Cisco MDS 9000 Series Inter-VSAN Routing Configuration Guide, Release 8.x

First Published: 2016-06-14

Last Modified: 2020-07-29

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

CONTENTS

Preface

This preface describes the audience, organization of, and conventions used in the Cisco MDS 9000 Series Configuration Guides. It also provides information on how to obtain related documentation, and contains the following chapters:

Audience

To use this installation guide, you need to be familiar with electronic circuitry and wiring practices, and preferably be an electronic or electromechanical technician.

Document Conventions

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.

Warnings use the following conventions:

Warning This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071.

Related Documentation

The documentation set for the Cisco MDS 9000 Series Switches includes the following documents.

Release Notes

http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-release-notes-list.html

Regulatory Compliance and Safety Information

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/hw/regulatory/compliance/RCSI.html

Compatibility Information

http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-device-support-tables-list.html

Installation and Upgrade

http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-installation-guides-list.html

Configuration

http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-installation-and-configuration-guides-list.html

CLI

http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-command-reference-list.html

Troubleshooting and Reference

http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/tsd-products-support-troubleshoot-and-alerts.html

To find a document online, use the Cisco MDS NX-OS Documentation Locator at:

http://www.cisco.com/c/en/us/td/docs/storage/san_switches/mds9000/roadmaps/doclocater.html

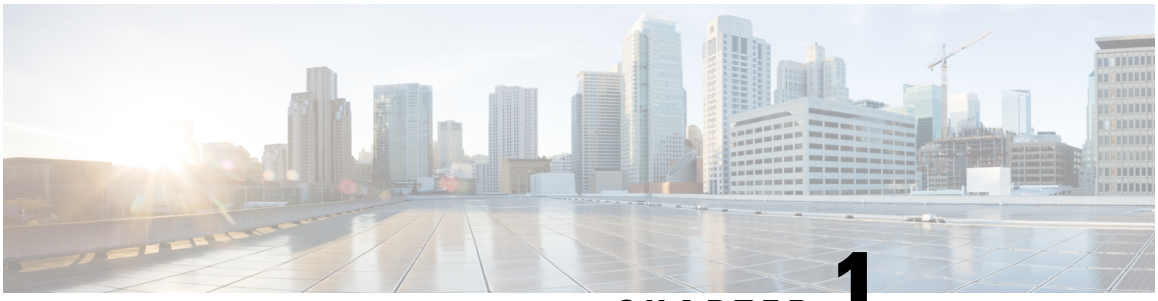
Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

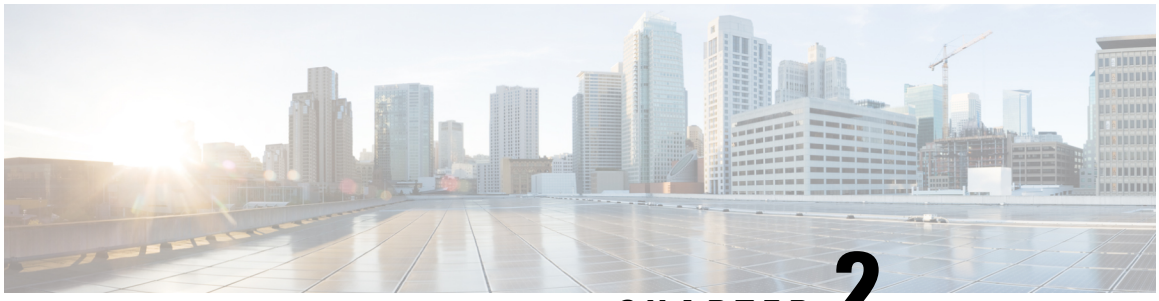
Preface



CHAPTER 1

New and Changed Information

There are no new features in the Cisco MDS 9000 Series Inter-VSAN Routing Configuration Guide for Cisco MDS NX-OS Release 8.x



CHAPTER 2

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 Advanced Inter-VSAN Routing Configuration, on page 31 if you need to set up an advanced IVR configuration.

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.

IVR Features

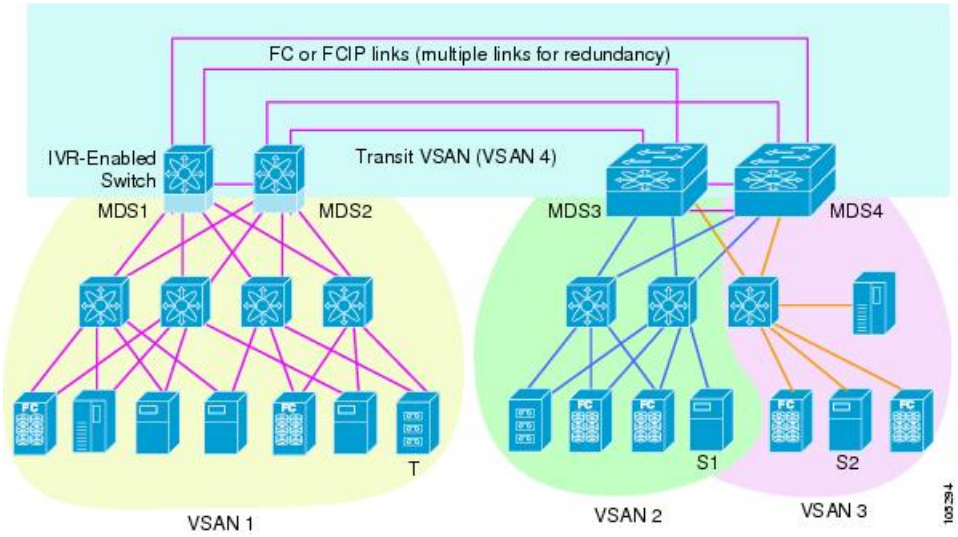
IVR supports the following features:

- Accesses resources across VSANs without compromising other VSAN benefits.
- Transports data traffic between specific initiators and targets on different VSANs without merging VSANs into single logical fabric.
- Establishes proper interconnected routes that travels one or more VSANs across multiple switches. IVR is not limited to VSANs present on a common switch.
- Shares valuable resources (such as tape libraries) across VSANs without compromise. Fibre Channel traffic does not flow between VSANs, nor can initiators access resources across VSANs other than the designated VSAN.

- Provides efficient business continuity or disaster recovery solutions when used in conjunction with FCIP. See the figure, Figure 1: Traffic Continuity Using IVR and FCIP.
- 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 To configure the sample scenario shown in the following figure, follow the steps in IVR Auto Topology Mode Configuration Example.

Figure 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 could 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 Series. 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. VSANs 1, 2, and 3 (see Figure 1: Traffic Continuity Using IVR and FCIP, on page 4), 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. VSAN 4 is a transit VSAN(see Figure 1: Traffic Continuity Using IVR and FCIP, on page 4).

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(see Figure 1: Traffic Continuity Using IVR and FCIP, on page 4), 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

For information on IVR configuration limits, see Cisco MDS NX-OS Configuration Limits, Release 8.x.

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

To use IVR NAT, it must be enabled on all IVR-enabled switches in the fabric. For information on distributing the IVR configuring using CFS, see Distributing the IVR Configuration Using CFS, on page 8. By default, IVR NAT and IVR configuration distributions are disabled on all switches in the Cisco MDS 9000 Family.

See About IVR NAT and IVR Auto Topology Mode, on page 10 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.

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

Using IVR auto topology mode, you no longer need to manually update the IVR VSAN topology when reconfigurations occur in your fabric. If an IVR manual topology database exists, IVR auto topology mode initially uses that topology information. The automatic update 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 IVR auto topology mode is enabled, it starts with the previously active IVR manual topology if it exists, and then the discovery process begins. New, alternate, or better paths my be discovered. 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 IVR auto topology 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 Task List

To configure IVR, follow these steps:

Step 1 See Enabling IVR NAT, on page 12

Enable IVR NAT.

Step 2 See Enabling IVR , on page 7.

Enable IVR on all border switches.

Step 3 See Distributing the IVR Configuration Using CFS, on page 8.

Enable IVR distribution.

Step 4 See About IVR NAT and IVR Auto Topology Mode, on page 10 .

Enable IVR auto topology mode.

Step 5 Configure IVR virtual domains.

Step 6 See Configuring IVR Zones and IVR Zone Sets, on page 17.

Configure and activate zone sets.

Step 7 See Committing the Changes, on page 9.

Commit the IVR configuration.

Step 8 See Verifying IVR Zone and IVR Zone Set Configuration, on page 20.

Verify the IVR configuration.

Basic IVR Configuration

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

Enabling IVR

The IVR feature must be enabled in all border switches in the fabric that participate in the IVR. By default, this feature is disabled in all Cisco MDS 9000 Series switches. You can manually enable IVR on all required switches in the fabric or configure fabric-wide distribution of the IVR configuration. See Distributing the IVR Configuration Using CFS, on page 8.

Note The configuration and verification commands for the IVR feature are only available when IVR is enabled on a switch. When you disable this configuration, all related configurations are automatically discarded.

To enable IVR on any participating switch, follow these steps:

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Enables IVR NAT on the switch.

switch(config)# **ivr nat**

Step 3 Enables IVR on the switch.

switch(config)# **feature ivr**

Step 4 Disables (default) IVR on the switch.

switch(config)# **no feature ivr**

Distributing the IVR Configuration Using CFS

The IVR feature uses the Cisco Fabric Services (CFS) infrastructure to enable efficient configuration management and to provide a single point of configuration for the entire fabric in the VSAN. For information on CFS, refer to the *Cisco MDS 9000 Series System Management Configuration Guide* .

The following configurations are distributed:

- IVR zones
- IVR zone sets
- IVR VSAN topology
- IVR active topology and zone set (activating these features in one switch propagates the configuration to all other distribution-enabled switches in the fabric)
- AFID database

Note IVR configuration distribution is disabled by default. For the feature to function correctly, you must enable it on all IVR-enabled switches in the network.

Database Implementation

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

- Configured database—The database is manually configured by the user.
- Active database—The database is currently enforced by the fabric.
- Pending database—If you modify the configuration, you need to commit or discard the configured database changes to the pending database. The fabric remains locked during this period. Changes to the pending database are not reflected in the active database until you commit the changes to CFS.

Enabling Configuration Distribution

To enable IVR configuration distribution, follow these steps:

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Enables IVR distribution.

switch(config)# **ivr distribute**

Step 3 Disables (default) IVR distribution.

switch(config)# **no ivr distribute**

Locking the Fabric

The first action that modifies the database creates the pending database and locks the feature in the VSAN. Once you lock the fabric, the following situations apply:

- No other user can make any configuration changes to this feature.
- A copy of the configuration database becomes the pending database along with the first active change.

Committing the Changes

If you commit the changes made to the active database, the configuration is committed to all the switches in the fabric. On a successful commit, the configuration change is applied throughout the fabric and the lock is released.

To commit IVR configuration changes, follow these steps:

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Commits the IVR changes.

switch(config)# **ivr commit**

Discarding the Changes

If you discard (terminate) the changes made to the pending database, the configuration database remains unaffected and the lock is released.

To discard IVR configuration changes, follow these steps:

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Discards the IVR changes and clears the pending configuration database.

switch(config)# **ivr abort**

Clearing a Locked Session

If you have performed an IVR 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 pending database are discarded and the fabric lock is released.

Tip The 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, use the **clear ivr session** command in EXEC mode.

```
switch# clear ivr session
```

About IVR NAT and IVR Auto Topology Mode

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

- Configure IVR only in the relevant switches.
- Enable CFS for IVR on all switches in the fabric.
- 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 Release 2.1(1a) or later and one active IPS card for this feature. For information on licensing, refer to the *Cisco MDS 9000 Series 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 terminated 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.

- IVR non-NAT mode is not supported from Cisco NX-OS Release 5.2(x) and later releases. If you have IVR non-NAT mode configured, see the Upgrading Guidelines Specific to NX-OS Release 5.2(8c) section for instructions on how to migrate to IVR NAT mode.
- 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 destination IDs are included in the packet data. 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 the following table.

Table 1: 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 packet data, you cannot use IVR with NAT in your topology.

Note Don't enable IVR NAT when IVR Topology includes FICON VSANs. If IVR NAT is enabled along with FICON VSAN, the switch throws the **fcid-nat cannot be enabled if FICON enabled VSANs and topology VSANs overlap** error.

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.

Enabling IVR NAT

This section includes instructions on how to enable IVR NAT and how to enable IVR auto topology mode.

To enable IVR NAT, follow these steps:

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Enables IVR NAT on the switch.

switch(config)# **ivr nat**

Step 3 Disables (default) IVR NAT on the switch.

switch(config)# **no ivr nat**

Enabling IVR Auto Topology Mode

Note IVR configuration distribution must be enabled before configuring IVR auto topology mode (see Distributing the IVR Configuration Using CFS, on page 8). Once IVR auto topology mode is enabled, you cannot disable IVR configuration distribution.

To enable IVR auto topology mode, follow these steps:

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Enables IVR auto topology mode.

switch(config)# **ivr vsan-topology auto**

What to do next

To view an automatically discovered IVR topology, use the **show ivr vsan-topology** command.

```
switch# show ivr vsan-topology

AFID  SWITCH WWN                 Active   Cfg. VSANS
--------------------------------------------------------------
   1  20:00:54:7f:ee:1b:0b:d0     yes      no  11,1109
   1  20:00:54:7f:ee:1c:0e:00 *   yes      no  2,11-12,28,1110


Total:   2 entries in active and configured IVR VSAN-Topology
```

Note The asterisk (*) indicates the local switch.

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.

Use the **ivr withdraw domain** command in EXEC mode to temporarily withdraw the overlapping virtual domain interfaces from the affected VSAN.

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 in a specified VSAN, follow these steps:

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Adds the IVR virtual domains in VSAN 1. Perform this step on all IVR switches.

switch(config)# **ivr virtual-fcdomain-add vsan-ranges 1-4093**

Step 3 Reverts to the factory default of not adding IVR virtual domains and removes the currently active virtual domains for that VSAN from the fcdomain manager list.

switch(config)# no **ivr virtual-fcdomain-add vsan-ranges 1-4093**

Manually Configuring Fabric-wide IVR Virtual Domains

Note As of Cisco SAN-OS Release 3.1(2), Cisco Fabric Configuration Services (FCS) supports the discovery of virtual devices. The **fcs virtual-device-add vsan-ranges** command, issued in FCS configuration submode, allows you to discover virtual devices in a particular VSAN or in all VSANs. To discover the devices that are zoned for IVR using this command, the devices must have request domain_ID (RDI) enabled. For information on using FCS, refer to the Cisco MDS 9000 Series System Management Configuration Guide .

To configure fabric-wide IVR virtual domains in a specified VSAN, follow these steps:

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Adds the IVR virtual domains in VSAN 1. Perform this step on all IVR switches.

switch(config)# **ivr virtual-fcdomain-add 2 vsan-ranges 1-4093**

Step 3 Commits the fabric-wide configuration.

switch(config)# **ivr commit**

Step 4 Reverts to the factory default of not adding IVR virtual domains and removes the currently active virtual domains for that VSAN from the fcdomain manager list.

switch(config)# no **ivr virtual-fcdomain-add2 vsan-ranges 1-4093**

Verifying an IVR Virtual Domain Configuration

To view the status of the IVR virtual domain configuration, use the **show ivr virtual-fcdomain-add-status** command.

```
switch# show ivr virtual-fcdomain-add-status
IVR virtual domains are added to fcdomain list in VSANS: 1
(As well as to VSANs in interoperability mode 2 or 3)
```

Clearing an IVR fcdomain Database

To clear the IVR fcdomain database, use the following command:

```
switch# clear ivr fcdomain database
```

IVR Zones and IVR Zone Sets

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

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.

The following table identifies the key differences between IVR zones and zones.

Table 2: 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

The following table identifies the IVR zone limits per physical fabric.

Table 3: 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 Database Merge Guidelines, on page 23.

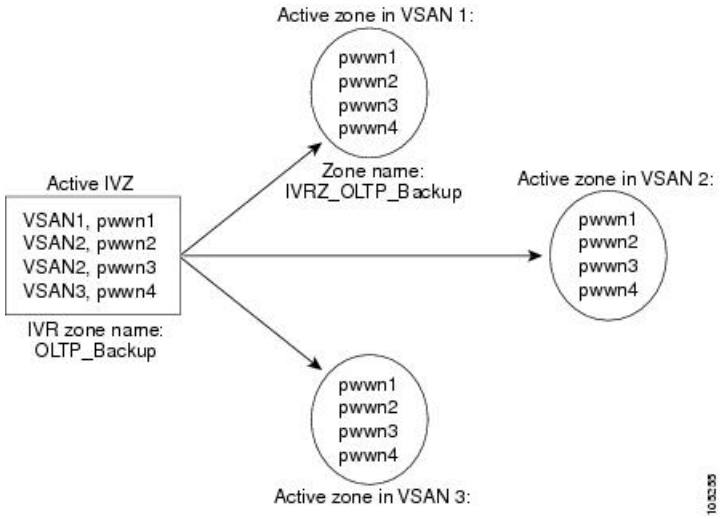
Caution If you want to downgrade to a release prior to Cisco SAN-OS Release 3.0(3), the number of IVR zones cannot exceed 2000 and the number of IVR zone members cannot exceed 10,000.

Automatic IVR Zone Creation

The following figure 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 2: 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 Database Merge Guidelines, on page 23 .

Configuring IVR Zones and IVR Zone Sets

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

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Creates an IVR zone named sample_vsan2-3.

switch(config)# **ivr zone name sample_vsan2-3**

Step 3 Adds the specified pWWN in VSAN 3 as an IVR zone member.

switch(config-ivr-zone)# **member pwwn 21:00:00:e0:8b:02:ca:4a vsan 3**

Step 4 Adds the specified pWWN in VSAN 2 as an IVR zone member.

switch(config-ivr-zone)# **member pwwn 21:00:00:20:37:c8:5c:6b vsan 2**

Step 5 Returns to configuration mode.

switch(config-ivr-zone)# **exit**

Step 6 Creates an IVR zone named sample_vsan4-5.

switch(config)# **ivr zone name sample_vsan4-5**

Step 7 Adds the specified pWWN in VSAN 4 as an IVR zone member.

switch(config-ivr-zone)# **member pwwn 21:00:00:e0:8b:06:d9:1d vsan 4**

Step 8 Adds the specified pWWN in VSAN 4 as an IVR zone member.

switch(config-ivr-zone)# **member pwwn 21:01:00:e0:8b:2e:80:93 vsan 4**

Step 9 Adds the specified pWWN in VSAN 5 as an IVR zone member.

switch(config-ivr-zone)# **member pwwn 10:00:00:00:c9:2d:5a:dd vsan 5**

Step 10 Returns to configuration mode.

switch(config-ivr-zone)# **exit**

Step 11 Creates an IVR zone set named Ivr_zoneset1.

switch(config)# **ivr zoneset name Ivr_zoneset1**

Step 12 Adds the sample_vsan2-3 IVR zone as an IVR zone set member.

switch(config-ivr-zoneset)# **member sample_vsan2-3**

Step 13 Adds the sample_vsan4-5 IVR zone as an IVR zone set member.

switch(config-ivr-zoneset)# **member sample_vsan4-5**

Step 14 Returns to configuration mode.

switch(config-ivr-zoneset)# **exit**

Step 15 Activates the newly created IVR zone set.

switch(config)# **ivr zoneset activate name IVR_ZoneSet1**

Step 16 Forcefully activates the specified IVR zone set.

switch(config)# **ivr zoneset activate name IVR_ZoneSet1 force**

Step 17 Deactivates the specified IVR zone set.

switch(config)# **no ivr zoneset activate name IVR_ZoneSet1**

Step 18 Returns to EXEC mode.

```
switch(config)# end
```

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.
- If a segmented VSAN is present in an IVR topology, then the IVR zone set will not be activated.

You can also use the **force** command to activate IVR zone sets. The following table lists the various scenarios with and without the **force command** option.

Table 4: IVR Scenarios with and without the force Command

Case	Default Zone Policy	Active Zone Set before IVR Zone Activation	force command 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** command 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** command 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, follow these steps:

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Activates the newly created IVR zone set.

switch(config)# **ivr zoneset activate name IVR_ZoneSet1**

Step 3 Forcefully activates the specified IVR zone set.

switch(config)# **ivr zoneset activate name IVR_ZoneSet1 force**

Step 4 Deactivates the specified IVR zone set.

switch(config)# **no ivr zoneset activate name IVR_ZoneSet1**

What to do next

Note To replace the active IVR zone set with a new IVR zone set without disrupting traffic, activate the new IVR zone set without deactivating the current active IVR zone set.

Verifying IVR Zone and IVR Zone Set Configuration

Verify the IVR zone and IVR zone set configurations using the **show ivr zone** and **show ivr zoneset** commands.

Displays the IVR Zone Configuration

```
switch# show ivr zone
zone name sample_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
zone name ivr_qa_z_all
    pwwn 21:00:00:e0:8b:06:d9:1d vsan 1
    pwwn 21:01:00:e0:8b:2e:80:93 vsan 4
    pwwn 10:00:00:00:c9:2d:5a:dd vsan 1
```

```
    pwwn 10:00:00:00:c9:2d:5a:de vsan 2
    pwwn 21:00:00:20:37:5b:ce:af vsan 6
    pwwn 21:00:00:20:37:39:6b:dd vsan 6
    pwwn 22:00:00:20:37:39:6b:dd vsan 3
    pwwn 22:00:00:20:37:5b:ce:af vsan 3
    pwwn 50:06:04:82:bc:01:c3:84 vsan 5
```

Displays Information for a Specified IVR Zone

```
switch# show ivr zone name sample_vsan2-3
zone name sample_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

Displays the Specified Zone in the Active IVR Zone

```
switch# show ivr zone name sample_vsan2-3 active
zone name sample_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

Displays the IVR Zone Set Configuration

```
switch# show ivr zoneset
zoneset name ivr_qa_zs_all
  zone name ivr_qa_z_all
    pwwn 21:00:00:e0:8b:06:d9:1d vsan 1
    pwwn 21:01:00:e0:8b:2e:80:93 vsan 4
    pwwn 10:00:00:00:c9:2d:5a:dd vsan 1
    pwwn 10:00:00:00:c9:2d:5a:de vsan 2
    pwwn 21:00:00:20:37:5b:ce:af vsan 6
    pwwn 21:00:00:20:37:39:6b:dd vsan 6
    pwwn 22:00:00:20:37:39:6b:dd vsan 3
    pwwn 22:00:00:20:37:5b:ce:af vsan 3
    pwwn 50:06:04:82:bc:01:c3:84 vsan 5
zoneset name IVR_ZoneSet1
  zone name sample_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

Displays the Active IVR Zone Set Configuration

```
switch# show ivr zoneset active
zoneset name IVR_ZoneSet1
  zone name sample_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

Displays the Specified IVR Zone Set Configuration

```
switch# show ivr zoneset name IVR_ZoneSet1
zoneset name IVR_ZoneSet1
  zone name sample_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

Displays Brief Information for All IVR Zone Sets

```
switch# show ivr zoneset brief Active
zoneset name IVR_ZoneSet1
  zone name sample_vsan2-3
```

Displays Brief Information for the Active IVR Zone Set

```
switch# show ivr zoneset brief Active
zoneset name IVR_ZoneSet1
  zone name sample_vsan2-3
```

Displays Status Information for the IVR Zone Set

```
switch# show ivr zoneset status
Zoneset Status
_______________
    name               : IVR_ZoneSet1
    state              : activation success
    last activate time : Sat Mar 22 21:38:46 1980
    force option       : off
status per vsan:
__________________
     vsan     status
     ____     ______
       1      active
       2      active
```

Tip Repeat this configuration in all border switches participating in the IVR configuration.

Note You can use Cisco Fabric Manager to distribute IVR zone configurations to all IVR-capable switches in the interconnected VSAN network. Refer to the *Cisco Fabric Manager Inter-VSAN Routing Configuration Guide*.

Clearing the IVR Zone Database

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

To clear the IVR zone database, use the **clear ivr zone database** command.

```
switch# clear ivr zone database
```

This command clears all configured IVR zone information.

Note After issuing a **clear ivr zone database** command, you need to explicitly issue the **copy running-config startup-config** command to ensure that the running configuration is used when you next start the switch.

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 and verify the logging levels:

Configuring IVR Logging Severity Levels

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

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Configures Telnet or SSH logging for the IVR feature at level 4 (warning). As a result, logging messages with a severity level of 4 or above are displayed.

switch(config)# **logging level ivr 4**

Verifying Logging Level Configuration

Use the **show logging level** command to view the configured logging level for the IVR feature.

```
switch# show logging level
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
...
ivr                     5                       4
...
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
```

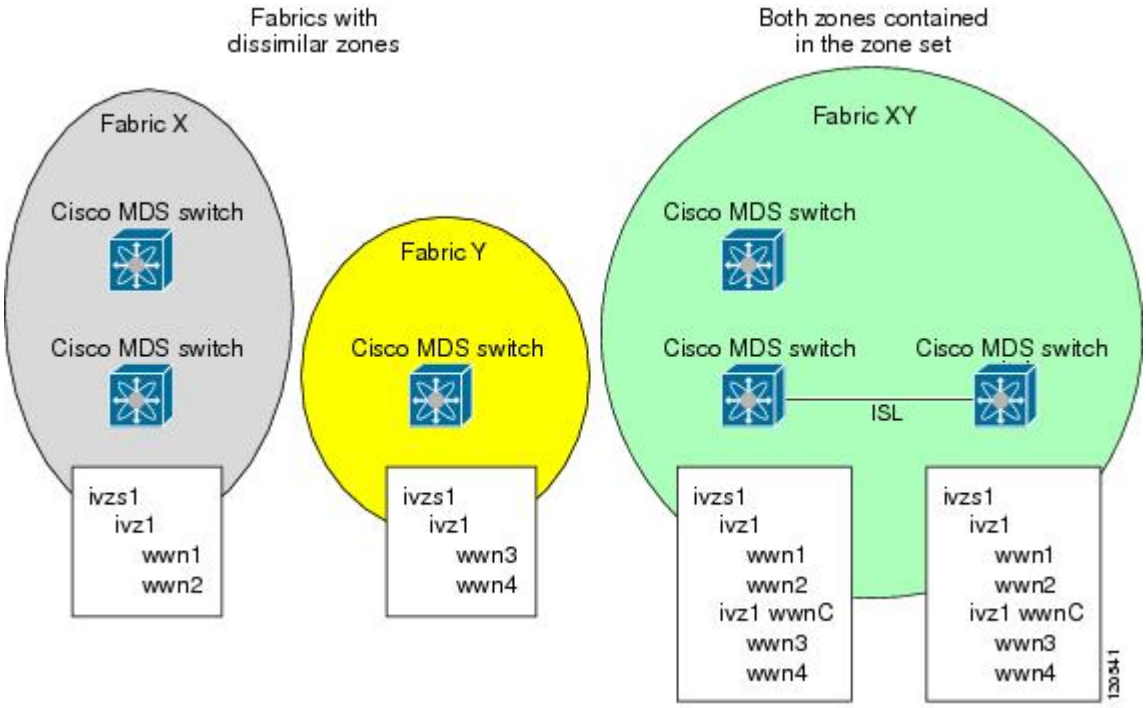
Database Merge Guidelines

A database merge refers to the combination of the configuration database and static (unlearned) entries in the active database. For information on CFS merge support, refer to the *Cisco MDS 9000 Series System Management Configuration Guide* or *Cisco Fabric Manager System Management Configuration Guide* .

Consider the following 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.

Figure 3: 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 combination 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 combination 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 combination 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.

The following table describes the results of a CFS merge of two IVR-enabled fabrics under different conditions.

Table 5: Results of Merging Two IVR-Enabled Fabrics

IVR Fabric 1	IVR Fabric 2	After Merge
NAT enabled	NAT disabled	Merge succeeds and NAT is enabled
Auto mode enabled	Auto mode disabled	Merge succeeds and IVR auto topology mode is enabled
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.

Resolving Database Merge Failures

If a merge failure occurs, you can use the following CLI commands to display the error conditions:

- **show ivr merge status**
- **show cfs merge status name ivr**

- **show logging last** *lines* (and look for MERGE failures)

To resolve merge failures, review the failure information indicated in the **show** command outputs, then find the scenario in this list that relates to the failure and follow the troubleshooting instructions:

Note After a successful CFS commit, the merge will be successful.

IVR Auto Topology Mode Configuration Example

This section provides example configuration steps for enabling IVR auto topology mode.

Step 1 Enable IVR on every border switch in the fabric.

Example:

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# feature ivr
switch(config)# exit
switch#
```

Step 2 Verify that IVR is enabled on every IVR-enabled switch.

Example:

```
switch# show ivr
Inter-VSAN Routing is enabled
Inter-VSAN enabled switches
---------------------------
No IVR-enabled VSAN is active. Check VSAN-Topology configuration.
Inter-VSAN topology status
--------------------------
Current Status: Inter-VSAN topology is INACTIVE
Inter-VSAN zoneset status
-------------------------
    name               :
    state              : idle
    last activate time :
Fabric distribution status
----------------------
fabric distribution disabled
Last Action                : None
Last Action Result         : None
Last Action Failure Reason : None
Inter-VSAN NAT mode status
--------------------------
FCID-NAT is disabled
License status
-----------------
IVR is running based on the following license(s)
ENTERPRISE_PKG
```

Step 3 Enable CFS distribution on every IVR-enabled switch in the fabric.

Example:

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

Step 4 Enable IVR auto topology mode.

Example:

```
switch(config)# ivr vsan-topology auto
fabric is locked for configuration. Please commit after configuration is done.
```

Step 5 Commit the change to the fabric.

Example:

```
switch(config)# ivr commit
switch(config)# exit
switch#
```

Step 6 Verify the status of the commit request.

Example:

```
switch# show ivr session status
Last Action                : Commit
Last Action Result         : Success
Last Action Failure Reason : None
```

Step 7 Verify the active IVR auto topology.

Example:

```
switch# show ivr vsan-topology active
AFID  SWITCH WWN                 Active   Cfg. VSANS
------------------------------------------------------------
   1  20:00:00:0d:ec:08:6e:40 *  yes      no   1,336-338
   1  20:00:00:0d:ec:0c:99:40    yes      no   336,339
```

Step 8 Configure IVR zone set and zones. Two zones are required:

- One zone has tape T (pwwn 10:02:50:45:32:20:7a:52) and server S1 (pwwn 10:02:66:45:00:20:89:04).
- Another zone has tape T and server S2 (pwwn 10:00:ad:51:78:33:f9:86).

Tip Instead of creating two IVR zones, you can also create one IVR zone with the tape and both servers.

Example:

```
mds(config)# ivr zoneset name tape_server1_server2
mds(config-ivr-zoneset)# zone name tape_server1
mds(config-ivr-zoneset-zone)# member pwwn 10:02:50:45:32:20:7a:52 vsan 1
mds(config-ivr-zoneset-zone)# member pwwn 10:02:66:45:00:20:89:04 vsan 2
mds(config-ivr-zoneset-zone)# exit
mds(config-ivr-zoneset)# zone name tape_server2
mds(config-ivr-zoneset-zone)# member pwwn 10:02:50:45:32:20:7a:52 vsan 1
mds(config-ivr-zoneset-zone)# member pwwn 10:00:ad:51:78:33:f9:86 vsan 3
mds(config-ivr-zoneset-zone)# exit
```

Step 9 View the IVR zone configuration to confirm that the IVR zone set and IVR zones are properly configured.

Example:

```
mds(config)# do show ivr zoneset
zoneset name tape_server1_server2
  zone name tape_server1
      pwwn 10:02:50:45:32:20:7a:52 vsan 1
      pwwn 10:02:66:45:00:20:89:04 vsan 2
  zone name tape_server2
      pwwn 10:02:50:45:32:20:7a:52 vsan 1
      pwwn 10:00:ad:51:78:33:f9:86 vsan 3
```

Step 10 View the zone set prior to IVR zone set activation. Prior to activating the IVR zone set, view the active zone set. Repeat this step for VSANs 2 and 3.

Example:

```
mds(config)# do show zoneset active vsan 1
zoneset name finance_dept vsan 1
  zone name accounts_database vsan 1
    pwwn 10:00:23:11:ed:f6:23:12
    pwwn 10:00:56:43:11:56:fe:ee

  zone name $default_zone$ vsan 1
```

Step 11 Activate the configured IVR zone set.

Example:

```
mds(config)# ivr zoneset activate name tape_server1_server2
zoneset activation initiated. check inter-VSAN zoneset status
mds(config)# exit
mds#
```

Step 12 Verify the IVR zone set activation.

Example:

```
mds# show ivr zoneset active
zoneset name tape_server1_server2
  zone name tape_server1
      pwwn 10:02:50:45:32:20:7a:52 vsan 1
      pwwn 10:02:66:45:00:20:89:04 vsan 2
  zone name tape_server2
      pwwn 10:02:50:45:32:20:7a:52 vsan 1
      pwwn 10:00:ad:51:78:33:f9:86 vsan 3
```

Step 13 Verify the zone set updates. Upon successful IVR zone set activation, verify that appropriate zones are added to the active zone set. Repeat this step for VSANs 2 and 3.

Example:

```
mds# show zoneset active vsan 1
zoneset name finance_dept vsan 1
  zone name accounts_database vsan 1
    pwwn 10:00:23:11:ed:f6:23:12
    pwwn 10:00:56:43:11:56:fe:ee

  zone name IVRZ_tape_server1 vsan 1
    pwwn 10:02:66:45:00:20:89:04
    pwwn 10:02:50:45:32:20:7a:52

  zone name IVRZ_tape_server2 vsan 1
    pwwn 10:02:50:45:32:20:7a:52
```

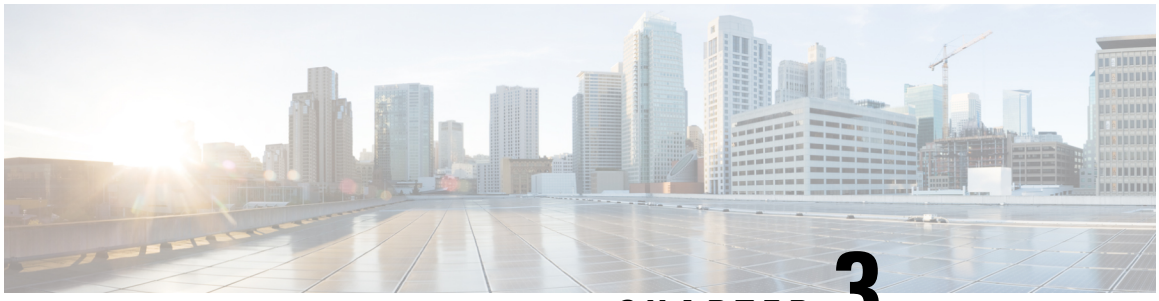
```
    pwwn 10:00:ad:51:78:33:f9:86

  zone name $default_zone$ vsan 1
mds# show ivr zoneset status
Zoneset Status
_______________
    name               : tape_server1_server2
    state              : activation success
    last activate time : Tue May 20 23:23:01 1980
    force option       : on
status per vsan:
___________________
     vsan     status
     ____     ______
     1        active
```

Default Settings

The following table lists the default settings for IVR parameters.

Table 6: 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 3

Advanced Inter-VSAN Routing Configuration

This chapter provides advanced configuration information and instructions. Before setting up advanced IVR configurations, see Basic Inter-VSAN Routing Configuration, on page 3 includes basic configuration instructions and descriptions of IVR features, limits, and terminology.

Advanced IVR Configuration Task List

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

Step 1 See IVR Network Address Translation, on page 6 and IVR NAT Requirements and Guidelines, on page 10.

Determine whether or not to use IVR Network Address Translation (NAT).

Step 2 See Domain ID Guidelines, on page 37.

If you do not plan to use IVR NAT, verify that unique domain IDs are configured in all switches and VSANs participating in IVR.

Step 3 See Enabling IVR , on page 7.

Enable IVR in the border switches.

Step 4 See IVR Service Groups, on page 32.

Configure the service group as required.

Step 5 See Distributing the IVR Configuration Using CFS, on page 8.

Configure the IVR distribution as required.

Step 6 Configure the IVR topology, either manually or automatically.

See Manually Configuring and Activating an IVR Topology, on page 38 and Advanced IVR Configuration, on page 32.

Step 7 See Advanced IVR Zones and IVR Zone Sets, on page 46.

Create and activate IVR zone sets in *all* of the IVR-enabled border switches, either manually or using fabric distribution.

Step 8 See Verifying the IVR Topology, on page 43.

Verify the IVR configuration.

Advanced IVR Configuration

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

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.

Service Group Guidelines

When configuring IVR service groups, consider these guidelines:

- If you use service groups with IVR auto topology mode, you should enable IVR and configure your service groups first, then distribute them with CFS before setting the IVR auto topology mode.
- The CFS distribution is restricted within the service group only when the IVR VSAN topology is in IVR auto topology mode. See IVR VSAN Topology, on page 6 .
- 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 Configuring IVR Service Groups, on page 33. 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, follow these steps:

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Configures the IVR service group called IVR-SG1 and enters IVR server group configuration mode.

switch(config)# **ivr service-group name IVR-SG1**

Step 3 Deletes the IVR service group.

switch(config)# **no ivr service-group name IVR-SG1**

Step 4 Configures AFID 10 for VSANs 1, 2, and 6 through 10.

switch(config-ivr-sg)# **autonomous-fabric-id 10 vsan-ranges 1,2,6-10**

Step 5 Configures AFID 11 for VSAN 1.

switch(config-ivr-sg)# **autonomous-fabric-id 11 vsan-ranges 1**

Step 6 Configures AFID 12 for VSANs 3 through 5.

switch(config-ivr-sg)# **autonomous-fabric-id 12 vsan-ranges 3-5**

Step 7 Removes the association between AFID 12 and VSANs 3 through 5.

switch(config-ivr-sg)# **no autonomous-fabric-id 12 vsan-ranges 3-5**

Step 8 Returns to configuration mode.

switch(config-ivr-sg)# **exit**

Step 9 Configures the IVR service group called IVR-SG2 and enters IVR server group configuration mode.

switch(config)# **ivr service-group name IVR-SG2**

Step 10 Configures AFID 20 for VSANs 3 through 5.

switch(config-ivr-sg)# **autonomous-fabric-id 20 vsan-ranges 3-5**

Step 11 Returns to configuration mode.

switch(config-ivr-sg)# **exit**

Step 12 Activates the service group configuration and sets the communication policy between switches in the default service group as allow (default).

switch(config)# **ivr service-group activate**

Step 13 Activates the service group configuration and sets the communication policy between switches in the default service group to deny.

switch(config)# **ivr service-group activate default-sg-deny**

Note To change the communication policy back to allow, you must issue the **ivr service-group activate** command again.

Step 14 Deactivates (default) the service group configuration.

switch(config)# **no ivr service-group activate**

Step 15 Activates the VSAN topology.

switch(config)# **ivr vsan-topology activate**

Step 16 Enables CFS distribution for the IVR configuration.

switch(config)# **ivr distribute**

Step 17 Commits the IVR configuration to the fabric.

switch(config)# **ivr commit**

Copying the Active IVR Service Group Database

You can modify the configured IVR service group database; however, you cannot modify the active IVR service group database. To copy the active IVR service group database to the manually configured service group database, use the following command in EXEC mode:

```
switch# ivr copy active-service-group user-configured-service-group
```

Clearing IVR Service Group Database

You can clear all entries in the IVR service group database by using the **clear ivr service-group databas**e command in EXEC mode. This command only clears the configured database, not the active database.

```
switch# clear ivr service-group database
```

Verifying IVR Service Group Configuration

Use the **show ivr service-group active** command to view the active IVR service group database.

```
switch# show ivr service-group active
IVR ACTIVE Service Group
====================================
SG-ID  SG-NAME    AFID  VSANS
--------------------------------------------------------------------------------
 1     IVR-SG1      10  1-2,6-10
 1     IVR-SG1      11  1
 2     IVR-SG2      20  3-5
Total:   3 entries in active service group table
```

Use the **show ivr service-group configured** command to view the configured IVR service group database.

```
switch# show ivr service-group configured
IVR CONFIGURED Service Group
====================================
SG-ID  SG-NAME    AFID  VSANS
--------------------------------------------------------------------------------
 1     IVR-SG1      10  1-2,6-10
 1     IVR-SG1      11  1
 2     IVR-SG2      20  3-5
Total:   3 entries in configured service group table
```

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 MDS NX-OS Release 4.2(1) supports AFIDs 1 through 64. AFIDs are used in conjunction with IVR auto topology mode to allow segmented VSANs in the IVR VSAN topology database.

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 IVR auto topology mode. In IVR manual 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 cannot 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 the following example, IVR will set up the connection between the devices across the switches even though they have the same VSAN.

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 the default AFID, follow these steps:

Step 1 Enters configuration mode.

switch# **config terminal**

Step 2 Enters AFID database configuration submode.

switch(config)# **autonomous-fabric-id** database

Step 3 Configures the default AFID for all VSANs not explicitly associated with an AFID. The valid range for the default AFID is 1 to 64.

switch(config-afid-db)# **switch-wwn 20:00:00:0c:91:90:3e:80 default-autonomous-fabric-id 5**

Step 4 Reverts to the default value (1) for the default AFID.

switch(config-afid-db)# **no switch-wwn 20:00:00:0c:91:90:3e:80 default-autonomous-fabric-id 5**

Configuring Individual AFIDs

To configure individual AFIDs, follow these steps:

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Enters AFID database configuration submode.

switch(config)# **autonomous-fabric-id** database

Step 3 Configures an AFID and VSAN range for a switch. The valid range for AFIDs is 1 to 64.

switch(config-afid-db)# **switch-wwn 20:00:00:0c:91:90:3e:80 autonomous-fabric-id 10 vsan-ranges 1,2,5-8**

Step 4 Deletes VSAN 2 from AFID 10.

switch(config-afid-db)# **no switch-wwn 20:00:00:0c:91:90:3e:80 autonomous-fabric-id 10 vsan-ranges 2**

Verifying the AFID Database Configuration

To view the contents of the AFID database, use the **show autonomous-fabric-id database** command.

```
switch# show autonomous-fabric-id database
SWITCH WWN                   Default-AFID
------------------------------------------------------------
20:00:00:0c:91:90:3e:80          5
Total:   1 entry in default AFID table
SWITCH WWN                   AFID      VSANS
------------------------------------------------------------
20:00:00:0c:91:90:3e:80          10    1,2,5-8
Total:   1 entry in AFID table
```

IVR Auto Topology Guidelines

Before configuring an IVR SAN fabric without IVR in NAT mode or IVR auto topology 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.

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.

Manually Configuring and Activating an IVR Topology

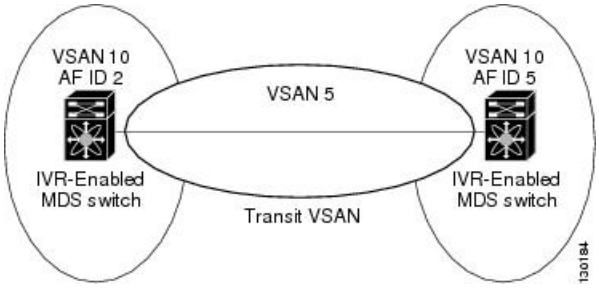
You must create the IVR topology on every IVR-enabled switch in the fabric if you have not enabled IVR auto topology mode. To use IVR manual topology mode, follow the instructions in this section.

Manual Configuration Guidelines

Consider the following guidelines when using IVR manual topology mode:

- You can configure a maximum of 128 IVR-enabled switches and 128 distinct VSANs in an IVR topology (see Figure 4: Example: IVR Topology with Non-Unique VSAN IDs Using AFIDs, on page 39).
- 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.

Figure 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 Use the sh**ow wwn switch** command to obtain the switch WWNs of the IVR-enabled switches.

To manually configure an IVR topology using Cisco NX-OS, follow these steps:

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Enters the VSAN topology database configuration mode for the IVR feature.

switch(config)# **ivr vsan-topology database**.

Step 3 Configures VSANs 1, 2, and 6 to participate in IVR for this switch.

switch(config-ivr-topology-db)# **autonomous-fabric-id 1 switch 20:00:00:05:30:01:1b:b8 vsan-ranges 1-2,6**.

Step 4 Configures VSANs 1, 2 and 3 to participate in IVR for this switch.

switch(config-ivr-topology-db)# **autonomous-fabric-id 1 switch 20:00:00:05:30:01:1b:c2 vsan-ranges 1-3**.

Step 5 Removes VSANs 1 and 2 from IVR for this switch.

switch(config-ivr-topology-db)# **no autonomous-fabric-id 1 switch 20:00:00:05:30:01:1b:c2 vsan-ranges 1-2**.

Step 6 Returns to EXEC mode.

switch(config-ivr-topology-db)# **end**

What to do next

View the IVR topology using the **show ivr vsan-topology** command. In the following example output, VSAN 2 is the transit VSAN between VSANs 1, 5, and 6.

```
switch# show ivr vsan-topology
AFID  SWITCH WWN                 Active   Cfg. VSANS
--------------------------------------------------------------
   1  20:00:00:05:30:01:1b:c2 *   no      yes  1-2
   1  20:02:00:44:22:00:4a:05     no      yes  1-2,6
   1  20:02:00:44:22:00:4a:07     no      yes  2-5
Total:   3 entries in active and configured IVR VSAN-Topology

Current Status: Inter-VSAN topology is INACTIVE
```

Repeat this configuration on all IVR-enabled switches or distribute the IVR configuration using CFS. See Distributing the IVR Configuration Using CFS, on page 8.

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 auto topology mode.

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

Step 1 Enters configuration mode.

switch# **config terminal**

Step 2 Activates the manually configured IVR topology.

switch(config)# **ivr vsan-topology activate**

Viewing an Active IVR Topology

View the active IVR topology using the **show ivr vsan-topology** command.

```
switch# show ivr vsan-topology
AFID  SWITCH WWN                 Active   Cfg. VSANS
--------------------------------------------------------------
   1  20:00:00:05:30:01:1b:c2 *   yes     yes  1-2
   1  20:02:00:44:22:00:4a:05     yes     yes  1-2,6
   1  20:02:00:44:22:00:4a:07     yes     yes  2-5
Total:   3 entries in active and configured IVR VSAN-Topology
Current Status: Inter-VSAN topology is ACTIVE
Last activation time: Mon Mar 24 07:19:53 2009
```

Note The asterisk (*) indicates the local switch.

Working with Existing IVR Topologies

This section includes advanced IVR configurations for existing IVR topologies:

Adding an IVR-Enabled Switch to an Existing IVR Topology

Before adding an IVR-enabled switch to an existing fabric, you must add an entry to the IVR topology for the new switch and activate the new IVR topology.

To add the IVR-enabled switch to an existing IVR topology, follow these steps:

Step 1 Enters configuration mode.

switch# **config terminal**

Step 2 Enters IVR VSAN topology database configuration submode.

mds(config)# ivr vsan-topology database

Step 3 Adds the new IVR-enabled switch to the topology.

mds(config-ivr-topology-db)# **autonomous-fabric-id 1 switch-wwn 20:00:00:05:40:01:1b:c2 vsan-ranges 1,4**

Step 4 Returns to configuration mode.

switch(config-ivr-topology-db)# **exit**

Step 5 Activates the IVR VSAN topology.

switch(config)# ivr vsan-topology activate

Step 6 Commits the IVR configuration change to the fabric.

switch(config)# **ivr commit**

Step 7 Returns to EXEC mode.

switch(config)# **exit**

Step 8 Saves the running configuration.

switch# **copy running-config startup-config**

What to do next

After adding the switch to the IVR topology, enable IVR and CFS on the new switch (see Enabling IVR , on page 7 and Distributing the IVR Configuration Using CFS, on page 8).

Adding VSANs to an Existing IVR Topology

To add VSANs to an existing IVR topology you need to specify all VSANs in the command syntax. First IVR Configuration with VSANs 1101-1102 and 2101-2102, on page 42 shows an IVR configuration with VSANs 1101-1102 and VSANs 2101-2102. Adding VSANs 1103 and 2103 to the IVR Configuration, on page 42 shows the addition of VSANs 1103 and 2103 to the IVR topology.

First IVR Configuration with VSANs 1101-1102 and 2101-2102

```
switch(config)# ivr enable
switch(config)# ivr distribute
switch(config)# ivr vsan-topology database
switch(config-ivr-topology-db)# autonomous-fabric-id    1 switch-wwn 20:00:00:0d:ec:4a:5e:00
 vsan-ranges 1101-1102,1199,3100,3150
switch(config-ivr-topology-db)# autonomous-fabric-id    1 switch-wwn 20:00:00:0d:ec:4a:5f:00
 vsan-ranges 2101-2102,2199,3100,3150
switch(config)# ivr vsan-topology activate
```

Adding VSANs 1103 and 2103 to the IVR Configuration

```
switch(config)# ivr enable
switch(config)# ivr distribute
switch(config)# ivr vsan-topology database
switch(config-ivr-topology-db)# autonomous-fabric-id    1 switch-wwn 20:00:00:0d:ec:4a:5e:00
 vsan-ranges 1101-1103,1199,3100,3150
switch(config-ivr-topology-db)# autonomous-fabric-id    1 switch-wwn 20:00:00:0d:ec:4a:5f:00
 vsan-ranges 2101-2103,2199,3100,3150
switch(config)# ivr vsan-topology activate
```

Copying the Active IVR Topology

You can edit a manually configured IVR topology; however, you cannot edit an active IVR topology. To copy the active IVR topology database to the manually configure topology, issue the **ivr copy active-topology user-configured-topology** command in EXEC mode:

```
switch# ivr copy active-topology user-configured-topology
```

Clearing a Manually Configured IVR Topology Database

To clear a manually configured IVR topology database, follow these steps:

Step 1 Enters configuration mode.

switch# **config terminal**

Step 2 Clears the previously created IVR topology.

switch(config)# no **ivr vsan-topology database**

Verifying the IVR Topology

To verify the IVR topology, issue the **show ivr vsan-topology** command.

Displays the Configured IVR VSAN Topology

```
switch# show ivr vsan-topology
AFID    SWITCH WWN                 Active   Cfg. VSANS
------------------------------------------------------------
   1    20:00:00:05:30:01:1b:c2 *   yes     yes  1-2
   1    20:02:00:44:22:00:4a:05     yes     yes  1-2,6
   1    20:02:00:44:22:00:4a:07     yes     yes  2-5
Total:   5 entries in active and configured IVR VSAN-Topology
Current Status: Inter-VSAN topology is ACTIVE
Last activation time: Sat Mar 22 21:46:15 1980
```

Note The asterisk (*) indicates the local switch.

Displays the Active IVR VSAN Topology

```
switch# show ivr vsan-topology active
AFID   SWITCH WWN                 Active   Cfg. VSANS
------------------------------------------------------------
    1  20:00:00:05:30:01:1b:c2 *   yes     yes  1-2
    1  20:02:00:44:22:00:4a:05     yes     yes  1-2,6
    1  20:02:00:44:22:00:4a:07     yes     yes  2-5
Total:   5 entries in active IVR VSAN-Topology
Current Status: Inter-VSAN topology is ACTIVE
Last activation time: Sat Mar 22 21:46:15
```

Displays the Configured IVR VSAN Topology

```
switch# show ivr vsan-topology configured
AFID  SWITCH WWN                 Active   Cfg. VSANS
------------------------------------------------------------
    1  20:00:00:05:30:01:1b:c2 *   yes     yes  1-2
    1  20:02:00:44:22:00:4a:05     yes     yes  1-2,6
    1  20:02:00:44:22:00:4a:07     yes     yes  2-5
Total:   5 entries in configured IVR VSAN-Topology
```

Migrating from IVR Auto Topology Mode to IVR Manual Topology Mode

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

To migrate from IVR auto topology mode to IVR manual topology mode, follow these steps:

Step 1 Copies the automatic IVR topology database to the user-configured IVR topology.

switch# **ivr copy auto-topology user-configured-topology**

Step 2 Enters configuration mode.

switch# **config t**

Step 3 Disables IVR auto topology mode for the IVR topology database and enables IVR manual topology mode.

switch(config)# **ivr vsan-topology activate**

Persistent FC IDs for IVR

This section includes the following information:

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, follow these steps:

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Enters IVR fcdomain database configuration submode for current AFID 21 and VSAN 22

switch(config)# **ivr fcdomain database autonomous-fabric-num 21 vsan 22**.

Step 3 Deletes all the database entries, including all the corresponding persistent FC ID entries, for current AFID 21 and VSAN 22

switch(config)# **no ivr fcdomain database autonomous-fabric-num 21 vsan 22**.

Step 4 Adds or replaces a database entry for native AFID 20, native VSAN 11, and domain 12, and enters IVR fcdomain FC ID configuration submode. Domains of all the corresponding persistent FC ID entries, if any, are also changed to 12.

switch(config-fcdomain)# **native-autonomous-fabric-num 20 native-vsan 11 domain 12**

Step 5 Deletes the virtual domain entry native AFID 20 and native VSAN 11, and all corresponding FC ID entries

switch(config-fcdomain)# **no native-autonomous-fabric-num 20 native-vsan 11**.

Step 6 Adds or replaces a database entry for mapping the pWWN to the FC ID.

switch(config-fcdomain-fcid)# **pwwn 11:22:33:44:55:66:77:88 fcid 0x114466**

Step 7 Deletes the database entries for the pWWN

switch(config-fcdomain-fcid)# **no pwwn 11:22:33:44:55:66:77:88**.

Step 8 Adds a database entry for mapping the device alias to the FC ID.

switch(config-fcdomain-fcid)# **device-alias SampleName fcid 0x123456**

Step 9 Deletes the database entries for the device alias.

switch(config-fcdomain-fcid)# **no device-alias SampleName**

Verifying the Persistent FC ID Configuration

Verify the persistent FC ID configuration using the **show ivr fcdomain database** command.

Displays All IVR fcdomain Database Entries

```
switch# show ivr fcdomain database
-------------------------------------------------
  AFID  Vsan  Native-AFID  Native-Vsan  Virtual-domain
-------------------------------------------------
    1     2        10          11         0xc(12)
   21    22        20          11         0xc(12)
Number of Virtual-domain entries: 2
-------------------------------------------------
  AFID  Vsan          Pwwn           Virtual-fcid
-------------------------------------------------
   21    22  11:22:33:44:55:66:77:88  0x114466
   21    22  21:22:33:44:55:66:77:88  0x0c4466
   21    22  21:22:33:44:55:66:78:88  0x0c4466
Number of Virtual-fcid entries: 3
```

Displays the IVR fcdomain Database Entries for a Specific AFID and VSAN

```
switch# show ivr fcdomain database autonomous-fabric-num 21 vsan 22
-------------------------------------------------
  AFID  Vsan  Native-AFID  Native-Vsan  Virtual-domain
-------------------------------------------------
   21    22        20          11         0xc(12)
Number of Virtual-domain entries: 1
-------------------------------------------------
  AFID  Vsan          Pwwn           Virtual-fcid
-------------------------------------------------
   21    22  11:22:33:44:55:66:77:88  0x114466
   21    22  21:22:33:44:55:66:77:88  0x0c4466
   21    22  21:22:33:44:55:66:78:88  0x0c4466
Number of Virtual-fcid entries: 3
```

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 IVR Zones and IVR Zone Sets, on page 15.

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 Database Merge Guidelines, on page 23 .

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.

The following example shows samples of the warning messages that are displayed when configuration changes are made that affect ReadOnly, the QoS attribute, and LUN zoning.

IVR Zone Configuration Warning Messages

```
switch(config)# vsan database
switch(config-vsan-db)# vsan 2
switch(config-vsan-db)# vsan 2 interop 2
switch(config-vsan-db)# exit
switch(config)# ivr zoneset name ivr_zs1 switch(config-ivr-zoneset)# zone name ivr_z1
 switch(config-ivr-zoneset-zone)# member pwwn 21:00:00:14:c3:3d:45:22 lun 0x32 vsan 2 VSAN
 is in interop mode, and LUN zoning cannot be set.
switch(config)# ivr zoneset name ivr_zs1 switch(config-ivr-zoneset)# zone name ivr_z1
 switch(config-ivr-zoneset-zone)# member pwwn 21:00:00:14:c3:3d:45:22 vsan 2
 switch(config-ivr-zoneset-zone)# attribute read-only VSAN is in interop mode and zone
member has been configured, zone cannot be set to READ-ONLY.
switch(config-ivr-zoneset-zone)# attribute qos priority medium VSAN is in interop mode and
 zone member has been configured, QoS cannot be assigned to zone.
```

Configuring LUNs in IVR Zoning

LUN zoning can be used between members of active IVR zones.You can configure the service by creating and activating LUN zones between the desired IVR zone members in all relevant edge VSANs using the zoning interface or you can use LUN zoning directly supported by IVR. For more details on the advantages of LUN zoning, refer to the Cisco MDS 9000 Series *NX-OS Fabric Configuration Guide* or the *Cisco Fabric Manager Fabric Configuration Guide* .

To configure LUNs in IVR zoning, follow these steps:

Step 1 Enters configuration mode

switch# **config t**.

Step 2 Configures an IVR zone called IvrLunZone

switch(config)# **ivr zone name IvrLunZone**

Step 3 Configures an IVR zone member based on the specified pWWN and LUN value

switch(config-ivr-zone)# **member pwwn 10:00:00:23:45:67:89:ab lun 0x64 vsan 10**

Note The CLI interprets the LUN identifier value as a hexadecimal value whether or not the **0x** prefix is included.

Step 4 Configures an IVR zone member based on the specified pWWN, LUN value, and AFID.

switch(config-ivr-zone)# **member pwwn 10:00:00:23:45:67:89:ab lun 0x64 vsan 10 autonomous-fabric-id 20**

Step 5 Removes an IVR zone member.

switch(config-ivr-zone)# **no member pwwn 20:81:00:0c:85:90:3e:80 lun 0x32 vsan 13 autonomous-fabric-id 10**

What to do next

Note You can configure LUN zoning in an IVR zone set setup.

Configuring the QoS Attribute

To configure the QoS attribute for an IVR zone, follow these steps:

SUMMARY STEPS

1. Enters configuration mode.
2. Configures an IVR zone called IvrZone.
3. Configures the QoS for IVR zone traffic to medium
4. Reverts to the default QoS setting. The default is low.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Enters configuration mode.	switch# **config t**
Step 2	Configures an IVR zone called IvrZone.	switch(config)# **ivr zone name IvrZone**
Step 3	Configures the QoS for IVR zone traffic to medium	switch(config-ivr-zone)# **attribute qos priority medium**.
Step 4	Reverts to the default QoS setting. The default is low.	switch(config-ivr-zone)# **no attribute qos priority medium**

What to do next

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

Verifying the QoS Attribute For an IVR Zone

Use the **show ivr zone** command to verify the QoS attribute for an IVR zone.

```
switch(config)# show ivr zone
zone name IvrZone
    attribute qos priority medium
```

Renaming IVR Zones and IVR Zone Sets

To rename an IVR zone, use the **ivr zone rename** command in EXEC mode.

```
switch# ivr zone rename ivrzone1 ivrzone2
```

To rename an IVR zone set, use the **ivr zoneset rename** command in EXEC mode.

```
switch# ivr zoneset rename ivrzone1 ivrzone2
```

Clearing the Configured IVR Zone Database

Clearing a zone set erases the configured zone database, not the active zone database.

To clear the configured IVR zone database, use the **clear ivr zone database** command.

Step 1 Clears all configured IVR zone information.

switch# **clear ivr zone database**

Step 2 Ensures that the running configuration is used when you restart the switch.

switch# **copy running-config startup-config**

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.

Enabling Advanced Fabric Services on IVR Flows

Advanced fabric services (such as SME and IOA) use fabric-wide FC-Redirect infrastructure to redirect the traffic flows. These services can now be enabled on IVR flows using an internal feature, Abstract ACL Manager (AAM).

Configuration Guidelines and Restrictions

The following prerequisites must be considered before enabling AAM for IVR:

- CFS distribution must be enabled for IVR.
- AAM is supported only in IVR-NAT mode.
- The switches where the fabric services (such as SME and IOA) are enabled must be running the AAM supported NX-OS release 5.0(1) or later.
- FC-Redirect can be running in version 1 or version 2 mode.
- AAM support for IVR must be enabled before enabling IVR support for FCR.
- LUN zoning is not supported when AAM is enabled for IVR.
- IVR merge is supported only when both the fabrics have AAM enabled or both the fabrics have AAM disabled. The IVR merge will fail if one of the fabric has AAM enabled and the other fabric has AAM disabled.
- You must delete all the advanced fabric service (SME and IOA) configurations for IVR devices and then disable IVR support for FCR before disabling AAM support for IVR.
- Before downgrading to an earlier release to MDS NX-OS Release 5.0(1), you must delete all the advanced fabric service (SME and IOA) configurations for IVR devices, disable IVR support for FCR, and then disable AAM support for IVR.

Enabling AAM Support for IVR

To enable AAM for IVR, follow these steps:

Step 1 Enters the configuration mode.

switch# **config t**

Step 2 Enables IVR.

switch(config)# **feature ivr**

Step 3 Enables CFS distribution for IVR.

switch(config)# **ivr distribute**

Step 4 Enables NAT mode for IVR.

switch(config)# **ivr nat**

Step 5 Commits IVR configuration changes.

switch(config)# **ivr commit**

Step 6 Enables AAM for IVR.

switch(config)# **ivr aam register**

Step 7 Commits IVR configuration changes.

switch(config)# **ivr commit**

What to do next

You can use the **show ivr aam** command to verify if AAM support is enabled for IVR.

```
switch(config)# show ivr aam
AAM mode status
--------------------------
AAM is enabled
```

Enabling IVR Support for FCR

To enable IVR support for FCR, follow these steps:

Step 1 Enters the configuration mode.

switch# **config t**

Step 2 Enables IVR support for FCR.

switch(config)# **fc-redirect ivr-support enable**

What to do next

You can use the **show fc-redirect config** command to verify if AAM support is enabled for FCR.

```
switch(config)# show fc-redirect config
switch(config)#
switch(config)#
switch(config)#
```

Disabling AAM Support for IVR

To disable AAM support for IVR, follow these steps:

Step 1 Enters the configuration mode.

switch# **config t**

Step 2 Checks for the existence of advanced fabric service configurations for IVR devices

switch(config)# **ivr aam pre-deregister-check**.

Step 3 Displays the status of the advanced fabric service configurations for IVR devices

switch(config)# **show ivr aam pre-deregister-check**.

Step 4 Delete all the advanced fabric service (SME and IOA) configurations for IVR devices

Refer to the Cisco MDS 9000 Series SME and IOA Configuration Guides..

Step 5 Disables IVR support for FCR.

switch(config)# **no fc-redirect ivr-support enable**

Step 6 Disables AAM support for IVR.

switch(config)# **no ivr aam register**.

Step 7 Commits IVR configuration changes.

switch(config)# **ivr commit**

What to do next

You must use the **ivr aam pre-deregister-check** command to see if there is any SME or IOA configuration for IVR devices, before disabling AAM support for IVR.

```
switch(config)# show ivr aam pre-deregister-check
AAM pre-deregister check status
--------------------------
Run the "ivr aam pre-deregister-check" command first to check whether an ivr aam deregister
 can be done.
switch(config)# ivr aam pre-deregister-check
switch(config)# show ivr aam pre-deregister-check
AAM pre-deregister check status
-------------------------
FAILURE
There are merged entries or AAM has not been enabled with the following switches:
  switch swwn 20:00:00:05:30:00:15:de
User has two options:
 1. User can go ahead to issue ivr commit, but the above switches in the fabric may fail
to deregister.
 2. User may also run "ivr abort", then resolve above switches and re-issue the ivr aam
deregister.
Warning: IVR AAM pre-deregister-check status may not be up-to-date. Please issue the command
 "ivr aam pre-deregister-check" to get updated status.
switch(config)# ivr aam pre-deregister-check
switch(config)# show ivr aam pre-deregister-check
AAM pre-deregister check status
--------------------------
SUCCESS
Warning: IVR AAM pre-deregister-check status may not be up-to-date. Please issue the command
 "ivr aam pre-deregister-check" to get updated status.
```