Send documentation comments to mdsfeedback-doc@cisco.com

Cisco Fabric Manager Inter-VSAN Routing Configuration Guide

Cisco Fabric Manager Release 4.2(1)
July, 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-19989-01

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

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

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

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

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Fabric Manager Inter-VSAN Routing Configuration Guide

CONTENTS

New and Changed Information

As of Cisco Fabric Manager 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 Cisco Fabric Manager 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 Fabric Manager Release 4.2(1), see the *Cisco MDS 9000 Family Release Notes* available at the following Cisco Systems website:

http://www.cisco.com/en/US/products/ps5989/prod_release_notes_list.htm

About This Guide

The information in the new *Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide* previously existed in the Fabric Configuration section in the *Cisco MDS 9000 Family Fabric Manager Configuration Guide, Release 4.x.*

Table 1 lists the New and Changed features for this guide, starting with Cisco Fabric Manager Release 4.2(1).

Table 1 New and Changed Features for Cisco Fabric Manager Release 4.2(1)

Feature	New or Changed Topics	Changed in Release	Where Documented
Basic IVR configuration	Reorganized basic IVR configuration information.	4.2(1)	Chapter 1, "Basic Inter-VSAN Routing Configuration"
Advanced IVR configuration	Reorganized advanced IVR configuration information. Added "Working with Existing IVR Topologies" section. Added "Advanced Configuration Task List" section. Added IVR Zone configuration guidelines.	4.2(1)	Chapter 2, "Advanced Inter-VSAN Routing Configuration" Working With Existing IVR Topologies, page 11 Advanced IVR Configuration Task List, page 2 IVR Zone Configuration Guidelines, page 14

Preface

This preface describes the audience, organization, and conventions of the *Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide*. The preface also provides information on how to obtain related documentation.

Audience

This guide is for experienced network administrators who are responsible for planning, installing, configuring, and maintaining Cisco Inter-VSAN Routing.

Organization

This document is organized as follows:

Chapter	Title	Description
Chapter 1	Basic Inter-VSAN Routing Configuration	Presents concepts and instructions for basic IVR configurations.
Chapter 2	Advanced Inter-VSAN Routing Configuration	Presents concepts and instructions for advanced IVR configurations.

Document Conventions

Command descriptions use these conventions:

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

Screen examples use these conventions:

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

This document uses the following conventions:

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

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

Related Documentation

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

http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/roadmaps/doclocater.htm

Release Notes

- *Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Releases*
- *Cisco MDS 9000 Family Release Notes for MDS SAN-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*
- *Release Notes for Cisco MDS 9000 Family Fabric Manager*

Regulatory Compliance and Safety Information

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

Compatibility Information

- *Cisco Data Center Interoperability Support Matrix*
- *Cisco MDS 9000 NX-OS Hardware and Software Compatibility Information and Feature Lists*
- *Cisco MDS NX-OS Release Compatibility Matrix for Storage Service Interface Images*
- *Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*
- *Cisco MDS NX-OS Release Compatibility Matrix for IBM SAN Volume Controller Software for Cisco MDS 9000*
- *Cisco MDS SAN-OS Release Compatibility Matrix for VERITAS Storage Foundation for Networks Software*

Hardware Installation

- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9124 and Cisco MDS 9134 Multilayer Fabric Switch Quick Start Guide*

Software Installation and Upgrade

- *Cisco MDS 9000 NX-OS Release 4.1(x) and SAN-OS 3(x) Software Upgrade and Downgrade Guide*
- *Cisco MDS 9000 Family Storage Services Interface Image Install and Upgrade Guide*
- *Cisco MDS 9000 Family Storage Services Module Software Installation and Upgrade Guide*

Cisco NX-OS

- *Cisco MDS 9000 Family NX-OS Licensing Guide*
- *Cisco MDS 9000 Family NX-OS Fundamentals Configuration 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 Intelligent Storage Services Configuration Guide*
- *Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide*

Cisco Fabric Manager

- *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 Fabric Manager Inter-VSAN Routing Configuration Guide*
- *Cisco Fabric Manager Online Help*
- *Cisco Fabric Manager Web Services Online Help*

Command-Line Interface

- *Cisco MDS 9000 Family Command Reference*

Intelligent Storage Networking Services Configuration Guides

- *Cisco MDS 9000 I/O Acceleration 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*
- *Cisco MDS 9000 Family Cookbook for Cisco MDS SAN-OS*

Troubleshooting and Reference

- *Cisco NX-OS System Messages Reference*
- *Cisco MDS 9000 Family NX-OS Troubleshooting Guide*
- *Cisco MDS 9000 Family NX-OS MIB Quick Reference*
- *Cisco MDS 9000 Family NX-OS SMI-S Programming Reference*
- *Cisco MDS 9000 Family Fabric Manager Server Database Schema*

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:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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

Basic Inter-VSAN Routing Configuration

This chapter describes the Inter-VSAN Routing (IVR) feature and provides basic instructions on sharing resources across VSANs using IVR management interfaces. After setting up a basic IVR configuration, see *Chapter 2, "Advanced Inter-VSAN Routing Configuration."* if you need to set up an advanced IVR configuration.

This chapter includes the following sections on IVR basic configuration:

- About Inter-VSAN Routing, page 1-1
- Basic IVR Configuration, page 1-5
- IVR Virtual Domains, page 1-11
- IVR Zones and IVR Zone Sets, page 1-12
- IVR Logging, page 1-20
- Database Merge Guidelines, page 1-21
- Default Settings, page 1-23

About Inter-VSAN Routing

Virtual SANs (VSANs) improve storage area network (SAN) scalability, availability, and security by allowing multiple Fibre Channel SANs to share a common physical infrastructure of switches and ISLs. These benefits are derived from the separation of Fibre Channel services in each VSAN and the isolation of traffic between VSANs. Data traffic isolation between the VSANs also inherently prevents sharing of resources attached to a VSAN, such as robotic tape libraries. Using IVR, you can access resources across VSANs without compromising other VSAN benefits.

This section includes the following topics:

- IVR Features, page 1-2
- IVR Terminology, page 1-3
- IVR Configuration Limits, page 1-4
- Fibre Channel Header Modifications, page 1-4
- IVR Network Address Translation, page 1-4
- IVR VSAN Topology, page 1-5
- IVR Interoperability, page 1-5

IVR Features

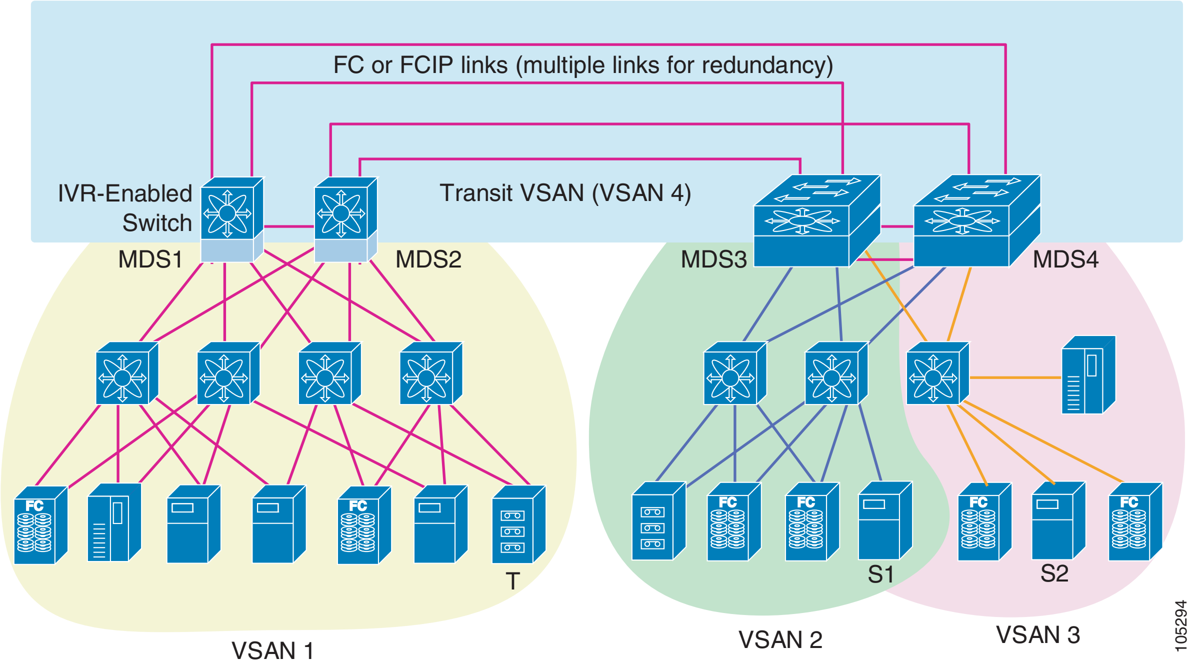
IVR supports the following features:

- Accesses resources across VSANs without compromising other VSAN benefits.
- Transports data traffic between specific initiators and targets on different VSANs without merging VSANs into a single logical fabric.
- IVR is not limited to VSANs present on a common switch. Routes that traverse one or more VSANs across multiple switches can be established, if necessary, to establish proper interconnections.
- Shares valuable resources (such as tape libraries) across VSANs without compromise. Fibre Channel traffic does not flow between VSANs, nor can initiators access any resource across VSANs other than the designated VSAN.
- Provides efficient business continuity or disaster recovery solutions when used in conjunction with FCIP (see Figure 1-1).
- Is in compliance with Fibre Channel standards.
- Incorporates third-party switches, however, IVR-enabled VSANs may need to be configured in one of the interop modes.

Note IVR is not 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.

Originator Exchange ID (OX ID) load balancing of IVR traffic from IVR- enabled switches is not supported on Generation 1 switching modules. OX ID-based load balancing of IVR traffic from a non-IVR MDS switch could work in some environments. Generation 2 switching modules support OX ID-based load balancing of IVR traffic from IVR-enabled switches.

Figure 1-1 Traffic Continuity Using IVR and FCIP



IVR Terminology

The following IVR-related terms are used in the IVR documentation:

- Native VSAN—The VSAN to which an end device logs on is the native VSAN for that end device.
- Current VSAN—The VSAN currently being configured for IVR.
- Inter-VSAN Routing zone (IVR zone)—A set of end devices that are allowed to communicate across VSANs within their interconnected SAN fabric. This definition is based on their port world wide names (pWWNs) and their native VSAN associations. Prior to Cisco SAN-OS Release 3.0(3), you can configure up to 2000 IVR zones and 10,000 IVR zone members on the switches in the network. As of Cisco SAN-OS Release 3.0(3), you can configure up to 8000 IVR zones and 20,000 IVR zone members on the switches in the network.
- Inter-VSAN routing zone sets (IVR zone sets)—One or more IVR zones make up an IVR zone set. You can configure up to 32 IVR zone sets on any switch in the Cisco MDS 9000 Family. Only one IVR zone set can be active at any time.
- IVR path—An IVR path is a set of switches and Inter-Switch Links (ISLs) through which a frame from an end device in one VSAN can reach another end device in some other VSAN. Multiple paths can exist between two such end devices.
- IVR-enabled switch—A switch on which the IVR feature is enabled.
- Edge VSAN—A VSAN that initiates (source edge-VSAN) or terminates (destination edge-VSAN) an IVR path. Edge VSANs may be adjacent to each other or they may be connected by one or more transit VSANs. In Figure 1-1, VSANs 1, 2, and 3 are edge VSANs.

Note An edge VSAN for one IVR path can be a transit VSAN for another IVR path.

- Transit VSAN—A VSAN that exists along an IVR path from the source edge VSAN of that path to the destination edge VSAN of that path. In Figure 1-1, VSAN 4 is a transit VSAN.

Note When the source and destination edge VSANs are adjacent to each other, then a transit VSAN is not required between them.

- Border switch—An IVR-enabled switch that is a member of two or more VSANs. Border switches, such as the IVR-enabled switch between VSAN 1 and VSAN 4 in Figure 1-1, span two or more different color-coded VSANs.
- Edge switch—A switch to which a member of an IVR zone has logged in to. Edge switches are unaware of the IVR configurations in the border switches. Edge switches do not need to be IVR-enabled.
- Autonomous Fabric Identifier (AFID)—Allows you to configure more than one VSAN in the network with the same VSAN ID and avoid downtime when configuring IVR between fabrics that contain VSANs with the same ID.
- Service group—Allows you to reduce the amount of IVR traffic to non-IVR-enabled VSANs by configuring one or more service groups that restrict the traffic to the IVR-enabled VSANs.

IVR Configuration Limits

Table 1-1 summarizes the configuration limits for IVR.

Table 1-1 IVR Configuration Limits

IVR Feature	Maximum Limit
IVR VSANs	128
IVR zone members	As of Cisco SAN-OS Release 3.0(3), 20,000 IVR zone members per physical fabric Prior to Cisco SAN-OS Release 3.0(3), 10,000 IVR zone members per physical fabric
IVR zones	As of Cisco SAN-OS Release 3.0(3), 8000 IVR zones per physical fabric Prior to Cisco SAN-OS Release 3.0(3), 2000 IVR zones per physical fabric
IVR zone sets	32 IVR zone sets per physical fabric.
IVR service groups	16 service groups per physical fabric.
IVR switches	25 (automatic topology) **Note** We recommend manual topology if you have more than 25 IVR switches.

Fibre Channel Header Modifications

IVR virtualizes the remote end devices in the native VSAN using a virtual domain. When IVR is configured to link end devices in two disparate VSANs, the IVR border switches are responsible for modifying the Fibre Channel headers for all communication between the end devices. The sections of the Fibre Channel frame headers that are modified include:

- VSAN number
- Source FCID
- Destination FCID

When a frame travels from the initiator to the target, the Fibre Channel frame header is modified such that the initiator VSAN number is changed to the target VSAN number. If IVR Network Address Translation (NAT) is enabled, then the source and destination FCIDs are also translated at the edge border switch. If IVR NAT is not enabled, then you must configure unique domain IDs for all switches involved in the IVR path.

IVR Network Address Translation

IVR Network Address Translation (NAT) can be enabled to allow non-unique domain IDs; however, without NAT, IVR requires unique domain IDs for all switches in the fabric. IVR NAT simplifies the deployment of IVR in an existing fabric where non-unique domain IDs might be present.

To use IVR NAT, it must be enabled on all IVR-enabled switches in the fabric. By default, IVR NAT and IVR configuration distribution are disabled on all switches in the Cisco MDS 9000 Family.

See the "About IVR NAT and Auto Topology" section on page 1-8 for information on IVR requirements and guidelines as well as configuration information.

IVR VSAN Topology

IVR uses a configured IVR VSAN topology to determine how to route traffic between the initiator and the target across the fabric.

Auto mode automatically builds the IVR VSAN topology and maintains the topology database when fabric reconfigurations occur. Auto mode distributes the IVR VSAN topology to IVR-enabled switches using CFS.

Using Auto mode, you no longer need to manually update the IVR VSAN topology when reconfigurations occur in your fabric. If a manually configured IVR topology database exists, Auto mode initially uses that topology information. This reduces disruption in the network by gradually migrating from the user-specified topology database to the automatically learned topology database. User configured topology entries that are not part of the network are aged out in about three minutes. New entries that are not part of the user-configured database are added as they are discovered in the network.

When auto IVR topology is enabled, it starts with the previously active manual IVR topology if it exists. Auto topology then begins the discovery process. It may discover new, alternate, or better paths. If the traffic is switched to an alternate or better path, there may be temporary traffic disruptions that are normally associated with switching paths.

Note IVR topology in Auto mode requires Cisco MDS SAN-OS Release 2.1(1a) or later and CFS must be enabled for IVR on all switches in the fabric.

IVR Interoperability

When using the IVR feature, all border switches in a fabric must be Cisco MDS switches. However, other switches in the fabric may be non-MDS switches. For example, end devices that are members of the active IVR zone set may be connected to non-MDS switches. Non-MDS switches may also be present in the transit VSAN(s) or in the edge VSANs if one of the interop modes is enabled.

For additional information on switch interoperability, refer to the *Cisco Data Center Interoperability Support Matrix*.

Basic IVR Configuration

This section describes how to configure IVR and contains the following sections:

- Configuring IVR and IVR Zones Using the IVR Zone Wizard, page 1-6
- About IVR NAT and Auto Topology, page 1-8
- IVR NAT Requirements and Guidelines, page 1-8
- Configuring IVR NAT and IVR Auto Topology, page 1-10

Configuring IVR and IVR Zones Using the IVR Zone Wizard

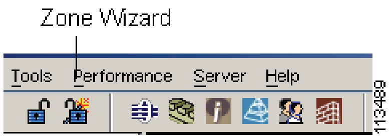
The IVR Zone Wizard simplifies the process of configuring IVR zones in a fabric. The IVR Zone Wizard checks the following conditions and identifies any related issues:

- Checks all switches in the fabric to identify the SAN-OS or NX-OS release that is running on the switch. If Cisco MDS SAN-OS Release 2.1(1a) or later is running on the switch, you can decide to migrate to IVR NAT with Auto topology.
- Checks all switches in the fabric to identify the SAN-OS or NX-OS release that is running on the switch. If Cisco MDS SAN-OS Release 2.1(1a) or later is running on the switch, you can decide to upgrade the necessary switches or to disable IVR NAT or Auto topology if they are enabled.

To configure IVR and IVR zones using the Fabric Manager IVR Zone Wizard, follow these steps:

Step 1 Click the **IVR Zone Wizard** icon in the Zone toolbar (see Figure 1-2).

Figure 1-2 IVR Zone Wizard Icon

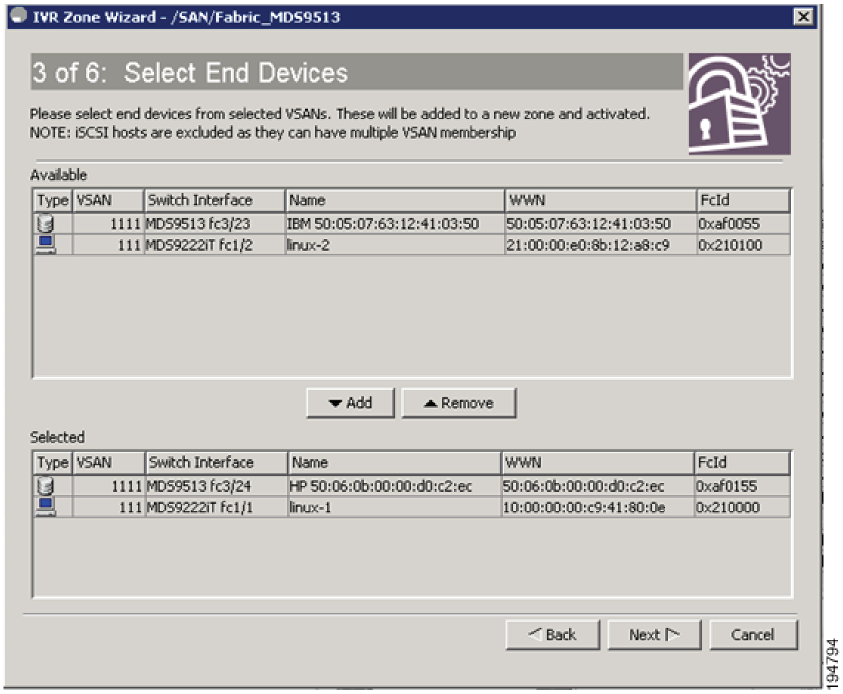


To migrate to IVR NAT mode click **Yes**, otherwise click **No**. You see the IVR Zone Wizard dialog box.

Step 2 Select the VSANs that will participate in IVR in the fabric. Click **Next**.

Figure 1-3 shows the Select End Devices dialog box.

Figure 1-3 Select End Devices Dialog Box



IVR Zone Wizard - /SAN/Fabric_MDS9513

3 of 6: Select End Devices

Please select end devices from selected VSANs. These will be added to a new zone and activated.
NOTE: iSCSI hosts are excluded as they can have multiple VSAN membership

Available

Type	VSAN	Switch Interface	Name	WWN	FcId
	1111	MDS9513 fc3/23	IBM 50:05:07:63:12:41:03:50	50:05:07:63:12:41:03:50	0xaf0055
	111	MDS9222iT fc1/2	linux-2	21:00:00:e0:8b:12:a8:c9	0x210100

Selected

Type	VSAN	Switch Interface	Name	WWN	FcId
	1111	MDS9513 fc3/24	HP 50:06:0b:00:00:d0:c2:ec	50:06:0b:00:00:d0:c2:ec	0xaf0155
	111	MDS9222iT fc1/1	linux-1	10:00:00:00:c9:41:80:0e	0x210000

Step 3 Select the end devices that you want to connect using IVR.

Note If you are not using IVR NAT, Fabric Manager may display an error message if all the switches participating in IVR do not have unique domain IDs. You must reconfigure those switches before configuring IVR. See Step 6.

Step 4 If you enable IVR NAT, verify switches that Fabric Manager will enable with IVR NAT, CFS for IVR, and IVR topology in Auto mode.

Step 5 Enter the VSAN ID of the VSAN you want to use as the transit VSAN between the VSANs selected for the IVR zone. Click **Next**.

Step 6 Optionally, configure a unique AFID for switches in the fabric that have non-unique VSAN IDs in the Select AFID dialog box.

Step 7 If you did not enable IVR NAT, verify the transit VSAN or configure the transit VSAN if Fabric Manager cannot find an appropriate transit VSAN.

Step 8 Set the IVR zone and IVR zone set.

Step 9 Verify all steps that Fabric Manager will take to configure IVR in the fabric.

Step 10 Click **Finish** if you want to enable IVR NAT and IVR topology and to create the associated IVR zones and IVR zone set.

You see the **Save Configuration** dialog box. You can save the configuration of the master switch to be copied to other IVR-enabled switches.

Step 11 Click **Continue Activation,** or click **Cancel**.

Step 12 Click **Finish**.

Note IVR NAT and Auto topology can be configured independently if you configure these features outside the IVR Zone Wizard. See the “Basic IVR Configuration” section on page 1-5.

About IVR NAT and Auto Topology

Before configuring an IVR SAN fabric to use IVR NAT and Auto topology, consider the following:

- Configure IVR only in the relevant switches.
- Enable CFS for IVR on all switches in the fabric. You must first click the CFS tab in order for the other tabs on the dialog boxes to become available.
- Verify that all switches in the fabric are running Cisco MDS SAN-OS Release 2.1(1a) or later.
- Acquire a mandatory Enterprise License Package or SAN-EXTENSION license package if you have Cisco MDS SAN-OS Release2.1(1a) or later and one active IPS card for this feature. For information on licensing, refer to the *Cisco MDS 9000 Family NX-OS Licensing Guide*.

Note The IVR over FCIP feature is bundled with the Cisco MDS 9216i Switch and does not require the SAN extension over IP package for the fixed IP ports on the supervisor module.

Tip If you change any FSPF link cost, ensure that the FSPF path distance (that is, the sum of the link costs on the path) of any IVR path is less than 30,000.

Note IVR-enabled VSANs can be configured when the interop mode is enabled (any interop mode) or disabled (no interop mode).

IVR NAT Requirements and Guidelines

The requirements and guidelines for using IVR NAT are listed below:

- IVR NAT port login (PLOGI) requests that are received from hosts are delayed a few seconds to perform the rewrite on the FC ID address. If the host's PLOGI timeout value is set to a value less than five seconds, it may result in the PLOGI being unnecessarily aborted and the host being unable to access the target. We recommend that you configure the host bus adapter for a timeout of at least ten seconds (most HBAs default to a value of 10 or 20 seconds).
- IVR NAT requires Cisco MDS SAN-OS Release 2.1(1a) or later on all IVR switches in the fabric. If you have isolated switches with an earlier release that are configured in IVR topology, you must remove any isolated fabrics from monitoring by the Fabric Manager server and then re-open the fabric to use IVR NAT. See the *Cisco Fabric Manager Fundamentals Guide* for information on selecting a fabric to manage continuously.
- Load balancing of IVR NAT traffic across equal cost paths from an IVR-enabled switch is not supported. However, load balancing of IVR NAT traffic over PortChannel links is supported. The load balancing algorithm for IVR NAT traffic over port-channel with Generation 1 linecards is SRC/DST only. Generation 2 linecards support SRC/DST/OXID based load balancing of IVR NAT traffic across a port-channel.
- You cannot configure IVR NAT and preferred Fibre Channel routes on Generation 1 module interfaces.
- IVR NAT allows you to set up IVR in a fabric without needing unique domain IDs on every switch in the IVR path. IVR NAT virtualizes the switches in other VSANs by using local VSAN for the destination IDs in the Fibre Channel headers. In some Extended Link Service message types, the

destinations IDs are part of the payload. In these cases, IVR NAT replaces the actual destination ID with the virtualized destination ID. IVR NAT supports destination ID replacement in the Extended Link Service messages described in Table 1-2.

Table 1-2 Extended Link Service Messages Supported by IVR NAT

Extended Link Service Messages	Link Service Command (LS_COMMAND)	Mnemonic
Abort Exchange	0x06 00 00 00	ABTX
Discover Address	0x52 00 00 00	ADISC
Discover Address Accept	0x02 00 00 00	ADISC ACC
Fibre Channel Address Resolution Protocol Reply	0x55 00 00 00	FARP-REPLY
Fibre Channel Address Resolution Protocol Request	0x54 00 00 00	FARP-REQ
Logout	0x05 00 00 00	LOGO
Port Login	0x30 00 00 00	PLOGI
Read Exchange Concise	0x13 00 00 00	REC
Read Exchange Concise Accept	0x02 00 00 00	REC ACC
Read Exchange Status Block	0x08 00 00 00	RES
Read Exchange Status Block Accept	0x02 00 00 00	RES ACC
Read Link Error Status Block	0x0F 00 00 00	RLS
Read Sequence Status Block	0x09 00 00 00	RSS
Reinstate Recovery Qualifier	0x12 00 00 00	RRQ
Request Sequence Initiative	0x0A 00 00 00	RSI
Scan Remote Loop	0x7B 00 00 00	RSL
Third Party Process Logout	0x24 00 00 00	TPRLO
Third Party Process Logout Accept	0x02 00 00 00	TPRLO ACC

- If you have a message that is not recognized by IVR NAT and contains the destination ID in the payload, you cannot use IVR with NAT in your topology. You can still use IVR with unique domain IDs.

Transit VSAN Guidelines

Consider the following guidelines for transit VSANs:

- In addition to defining the IVR zone membership, you can choose to specify a set of transit VSANs to provide connectivity between two edge VSANs:
  - If two edge VSANs in an IVR zone overlap, then a transit VSAN is not required (though, not prohibited) to provide connectivity.
  - If two edge VSANs in an IVR zone do not overlap, you may need one or more transit VSANs to provide connectivity. Two edge VSANs in an IVR zone will not overlap if IVR is not enabled on a switch that is a member of both the source and destination edge VSANs.
- Traffic between the edge VSANs only traverses through the shortest IVR path.

- Transit VSAN information is common to all IVR zone sets. Sometimes, a transit VSAN can also act as an edge VSAN in another IVR zone.

Border Switch Guidelines

Before configuring border switches, consider the following guidelines:

- Border switches require Cisco MDS SAN-OS Release 2.1(1a) or later.
- A border switch must be a member of two or more VSANs.
- A border switch that facilitates IVR communications must be IVR-enabled.
- IVR can (optionally) be enabled on additional border switches to provide redundant paths between active IVR zone members.
- The VSAN topology configuration updates automatically when a border switch is added or removed.

Configuring IVR NAT and IVR Auto Topology

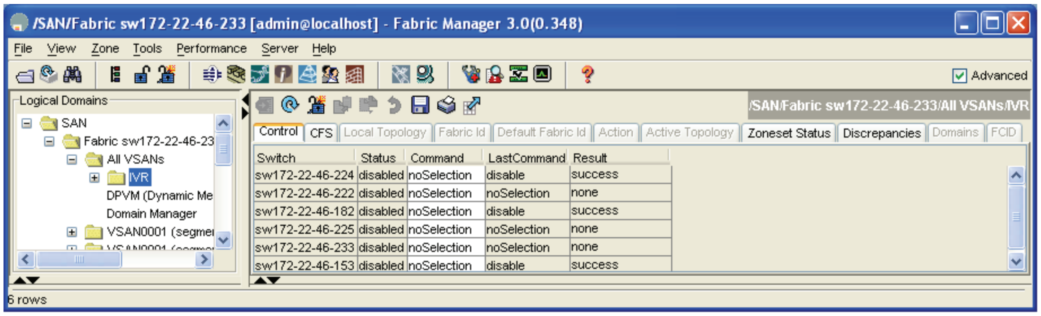
This section includes instructions on how to enable NAT and how to enable auto-discovery of IVR topologies.

To configure IVR in NAT mode and IVR topology in Auto mode using Fabric Manager, follow these steps:

Step 1 Expand **All VSANs** and then select **IVR** in the Logical Domains pane.

You see the inter-VSAN routing configuration in the Information pane shown in Figure 1-4.

Figure 1-4 IVR Routing Configuration Control Tab



/SAN/Fabric sw172-22-46-233 [admin@localhost] - Fabric Manager 3.0(0.348)

/SAN/Fabric sw172-22-46-233/All VSANs/IVR

Switch	Status	Command	LastCommand	Result
sw172-22-46-224	disabled	noSelection	disable	success
sw172-22-46-222	disabled	noSelection	noSelection	none
sw172-22-46-182	disabled	noSelection	disable	success
sw172-22-46-225	disabled	noSelection	noSelection	none
sw172-22-46-233	disabled	noSelection	noSelection	none
sw172-22-46-153	disabled	noSelection	disable	success

6 rows

Step 2 Select **enable** from the Admin column drop-down menu for the primary switch.

Step 3 Click the **Apply Changes** icon to distribute this change to all switches in the fabric.

Step 4 Click the **Action** tab.

Step 5 Check the **Enable IVR NAT** check box to enable IVR in NAT mode.

Step 6 Check the **Auto Discover Topology** check box to enable IVR topology in Auto mode.

Step 7 Click the **Apply Changes** icon to enable IVR on the switches.

IVR Virtual Domains

In a remote VSAN the IVR application does not automatically add the virtual domain to the assigned domains list. Some switches (for example, the Cisco SN5428 switch) do not query the remote name server until the remote domain appears in the assigned domains list in the fabric. In such cases, add the IVR virtual domains in a specific VSAN to the assigned domains list in that VSAN. When adding IVR domains, all IVR virtual domains that are currently present in the fabric (and any virtual domain that is created in the future) will appear in the assigned domains list for that VSAN.

Tip Be sure to add IVR virtual domains if Cisco SN5428 or MDS 9020 switches exist in the VSAN.

When you enable the IVR virtual domains, links may fail to come up due to overlapping virtual domain identifiers. If this occurs, temporarily withdraw the overlapping virtual domain from that VSAN.

Note Withdrawing an overlapping virtual domain from an IVR VSAN disrupts IVR traffic to and from that domain.

Tip Only add IVR domains in the edge VSANs and not in transit VSANs.

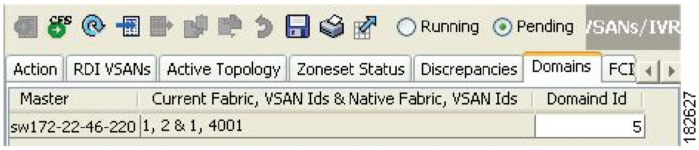
Manually Configuring IVR Virtual Domains

To manually configure an IVR virtual domain using Fabric Manager, follow these steps:

Step 1 Expand **All VSANs** and then select **IVR** in the Logical Domains pane.

You see the IVR configuration in the Information pane.

Figure 1-5 Domains Tab



Master	Current Fabric, VSAN Ids & Native Fabric, VSAN Ids	Domaind Id
sw172-22-46-220	1, 2 & 1, 4001	5

Step 2 Click the **Domains** tab to display the existing IVR topology.

Step 3 Click the **Create Row** icon to create rows in the IVR topology (see Figure 1-5).

Step 4 Enter the Current Fabric, Current VSAN, Native Fabric, Native VSAN and Domain ID in the dialog box. These are the VSANs that will add the IVR virtual domains to the assigned domains list.

Step 5 Click **Create** to create this new row.

IVR Zones and IVR Zone Sets

This section describes configuring IVR zones and IVR zone sets and includes the following topics:

- About IVR Zones, page 1-12
- IVR Zone Limits and Image Downgrading Considerations, page 1-12
- Automatic IVR Zone Creation, page 1-13
- Configuring IVR Zones and IVR Zone Sets, page 1-14
- About Activating Zone Sets and Using the force Option, page 1-17
- Recovering an IVR Full Zone Database, page 1-19
- Recovering an IVR Full Topology, page 1-20

About IVR Zones

As part of the IVR configuration, you need to configure one or more IVR zones to enable cross-VSAN communication. To achieve this result, you must specify each IVR zone as a set of (pWWN, VSAN) entries. Like zones, several IVR zone sets can be configured to belong to an IVR zone. You can define several IVR zone sets and activate only one of the defined IVR zone sets.

Note The same IVR zone set must be activated on *all* of the IVR-enabled switches.

Table 1-3 identifies the key differences between IVR zones and zones.

Table 1-3 Key Differences Between IVR Zones and Zones

IVR Zones	Zones
IVR zone membership is specified using the VSAN and pWWN combination.	Zone membership is specified using pWWN, fabric WWN, sWWN, or the AFID.
Default zone policy is always deny (not configurable).	Default zone policy is deny (configurable).

IVR Zone Limits and Image Downgrading Considerations

Table 1-4 identifies the IVR zone limits per physical fabric.

Table 1-4 IVR Zone Limits

Cisco Release	IVR Zone Limit	IVR Zone Member Limit	IVR Zone Set Limit
SAN-OS Release 3.0(3 or later	8000	20,000	32
SAN-OS Release 3.0(2b) or earlier	2000	10,000	32

Note A zone member is counted twice if it exists in two zones. See the "Database Merge Guidelines" section on page 1-21.

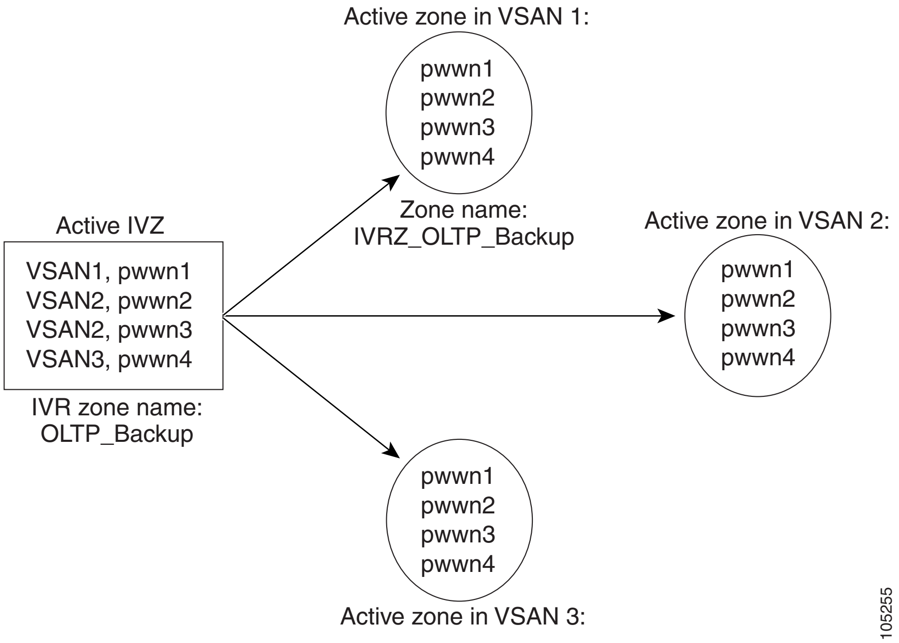
Caution If you want to downgrade to a release prior to Cisco SAN-OS Release 3.0(3), the number of IVR zones cannot exceed 2000 and the number of IVR zone members cannot exceed 10,000.

Automatic IVR Zone Creation

Figure 1-6 depicts an IVR zone consisting of four members. To allow pwwn1 to communicate with pwwn2, they must be in the same zone in VSAN 1, as well as in VSAN 2. If they are not in the same zone, then the hard-zoning ACL entries will prohibit pwwn1 from communicating with pwwn2.

A zone corresponding to each active IVR zone is automatically created in each edge VSAN specified in the active IVR zone. All pWWNs in the IVR zone are members of these zones in each VSAN.

Figure 1-6 Creating Zones Upon IVR Zone Activation



The zones are created automatically by the IVR process when an IVR zone set is activated. They are not stored in a full zone set database and are lost when the switch reboots or when a new zone set is activated. The IVR feature monitors these events and adds the zones corresponding to the active IVR zone set configuration when a new zone set is activated. Like zone sets, IVR zone sets are also activated nondisruptively.

Note If pwwn1 and pwwn2 are in an IVR zone in the current as well as the new IVR zone set, then activation of the new IVR zone set does not cause any traffic disruption between them.

IVR zone and IVR zone set names are restricted to 64 alphanumeric characters.

Caution Prior to Cisco SAN-OS Release 3.0(3), you can only configure a total of 2000 IVR zones and 32 IVR zone sets on the switches in the network. As of Cisco SAN-OS Release 3.0(3), you can only configure a total of 8000 IVR zones and 32 IVR zone sets on the switches in the network. See the "Database Merge Guidelines" section on page 1-21.

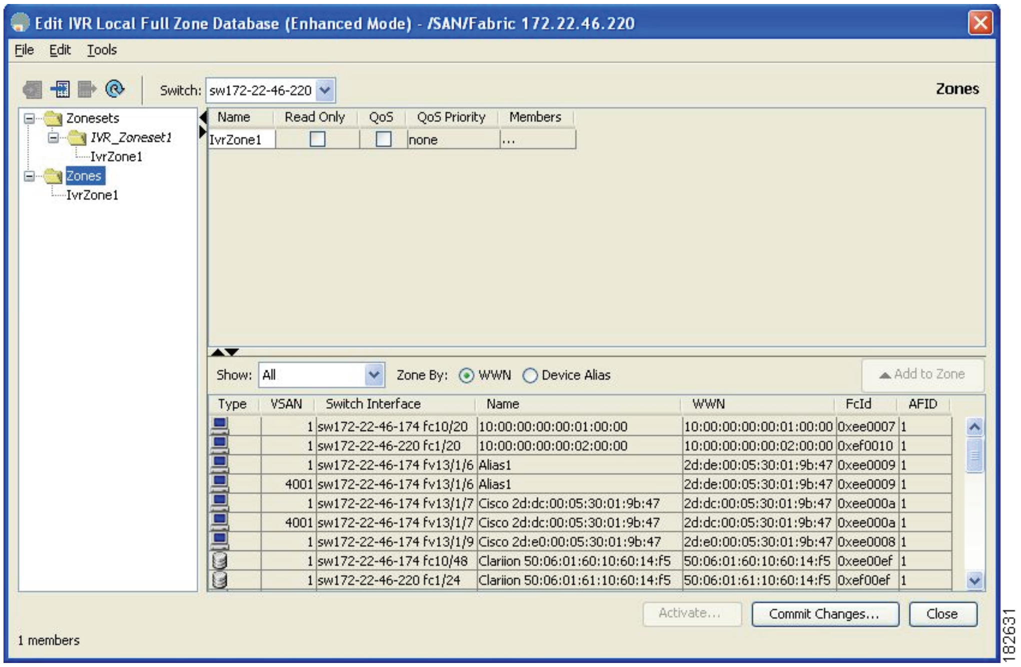
Configuring IVR Zones and IVR Zone Sets

To create IVR zones and IVR zone sets using Fabric Manager, follow these steps:

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

You see the Edit IVR Local Full Zone Database dialog box for the selected VSAN (see Figure 1-7).

Figure 1-7 Edit IVR Local Full Zone Database Dialog Box



Name	Read Only	QoS	QoS Priority	Members
IvrZone1	□	□	none	...

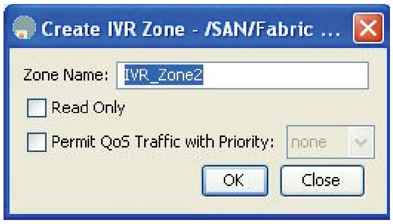
Type	VSAN	Switch Interface	Name	WWN	FcId	AFID
	1	sw172-22-46-174 fc10/20	10:00:00:00:00:01:00:00	10:00:00:00:00:01:00:00	0xee0007	1
	1	sw172-22-46-220 fc1/20	10:00:00:00:00:02:00:00	10:00:00:00:00:02:00:00	0xef0010	1
	1	sw172-22-46-174 fv13/1/6	Alias1	2d:de:00:05:30:01:9b:47	0xee0009	1
	4001	sw172-22-46-174 fv13/1/6	Alias1	2d:de:00:05:30:01:9b:47	0xee0009	1
	1	sw172-22-46-174 fv13/1/7	Cisco 2d:dc:00:05:30:01:9b:47	2d:dc:00:05:30:01:9b:47	0xee000a	1
	4001	sw172-22-46-174 fv13/1/7	Cisco 2d:dc:00:05:30:01:9b:47	2d:dc:00:05:30:01:9b:47	0xee000a	1
	1	sw172-22-46-174 fv13/1/9	Cisco 2d:e0:00:05:30:01:9b:47	2d:e0:00:05:30:01:9b:47	0xee0008	1
	1	sw172-22-46-174 fc10/48	Clariion 50:06:01:60:10:60:14:f5	50:06:01:60:10:60:14:f5	0xee00ef	1
	1	sw172-22-46-220 fc1/24	Clariion 50:06:01:61:10:60:14:f5	50:06:01:61:10:60:14:f5	0xef00ef	1

If you want to view zone membership information, right-click in the **Members** column, and then click **Show Details** for the current row or all rows from the pop-up menu.

Step 2 Click **Zones** in the left pane and click the **Insert** icon to create a zone.

You see the Create IVR Zone dialog box shown in Figure 1-8.

Figure 1-8 Create IVR Zone Dialog Box



Zone Name: IVR_Zone2

□ Read Only

□ Permit QoS Traffic with Priority: none

Step 3 Enter an IVR zone name.

Step 4 Check one of the following check boxes:

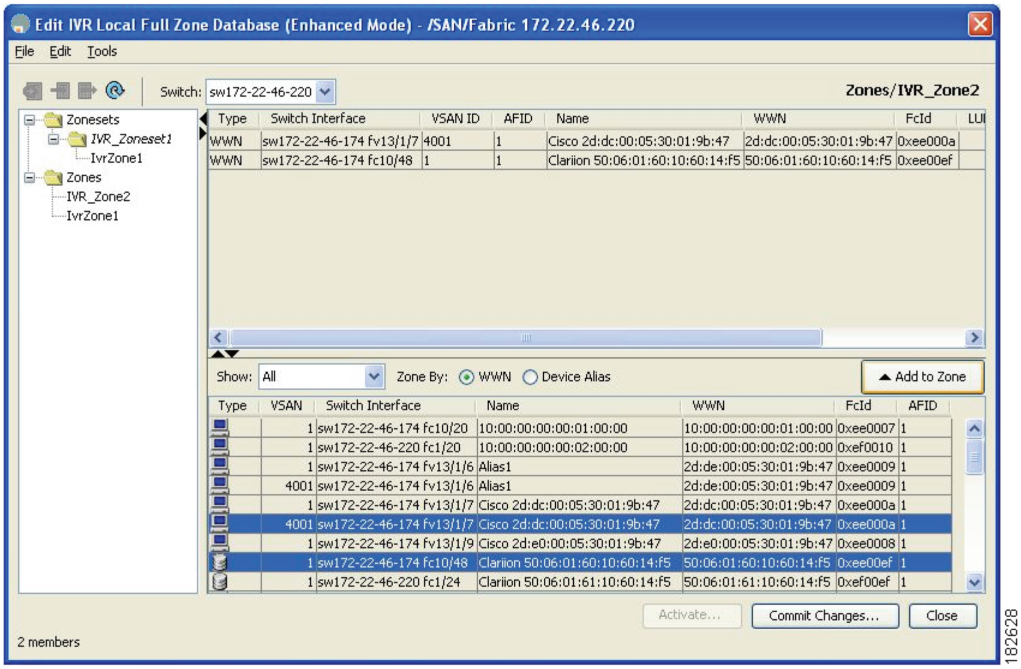
a. **Read Only**—The zone permits read and denies write.

b. **Permit QoS traffic with Priority**—You set the priority from the drop-down menu.

Step 5 Click **OK** to create the IVR zone.

Step 6 To add members to this zone, select the members you want to add from the Fabric pane (see Figure 1-9) and click **Add to Zone**.

Figure 1-9 Edit IVR Local Full Zone Database Dialog Box



Switch: sw172-22-46-220

Zones/IVR_Zone2

Type	Switch Interface	VSAN ID	AFID	Name	WWN	FcId	LUI
WWN	sw172-22-46-174 fv13/1/7	4001	1	Cisco 2d:dc:00:05:30:01:9b:47	2d:dc:00:05:30:01:9b:47	0xee000a	
WWN	sw172-22-46-174 fc10/48	1	1	Clariion 50:06:01:60:10:60:14:f5	50:06:01:60:10:60:14:f5	0xee00ef	

Show: All

Zone By: ● WWN ○ Device Alias

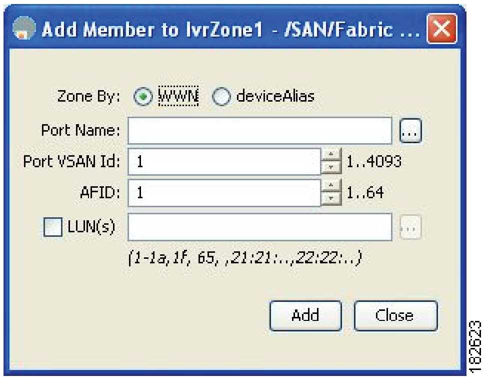
Type	VSAN	Switch Interface	Name	WWN	FcId	AFID
🖥	1	sw172-22-46-174 fc10/20	10:00:00:00:00:01:00:00	10:00:00:00:00:01:00:00	0xee0007	1
🖥	1	sw172-22-46-220 fc1/20	10:00:00:00:00:02:00:00	10:00:00:00:00:02:00:00	0xef0010	1
🖥	1	sw172-22-46-174 fv13/1/6	Alias1	2d:de:00:05:30:01:9b:47	0xee0009	1
🖥	4001	sw172-22-46-174 fv13/1/6	Alias1	2d:de:00:05:30:01:9b:47	0xee0009	1
🖥	1	sw172-22-46-174 fv13/1/7	Cisco 2d:dc:00:05:30:01:9b:47	2d:dc:00:05:30:01:9b:47	0xee000a	1
🖥	4001	sw172-22-46-174 fv13/1/7	Cisco 2d:dc:00:05:30:01:9b:47	2d:dc:00:05:30:01:9b:47	0xee000a	1
🖥	1	sw172-22-46-174 fv13/1/9	Cisco 2d:e0:00:05:30:01:9b:47	2d:e0:00:05:30:01:9b:47	0xee0008	1
🛢	1	sw172-22-46-174 fc10/48	Clariion 50:06:01:60:10:60:14:f5	50:06:01:60:10:60:14:f5	0xee00ef	1
🛢	1	sw172-22-46-220 fc1/24	Clariion 50:06:01:61:10:60:14:f5	50:06:01:61:10:60:14:f5	0xef00ef	1

2 members

Step 7 Alternatively, 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 1-10.

Figure 1-10 Add Member to IVR Zone Dialog Box



Add Member to IvrZone1 - /SAN/Fabric ...

Zone By: ● WWN ○ deviceAlias

Port Name:

Port VSAN Id: 1 1..4093

AFID: 1 1..64

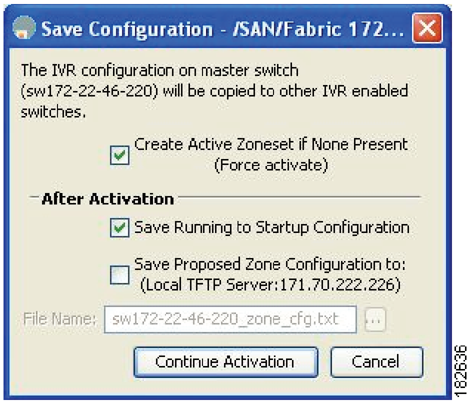
□ LUN(s)

(1-1a,1f, 65, ,21:21:..,22:22:..)

Step 8 If you added a zone set, select the new zone set and then click **Activate**.

You see the Save Configuration dialog box shown in Figure 1-11.

Figure 1-11 Save Configuration Dialog Box



Save Configuration - /SAN/Fabric 172...

The IVR configuration on master switch (sw172-22-46-220) will be copied to other IVR enabled switches.

☑ Create Active Zoneset if None Present (Force activate)

After Activation

☑ Save Running to Startup Configuration

□ Save Proposed Zone Configuration to: (Local TFTP Server:171.70.222.226)

File Name: sw172-22-46-220_zone_cfg.txt

Step 9 Check the **Save Running to Startup Configuration** check box to save all changes to the startup configuration.

Step 10 Click **Continue Activation** to activate the zone set.

Note Sometimes zone names beginning with prefix IVRZ and a zone set with name **nozoneset** appear in a logical view. The zones with prefix IVRZ are IVR zones that get appended to regular active zones. The prefix IVRZ is appended to active IVR zones by the system. Similarly the zone set with name **nozoneset** is an IVR active zone set created by the system if no active zone set is available for that VSAN and if the ivrZonesetActivateForce flag is enabled on the switch.

In the server.properties file, you can set the property zone.ignoreIVRZones to **true** or **false** to either hide or view IVR zones as part of regular active zones. For information on the server.properties file, refer to the *Cisco Fabric Manager Fundamentals Configuration Guide*.

Note Do not create a zone with prefix the IVRZ or a zone set with name no zoneset. These names are used by the system for identifying IVR zones.

Step 11 Select the new zone or zone set from the list in the Information pane and then click **Distribute**.

About Activating Zone Sets and Using the force Option

Once the zone sets have been created and populated, you must activate the zone set. When you activate an IVR zone set, IVR automatically adds an IVR zone to the regular active zone set of each edge VSAN. If a VSAN does not have an active zone set, IVR can only activate an IVR zone set using the force option, which causes IVR to create an active zone set called “nozoneset” and adds the IVR zone to that active zone set.

Caution If you deactivate the regular active zone set in a VSAN, the IVR zone set is also deactivated. This occurs because the IVR zone in the regular active zone set, and all IVR traffic to and from the switch, is stopped. To reactivate the IVR zone set, you must reactivate the regular zone set.

Note If IVR and iSLB are enabled in the same fabric, at least one switch in the fabric must have both features enabled. Any zoning-related configuration or activation operation (for normal zones, IVR zones, or iSLB zones) must be performed on this switch. Otherwise, traffic might be disrupted in the fabric.

You can also use the **force activate option** to activate IVR zone sets. Table 1-5 lists the various scenarios with and without the **force activate** option.

Table 1-5 IVR Scenarios With and Without the Force Activate Option

Case	Default Zone Policy	Active Zone Set before IVR Zone Activation	`Force Activate` Option Used?	IVR Zone Set Activation Status	Active IVR Zone Created?	Possible Traffic Disruption
1	Deny	No active zone set	No	Failure	No	No
2			Yes	Success	Yes	No
3[1]	Deny	Active zone set present	No/Yes	Success	Yes	No
4	Permit	No active zone set *or* Active zone set present	No	Failure	No	No
5			Yes	Success	Yes	Yes

[1] We recommend that you use the Case 3 scenario.

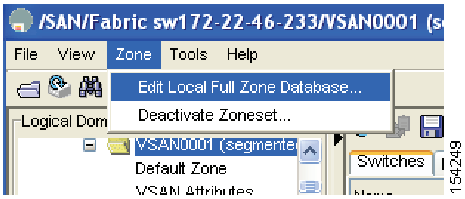
Caution Using the **force activate option** of IVR zone set activation may cause traffic disruption, even for devices that are not involved in IVR. For example, if your configuration does not have any active zone sets and the default zone policy is permit, then an IVR zone set activation will fail. However, IVR zone set activation will be successful if the **force activate option** is used. Because zones are created in the edge VSANs corresponding to each IVR zone, traffic may be disrupted in edge VSANs where the default zone policy is permit.

Activating or Deactivating IVR Zone Sets

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

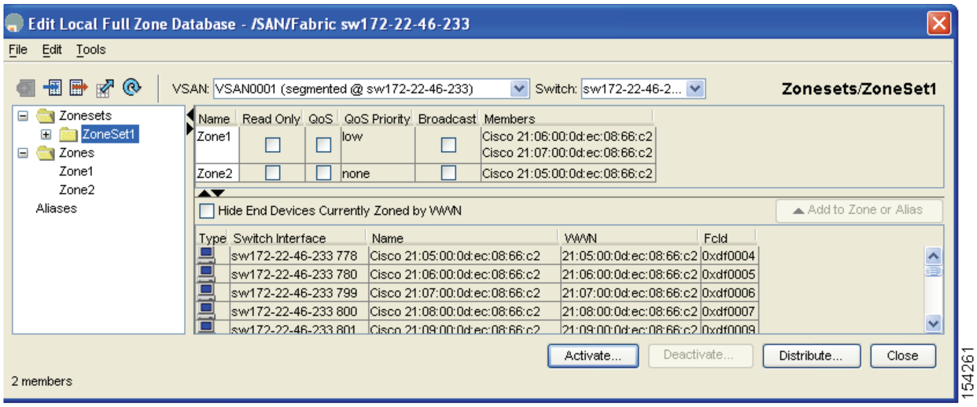
Step 1 Click **Zone** and then select **Edit Local Full Zone Database** as shown in Figure 1-12.

Figure 1-12 Zone Menu



You see the Edit Local Full Zone Database dialog box in Figure 1-13.

Figure 1-13 Edit Zone Database Dialog Box



VSAN: VSAN0001 (segmented @ sw172-22-46-233) Switch: sw172-22-46-2...

Zonesets/ZoneSet1

Name	Read Only	QoS	QoS Priority	Broadcast	Members
Zone1	□	□	low	□	Cisco 21:06:00:0d:ec:08:66:c2 Cisco 21:07:00:0d:ec:08:66:c2
Zone2	□	□	none	□	Cisco 21:05:00:0d:ec:08:66:c2

□ Hide End Devices Currently Zoned by WWN

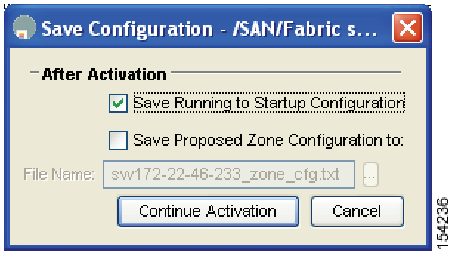
Type	Switch Interface	Name	WWN	FcId
	sw172-22-46-233 778	Cisco 21:05:00:0d:ec:08:66:c2	21:05:00:0d:ec:08:66:c2	0xdf0004
	sw172-22-46-233 780	Cisco 21:06:00:0d:ec:08:66:c2	21:06:00:0d:ec:08:66:c2	0xdf0005
	sw172-22-46-233 799	Cisco 21:07:00:0d:ec:08:66:c2	21:07:00:0d:ec:08:66:c2	0xdf0006
	sw172-22-46-233 800	Cisco 21:08:00:0d:ec:08:66:c2	21:08:00:0d:ec:08:66:c2	0xdf0007
	sw172-22-46-233 801	Cisco 21:09:00:0d:ec:08:66:c2	21:09:00:0d:ec:08:66:c2	0xdf0009

2 members

Step 2 Select a **Zoneset** folder and then click **Activate** to activate the zone set (shown in Figure 1-13) or click **Deactivate** to deactivate an activated zone set.

You see the Save Configuration dialog box shown in Figure 1-14.

Figure 1-14 Save Configuration Options for a New Zone Set


Save Configuration - /SAN/Fabric s...

After Activation

☑ Save Running to Startup Configuration

□ Save Proposed Zone Configuration to:

File Name: sw172-22-46-233_zone_cfg.txt

Step 3 Optionally, check one of the **Save Running to Configuration** check boxes to save these changes to the startup configuration (see Figure 1-14).

Step 4 Click **Continue Activation** to activate the zone set (see Figure 1-14) or **Yes** if you are deactivating the zone set.

Note The active zone set in Edit Zone is shown in bold if any change has been made to the full zone set resulting in a difference between the active zone set and full zone set. Activating the zone set, unbolds it.

Recovering an IVR Full Zone Database

You can recover an IVR zone database by copying the IVR full zone database from another switch.

To recover an IVR zone database using Fabric Manager, follow these steps:

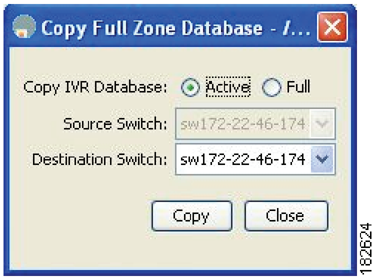
Step 1 Choose **Zone** > **IVR** > **Edit Local Full Zone Database**.

You see the Edit IVR Local Full Zone Database dialog box.

Step 2 Choose **Edit** > **Copy Full Zone Database**.

You see the Copy Full Zone Database dialog box shown in Figure 1-15.

Figure 1-15 Copy Full Zone Database Dialog Box


Copy Full Zone Database - /...

Copy IVR Database: ● Active ○ Full

Source Switch: sw172-22-46-174

Destination Switch: sw172-22-46-174

Step 3 Choose either **Active** or **Full**, depending on which type of IVR database you want to copy.

Step 4 Select the source switch from which to copy the information from the drop-down list.

Step 5 Select the destination switch from the drop-down list.

Step 6 Click **Copy** to copy the database.

Recovering an IVR Full Topology

You can recover a topology by copying from the active zone database or the full zone database.

To recover a zone topology using Fabric Manager, follow these steps:

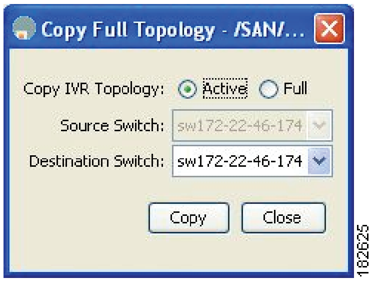
Step 1 Choose **Zone** > **IVR** > **Edit Local Full Zone Database**.

You see the Edit IVR Local Full Zone Database dialog box.

Step 2 Choose **Edit** > **Copy Full Topology**.

You see the Copy Full Topology dialog box shown in Figure 1-16.

Figure 1-16 Copy Full Topology Dialog Box



Copy Full Topology - /SAN/...

Copy IVR Topology: ● Active ○ Full

Source Switch: sw172-22-46-174

Destination Switch: sw172-22-46-174

Step 3 Choose either **Active** or **Full**, depending on which type of IVR database you want to copy from.

Step 4 Select the source switch from which to copy the information from the drop-down list.

Step 5 Select the destination switch from the drop-down list.

Step 6 Click **Copy** to copy the topology.

IVR Logging

You can configure Telnet or SSH logging for the IVR feature. For example, if you configure the IVR logging level at level 4 (warning), then messages with a severity level of 4 or above are displayed. Use the instructions in this section to configure the logging levels:

- Configuring IVR Logging Severity Levels, page 1-20

Configuring IVR Logging Severity Levels

To configure the severity level for logging messages from the IVR feature using Fabric Manager, follow these steps:

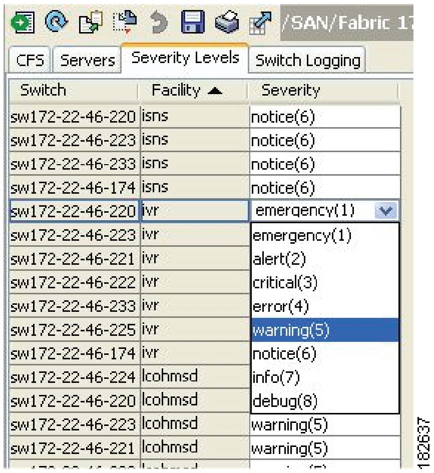
Step 1 Expand **Switches** > **Events** and then select **Syslog** from the Physical Attributes pane.

Step 2 Click the **Severity Levels** tab.

Step 3 Click the **Facility** column header to sort the table by facility name.

Step 4 Select the severity level at which the IVR logs system messages from the Severity drop-down menu (see Figure 1-17).

Figure 1-17 Syslog Severity Drop-Down Menu



Switch	Facility ▲	Severity
sw172-22-46-220	isns	notice(6)
sw172-22-46-223	isns	notice(6)
sw172-22-46-233	isns	notice(6)
sw172-22-46-174	isns	notice(6)
sw172-22-46-220	ivr	emergency(1)
sw172-22-46-223	ivr	emergency(1)
sw172-22-46-221	ivr	alert(2)
sw172-22-46-222	ivr	critical(3)
sw172-22-46-233	ivr	error(4)
sw172-22-46-225	ivr	warning(5)
sw172-22-46-174	ivr	notice(6)
sw172-22-46-224	lcohmsd	info(7)
sw172-22-46-220	lcohmsd	debug(8)
sw172-22-46-223	lcohmsd	warning(5)
sw172-22-46-221	lcohmsd	warning(5)

Tip Setting the severity to **warning** means that all IVR messages at the warning level or above will be logged to Fabric Manager.

Step 5 Click the **Apply Changes** icon to save these changes locally.

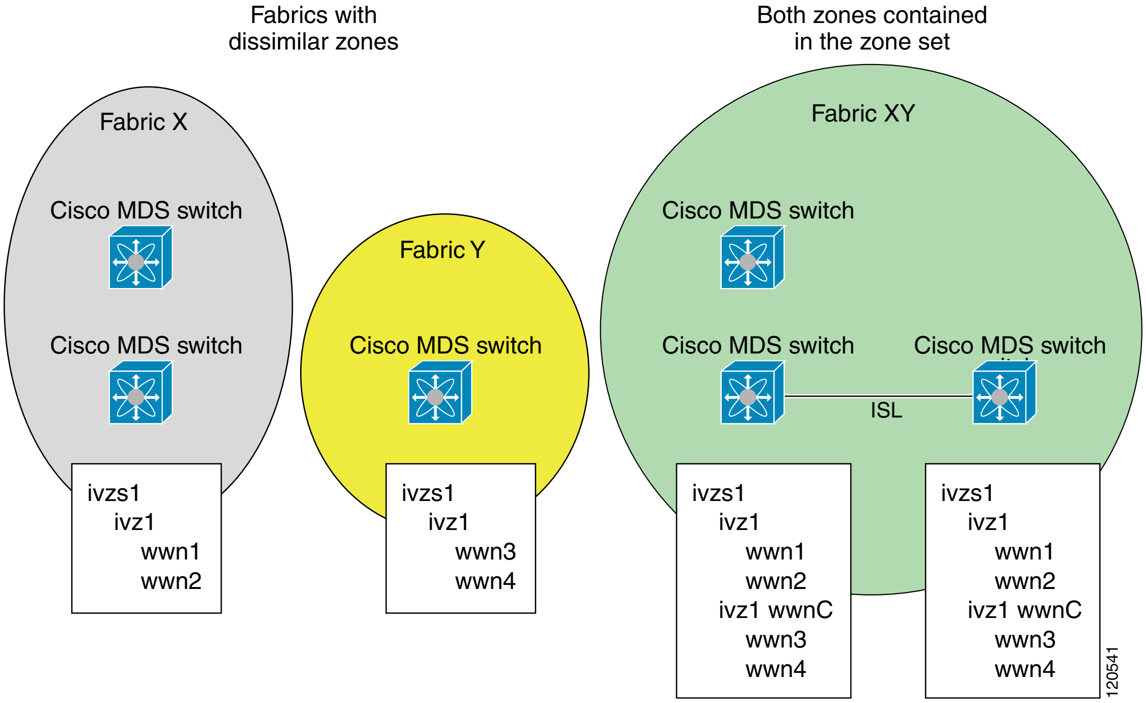
.

Database Merge Guidelines

A database merge refers to a union of the configuration database and static (unlearned) entries in the active database. For information on CFS Merge Support, refer to the *Cisco MDS 9000 Family NX-OS System Management Configuration Guide* or *Cisco Fabric Manager System Management Configuration Guide*.

- Consider the following conditions when merging two IVR fabrics:
  - The IVR configurations are merged even if two fabrics contain different configurations.
  - If dissimilar zones exist in two merged fabrics, the zone from each fabric is cloned in the distributed zone set with appropriate names (see Figure 1-18).

Figure 1-18 Fabric Merge Consequences



- You can configure different IVR configurations in different Cisco MDS switches.
- To avoid traffic disruption, after the database merge is complete, the configuration is a union of the configurations that were present on the two switches involved in the merge.
  - The configurations are merged even if both fabrics have different configurations.
  - A union of zones and zone sets are used to get the merged zones and zone sets. If a dissimilar zone exists in two fabrics, the dissimilar zones are cloned into the zone set with appropriate names so both zones are present.
  - The merged topology contains a union of the topology entries for both fabrics.
  - The merge will fail if the merged database contains more topology entries than the allowed maximum.
  - The total number of VSANs across the two fabrics cannot exceed 128.

Note VSANs with the same VSAN ID but different AFIDs are counted as two separate VSANs.

  - The total number of IVR-enabled switches across the two fabrics cannot exceed 128.
  - The total number of zone members across the two fabrics cannot exceed 10,000. As of Cisco SAN-OS Release 3.0(3), the total number of zone members across the two fabrics cannot exceed 20,000. A zone member is counted twice if it exists in two zones.

Note If one or more of the fabric switches are running Cisco SAN-OS Release 3.0(3) or later, and the number of zone members exceeds 10,000, you must either reduce the number of zone members in the fabric or upgrade all switches in both fabrics to Cisco SAN-OS Release 3.0(3) or later.

- The total number of zones across the two fabrics cannot exceed 2000. As of Cisco SAN-OS Release 3.0(3), the total number of zones across the two fabrics cannot exceed 8000.

Note If only some of the switches in the fabrics are running Cisco SAN-OS Release 3.0(3) or later, and if the number of zones exceeds 2000, you must either reduce the number of zones in the fabric or upgrade all switches in both fabrics to Cisco SAN-OS Release 3.0(3) or later.

- The total number or zone sets across the two fabrics cannot exceed 32.

Table 1-6 describes the results of a CFS merge of two IVR-enabled fabrics under different conditions.

Table 1-6 Results of Merging Two IVR-Enabled Fabrics

IVR Fabric 1	IVR Fabric 2	After Merge
NAT enabled	NAT disabled	Merge succeeds and NAT enabled
Auto mode on	Auto mode off	Merge succeeds and Auto mode on
Conflicting AFID database		Merge fails
Conflicting IVR zone set database		Merge succeeds with new zones created to resolve conflicts
Combined configuration exceeds limits (such as maximum number of zones or VSANs)		Merge fails
Service group 1	Service group 2	Merge succeeds with service groups combined
User-configured VSAN topology configuration with conflicts		Merge fails
User-configured VSAN topology configuration without conflicts		Merge succeeds

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

Default Settings

Table 1-7 lists the default settings for IVR parameters.

Table 1-7 Default IVR Parameters

Parameters	Default
IVR feature	Disabled
IVR VSANs	Not added to virtual domains
IVR NAT	Disabled
QoS for IVR zones	Low
Configuration distribution	Disabled

CHAPTER 2

Advanced Inter-VSAN Routing Configuration

This chapter provides advanced configuration information and instructions. Before setting up advanced IVR configurations, see Chapter 1, "Basic Inter-VSAN Routing Configuration" which includes basic configuration instructions and descriptions of IVR features, limits, and terminology.

This chapter includes the following sections:

Advanced IVR Configuration Task List

To configure an advanced IVR topology in a SAN fabric, follow these steps:

	Configuration Task	Resource
Step 1	Determine whether or not to use IVR Network Address Translation (NAT).	See "IVR Network Address Translation" section on page 1-4 and "IVR NAT Requirements and Guidelines" section on page 1-8.
Step 2	If you do not plan to use IVR NAT, verify that unique domain IDs are configured in all switches and VSANs participating in IVR.	See Domain ID Guidelines, page 2-7.
Step 3	Enable IVR in the border switches.	See Configuring IVR and IVR Zones Using the IVR Zone Wizard, page 1-6
Step 4	Configure the service group as required.	See IVR Service Groups, page 2-2.
Step 5	Configure the IVR distribution as required.	
Step 6	Configure the IVR topology, either manually or automatically.	SeeManually Configuring and Activating an IVR Topology, page 2-8 and Basic IVR Configuration, page 1-5.
Step 7	Create and activate IVR zone sets in *all* of the IVR-enabled border switches, either manually or using fabric distribution.	See Advanced IVR Zones and IVR Zone Sets, page 2-14.

Advanced IVR Configuration

This section includes instructions on advanced IVR configurations. It includes the following topics:

- IVR Service Groups, page 2-2
- Autonomous Fabric IDs, page 2-4
- Configuring IVR Without NAT, page 2-8

IVR Service Groups

In a complex network topology, you might only have a few IVR-enabled VSANs. To reduce the amount of traffic to non-IVR-enabled VSANs, you can configure service groups that restrict the traffic to the IVR-enabled VSANs. A maximum of 16 IVR service groups are allowed in a network. When a new IVR-enabled switch is added to the network, you must update the service groups to include the new VSANs.

This section includes the following information on service groups:

- Service Group Guidelines, page 2-3
- Default Service Group, page 2-3
- Service Group Activation, page 2-4

- Configuring IVR Service Groups, page 2-4

Service Group Guidelines

IVR service group guidelines are listed below:

- If you use service groups with IVR Auto topology, you should enable IVR and configure your service groups first, then distribute them with CFS before setting the IVR topology in Auto mode.
- The CFS distribution is restricted within the service group only when the IVR VSAN topology is in Auto mode. See the "IVR VSAN Topology" section on page 1-5.
- You can configure as many as 16 service groups in a network.
- When a new IVR-enabled switch is added to the network, you must update the service group to include the new VSANs.
- The same VSAN and AFID combination cannot be a member of more than one service group otherwise a CFS merge will fail.
- The total number of AFID and VSAN combinations in all the service groups combined cannot exceed 128. The maximum number of AFID and VSAN combinations in a single service group is 128.
- The IVR service group configuration is distributed in all IVR-enabled switches. IVR data traffic between two end devices belonging to a service group stays within that service group. For example, two members (for example, pWWN 1 and pWWN 2) cannot communicate if they belong to the same IVR zone and they belong to different service groups.
- During a CFS merge, service groups with the same name would be merged, as long as there are no conflicts with other service groups.
- If the total number of service groups exceeds 16 during a CFS merge, the CFS merge fails.
- CFS distributes service group configuration information to all reachable SANs. If you do not enable CFS distribution, you must ensure that the service group configuration is the same on all IVR-enabled switches in all VSANs.
- IVR end devices belonging to an IVR service group are not exported to any AFID or VSAN outside of its service group.
- When at least one service group is defined and an IVR zone member does not belong to the service group, that IVR zone member is not able to communicate with any other device.
- The default service group ID is zero (0).

Default Service Group

All AFID and VSAN combinations that are part of an IVR VSAN topology but are not part of any user-defined service group are members of the default service group. The identifier of the default service group is 0.

By default, IVR communication is permitted between members of the default service group. You can change the default policy to deny. To change the default policy, see the "Configuring IVR Service Groups" procedure on page 2-4. The default policy is not part of ASCII configuration.

Service Group Activation

A configured service group must be activated. Like zone set activation or VSAN topology activation, the activation of a configured service group replaces the currently active service group, if any, with the configured one. There is only one configured service group database and one active service group database. Each of these databases can have up to 16 service groups.

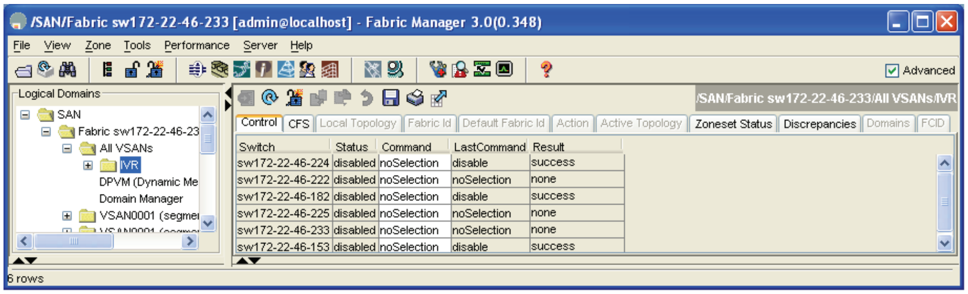
Configuring IVR Service Groups

To configure an IVR service group using Fabric Manager, follow these steps:

Step 1 Expand **All VSANs** and then select **IVR** in the Logical Domains pane.

You see the IVR configuration in the Information pane shown in Figure 2-1.

Figure 2-1 IVR Routing Configuration Control Tab



/SAN/Fabric sw172-22-46-233 [admin@localhost] - Fabric Manager 3.0(0.348)

/SAN/Fabric sw172-22-46-233/All VSANs/IVR

Switch	Status	Command	LastCommand	Result
sw172-22-46-224	disabled	noSelection	disable	success
sw172-22-46-222	disabled	noSelection	noSelection	none
sw172-22-46-182	disabled	noSelection	disable	success
sw172-22-46-225	disabled	noSelection	noSelection	none
sw172-22-46-233	disabled	noSelection	noSelection	none
sw172-22-46-153	disabled	noSelection	disable	success

6 rows

Step 2 Click the **Service Group** tab to display the existing service groups.

Step 3 Click the **Create Row** icon to make a new service group.

You see the service group dialog box.

Step 4 Check the switch check box for each switch involved in IVR.

Step 5 Complete the Name field for the service group and fill in the Fabric ID field for this entry.

Step 6 Enter a comma-separated list of VSAN IDs in the VSAN List text box.

Step 7 Click **Create** to create this entry or click **Cancel** to discard all changes.

Step 8 Repeat Step 1 through Step 7 for all switches and AFIDs associated with your IVR topology.

Autonomous Fabric IDs

The autonomous fabric ID (AFID) distinguishes segmented VSANS (for example, two VSANs that are logically and physically separate but have the same VSAN number). Cisco Fabric Manager Release 4.2(1) supports AFIDs 1 through 64. AFIDs are used in conjunction with Auto mode to allow segmented VSANs in the IVR VSAN topology database.

This section includes the following information about AFIDs:

- Autonomous Fabric ID Guidelines, page 2-5
- Configuring Default AFIDs, page 2-5

- Configuring Individual AFIDs, page 2-6

Autonomous Fabric ID Guidelines

You can configure AFIDs individually for VSANs, or you can set the default AFIDs for all VSANs on a switch. If you configure an individual AFID for a subset of the VSANs on a switch that has a default AFID, that subset uses the configured AFID while all other VSANs on that switch use the default AFID.

You can only use an AFID configuration when the VSAN topology is in Auto mode. In a manually configured VSAN topology mode, the AFIDs are specified in the VSAN topology configuration itself and a separate AFID configuration is not needed.

Note Two VSANs with the same VSAN number but different AFIDs are counted as two VSANs out of the total 128 VSANs allowed in the fabric.

When devices attached to multiple switches belong to one VSAN, they can not communicate with each other by configuring the regular zone set because the AFIDs are different. You can consider that the different AFIDs are different fabrics; therefore the three switches represent three separate fabrics.

If we specify the IVR VSAN topology as shown in Example 2-1, IVR will set up the connection between the devices across the switches even though they have the same VSAN.

Example 2-1 IVR VSAN Topology With the Same VSAN

```
switch# show ivr vsan-topology
AFID  SWITCH WWN                 Active   Cfg.    VSANS
------------------------------------------------------
   1  20:00:00:0d:ec:27:6b:c0     yes     yes       1
   2  20:00:00:0d:ec:27:6c:00     yes     yes       1
   3  20:00:00:0d:ec:27:6c:40     yes     yes       1

Total:   3 entries in active and configured IVR VSAN-Topology
```

Configuring Default AFIDs

To configure default AFIDs using Fabric Manager, follow these steps:

Step 1 Expand **All VSANs** and then select **IVR** in the Logical Domains pane.

You see the IVR configuration in the Information pane.

Step 2 Click the **Default Fabric ID** tab to display the existing default AFIDs.

Step 3 Click the **Create Row** icon to create a default AFID.

Step 4 Check the check boxes next to each switch involved in IVR that you want to use this default AFID.

Step 5 Provide a name for each SwitchWWN and set the default Fabric ID.

Step 6 Click **Create** to create this entry.

Step 7 Repeat Step 1 through Step 6 for all default AFIDs that you want to configure in your IVR topology.

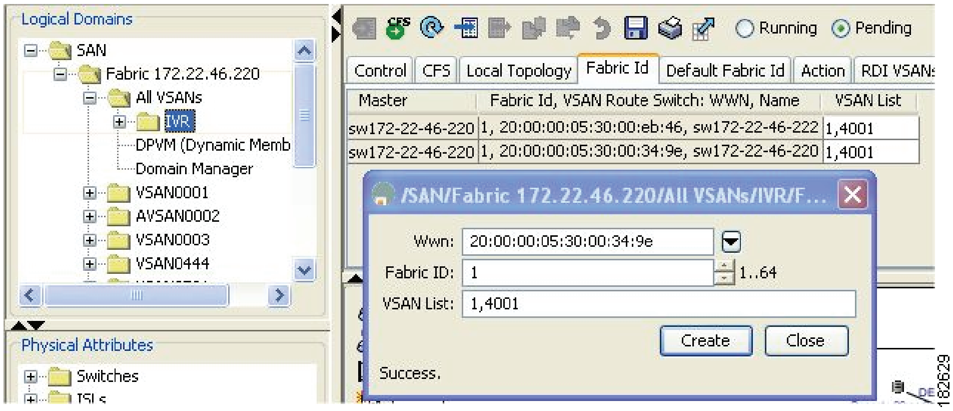
Configuring Individual AFIDs

To configure individual AFIDs using Fabric Manager, follow these steps:

Step 1 Expand **All VSANs** and then select **IVR** in the Logical Domains pane.

You see the IVR configuration in the Information pane.

Figure 2-2 Fabric ID Tab



Master	Fabric Id, VSAN Route Switch: WWN, Name	VSAN List
sw172-22-46-220	1, 20:00:00:05:30:00:eb:46, sw172-22-46-222	1,4001
sw172-22-46-220	1, 20:00:00:05:30:00:34:9e, sw172-22-46-220	1,4001

Wwn: 20:00:00:05:30:00:34:9e

Fabric ID: 1 1..64

VSAN List: 1,4001

Success.

Step 2 Click the **Fabric ID** tab to display the existing AFIDs (see Figure 2-2).

Step 3 Click the **Create Row** icon to create an AFID.

Step 4 Check the check box next to each switch involved in IVR that you want to use this default AFID.

Step 5 Provide a name for each SwitchWWN and set the Fabric ID.

Step 6 Enter a comma-separated list of VSAN IDs in the VSAN List text box.

Step 7 Click **Create** to create this entry.

Step 8 Repeat Step 1 through Step 6 for all switches and AFIDs you want to configure in your IVR topology.

IVR Without IVR NAT or Auto Topology

This section includes the following sections on IVR Without IVR NAT or Auto Topology

- IVR Without IVR NAT or Auto Topology Guidelines, page 2-6
- Configuring IVR Without NAT, page 2-8
- Manually Configuring an IVR Topology, page 2-9

IVR Without IVR NAT or Auto Topology Guidelines

Before configuring an IVR SAN fabric without IVR in NAT mode or IVR topology in Auto mode, consider the following general guidelines:

- Acquire a mandatory Enterprise License Package or SAN-EXTENSION license package and one active IPS card for this feature.
- If you change an FSPF link cost, ensure that the FSPF path distance (the sum of the link costs on the path) of any IVR path is less than 30,000.
- IVR-enabled VSANs can be configured when an interop mode is enabled or disabled.

This section also includes the following:

- Domain ID Guidelines, page 2-7
- Transit VSAN Guidelines, page 2-7
- Border Switch Guidelines, page 2-8

Domain ID Guidelines

Before configuring domain IDs, consider the following guidelines:

- Configure unique domain IDs across all VSANs and switches participating in IVR operations if you are not using IVR NAT. The following switches participate in IVR operations:
  - All edge switches in the edge VSANs (source and destination)
  - All switches in transit VSANs
- Minimize the number of switches that require a domain ID assignment. This ensures minimum traffic disruption.
- Minimize the coordination between interconnected VSANs when configuring the SAN for the first time as well as when you add each new switch.

You can configure domain IDs using one of two options:

- Configure the allowed-domains list so that the domains in different VSANs are non-overlapping on all participating switches and VSANs.
- Configure static, non-overlapping domains for each participating switch and VSAN.

Note In a configuration involving IVR without NAT, if one VSAN in the IVR topology is configured with static domain IDs, then the other VSANs (edge or transit) in the topology must be configured with static domain IDs.

Transit VSAN Guidelines

Before configuring transit VSANS, consider the following guidelines:

- Besides defining the IVR zone membership, you can choose to specify a set of transit VSANs to provide connectivity between two edge VSANs:
  - If two edge VSANs in an IVR zone overlap, then a transit VSAN is not required (though, not prohibited) to provide connectivity.
  - If two edge VSANs in an IVR zone do not overlap, you may need one or more transit VSANs to provide connectivity. Two edge VSANs in an IVR zone will not overlap if IVR is not enabled on a switch that is a member of both the source and destination edge VSANs.
- Traffic between the edge VSANs only traverses through the shortest IVR path.
- Transit VSAN information is common to all IVR zone sets. Sometimes, a transit VSAN can also act as an edge VSAN in another IVR zone.

Border Switch Guidelines

Before configuring border switches, consider the following guidelines:

- Configure IVR only in the relevant border switches.
- Border switches require Cisco MDS SAN-OS Release 1.3(1) or later.
- A border switch must be a member of two or more VSANs.
- A border switch that facilitates IVR communications must be IVR enabled.
- IVR can also be enabled on additional border switches to provide redundant paths between active IVR zone members.
- The VSAN topology configuration must be updated before a border switch is added or removed.

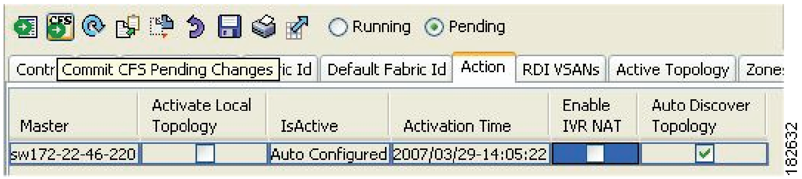
Configuring IVR Without NAT

To enable IVR in without NAT using Fabric Manager, follow these steps:

Step 1 Expand **All VSANs** and then select **IVR** in the Logical Domains pane.

You see the IVR configuration in the Information pane.

Figure 2-3 Action Tab



Master	Activate Local Topology	IsActive	Activation Time	Enable IVR NAT	Auto Discover Topology
sw172-22-46-220	□	Auto Configured	2007/03/29-14:05:22	□	☑

Step 2 Click the **Action** tab.

Step 3 Uncheck the **Enable IVR NAT** check box (see Figure 2-3).

Step 4 Click the **Apply Changes** icon to distribute this change to all switches in the fabric.

Manually Configuring and Activating an IVR Topology

You must create the IVR topology on every IVR-enabled switch in the fabric if you have not configured IVR topology in Auto mode. If you choose to manually configure IVR instead of using Auto mode, follow the instructions in this section.

This section includes the following:

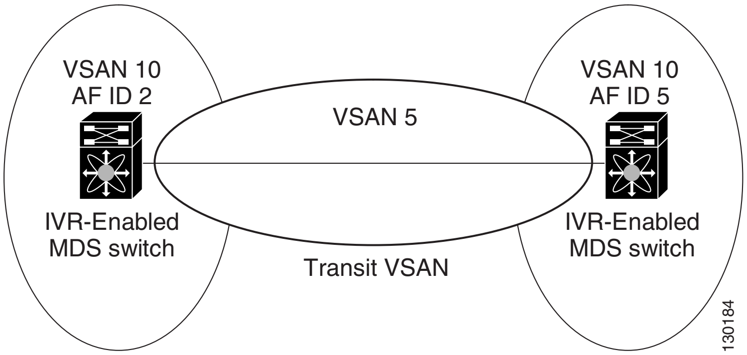
- Manual Configuration Guidelines, page 2-9
- Manually Configuring an IVR Topology, page 2-9
- Activating a Manually Configured IVR Topology, page 2-10

Manual Configuration Guidelines

Consider the following guidelines when manually configuring an IVR topology:

- You can configure a maximum of 128 IVR-enabled switches and 128 distinct VSANs in an IVR topology (see the "Database Merge Guidelines" section on page 1-21).
- You will need to specify the IVR topology using the following information:
  - The switch WWNs of the IVR-enabled switches.
  - A minimum of two VSANs to which the IVR-enabled switch belongs.
  - The AFID, which distinguishes two VSANs that are logically and physically separate, but have the same VSAN number. You can specify up to 64 AFIDs. See Figure 2-4.

Figure 2-4 Example IVR Topology with Non-Unique VSAN IDs Using AFIDs



- If two VSANs in an IVR topology have the same VSAN ID and different AFIDs, they count as two VSANs for the 128-VSAN limit for IVR.
- The use of a single AFID does not allow for segmented VSANs in an inter-VSAN routing topology.

Manually Configuring an IVR Topology

Note

You can configure IVR using the IVR tables in the Information pane in Fabric Manager. Use these tables only if you are familiar with all IVR concepts. We recommend you configure IVR using the IVR Wizard. See "Configuring IVR and IVR Zones Using the IVR Zone Wizard" section on page 1-6.

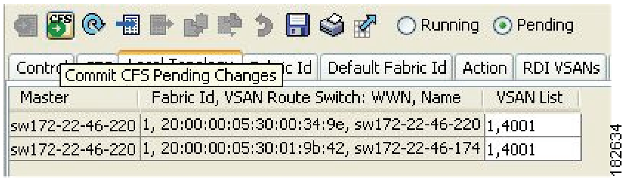
Note Most tabs in the Information pane for features using CFS are dimmed until you click the CFS tab. The CFS tab shows which switches have CFS enabled and shows the master switch for this feature. Once the CFS tab is clicked, the other tabs in the Information pane are activated.

To manually configure an IVR topology using Fabric Manager, follow these steps:

Step 1 Expand **All VSANs** and then select **IVR** in the Logical Domains pane.

You see the IVR configuration in the Information pane.

Figure 2-5 Local Topology Tab



Master	Fabric Id, VSAN Route Switch: WWN, Name	VSAN List
sw172-22-46-220	1, 20:00:00:05:30:00:34:9e, sw172-22-46-220	1,4001
sw172-22-46-220	1, 20:00:00:05:30:01:9b:42, sw172-22-46-174	1,4001

Step 2 Click the **Local Topology** tab to display the existing IVR topology.

Step 3 Click the **Create Row** icon to create rows in the IVR topology (see Figure 2-5).

Step 4 Select the switch, switch WWN, and a comma-separated list of VSAN IDs for this topology.

Step 5 Click **Create** to create this new row.

Step 6 Click the **Apply Changes** icon to create the IVR topology.

Repeat this configuration on all IVR-enabled switches or distribute the IVR configuration using CFS.

Tip Transit VSANs are deduced based on your configuration. The IVR feature does not have an explicit transit-VSAN configuration.

Activating a Manually Configured IVR Topology

After manually configuring the IVR topology, you must activate it.

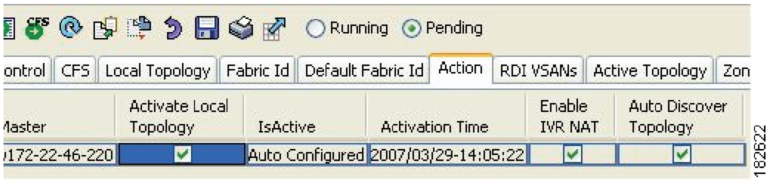
Caution Active IVR topologies cannot be deactivated. You can only switch to IVR topology Auto mode.

To activate a manually configured IVR topology using Fabric Manager, follow these steps:

Step 1 Expand **All VSANs** and then select **IVR** in the Logical Domains pane.

You see the IVR configuration in the Information pane.

Figure 2-6 Action Tab



laster	Activate Local Topology	IsActive	Activation Time	Enable IVR NAT	Auto Discover Topology
172-22-46-220	☑	Auto Configured	2007/03/29-14:05:22	☑	☑

Step 2 Click the **Action** tab to display the existing IVR topology.

Step 3 Check the **Activate Local Topology** check box (see Figure 2-6).

Step 4 Click the **Apply Changes** icon to activate the IVR topology.

Working With Existing IVR Topologies

This section includes advanced IVR configurations for existing IVR topologies:

- Clearing a Manually Configured IVR Topology, page 2-11
- Migrating from IVR Auto Topology Mode to Manual Mode, page 2-11

Clearing a Manually Configured IVR Topology

You can only clear manually created IVR VSAN topology entries.

To clear a manually created IVR topology using Fabric Manager, follow these steps:

Step 1 Expand **All VSANs and** then select **IVR** in the Logical Domains pane.

Step 2 Click the **Control** tab if it is not already displayed.

Step 3 Highlight the rows you want to delete from the IVR topology.

Step 4 Click the **Delete Row** icon to delete these rows from the IVR topology.

Step 5 Click the **Apply Changes** icon to delete the IVR topology.

Migrating from IVR Auto Topology Mode to Manual Mode

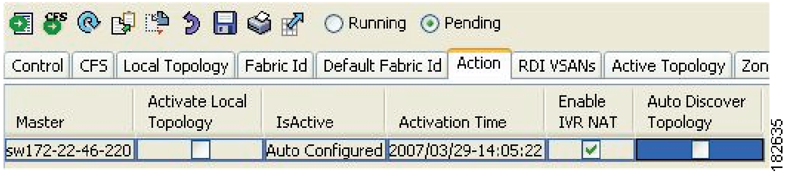
If you want to migrate from Auto mode to Manual mode, copy the active IVR VSAN topology database to the user-configured IVR VSAN topology database before switching modes.

To migrate from Auto mode to Manual mode using Fabric Manager, follow these steps:

Step 1 Expand **All VSANs** and then select **IVR** in the Logical Domains pane.

You see the IVR configuration in the Information pane.

Figure 2-7 Action Tab



Master	Activate Local Topology	IsActive	Activation Time	Enable IVR NAT	Auto Discover Topology
sw172-22-46-220	□	Auto Configured	2007/03/29-14:05:22	☑	□

Step 2 Click the **Action** tab.

Step 3 Highlight the switch on which you want to disable auto topology mode.

Step 4 Uncheck the **Auto Discover Topology** check box (see Figure 2-7).

Step 5 Click the **Apply Changes** icon.

Persistent FC IDs for IVR

This section includes the following information:

- FC ID Features and Benefits, page 2-12
- FC ID Guidelines, page 2-12
- Configuring Persistent FC IDs for IVR, page 2-13

FC ID Features and Benefits

FC ID persistence improves IVR management by providing the following features:

- Allows you to control and assign a specific virtual domain to use in a native VSAN.
- Allows you to control and assign a specific virtual FC ID for a device.

The benefits of persistent FC IDs for IVR are as follows:

- Host devices always see the same FC ID for targets.
- FC IDs help you plan your SAN layout better by assigning virtual domains for IVR to use.
- FC IDs can make SAN monitoring and management easier. When you see the same domain or FC ID consistently assigned, you can readily determine the native VSAN or device to which it refers.

FC ID Guidelines

Before configuring persistent FC IDs, consider the following:

- You can configure two types of database entries for persistent IVR FC IDs:
  - Virtual domain entries—Contain the virtual domain that should be used to represent a native VSAN in a specific VSAN (current VSAN). Virtual domain entries contain the following information:

    Native AFID

    Native VSAN

    Current AFID

    Current VSAN

    Virtual domain to be used for the native AFID and VSAN in current AFID and VSAN

  - Virtual FC ID entries—Contain the virtual FC ID that should be used to represent a device in a specific VSAN (current VSAN). Virtual FC ID entries contain the following information:

    Port WWN

    Current AFID

    Current VSAN

    Virtual FC ID to be used to represent a device for the given pWWN in the current AFID and VSAN

- If you use persistent FC IDs for IVR, we recommend that you use them for all the devices in the IVR zone set. We do not recommend using persistent FC IDs for some of the IVR devices while using automatic allocation for other devices.
- IVR NAT must be enabled to use IVR persistent FC IDs.
- In an IVR NAT configuration, if one VSAN in the IVR topology is configured with static domain IDs, then the IVR domains that can be exported to that VSAN must also be assigned static domains.

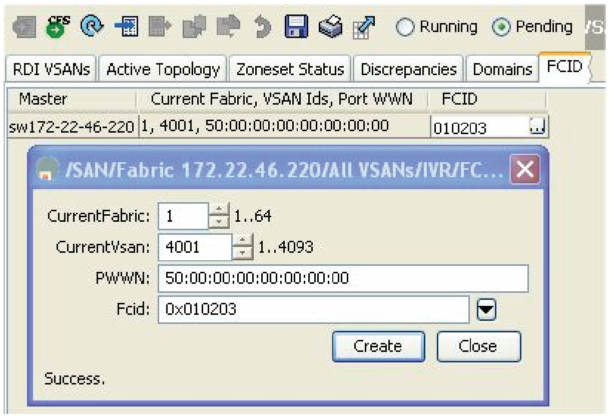
Configuring Persistent FC IDs for IVR

To configure persistent FC IDs for IVR using Fabric Manager, follow these steps:

Step 1 Expand **All VSANs** and then select **IVR** in the Logical Domains pane.

You see the IVR configuration in the Information pane.

Figure 2-8 FCID Tab



Master	Current Fabric, VSAN Ids, Port WWN	FCID
sw172-22-46-220	1, 4001, 50:00:00:00:00:00:00:00	010203

CurrentFabric: 1 1..64
CurrentVsan: 4001 1..4093
PWWN: 50:00:00:00:00:00:00:00
Fcid: 0x010203

Success.

Step 2 Click the **FCID** tab.

Step 3 Click the **Create Row** icon to create an FC ID (see Figure 2-8).

Step 4 Select the switch for which you are configuring the virtual FC ID to be used to represent a device in a specific VSAN (current VSAN).

Step 5 Enter the current fabric in the **Current Fabric ID** field for the fcdomain database.

Step 6 Enter the current VSAN in the **Current VSAN ID** field for the fcdomain database.

Step 7 Enter the **pWWN.**

Step 8 Click the drop-down menu to select the FC ID to map to the pWWN you selected.

Step 9 Click **Create** to create this new row.

Advanced IVR Zones and IVR Zone Sets

This section describes advanced configuration information for IVR zones and IVR zone sets. For basic information on configuring IVR zones and zone sets, see the "IVR Zones and IVR Zone Sets" section on page 1-12.

As part of the IVR configuration, you need to configure one or more IVR zone to enable cross-VSAN communication. To achieve this, you must specify each IVR zone as a set of (pWWN, VSAN) entries. Different IVR zone sets can contain the same IVR zone, because IVR zones can be members of one or more IVR zone sets.

Note The same IVR zone set must be activated on *all* of the IVR-enabled switches.

Caution Prior to Cisco SAN-OS Release 3.0(3) you can only configure a total of 10,000 zone members on all switches in a network. As of Cisco SAN-OS Release 3.0(3) you can only configure a total of 20,000 zone members on all switches in a network. A zone member is counted twice if it exists in two zones. See the Database Merge Guidelines, page 1-21.

This section includes the following topics:

- IVR Zone Configuration Guidelines, page 2-14
- Configuring QoS for IVR Zones, page 2-14
- Renaming IVR Zones and IVR Zone Sets, page 2-15
- Configuring IVR Using Read-Only Zoning, page 2-15

IVR Zone Configuration Guidelines

When interop mode is enabled, consider the following IVR configuration guidelines:

- When a member's native VSAN is in interop mode (for example, when the interop mode is 2, 3, or 4), then ReadOnly, the QoS attribute, and LUN zoning are not permitted.
- When a member's VSAN is already in interop mode and an attempt is made to configure ReadOnly, the QoS attribute, or LUN zoning, a warning message is displayed to indicate that the configuration is not permitted.
- When you configure ReadOnly, the QoS attribute, or LUN zoning first, and then change the member's VSAN interop mode, a warning message is displayed to indicate the configuration is not permitted. You are then prompted to change the configuration.

Configuring QoS for IVR Zones

To configure QoS for an IVR zone using Fabric Manager, follow these steps:

Note The default QoS attribute setting is low.

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

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

Step 2 Select **Zones** or a zone set.

Step 3 Check the **QoS** check box and set the QoS priority.

Step 4 Click **Activate** to make the changes.

Note If other QoS attributes are configured, the highest setting takes priority.

Renaming IVR Zones and IVR Zone Sets

To rename an IVR zone or IVR zone set, using Fabric Manager, follow the steps below:

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

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

Step 2 Click a zone or zone set in the left pane.

Step 3 Choose **Edit > Rename**.

An edit box appears around the zone or zone set name.

Step 4 Enter a new name.

Step 5 Click **Activate** or **Commit Changes**.

Configuring IVR Using Read-Only Zoning

Read-only zoning (with or without LUNs) can be used between members of active IVR zones. To configure this service, you must create and activate read-only zones between the desired IVR zone members in all relevant edge VSANs using the zoning interface.

Note Read-only zoning cannot be configured in an IVR zone set setup.

INDEX

Text Part Number: