see **Figure 12-11**). The VSANs tab is the default tab.

**Figure 12-11  FICON VSANs Tab in Device Manager**

**Step 2**

Choose an option from the CodePage drop-down menu for the FICON VSAN you want to configure (US-Canada is configured in **Figure 12-11**).

**Step 3**

Click **Apply** to save the changes.

Assigning FC ID Last Byte

**Caution**

If the FICON feature is configured in cascaded mode, the Cisco MDS switches use ISLs to connect to other switches.

To assign the last byte for the FC ID using Fabric Manager, follow these steps:

**Step 1**

Choose **All VSANs > Domain Manager**.

**Step 2**

Click the **Persistent FCIDs** tab.

You see the Persistent FcIds tab (see **Figure 12-12**).
Step 3  Select **single** in the Mask column and then assign the entire FC ID at once. The single option allows you to enter the FC ID in the ###### format.

Step 4  Click the **Apply Changes** icon to save these changes.

---

**Allowing the Host to Move the Switch Offline**

By default, hosts are allowed to move the switch to an offline state. To do this, the host sends a "Set offline" command (xFD') to the control unit port (CUP).

To allow the host (mainframe) to move the switch to an offline state using Fabric Manager, follow these steps:

Step 1  Choose **VSAN > FICON**.

You see a list of switches under the Control tab in the Information pane.

Step 2  Click the **VSANs** tab.

You see the FICON VSAN configuration information in the Information pane (see Figure 12-13).

Step 3  Check the **Host Can Offline Sw** check box to allow the mainframe to move a switch to the offline state.

Step 4  Check the **Host Can Sync Time** check box to allow the mainframe to set the system time on the switch.

Step 5  Click the **Apply Changes** icon to save the changes.
Allowing the Host to Change FICON Port Parameters

By default, mainframe users are not allowed to configure FICON parameters on Cisco MDS switches—they can only query the switch.

To allow the host (mainframe) to configure FICON parameters on the Cisco MDS switch using Fabric Manager, follow these steps:

**Step 1** Choose VSAN > FICON.

You see a list of switches under the Control tab in the Information pane.

**Step 2** Click the VSANs tab.

You see the FICON VSAN configuration information in the Information pane (see Figure 12-13).

**Step 3** Check the Port Control By Host check box to allow the mainframe to control a switch.

**Step 4** Click the Apply Changes icon to save the changes.

Allowing the Host to Control the Timestamp

By default, the clock in each VSAN is the same as the switch hardware clock. Each VSAN in a Cisco MDS 9000 Family switch represents a virtual director. The clock and time present in each virtual director can be different. To maintain separate clocks for each VSAN, the Cisco NX-OS software maintains the difference of the VSAN-specific clock and the hardware-based director clock. When a host (mainframe) sets the time, the Cisco NX-OS software updates this difference between the clocks. When a host reads the clock, it computes the difference between the VSAN-clock and the current director hardware clock and presents a value to the mainframe.

To configure host (mainframe) control for the VSAN time stamp using Fabric Manager, follow these steps:

**Step 1** Choose VSAN > FICON.

You see a list of switches under the Control tab in the Information pane.

**Step 2** Click the VSANs tab.

You see the FICON VSAN configuration information in the Information pane (see Figure 12-13).

**Step 3** Check the Host Can Sync Time checkbox to allow the mainframe to set the system time on the switch.

**Step 4** Click the Apply Changes icon to save these changes.

Configuring SNMP Control of FICON Parameters

By default, SNMP users can configure FICON parameters through the Cisco MDS 9000 Family Fabric Manager.
To configure SNMP control of FICON parameters using Fabric Manager, follow these steps:

**Step 1** Choose **VSAN > FICON**.
You see a list of switches under the Control tab in the Information pane.

**Step 2** Click the **VSANs** tab.
You see the FICON VSAN configuration information in the Information pane (see Figure 12-13).

**Step 3** Check the **Port Control By SNMP** checkbox to allow SNMP users to configure FICON on the switch.

**Step 4** Click the **Apply Changes** icon to save these changes.

---

**FICON Information Refresh**

When viewing FICON information through the Device Manager dialog boxes, you must manually refresh the display by clicking the **Refresh** button to see the latest updates. You need to take this step whether you configure FICON through the CLI or through the Device Manager.

There is no automatic refresh of FICON information. This information would be refreshed so often that it would affect performance.

---

**About FICON Device Allegiance**

FICON requires serialization of access among multiple mainframes, CLI, and SNMP sessions be maintained on Cisco MDS 9000 Family switches by controlling device allegiance for the currently executing session. Any other session is denied permission to perform configuration changes unless the required allegiance is available.

**Caution**

This task discards the currently executing session.

---

**Automatically Saving the Running Configuration**

Cisco MDS NX-OS provides an option to automatically save any configuration changes to the startup configuration. This ensures that the new configuration is present after a switch reboot. The **Active=Saved** option can be enabled on any FICON VSAN.

**Table 12-2** displays the results of the **Active = Saved** option and the implicit copy from the running configuration to the startup configuration (**copy running start**) in various scenarios.

If the **Active=Saved** option is enabled in any FICON-enabled VSAN in the fabric, then the following apply (see Number 1 and 2 in Table 12-2):

- All configuration changes (FICON-specific or not) are automatically saved to persistent storage (implicit **copy running start**) and stored in the startup configuration.
**Configuring FICON Ports**

You can perform FICON configurations on a per-port address basis in the Cisco MDS 9000 Family switches. Even if a port is uninstalled, the port address-based configuration is accepted by the Cisco MDS switch. This configuration is applied to the port when the port becomes installed.

This section includes the following topics:

- Configuring Port Blocking, page 12-25

---

**Table 12-2  Saving the Active FICON and Switch Configuration**

<table>
<thead>
<tr>
<th>Number</th>
<th>FICON-enabled VSAN?</th>
<th>active equals saved Enabled?</th>
<th>Implicit copy running start Issued?</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Yes</td>
<td>Yes (in all FICON VSANs)</td>
<td>Implicit</td>
<td>FICON changes written to the IPL file. Non-FICON changes saved to startup configuration and persistent storage.</td>
</tr>
<tr>
<td>2</td>
<td>Yes</td>
<td>Yes (even in one FICON VSAN)</td>
<td>Implicit</td>
<td>FICON changes written to IPL file for only the VSAN that has active equals saved option enabled. Non-FICON changes saved to startup configuration and persistent storage.</td>
</tr>
<tr>
<td>3</td>
<td>Yes</td>
<td>Not in any FICON VSAN</td>
<td>Not implicit</td>
<td>FICON changes are not written to the IPL file. Non-FICON changes are saved in persistent storage—only if you explicitly issue the copy running start command.</td>
</tr>
<tr>
<td>4</td>
<td>No</td>
<td>Not applicable</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To save the running config, follow these steps:

**Step 1** Choose VSAN > FICON.
You see a list of switches under the Control tab in the Information pane.

**Step 2** Click the VSANs tab.
You see the FICON VSAN configuration information in the Information pane (see Figure 12-13).

**Step 3** Check the Active=Saved check box to automatically save the running configuration to the startup configuration whenever there is a FICON configuration change.

**Step 4** Click the Apply Changes icon to save these changes.
Configuring Port Blocking

If you block a port, the port is retained in the operationally down state. If you unblock a port, a port initialization is attempted. When a port is blocked, data and control traffic are not allowed on that port. Physical Fibre Channel port blocks will continue to transmit an Off-line state (OLS) primitive sequence on a blocked port.

**Caution**

You cannot block or prohibit the CUP port (0xFE).

If a port is shut down, unblocking that port does not initialize the port.

**Note**

The shutdown/no shutdown port state is independent of the block/no block port state.

To block or unblock port addresses in a VSAN using Device Manager, follow these steps:

**Step 1**
Choose **FICON > VSANs**.

**Step 2**
Select a VSAN ID and click **Port Configuration**.

You see the FICON Port Configuration dialog box for the selected VSAN (see Figure 12-14).

**Figure 12-14  FICON Port Configuration Dialog Box**

**Step 3**
Check the **Blocked** check box for the port that you want to block.

**Step 4**
Click **Apply** to save the changes.
Viewing ESCON Style Ports

To view the available and prohibited ESCON style ports using Device Manager, follow these steps:

**Step 1**  
Check the **ESCON Style** check box to see the available and prohibited ESCON style ports.  
In Figure 12-15, A stands for available and P stands for prohibited.  
When the port address is highlighted red, it represents the E/TE port or multiple interfaces.

**Figure 12-15  ESCON Style**

![ESCON Style Configuration](image-url)  

**Step 2**  
Click **Apply** to save the changes.

Port Prohibiting

To prevent implemented ports from talking to each other, configure prohibits between two or more ports.  
If you prohibit ports, the specified ports are prevented from communicating with each other.

**Tip**

You cannot prohibit a PortChannel or FCIP interface.

Unimplemented ports are always prohibited. In addition, prohibit configurations are always symmetrically applied—if you prohibit port 0 from talking to port 15, port 15 is automatically prohibited from talking to port 0.

**Note**

If an interface is already configured in E or TE mode and you try to prohibit that port, your prohibit configuration is rejected. Similarly, if a port is not up and you prohibit that port, the port is not allowed to come up in E mode or in TE mode.

Configuring Port Prohibiting

To prohibit port addresses in a VSAN using Device Manager, follow these steps:
**Send documentation comments to mdsfeedback-doc@cisco.com**

---

**Step 1** Choose **FICON > VSANs**.

**Step 2** Select a VASAN ID and click **Port Configuration**.

You see the FICON Port Configuration dialog box (see Figure 12-14).

**Step 3** Set the port prohibit configuration for the selected FICON VSANs.

**Step 4** Click **Apply** to save these changes.

---

### Assigning a Port Address Name

**Note**

To view the latest FICON information, you must click the **Refresh** button. See the “Automatically Saving the Running Configuration” section on page 12-23.

To assign a port address name in Device Manager, follow these steps:

**Step 1** Choose **FICON > VSANs**.

**Step 2** Select a VSAN ID and click **Port Configuration**.

You see the FICON Port Configuration dialog box (see Figure 12-14).

**Step 3** Enter the Port Configuration information.

**Step 4** Click **Apply** to save the configuration information.

---

### About RLIR

The Registered Link Incident Report (RLIR) application provides a method for a switch port to send an Link Incident Record (LIR) to a registered Nx port. It is a highly available application.

When an LIR is detected in FICON-enabled switches in the Cisco MDS 9000 Family from a RLIR Extended Link Service (ELS), the switch sends that record to the members in its Established Registration List (ERL).

In case of multiswitch topology, a Distribute Registered Link Incident Record (DRLIR) Inter-Link Service (ILS) is sent to all reachable remote domains along with the RLIR ELS. On receiving the DRLIR ILS, the switch extracts the RLIR ELS and sends it to the members of the ERL.

The Nx ports interested in receiving the RLIR ELS send the Link Incident Record Registration (LIRR) ELS request to the management server on the switch. The RLIRs are processed on a per-VSAN basis.

The RLIR data is written to persistent storage when you **copy** the running configuration to the startup configuration.

---

### Displaying RLIR Information

To view RLIR information using Device Manager, follow these steps:
Step 1  Choose FICON > RLIR ERL.
You see the Show RLIR ERL dialog box (see Figure 12-16).

Figure 12-16  Show RLIR ERL Dialog Box

Step 2  Click Close to close the dialog box.

FICON Configuration Files

You can save up to 16 FICON configuration files on each FICON-enabled VSAN (in persistent storage). The file format is proprietary to IBM. These files can be read and written by IBM hosts using the in-band CUP protocol. Additionally, you can use the Cisco MDS CLI or Fabric Manager applications to operate on these FICON configuration files.

Note
Multiple FICON configuration files with the same name can exist in the same switch, provided they reside in different VSANs. For example, you can create a configuration file named XYZ in both VSAN 1 and VSAN 3.

When you enable the FICON feature in a VSAN, the switches always use the startup FICON configuration file, called IPL. This file is created with a default configuration as soon as FICON is enabled in a VSAN.

Caution
When FICON is disabled on a VSAN, all the FICON configuration files are irretrievably lost.

FICON configuration files contain the following configuration for each implemented port address:
- Block
- Prohibit mask
- Port address name
About FICON Configuration Files

Only one user can access the configuration file at any given time:

- If this file is being accessed by user 1, user 2 cannot access this file.
- If user 2 does attempt to access this file, an error is issued to user 2.
- If user 1 is inactive for more than 15 seconds, the file is automatically closed and available for use by any other permitted user.

FICON configuration files can be accessed by any host, SNMP, or CLI user who is permitted to access the switch. The locking mechanism in the Cisco NX-OS software restricts access to one user at a time per file. This lock applies to newly created files and previously saved files. Before accessing any file, you must lock the file and obtain the file key. A new file key is used by the locking mechanism for each lock request. The key is discarded when the lock timeout of 15 seconds expires. The lock timeout value cannot be changed.

Applying the Saved Configuration Files to the Running Configuration

To apply the saved configuration files to the running configuration using Device Manager, follow these steps:

Step 1 Choose FICON > VSANs.

Step 2 Click the Files tab.

You see the FICON Files dialog box (see Figure 12-17).
Figure 12-17  FICON VSANs Dialog Box

Step 3  Highlight the file you want to apply and click Apply File to apply the configuration to the running configuration.

Editing FICON Configuration Files

The configuration file submode allows you to create and edit FICON configuration files. If a specified file does not exist, it is created. Up to 16 files can be saved. Each file name is restricted to eight alphanumeric characters.

To view the latest FICON information, you must click the Refresh button. See the “Automatically Saving the Running Configuration” section on page 12-23.

To edit the contents of a specified FICON configuration file using Device Manager, follow these steps:

Step 1  Choose FICON > VSANs.
Step 2  Click the Files tab.
Step 3  Select a VSAN ID and then click Open to edit the FICON configuration file.
Step 4  Select a VSAN ID and then click Delete to delete the FICON configuration file.
Step 5  Click Apply to apply the changed FICON configuration file.

Displaying FICON Configuration Files

To open and view configuration files in Fabric Manager, follow these steps:

Step 1  Choose FICON > VSAN.
Step 2  Click the Files tab.
Step 3  Select the file you want to open.
Copy FICON Configuration Files

To copy an existing FICON configuration file using Device Manager, follow these steps:

**Step 1** Choose FICON > VSANs.

**Step 2** Click the Files tab.

You see the FICON VSANs dialog box (see Figure 12-17).

**Step 3** Click Create to create a FICON configuration file.

You see the Create FICON VSANs Files dialog box shown in Figure 12-18.

**Figure 12-18 Create FICON VSANs Files Dialog Box in Device Manager**

- Select a VSAN ID for the FICON VSAN you want to configure.
- Enter the file name and the description.
- Click Create to create the file.

**Step 4** Click Copy to copy the file to a new file.

**Step 5** Click Apply to apply the FICON configuration file.

Port Swapping

The FICON port-swapping feature is only provided for maintenance purposes.

The FICON port-swapping feature causes all configurations associated with old-port-number and new port-number to be swapped, including VSAN configurations.

Cisco MDS switches allow port swapping for nonexistent ports as follows:

- Only FICON-specific configurations (prohibit, block, and port address mapping) are swapped.
- No other system configuration is swapped.
- All other system configurations are only maintained for existing ports.
If you swap a port in a module that has unlimited oversubscription ratios enabled with a port in a module that has limited oversubscription ratios, then you may experience a degradation in bandwidth.

**Tip**
If you check the Active=Saved check box on any FICON VSAN, then the swapped configuration is automatically saved to startup. Otherwise, you must explicitly save the running configuration immediately after swapping the ports.

Once you swap ports, the switch automatically performs the following actions:
- Shuts down both the old and new ports.
- Swaps the port configuration.

If you attempt to bring the port up, you must explicitly shut down the port to resume traffic.

**Note**
To view the latest FICON information, you must click the Refresh button. See the “Automatically Saving the Running Configuration” section on page 12-23.

This section includes the following topics:
- About Port Swapping, page 12-32
- Swapping Ports, page 12-33

### About Port Swapping

Be sure to follow these guidelines when using the FICON port swapping feature:
- Port swapping is not supported for logical ports (PortChannels, FCIP links). Neither the old-port-number nor the new-port-number can be a logical port.
- Port swapping is not supported between physical ports that are part of a PortChannel. Neither the old-port-number nor the new-port-number can be a physical port that is part of a PortChannel.
- Before performing a port swap, the Cisco NX-OS software performs a compatibility check. If the two ports have incompatible configurations, the port swap is rejected with an appropriate reason code. For example, if a port with BB_credits as 25 is being swapped with an OSM port for which a maximum of 12 BB_credits is allowed (not a configurable parameter), the port swapping operation is rejected.
- Before performing a port swap, the Cisco NX-OS software performs a compatibility check to verify the extended BB_credits configuration.
- If ports have default values (for some incompatible parameters), then a port swap operation is allowed and the ports retain their default values.
- Port tracking information is not included in port swapping. This information must be configured separately (refer to the *Cisco MDS 9000 Family NX-OS Quality of Service Configuration Guide*).

**Note**
The 32-port module guidelines also apply for port swapping configurations.
Swapping Ports

To swap ports using Device Manager, follow these steps:

**Step 1** Select two Fibre Channel ports by holding down the **CTRL** key and clicking them.

**Step 2** Choose **FICON > Swap Selected Ports** (see Figure 12-19).

---

**FICON Tape Acceleration**

The sequential nature of tape devices causes each I/O operation to the tape device over an FCIP link to incur the latency of the FCIP link. Throughput drastically decreases as the round-trip time through the FCIP link increases, leading to longer backup windows. Also, after each I/O operation, the tape device is idle until the next I/O arrives. Starting and stopping of the tape head reduces the lifespan of the tape, except when I/O operations are directed to a virtual tape.

Cisco MDS NX-OS software provides acceleration for the following FICON tape write operations:

- The link between mainframe and native tape drives (both IBM and Sun/STK)
- The back-end link between the VSM (Virtual Storage Management) and tape drive (Sun/STK)

FICON tape acceleration over FCIP provides the following advantages:

- Efficiently utilizes the tape device by decreasing idle time
- More sustained throughput as latency increases
- Similar to FCP tape acceleration, and does not conflict with it

---

**Note**

FICON tape read acceleration over FCIP is not supported.

---

Figure 12-20 through Figure 12-23 show supported configurations:
Chapter 12      Configuring FICON

FICON Tape Acceleration

Send documentation comments to mdsfeedback-doc@cisco.com

Figure 12-20    Host Directly Accessing IBM/STK (StorageTek) Library

Figure 12-21    Host Accessing Standalone IBM-VTS (Virtual Tape Server) /STK-VSM (Virtual Shared Memory)

Figure 12-22    Host Accessing Peer-to-Peer VTS (Virtual Tape Server)
Configuring FICON Tape Acceleration

FICON tape acceleration has the following configuration considerations:

- In addition to the normal FICON configuration, FICON tape acceleration must be enabled on both ends of the FCIP interface. If only one end has FICON tape acceleration enabled, acceleration does not occur.
- FICON tape acceleration is enabled on a per VSAN basis.
- FICON tape acceleration cannot function if multiple ISLs are present in the same VSAN (PortChannels or FSPF load balanced).
- You can enable both Fibre Channel write acceleration and FICON tape acceleration on the same FCIP interface.
- Enabling or disabling FICON tape acceleration disrupts traffic on the FCIP interface.

To configure FICON tape acceleration over FCIP in Fabric Manager, follow these steps:

1. Expand ISL and then select FCIP in the Physical Attributes pane.
2. Click the Tunnels tab in the Information pane.

You see a list of available switches (Figure 12-24).

Note

For information about FCIP tape acceleration, refer to the Cisco MDS 9000 Family NX-OS IP Services Configuration Guide.
Step 3

Click the Create Row icon to create an FCIP tunnel.

You see the Create FCIP Tunnel dialog box shown in Figure 12-25.
**Configuring XRC Acceleration**

IBM z/OS Global Mirror eXtended Remote Copy (XRC) is supported on the MSM-18+4 modules. For XRC to function, XRC acceleration must be enabled on the FCIP tunnel interfaces on both ends. XRC acceleration is disabled by default.

**Note**

XRC acceleration and FICON tape acceleration cannot be enabled on the same FCIP tunnel interface and cannot exist in the same VSAN.

---

**Step 4**  
Configure the tunnel with the options shown in Figure 12-25.

**Step 5**  
Check the **TapeAccelerator** check box to enable FICON tape acceleration over this FCIP tunnel.

**Step 6**  
Click **Create**.
To configure XRC acceleration on a FCIP tunnel interface using Fabric Manager, follow these steps:

**Step 1** Expand ISL and then select FCIP in the Physical Attributes pane.
**Step 2** Click the Tunnels(Advanced) tab in the Information pane.
**Step 3** Check the check box in the XRC Emulator column to enable XRC acceleration over the FCIP tunnel.
**Step 4** Click Apply.

To configure XRC acceleration on an FCIP tunnel interface using Device Manager, follow these steps:

**Step 1** In the Device Manager window, click IP and then select FCIP from the menu.
**Step 2** Click the Tunnels(Advanced) tab in the Information pane.
**Step 3** Check the check box in the XRC Emulator column to enable XRC acceleration over the FCIP tunnel.
**Step 4** Click Apply.

### Displaying XRC Acceleration Statistics

To display XRC acceleration statistics using the Fabric Manager, follow these steps:

**Step 1** Expand ISL and then select FCIP in the Physical Attributes pane.
**Step 2** Click the XRC Statistics tab in the Information pane.
You see the XRC session statistics.

To display XRC acceleration statistics using the Device Manager, follow these steps:

**Step 1** In the Device Manager window, click IP and then select FCIP from the menu.
**Step 2** Click the XRC Statistics tab in the Information pane.
You see the XRC session statistics.

### CUP In-Band Management

The Control Unit Port (CUP) protocol configures access control and provides unified storage management capabilities from a mainframe computer. Cisco MDS 9000 FICON-enabled switches are fully IBM CUP standard compliant for in-band management using the IBM S/A OS/390 I/O operations console.
The CUP specification is proprietary to IBM.

CUP is supported by switches and directors in the Cisco MDS 9000 Family. The CUP function allows the mainframe to manage the Cisco MDS switches. Host communication includes control functions such as blocking and unblocking ports, as well as monitoring and error reporting functions.

**Step 1**
In Fabric Manager, choose **Zone > Edit Full Zoneset**, and then choose **Edit > Edit Default Zone Attributes** to set the default zone to permit for the required VSAN. (See **Figure 12-26**.)

**Figure 12-26 Setting the Default Zone Policy**

**Step 2**
In Device Manager, choose **FC > Name Server...** for the required VSAN and obtain the FICON:CUP WWN. See **Figure 12-27**.

**Figure 12-27 Finding pWWN for FICON:CUP**

**Note**
If more than one FICON:CUP WWN exists in this fabric, be sure to add all the FICON:CUP pWWNs to the required zone.

**Step 3**
In Fabric Manager, choose **Zone > Edit Full Zoneset** and add the FICON:CUP pWWN to the zone database. (See **Figure 12-28**.)
Calculating FICON Flow Load Balance

The FICON Flow Load Balance Calculator allows you to get the best load balancing configuration for your FICON flows. The calculator does not rely on any switch or flow discovery in the fabric. It is available from the Fabric Manager Tools menu.

To use the FICON Flow Load Balance Calculator from Fabric Manager, follow these steps:

**Step 1** Choose Tools > Other > Flow Load Balance Calculator.

You see the Flow Load Balance Calculator (see Figure 12-29).
Figure 12-29  Flow Load Balance Calculator

Step 2  Click Add to enter the source and destination(s) flows.
Step 3  Enter source and destination using 2 byte hex (by domain and area IDs). You can copy and paste these IDs, and then edit them if required.
Step 4  Enter (or select) the number of ISLs between the two switches (for example, between domain ID 0a and 0b).
Step 5  Select a row to remove it and click Remove.
Step 6  Select the module for which you are calculating the load balance.
Step 7  Click Calculate to show the recommended topology.

Note  If you change flows or ISLs, you must click Calculate to see the new recommendation.

Displaying FICON Information

This section includes the following topics:

- Receiving FICON Alerts, page 12-42
- Displaying FICON Port Address Information, page 12-42
- Displaying IPL File Information, page 12-42
- Viewing the History Buffer, page 12-42
Receiving FICON Alerts

To receive an alert to indicate any changes in the FICON configuration using Device Manager, follow these steps:

**Step 1** Choose FICON > VSANs.
You see the FICON VSANs dialog box.

**Step 2** Check the **User Alert Mode** check box to receive an alert when the FICON configuration changes.

**Step 3** Click **Apply** to apply this change.

Displaying FICON Port Address Information

To display FICON port address information using Device Manager, follow these steps:

**Step 1** Choose FICON > VSANs.
You see the FICON VSANs dialog box.

**Step 2** Select a VSAN ID and click **Port Configuration**.
You see the FICON Port Configuration dialog box.

**Step 3** Click **Close** to close the dialog box.

Displaying IPL File Information

To display the IPL file information using Device Manager, follow these steps:

**Step 1** Select VSANs from the FICON menu.
**Step 2** Click the **Files** tab.
You see the FICON VSANs dialog box.

**Step 3** Select the file that you want to view and click **Open**.

Viewing the History Buffer

In the directory history buffer, the **Key Counter** column displays the 32-bit value maintained by Cisco MDS switches. This value is incremented when any port changes state in that VSAN. The key counter (a 32-bit value) is incremented when a FICON-related configuration is changed. Host programs can increment this value at the start of the channel program and then perform operations on multiple ports. The director history buffer keeps a log of which port address configuration was changed for each key-counter value.
Send documentation comments to mdsfeedback-doc@cisco.com

The director history buffer provides a mechanism to determine the change in the port state from the previous time when a value was contained in the key counter. To view the directory history buffer using Device Manager, follow these steps:

Step 1 Choose **FICON > VSANs**.
   You see the FICON VSANs dialog box.
Step 2 Click the **Director History** button.
   You see the history buffer dialog box.
Step 3 Click **Close** to close the dialog box.

**Default Settings**

Table 12-3 lists the default settings for FICON features.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>FICON feature</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Port numbers</td>
<td>Same as port addresses.</td>
</tr>
<tr>
<td>FC ID last byte value</td>
<td>0 (zero).</td>
</tr>
<tr>
<td>EBCDIC format option</td>
<td>US-Canada.</td>
</tr>
<tr>
<td>Switch offline state</td>
<td>Hosts are allowed to move the switch to an offline state.</td>
</tr>
<tr>
<td>Mainframe users</td>
<td>Allowed to configure FICON parameters on Cisco MDS switches.</td>
</tr>
<tr>
<td>Clock in each VSAN</td>
<td>Same as the switch hardware clock.</td>
</tr>
<tr>
<td>Host clock control</td>
<td>Allows host to set the clock on this switch.</td>
</tr>
<tr>
<td>SNMP users</td>
<td>Configure FICON parameters.</td>
</tr>
<tr>
<td>Port address</td>
<td>Not blocked.</td>
</tr>
</tbody>
</table>
Advanced Features and Concepts

This chapter describes the advanced features provided in switches in the Cisco MDS 9000 Family. It includes the following sections:

- Common Information Model, page 13-1
- Fibre Channel Time-Out Values, page 13-2
- World Wide Names, page 13-5
- FC ID Allocation for HBAs, page 13-7
- Switch Interoperability, page 13-8
- Default Settings, page 13-13

Common Information Model

Common Information Model (CIM) is an object-oriented information model that extends the existing standards for describing management information in a network/enterprise environment.

CIM messages are independent of platform and implementation because they are encoded in Extensible Markup Language (XML). CIM consists of a specification and a schema. The specification defines the syntax and rules for describing management data and integrating with other management models. The schema provides the actual model descriptions for systems, applications, networks, and devices.

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

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

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

SSL Certificate Requirements and Format

To limit access to the CIM server to authorized clients, you can enable the HTTPS transport protocol between the CIM server and client. On the switch side, you must install a Secure Socket Library (SSL) certificate generated on the client and enable the HTTPS server. Certificates may be generated using third-party tools, such as openssl (available for UNIX, Mac and Windows), and may be certified by a CA or self-signed.

The SSL certificate that you install on the switch must meet the following requirements:
Fibre Channel Time-Out Values

You can modify Fibre Channel protocol related timer values for the switch by configuring the following time-out values (TOVs):

- Distributed services TOV (D_S_TOV)—The valid range is from 5,000 to 10,000 milliseconds. The default is 5,000 milliseconds.
- Error detect TOV (E_D_TOV)—The valid range is from 1,000 to 10,000 milliseconds. The default is 2,000 milliseconds. This value is matched with the other end during port initialization.
- Resource allocation TOV (R_A_TOV)—The valid range is from 5,000 to 10,000 milliseconds. The default is 10,000 milliseconds. This value is matched with the other end during port initialization.

Note: The fabric stability TOV (F_S_TOV) constant cannot be configured.

This section includes the following topics:
- Timer Configuration Across All VSANs, page 13-2
- Timer Configuration Per-VSAN, page 13-3
- About fctimer Distribution, page 13-4
- Enabling or Disabling fctimer Distribution, page 13-4
- Database Merge Guidelines, page 13-5

Timer Configuration Across All VSANs

You can modify Fibre Channel protocol related timer values for the switch.

Caution: The D_S_TOV, E_D_TOV, and R_A_TOV values cannot be globally changed unless all VSANs in the switch are suspended.

Note: If a VSAN is not specified when you change the timer value, the changed value is applied to all VSANs in the switch.
To configure timers in Fabric Manager, expand **Switches > FC Services** and then select **Timers & Policies** in the Physical Attributes pane. You see the timers for multiple switches in the Information pane. Click the **Change Timeouts** button to configure the timeout values.

You see the dialog box as shown in **Figure 13-1**.

**Figure 13-1 Configure Timers in Fabric Manager**

To configure timers in Device Manager, click **FC > Advanced > Timers/Policies**. You see the timers for a single switch in the dialog box as shown in **Figure 13-2**.

**Figure 13-2 Configure Timers in Device Manager**

**Timer Configuration Per-VSAN**

You can also issue the `fctimer` for a specified VSAN to configure different TOV values for VSANs with special links like FC or IP tunnels. You can configure different E_D_TOV, R_A_TOV, and D_S_TOV values for individual VSANs. Active VSANs are suspended and activated when their timer values are changed.

**Caution**

You cannot perform a nondisruptive downgrade to any earlier version that does not support per-VSAN FC timers.

**Note**

This configuration must be propagated to all switches in the fabric—be sure to configure the same value in all switches in the fabric.
Send documentation comments to mdsfeedback-doc@cisco.com

If a switch is downgraded to Cisco MDS SAN-OS Release 1.2 or 1.1 after the timer is configured for a VSAN, an error message is issued to warn against strict incompatibilities. The Cisco MDS 9000 Family Troubleshooting Guide.

To configure per-VSAN Fiber Channel timers using Device Manager, follow these steps:

**Step 1** Click FC > Advanced > VSAN Timers.

You see the VSANs Timer dialog box as shown in Figure 13-3.

**Figure 13-3 VSAN Timers in Device Manager**

![VSAN Timers in Device Manager](image)

**Step 2** Fill in the timer values that you want to configure.

**Step 3** Click Apply to save these changes.

### About fctimer Distribution

You can enable per-VSAN fctimer fabric distribution for all Cisco MDS switches in the fabric. When you perform fctimer configurations, and distribution is enabled, that configuration is distributed to all the switches in the fabric.

You automatically acquire a fabric-wide lock when you issue the first configuration command after you enabled distribution in a switch. The fctimer application uses the effective and pending database model to store or commit the commands based on your configuration.

Refer to the Cisco MDS 9000 Family NX-OS System Management Configuration Guide for more information on the CFS application.

### Enabling or Disabling fctimer Distribution

To enable and distribute fctimer configuration changes using Device Manager, follow these steps:

**Step 1** Choose FC > Advanced > VSAN Timers.

You see the VSANs Timer dialog box as shown in Figure 13-3.
**World Wide Names**

The world wide name (WWN) in the switch is equivalent to the Ethernet MAC address. As with the MAC address, you must uniquely associate the WWN to a single device. The principal switch selection and the allocation of domain IDs rely on the WWN. The WWN manager, a process-level manager residing on the switch’s supervisor module, assigns WWNs to each switch.

Cisco MDS 9000 Family switches support three network address authority (NAA) address formats (see Table 13-1).

**Table 13-1 Standardized NAA WWN Formats**

<table>
<thead>
<tr>
<th>NAA Address</th>
<th>NAA Type</th>
<th>WWN Format</th>
<th>48-bit MAC address</th>
<th>48-bit MAC address</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 48-bit address</td>
<td>Type 1 = 0001b</td>
<td>0000000000b</td>
<td>48-bit MAC address</td>
<td>48-bit MAC address</td>
</tr>
<tr>
<td>IEEE extended</td>
<td>Type 2 = 0010b</td>
<td>Locally assigned</td>
<td>48-bit MAC address</td>
<td>48-bit MAC address</td>
</tr>
<tr>
<td>IEEE registered</td>
<td>Type 5 = 0101b</td>
<td>IEEE company ID: 24 bits</td>
<td>VSID: 36 bits</td>
<td>VSID: 36 bits</td>
</tr>
</tbody>
</table>
World Wide Names

Caution
Changes to the world-wide names should be made by an administrator or individual who is completely familiar with switch operations.

This section includes the following topics:

- Displaying WWN Information, page 13-6
- Link Initialization WWN Usage, page 13-6
- Configuring a Secondary MAC Address, page 13-6

Displaying WWN Information

To display WWN information using Device Manager, choose FC > Advanced > WWN Manager. You see the list of allocated WWNs.

Link Initialization WWN Usage

Exchange Link Protocol (ELP) and Exchange Fabric Protocol (EFP) use WWNs during link initialization. The usage details differ based on the Cisco NX-OS software release.

Both ELPs and EFPs use the VSAN WWN by default during link initialization. However, the ELP usage changes based on the peer switch’s usage:

- If the peer switch ELP uses the switch WWN, then the local switch also uses the switch WWN.
- If the peer switch ELP uses the VSAN WWN, then the local switch also uses the VSAN WWN.

Note
As of Cisco SAN-OS Release 2.0(2b), the ELP is enhanced to be compliant with FC-SW-3.

Configuring a Secondary MAC Address

To allocate secondary MAC addresses using Device Manager, follow these steps:

Step 1  Choose FC > Advanced > WWN Manager.

You see the list of allocated WWNs as shown in Figure 13-4.
Step 2  Supply the BaseMacAddress and MacAddressRange fields.

Step 3  Click Apply to save these changes, or click Close to discard any unsaved changes.

**FC ID Allocation for HBAs**

Fibre Channel standards require a unique FC ID to be allocated to an N port attached to a Fx port in any switch. To conserve the number of FC IDs used, Cisco MDS 9000 Family switches use a special allocation scheme.

Some HBAs do not discover targets that have FC IDs with the same domain and area. Prior to Cisco SAN-OS Release 2.0(1b), the Cisco SAN-OS software maintained a list of tested company IDs that do not exhibit this behavior. These HBAs were allocated with single FC IDs, and for others a full area was allocated.

The FC ID allocation scheme available in Release 1.3 and earlier, allocates a full area to these HBAs. This allocation isolates them to that area and are listed with their pWWN during a fabric login. The allocated FC IDs are cached persistently and are still available in Cisco SAN-OS Release 2.0(1b) (see the “FC ID Allocation for HBAs” section on page 13-7).

To allow further scalability for switches with numerous ports, the Cisco NX-OS software maintains a list of HBAs exhibiting this behavior. Each HBA is identified by its company ID (also known as Organizational Unique Identifier, or OUI) used in the pWWN during a fabric login. A full area is allocated to the N ports with company IDs that are listed, and for the others a single FC ID is allocated. Regardless of the kind (whole area or single) of FC ID allocated, the FC ID entries remain persistent.

This section includes the following topics:

- Default Company ID List, page 13-8
- Verifying the Company ID Configuration, page 13-8
Switch Interoperability

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

### Default Company ID List

All switches in the Cisco MDS 9000 Family that ship with Cisco SAN-OS Release 2.0(1b) or later, or NX-OS 4.1(1) contain a default list of company IDs that require area allocation. Using the company ID reduces the number of configured persistent FC ID entries. You can configure or modify these entries using the CLI.

**Caution**

Persistent entries take precedence over company ID configuration. If the HBA fails to discover a target, verify that the HBA and the target are connected to the same switch and have the same area in their FC IDs, then perform the following procedure:

1. Shut down the port connected to the HBA.
2. Clear the persistent FC ID entry.
3. Get the company ID from the Port WWN.
4. Add the company ID to the list that requires area allocation.
5. Bring up the port.

The list of company IDs have the following characteristics:

- A persistent FC ID configuration always takes precedence over the list of company IDs. Even if the company ID is configured to receive an area, the persistent FC ID configuration results in the allocation of a single FC ID.
- New company IDs added to subsequent releases are automatically added to existing company IDs.
- The list of company IDs is saved as part of the running and saved configuration.
- The list of company IDs is used only when the fcinterop FC ID allocation scheme is in auto mode. By default, the interop FC ID allocation is set to auto, unless changed.

**Tip**

We recommend that you set the fcinterop FC ID allocation scheme to auto and use the company ID list and persistent FC ID configuration to manipulate the FC ID device allocation.

Refer to the *Cisco MDS 9000 Family CLI Configuration Guide* to change the FC ID allocation.

### Verifying the Company ID Configuration

To view the configured company IDs using Device Manager, choose **FC > Advanced > FcId Area Allocation**. You can implicitly derive the default entries shipped with a specific release by combining the list of Company IDs displayed without any identification with the list of deleted entries.

Some WWN formats do not support company IDs. In these cases, you may need to configure the FC ID persistent entry.

### Switch Interoperability

Interoperability enables the products of multiple vendors to interact with each other. Fibre Channel standards guide vendors towards common external Fibre Channel interfaces.
If all vendors followed the standards in the same manner, then interconnecting different products would become a trivial exercise. However, not all vendors follow the standards in the same way, thus resulting in interoperability modes. This section briefly explains the basic concepts of these modes.

Each vendor has a regular mode and an equivalent interoperability mode, which specifically turns off advanced or proprietary features and provides the product with a more amiable standards-compliant implementation.

This section includes the following topics:
- About Interop Mode, page 13-9
- Configuring Interop Mode 1, page 13-11
- Verifying Interoperating Status, page 13-12

### About Interop Mode

Cisco NX-OS software supports the following four interop modes:
- Mode 1—Standards based interop mode that requires all other vendors in the fabric to be in interop mode.
- Mode 2—Brocade native mode (Core PID 0).
- Mode 3—Brocade native mode (Core PID 1).
- Mode 4—McData native mode.

For information about configuring interop modes 2, 3, and 4, refer to the *Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*.

Table 13-2 lists the changes in switch behavior when you enable interoperability mode. These changes are specific to switches in the Cisco MDS 9000 Family while in interop mode.

<table>
<thead>
<tr>
<th>Switch Feature</th>
<th>Changes if Interoperability Is Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain IDs</td>
<td>Some vendors cannot use the full range of 239 domains within a fabric. Domain IDs are restricted to the range 97-127. This is to accommodate McData’s nominal restriction to this same range. They can either be set up statically (the Cisco MDS switch accept only one domain ID, if it does not get that domain ID it isolates itself from the fabric) or preferred. (If it does not get its requested domain ID, it accepts any assigned domain ID.)</td>
</tr>
<tr>
<td>Timers</td>
<td>All Fibre Channel timers must be the same on all switches as these values are exchanged by E ports when establishing an ISL. The timers are F_S_TOV, D_S_TOV, E_D_TOV, and R_A_TOV.</td>
</tr>
<tr>
<td>F_S_TOV</td>
<td>Verify that the Fabric Stability Time Out Value timers match exactly.</td>
</tr>
<tr>
<td>D_S_TOV</td>
<td>Verify that the Distributed Services Time Out Value timers match exactly.</td>
</tr>
<tr>
<td>E_D_TOV</td>
<td>Verify that the Error Detect Time Out Value timers match exactly.</td>
</tr>
<tr>
<td>R_A_TOV</td>
<td>Verify that the Resource Allocation Time Out Value timers match exactly.</td>
</tr>
<tr>
<td>Trunking</td>
<td>Trunking is not supported between two different vendor’s switches. This feature may be disabled on a per port or per switch basis.</td>
</tr>
<tr>
<td>Default zone</td>
<td>The default zone behavior of permit (all nodes can see all other nodes) or deny (all nodes are isolated when not explicitly placed in a zone) may change.</td>
</tr>
</tbody>
</table>
### Table 13-2  Changes in Switch Behavior When Interoperability Is Enabled (continued)

<table>
<thead>
<tr>
<th>Switch Feature</th>
<th>Changes if Interoperability Is Enabled</th>
</tr>
</thead>
</table>
| Zoning attributes | Zones may be limited to the pWWN and other proprietary zoning methods (physical port number) may be eliminated.  
**Note** Brocade uses the `cfgsave` command to save fabric-wide zoning configuration. This command does not have any effect on Cisco MDS 9000 Family switches if they are part of the same fabric. You must explicitly save the configuration on each switch in the Cisco MDS 9000 Family. |
| Zone propagation | Some vendors do not pass the full zone configuration to other switches, only the active zone set gets passed.  
Verify that the active zone set or zone configuration has correctly propagated to the other switches in the fabric. |
| VSAN | Interop mode only affects the specified VSAN.  
**Note** Interop modes cannot be enabled on FICON-enabled VSANs. |
| TE ports and PortChannels | TE ports and PortChannels cannot be used to connect Cisco MDS to non-Cisco MDS switches. Only E ports can be used to connect to non-Cisco MDS switches. TE ports and PortChannels can still be used to connect an Cisco MDS to other Cisco MDS switches even when in interop mode. |
| FSPF | The routing of frames within the fabric is not changed by the introduction of interop mode. The switch continues to use src-id, dst-id, and ox-id to load balance across multiple ISL links. |
| Domain reconfiguration disruptive | This is a switch-wide impacting event. Brocade and McData require the entire switch to be placed in offline mode and/or rebooted when changing domain IDs. |
| Domain reconfiguration nondisruptive | This event is limited to the affected VSAN. Only Cisco MDS 9000 Family switches have this capability—only the domain manager process for the affected VSAN is restarted and not the entire switch. |
| Name server | Verify that all vendors have the correct values in their respective name server database. |
| IVR | IVR-enabled VSANs can be configured in `no interop` (default) mode or in any of the `interop` modes. |
Configuring Interop Mode 1

The interop mode1 in Cisco MDS 9000 Family switches can be enabled disruptively or nondisruptively.

Note Brocade’s msplmgmtdeactivate command must explicitly be run prior to connecting from a Brocade switch to either Cisco MDS 9000 Family switches or to McData switches. This command uses Brocade proprietary frames to exchange platform information, which Cisco MDS 9000 Family switches or McData switches do not understand. Rejecting these frames causes the common E ports to become isolated.

To configure interop mode 1 for a VSAN using Fabric Manager, follow these steps:

Step 1 Choose VSANxxx > VSAN Attributes from the Logical Domains pane.
Step 2 Select Interop-1 from the Interop drop-down menu.
Step 3 Click Apply Changes to save this interop mode.
Step 4 Expand VSANxxx and then select Domain Manager from the Logical Domains pane.
You see the Domain Manager configuration in the Information pane as shown in Figure 13-5.

Figure 13-5 Domain Manager Configuration

Step 5 Set the Domain ID in the range of 97 (0x61) through 127 (0x7F).
   a. Click the Configuration tab.
   b. Click in the Configure Domain ID column under the Configuration tab.
   c. Click the Running tab and check that the change has been made.

Note This is a limitation imposed by the McData switches.

Note When changing the domain ID, the FC IDs assigned to N ports also change.

Step 6 Change the Fibre Channel timers (if they have been changed from the system defaults).
Switch Interoperability

Verifying Interoperating Status

This section highlights the steps used to verify if the fabric is up and running in interoperability mode.

To verify the interoperability status of any switch in the Cisco MDS 9000 Family using Fabric Manager, follow these steps:

Step 1 Choose Switches in the Physical Attributes pane and check the release number in the Information pane to verify the Cisco NX-OS release.

Step 2 Expand Switches > Interfaces and then select FC Physical to verify the interface modes for each switch.

Step 3 Expand Fabricxx in the Logical Domains pane and then select All VSANs to verify the interop mode for all VSANs.

Step 4 Expand Fabricxx > All VSANs and then select Domain Manager to verify the domain IDs, local, and principal sWWNs for all VSANs (see Figure 13-6).

Step 5 Using Device Manager, choose FC > Name Server to verify the name server information.

You see the Name Server dialog box as shown in Figure 13-7.
Step 6

Click Close to close the dialog box.

Note

The Cisco MDS name server shows both local and remote entries, and does not time out the entries.

Default Settings

Table 13-3 lists the default settings for the features included in this chapter.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIM server</td>
<td>Disabled</td>
</tr>
<tr>
<td>CIM server security protocol</td>
<td>HTTP</td>
</tr>
<tr>
<td>D_S_TOV</td>
<td>5,000 milliseconds.</td>
</tr>
<tr>
<td>E_D_TOV</td>
<td>2,000 milliseconds.</td>
</tr>
<tr>
<td>R_A_TOV</td>
<td>10,000 milliseconds.</td>
</tr>
<tr>
<td>Timeout period to invoke fctrace</td>
<td>5 seconds.</td>
</tr>
<tr>
<td>Number of frame sent by the fcping feature</td>
<td>5 frames.</td>
</tr>
<tr>
<td>Remote capture connection protocol</td>
<td>TCP.</td>
</tr>
<tr>
<td>Remote capture connection mode</td>
<td>Passive.</td>
</tr>
<tr>
<td>Local capture frame limits</td>
<td>10 frames.</td>
</tr>
<tr>
<td>FC ID allocation mode</td>
<td>Auto mode.</td>
</tr>
<tr>
<td>Loop monitoring</td>
<td>Disabled.</td>
</tr>
<tr>
<td>D_S_TOV</td>
<td>5,000 msec</td>
</tr>
<tr>
<td>E_D_TOV</td>
<td>2,000 msec</td>
</tr>
<tr>
<td>R_A_TOV</td>
<td>10,000 msec</td>
</tr>
<tr>
<td>Interop mode</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>
INDEX

A

active zone sets
  considerations  5-4
  enabling distribution  5-28
aliases
  switching between global device aliases and FC aliases  6-8

B

BB_credits
  FICON port swapping  12-32
broadcast
  routing  8-14
Brocade
  native interop mode  13-9

C

CIM
  configuring  13-1
  description  13-1
Cisco SAN-OS features
  changed (table)  i-xiv
  new (table)  i-xiv
code pages
  FICON text string formatting  12-19
Common Information Model. See CIM
company IDs
  FC ID allocations  13-7
configuration
  saving automatically for FICON  12-23
configuration files
  FICON  12-29
Control Unit Port. See CUP in-band management
CUP in-band management
  blocking restriction  12-25
  description  12-38
dead time intervals
  configuring for FSPF  8-8
  description  8-8
default VSANs
  description  2-8
default zones
  configuring  5-22
  configuring policies  5-40
  configuring QoS priorities  5-39
  description  5-21
  interoperability  13-9
  policies  5-21
destination IDs
  in-order delivery  8-15
  path selection  2-11
device alias database
  committing changes  6-6
  discarding changes  6-7
  distribution to fabric  6-5
  merging  6-8
device aliases
  clearing statistics  6-8
  comparison with zones (table)  6-4
  default settings  6-9
Send documentation comments to mdsfeedback-doc@cisco.com

Index

description 6-1
features 6-3
modifying the database 6-4
requirements 6-3
documentation
  additional publications i-xvii
  related documents i-xvii
domain IDs
  configuring fcalias members 5-22
  interoperability 13-9
DPVM
  default settings 4-15
  description 4-1
  enabling 4-2
  requirements 4-2
  using DPVM Setup Wizard (procedure) 4-2
DPVM databases
  autolearned entries 4-8
  clearing 4-9
  comparing differences 4-14
  configuring CFS distribution 4-10 to 4-13
  copying 4-14
  description 4-5
  enabling autolearning 4-9
  merging guidelines 4-13
drop latency time
  configuring 8-18
Dynamic Port VSAN Membership. See DPVM

E

EBCDIC
  FICON string format 12-19
enhanced zones
  advantages over basic zones 5-45
  changing from basic zones 5-46
  creating attribute groups 5-47
  default settings 5-50
  description 5-45
  enabling 5-47
  merging databases 5-47
E ports
  FSPF topologies 8-2
  recovering from link isolations 5-29
exchange IDs
  in-order delivery 8-15
  path selection 2-11
Extended Binary-Coded Decimal Interchange Code. See EBCDIC 12-19

F

Fabric-Device Management Interface. See FDMI
fabric login. See FLOGI
Fabric Manager features
  changed (table) i-xiv
  new (table) i-xiv
fabric pWWNs
  zone membership 5-2
Fabric Shortest Path First. See FSPF
fabric WWNs. See fWWNs
fault tolerant fabrics
  example (figure) 8-2
fcaliases
  adding members 5-23
  cloning 5-36
  configuring for zones 5-22
  creating 5-23
  renaming 5-35

FC ID allocation
  FICON implementation 12-14
FC IDs
  allocating 13-7
  allocating default company ID lists 13-8
  allocating for FICON 12-14
  allocation for HBAs 13-7
  configuring fcalias members 5-22
FCIP
Send documentation comments to mdsfeedback-doc@cisco.com

FICON support 12-5
reserving ports for FICON 12-13

FCoE 1-3, 7-1
configuring 7-1
  Device Manager 7-4
  Fabric Manager 7-3
enabling 7-2

FCoE Initialization Protocol 7-1

FCP
intermixing protocols 12-5
fctimers
distribution 13-4

FDMI
description 10-4
displaying database information 10-4

Fibre Channel
time out values 13-2 to 13-5
TOVs 13-3

Fibre Channel over Ethernet 1-3, 7-1

Fibre Channel Protocol. See FCP

Fibre Connection. See FICON

FICON
advantages on MDS switches 12-3 to 12-7
automatic configuration save 12-23
basic configuration 12-16
calculating flow load balance (procedure) 12-40
cascading 12-7
collection files 12-28 to 12-31
configuring 12-15 to 12-24
configuring ports 12-24 to 12-28
CUP in-band management 12-38
default settings 12-43
description 12-1 to 12-8
displaying information 12-41 to 12-43
FC4 protocols 12-2
FC ID allocations 12-14
FCIP support 12-5
host timestamp control 12-22
implemented ports 12-11

installed ports 12-12
manually enabling 12-18
MDS-supported features 12-5
PortChannel support 12-5
port numbering 12-8 to 12-14
port swapping 12-31 to 12-33
RLIRs 12-27 to 12-28
saving configuration changes 12-23
suspending a VSAN 12-19
tape acceleration 12-33 to 12-37
text string formatting codes 12-19
unimplemented port 12-11
VSAN offline state 12-19

FICON configuration files
applying to running configuration 12-29
copying 12-31
description 12-29
displaying 12-30
editing 12-30
view latest information 12-30

FICON port numbers
assigning to slots 12-13
default numbering scheme 12-8
FCIP interfaces 12-13
implemented addresses 12-11
installed ports 12-12
logical interfaces 12-13
numbering guidelines 12-12
PortChannel interfaces 12-13
port swapping 12-11
reserved numbering scheme 12-11
unimplemented addresses 12-11
uninstalled ports 12-12

FICON ports
assigning address names using Device Manager 12-27
blocking 12-25
displaying address information 12-42
prohibiting 12-26
swapping configurations 12-33
FICON port swapping
  configuring (procedure) 12-33
  guidelines 12-32
FICON tape acceleration
  configuration considerations 12-35
  configuring 12-35
  description 12-33
FIP 7-1
FLOGI
  description 10-1
  displaying details 10-1
FL ports
  DPVM support 4-8
F ports
  DPVM support 4-8
FSPF
  computing link cost 8-7
  configuring globally 8-4 to 8-6
  configuring Hello time intervals 8-7
  configuring link cost 8-6
  configuring on interfaces 8-6 to 8-10
  dead time intervals 8-8
  default settings 8-19
  description 8-2
  disabling on interfaces 8-9
  disabling routing protocols 8-6
  displaying databases 8-10
  fail-over with PortChannels 8-3
  fault tolerant fabrics 8-2
  flow statistics ?? to 8-19
  in-order delivery 8-15 to 8-19
  interoperability 13-10
  link state record defaults 8-4
  multicast root switches 8-14
  reconvergence times 8-2
  redundant links 8-3
  retransmitting intervals 8-8
  routing services 8-1
  topology examples 8-2 to 8-4
  FSPF multicast roots
    configuring switches 8-14
  FSPF routes
    configuring 8-12
    description 8-12
  FSPF routing
    multicast 8-14
  full zone sets
    considerations 5-4
    enabling distribution 5-28
fWWNs
  configuring fcalias members 5-22
Fx ports
  VSAN membership 2-4

H

hard zoning
  description 5-27
HBAs
  device aliases 6-1
  FC ID allocations 13-7
Hello time intervals
  configuring for FSPF 8-8
  description 8-7
host control
  FICON 12-21

I

IBM PPRC
  FICON support 12-5
in-band management
  CUP 12-38
in-order delivery
  configuring drop latency time 8-18
  enabling for VSANs 8-18
  enabling globally 8-18
guidelines 8-17
reordering network frames 8-15
reordering PortChannel frames 8-16

interfaces
assigning to VSANs 2-8
configuring fc alias members 5-22
VSAN membership 2-7

interoperability
configuring interop mode 1 13-11
description 13-8
verifying status 13-12
VSANs 2-12

interop modes
configuring mode 1 13-11
default settings 13-13
description 13-9

IOD. See in-order delivery

IPv4 addresses
configuring fc alias members 5-22
IPv6 addresses
configuring fc alias members 5-2, 5-22

isolated VSANs
description 2-8
displaying membership 2-9

IVR
SDV limitations 3-9

L

link costs
configuring for FSPF 8-7
description 8-6

Link Incident Records. See LIRs
LIRs
description 12-27

load balancing
attributes 2-11
attributes for VSANs 2-5
configuring 2-11

description 2-11

logical unit numbers. See LUNs
LUN zoning
configuring 5-42
description 5-41

M

MAC addresses
configuring secondary 13-6

mainframes
FICON parameters 12-22
VSAN clock 12-22

McData
native interop mode 13-9

multicast root switches
configuring 8-14
description 8-14

N

name servers
displaying database entries 10-3
interoperability 13-10
LUN information 11-1
proxy feature 10-2
registering proxies 10-2
rejecting duplicate pWWNs 10-3

NL ports
hard zoning 5-27
zone enforcement 5-27

node world wide names. See nWWNs

N ports
hard zoning 5-27
zone enforcement 5-27
zone membership 5-2
See also Nx ports

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

Index

Send documentation comments to mdsfeedback-doc@cisco.com

IN-6

Cisco Fabric Manager Fabric Configuration Guide

OL-19448-02, Cisco MDS NX-OS Release 4.2(x)

Index

P

PLOGI

name server 10-3
port addresses
FICON 12-11
PortChannels
FICON support 12-5
in-order guarantee 8-16
interoperability 13-10
link changes 8-16
link failures 8-3
reserving ports for FICON 12-13
ports
VSAN membership 2-7
port swapping. See FICON port swapping
port world wide names. See pWWNs
proxies
registering for name servers 10-2
pWWNs
configuring fcalias members 5-22
DPVM 4-1
rejecting duplicates 10-3
zone membership 5-2

R

read-only zones
configuration guidelines 5-43
configuring 5-44
default settings 5-50
description 5-43
redundancy
VSANs 2-4
redundant physical links
example (figure) 8-3
Registered Link Incident Reports. See RLIRs
Registered State Change Notifications. See RSCNs
retransmitting intervals
configuring for FSPF 8-9
description 8-8
RLIRs
description 12-27
displaying information (procedure) 12-27
route costs
computing 8-6
routing
multicast 8-14
See also broadcast routing
See also IP routing
RSCNs
clearing statistics 10-7
default settings 10-8
description 10-5
displaying information 10-5
multiple port IDs 10-6
runtime checks
static routes 8-12

S

scalability
VSANs 2-4
SCSI
displaying LUN discovery results 11-3
SCSI LUNs
customized discovery 11-2
discovering targets 11-1
displaying information 11-3
starting discoveries 11-2
SDV
IVR limitations 3-9
secondary MAC addresses
configuring 13-6
small computer system interface. See SCSI
SNMP
  FICON control  12-22
soft zoning
  description  5-27
  See also zoning
source IDs
  in-order delivery  8-15
  path selection  2-11
SPF
  computational hold times  8-4
static routes
  runtime checks  8-12
storage devices
  access control  5-1

T

tape acceleration
  FICON  12-33 to 12-37
TE ports
  FSPF topologies  8-2
  interoperability  13-10
  recovering from link isolations  5-29

time out values. See TOVs
timestamps
  FICON host control  12-22
TOVs
  configuring across all VSANs  13-2
  configuring for a VSAN  13-3
  default settings  13-13
  interoperability  13-9
  ranges  13-2
traffic isolation
  VSANs  2-4
trunking
  interoperability  13-9
trunking ports
  associated with VSANs  2-8

V
virtual interface
  limitations  7-1
VSAN IDs
  description  2-5
  range  2-4
  VSAN membership  2-4
VSANs
  advantages  2-3
  broadcast addresses  8-14
  clocks  12-22
  comparison with zones (table)  2-4
  configuring  2-6 to ??
  configuring FSPF  8-4
  default settings  2-18
  default VSANs  2-8
  deleting  2-9
  description  2-1 to 2-4
  fabric optimization for FICON  12-3
  FC IDs  2-1
  features  2-1
  FICON-enabled  2-12
  FSPF connectivity  8-2
  interop mode  13-10
  isolated  2-8
  load balancing  2-11
  load balancing attributes  2-5
  multiple zones  5-4
  names  2-5
  name server  10-2
  operational states  2-9
  port membership  2-7
  states  2-5
  suspending for FICON  12-19
  timer configuration  13-3
  traffic isolation  2-3
  trunking ports  2-8
<table>
<thead>
<tr>
<th>W</th>
<th>wizards</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Quick Config Wizard  5-7</td>
</tr>
<tr>
<td></td>
<td>world wide names. See WWNs</td>
</tr>
<tr>
<td></td>
<td>WWNs</td>
</tr>
<tr>
<td></td>
<td>configuring  13-5</td>
</tr>
<tr>
<td></td>
<td>displaying information  13-6</td>
</tr>
<tr>
<td></td>
<td>link initialization  13-6</td>
</tr>
<tr>
<td></td>
<td>secondary MAC addresses  13-6</td>
</tr>
<tr>
<td>X</td>
<td>XRC</td>
</tr>
<tr>
<td></td>
<td>FICON support  12-5</td>
</tr>
<tr>
<td>Z</td>
<td>zone attribute groups</td>
</tr>
<tr>
<td></td>
<td>cloning  5-36</td>
</tr>
<tr>
<td></td>
<td>zone databases</td>
</tr>
<tr>
<td></td>
<td>migrating a non-MDS database  5-37</td>
</tr>
<tr>
<td></td>
<td>zone members</td>
</tr>
<tr>
<td></td>
<td>adding to zones  5-14</td>
</tr>
<tr>
<td></td>
<td>converting to pWWN members  5-25</td>
</tr>
<tr>
<td></td>
<td>displaying information  5-21</td>
</tr>
<tr>
<td></td>
<td>zones</td>
</tr>
<tr>
<td></td>
<td>access control  5-16</td>
</tr>
<tr>
<td></td>
<td>adding zone members  5-14</td>
</tr>
<tr>
<td></td>
<td>assigning LUNs to storage subsystems  5-43</td>
</tr>
<tr>
<td></td>
<td>backing up (procedure)  5-32</td>
</tr>
<tr>
<td></td>
<td>changing from enhanced zones  5-46</td>
</tr>
<tr>
<td></td>
<td>cloning  5-36</td>
</tr>
<tr>
<td></td>
<td>compacting for downgrading  5-49</td>
</tr>
<tr>
<td></td>
<td>comparison with device aliases (table) 6-4</td>
</tr>
<tr>
<td></td>
<td>comparison with VSANs (table)  2-4</td>
</tr>
<tr>
<td></td>
<td>configuring  5-10 to 5-26</td>
</tr>
<tr>
<td></td>
<td>configuring aliases  5-22</td>
</tr>
<tr>
<td></td>
<td>configuring broadcasting  5-40</td>
</tr>
<tr>
<td></td>
<td>configuring fc aliases  5-22</td>
</tr>
<tr>
<td></td>
<td>default policies  5-2</td>
</tr>
<tr>
<td></td>
<td>default settings  5-50</td>
</tr>
<tr>
<td></td>
<td>editing full zone databases  5-11</td>
</tr>
<tr>
<td></td>
<td>enforcing restrictions  5-27</td>
</tr>
<tr>
<td></td>
<td>exporting databases  5-30</td>
</tr>
<tr>
<td></td>
<td>features  5-1, 5-3</td>
</tr>
<tr>
<td></td>
<td>importing databases  5-29</td>
</tr>
<tr>
<td></td>
<td>LUN-based  5-41</td>
</tr>
<tr>
<td></td>
<td>membership using pWWNs  2-4</td>
</tr>
<tr>
<td></td>
<td>renaming  5-35</td>
</tr>
<tr>
<td></td>
<td>restoring (procedure)  5-32</td>
</tr>
<tr>
<td></td>
<td>viewing information  5-44</td>
</tr>
<tr>
<td></td>
<td>See also default zones</td>
</tr>
<tr>
<td></td>
<td>See also enhanced zones</td>
</tr>
<tr>
<td></td>
<td>See also hard zoning; soft zoning</td>
</tr>
<tr>
<td></td>
<td>See also LUN zoning</td>
</tr>
<tr>
<td></td>
<td>See also read-only zones</td>
</tr>
<tr>
<td></td>
<td>See also zoning; zone sets</td>
</tr>
<tr>
<td></td>
<td>zone server databases</td>
</tr>
<tr>
<td></td>
<td>clearing  5-37</td>
</tr>
<tr>
<td></td>
<td>zone sets</td>
</tr>
<tr>
<td></td>
<td>activating  5-18</td>
</tr>
<tr>
<td></td>
<td>cloning  5-36</td>
</tr>
<tr>
<td></td>
<td>configuring  5-16 to 5-22</td>
</tr>
<tr>
<td></td>
<td>considering  5-4</td>
</tr>
<tr>
<td></td>
<td>copying  5-31</td>
</tr>
<tr>
<td></td>
<td>creating  5-16</td>
</tr>
<tr>
<td></td>
<td>default settings  5-50</td>
</tr>
<tr>
<td></td>
<td>distributing configuration  5-28</td>
</tr>
<tr>
<td></td>
<td>enabling distribution  5-28</td>
</tr>
<tr>
<td></td>
<td>exporting  5-30</td>
</tr>
<tr>
<td></td>
<td>exporting databases  5-30</td>
</tr>
<tr>
<td></td>
<td>features  5-1</td>
</tr>
<tr>
<td></td>
<td>importing  5-30</td>
</tr>
<tr>
<td></td>
<td>importing databases  5-29</td>
</tr>
<tr>
<td></td>
<td>one-time distribution  5-29</td>
</tr>
<tr>
<td></td>
<td>recovering from link isolations  5-29</td>
</tr>
<tr>
<td></td>
<td>renaming  5-35</td>
</tr>
</tbody>
</table>
viewing information  5-44
See also active zone sets
See also active zone sets; full zone sets
See also zones; zoning
zone traffic priorities
description  5-38
zoning
configuring broadcasting  5-40
description  5-1
example  5-2
implementation  5-3
Quick Config Wizard  5-7 to 5-10
See also LUN zoning
See also zones; zone sets