CHAPTER 23

Configuring Inter-VSAN Routing

This chapter explains the Inter-VSAN routing (IVR) feature and provides details on sharing resources across VSANs using IVR management interfaces provided in the switch.

This chapter includes the following sections:

- Inter-VSAN Routing, page 23-1
- IVR Configuration Task List, page 23-8
- Configuring IVR, page 23-8
- IVR Zones and IVR Zone Sets, page 23-28
- Database Merge Guidelines, page 23-36
- Example Configurations, page 23-39
- Default Settings, page 23-44

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 isolation of traffic between VSANs. Data traffic isolation between the VSANs also inherently prevents sharing of resources attached to a VSAN, such as robotic tape libraries. Using IVR, you can access resources across VSANs without compromising other VSAN benefits.

This section includes the following topics:

- About IVR, page 23-2
- IVR Features, page 23-3
- IVR Limits Summary, page 23-4
- IVR Terminology, page 23-3
- Fibre Channel Header Modifications, page 23-4
- IVR NAT, page 23-5
- IVR VSAN Topology, page 23-6
- IVR Service Groups, page 23-7
- IVR Interoperability, page 23-8

About IVR

Note IVR is not supported on the Cisco MDS 9124 Fabric Switch, the Cisco MDS 9134 Fabric Switch, the Cisco Fabric Switch for HP c-Class BladeSystem, and the Cisco Fabric Switch for IBM BladeCenter.

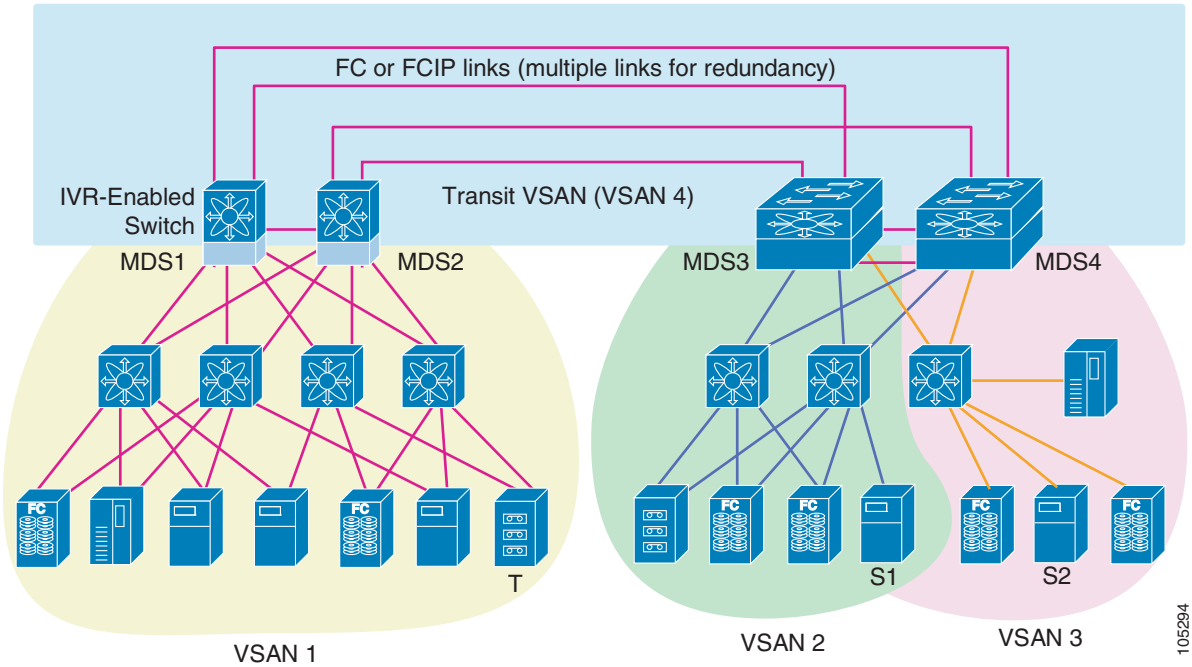
Data traffic is transported between specific initiators and targets on different VSANs without merging VSANs into a single logical fabric. Fibre Channel control traffic does not flow between VSANs, nor can initiators access any resource across VSANs other than the designated ones. Valuable resources such as tape libraries are easily shared across VSANs without compromise.

IVR is in compliance with Fibre Channel standards and incorporates third-party switches, however, IVR-enabled VSANs may have to be configured in one of the interop modes.

IVR is not limited to VSANs present on a common switch. Routes that traverse one or more VSANs across multiple switches can be established, if necessary, to establish proper interconnections. IVR used in conjunction with FCIP provides more efficient business continuity or disaster recovery solutions (see Figure 23-1).

Note See the "Example Configurations" section on page 23-39 for procedures to configure the sample scenario shown in Figure 23-1.

Figure 23-1 Traffic Continuity Using IVR and FCIP



Note OX ID based load balancing of IVR traffic from IVR- enabled switches is not supported on Generation 1 switching modules. OX ID based load balancing of IVR traffic from a non-IVR MDS switch should work. Generation 2 switching modules support OX ID based load balancing of IVR traffic from IVR-enabled switches.

IVR Features

IVR supports the following features:

- Accesses resources across VSANs without compromising other VSAN benefits.
- Transports data traffic between specific initiators and targets on different VSANs without merging VSANs into a single logical fabric.
- Shares valuable resources (like tape libraries) across VSANs without compromise.
- Provides efficient business continuity or disaster recovery solutions when used in conjunction with FCIP.
- Is in compliance with Fibre Channel standards.
- Incorporates third-party switches, however, IVR-enabled VSANs may have to be configured in one of the interop modes.

IVR Terminology

The following IVR-related terms are used in this chapter:

- Native VSAN—The VSAN to which an end device logs on is the native VSAN for that end device.
- Current VSAN—The VSAN currently being configured for IVR.
- Inter-VSAN routing zone (IVR zone)—A set of end devices that are allowed to communicate across VSANs within their interconnected SAN fabric. This definition is based on their port world wide names (pWWNs) and their native VSAN associations. Prior to Cisco SAN-OS Release 3.0(3), you can configure up to 2000 IVR zones and 10,000 IVR zone members on the switches in the network. As of Cisco SAN-OS Release 3.0(3), you can configure up to 8000 IVR zones and 20,000 IVR zone members on the switches in the network.
- Inter-VSAN routing zone sets (IVR zone sets)—One or more IVR zones make up an IVR zone set. You can configure up to 32 IVR zone sets on any switch in the Cisco MDS 9000 Family. Only one IVR zone set can be active at any time.
- IVR path—An IVR path is a set of switches and Inter-Switch Links (ISLs) through which a frame from an end device in one VSAN can reach another end device in some other VSAN. Multiple paths can exist between two such end devices.
- IVR-enabled switch—A switch on which the IVR feature is enabled.
- Edge VSAN—A VSAN that initiates (source edge-VSAN) or terminates (destination edge-VSAN) an IVR path. Edge VSANs may be adjacent to each other or they may be connected by one or more transit VSANs. In Figure 23-1, VSANs 1, 2, and 3 are edge VSANs.

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

- Transit VSAN—A VSAN that exists along an IVR path from the source edge VSAN of that path to the destination edge VSAN of that path. In Figure 23-1, VSAN 4 is a transit VSAN.

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

- Border switch—An IVR-enabled switch that is a member of two or more VSANs. Border switches, such as the IVR-enabled switch between VSAN 1 and VSAN 4 in Figure 23-1, span two or more different color-coded VSANs.
- Edge switch—A switch to which a member of an IVR zone has logged in. Edge switches are unaware of the IVR configurations in the border switches. Edge switches need not 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 enabling 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 Limits Summary

Table 23-1 summarizes the configuration limits for IVR. See Appendix E, "Configuration Limits for Cisco MDS SAN-OS Release 3.1(x) and 3.2(x)," for a complete list of Cisco MDS NX-OS feature configuration limits.

Table 23-1 IVR Configuration Limits

IVR Feature	Maximum Limit
IVR zone members	20,000 IVR zone members per physical fabric as of Cisco SAN-OS Release 3.0(3). 10,000 IVR zone members per physical fabric prior to Cisco SAN-OS Release 3.0(3).
IVR zones	8000 IVR zones per physical fabric as of Cisco SAN-OS Release 3.0(3). 2000 IVR zones per physical fabric prior to Cisco SAN-OS Release 3.0(3).
IVR zone sets	32 IVR zone sets per physical fabric.
IVR service groups	16 service groups per physical fabric.

Fibre Channel Header Modifications

IVR works by virtualizing 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 goes 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 NAT

Without Network Address Translation (NAT), IVR requires unique domain IDs for all switches in the fabric. You can enable IVR NAT to allow non-unique domain IDs. This feature simplifies the deployment of IVR in an existing fabric where non-unique domain IDs might be present.

To use IVR NAT, it must be enabled in all IVR-enabled switches in the fabric IVR configuration distribution (see the "Distributing the IVR Configuration using CFS" section on page 23-10). By default, IVR NAT and IVR configuration distribution are disabled in all switches in the Cisco MDS 9000 Family.

IVR NAT Requirements and Guidelines

Following are requirements and guidelines for using IVR NAT:

- For IVR NAT to function correctly in the network, all IVR-enabled switches must run Cisco MDS SAN-OS Release 2.1(1a) or later.
- IVR NAT port login (PLOGI) requests received from hosts are delayed a few seconds to perform the rewrite on the FC ID address. If the host's PLOGI timeout value is set to a value less than five seconds, it may result in the PLOGI being unnecessarily aborted and the host being unable to access the target. We recommend that you configure the host bus adapter for a timeout of at least ten seconds (most HBAs default to a value of 10 or 20 seconds).
- Load balancing of IVR NAT traffic across equal cost paths from an IVR-enabled switch is not supported. However, load balancing of IVR NAT traffic over PortChannel links is supported. The load balancing algorithm for IVR NAT traffic over port-channel with Generation 1 linecards is SRC/DST only. Generation 2 linecards support SRC/DST/OXID based load balancing of IVR NAT traffic across a port-channel.
- You cannot configure IVR NAT and preferred Fibre Channel routes on Generation 1 module interfaces.

IVR NAT allows you to set up IVR in a fabric without needing unique domain IDs on every switch in the IVR path. IVR NAT virtualizes the switches in other VSANs by using local VSAN for the destination IDs in the Fibre Channel headers. In some Extended Link Service message types, the destinations IDs are part of the payload. In these cases, IVR NAT replaces the actual destination ID with the virtualized destination ID. IVR NAT supports destination ID replacement in the Extended Link Service messages described in Table 23-2.

Table 23-2 Extended Link Service Messages Supported by IVR NAT

Extended Link Service Messages	Link Service Command (LS_COMMAND)	Mnemonic
Abort Exchange	0x06 00 00 00	ABTX
Discover Address	0x52 00 00 00	ADISC
Discover Address Accept	0x02 00 00 00	ADISC ACC
Fibre Channel Address Resolution Protocol Reply	0x55 00 00 00	FARP-REPLY
Fibre Channel Address Resolution Protocol Request	0x54 00 00 00	FARP-REQ
Logout	0x05 00 00 00	LOGO
Port Login	0x30 00 00 00	PLOGI

Table 23-2 Extended Link Service Messages Supported by IVR NAT (continued)

Extended Link Service Messages	Link Service Command (LS_COMMAND)	Mnemonic
Read Exchange Concise	0x13 00 00 00	REC
Read Exchange Concise Accept	0x02 00 00 00	REC ACC
Read Exchange Status Block	0x08 00 00 00	RES
Read Exchange Status Block Accept	0x02 00 00 00	RES ACC
Read Link Error Status Block	0x0F 00 00 00	RLS
Read Sequence Status Block	0x09 00 00 00	RSS
Reinstate Recovery Qualifier	0x12 00 00 00	RRQ
Request Sequence Initiative	0x0A 00 00 00	RSI
Scan Remote Loop	0x7B 00 00 00	RSL
Third Party Process Logout	0x24 00 00 00	TPRLO
Third Party Process Logout Accept	0x02 00 00 00	TPRLO ACC

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

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. You can configure this IVR VSAN topology manually on an IVR-enabled switch and distribute the configuration using CFS in Cisco MDS SAN-OS Release 2.0(1b) or later. Alternately, in Cisco MDS SAN-OS Release 2.1(1a) or later, you can configure IVR topology in auto mode. Prior to Cisco MDS SAN-OS Release 2.0(1b), you need to manually copy the IVR VSAN topology to each switch in the fabric.

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

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

When auto IVR topology is turned on it starts with the previously active, if any, manual IVR topology. Auto topology then commences its discovery process, and may come up with new, alternate or better paths. If the traffic is switched to an alternate or better path, there may be temporary traffic disruptions that are normally associated with switching paths.

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

Autonomous Fabric ID

The autonomous fabric ID (AFID) distinguishes segmented VSANS (that is, two VSANs that are logically and physically separate but have the same VSAN number). Cisco MDS NX-OS supports AFIDs from 1 through 64. AFIDs are used in conjunction with auto mode to allow segmented VSANS in the IVR VSAN topology database. You can configure up to 64 AFIDs.

The AFID can be configured individually for each switch and list of VSANs, or the default AFID can be configured for each switch.

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.

IVR Service Groups

IVR service groups have the following characteristics:

- 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/AFID combination cannot be a member of more than one service group. CFS merge fails if such a condition exists.
- Total number of AFID/VSAN combinations in all the service groups combined cannot exceed 128. The maximum number of AFID/VSAN combinations in a single service group is 128.
- IVR service group configurations are 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 pWWN 1 and pWWN 2 belonging to the same IVR zone but different service groups cannot communicate.
- During a CFS merge, service groups with 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 the reachable SANs. If you do not enable CFS distribution, you must ensure that the service group configuration is same at all the IVR-enabled switches in all the VSANs.
- IVR end devices belonging to an IVR service group are not exported to any AFID/VSAN outside of its service group.
- If at least one service group is defined and an IVR zone member that does not belong to a 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/VSAN combinations that are part of 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. The default policy is not part of ASCII configuration.

Service Group Activation

A configured service group must be activated for it take effect. Like zoneset activation or VSAN topology activation, the activation of a configured service group replaces the currently activate 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.

IVR Interoperability

When using the IVR feature, all border switches in a given 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.

See the "Switch Interoperability" section on page 37-15.

IVR Configuration Task List

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

Step 1 Determine whether to use IVR Network Address Translation (NAT).

Step 2 If you do not plan to use IVR NAT, verify that unique domain IDs are configured in all switches and VSANs participating in IVR.

Step 3 Enable IVR in the border switches.

Step 4 Configure the service group as required.

Step 5 Configure fabric distribution as required.

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

Step 7 Create and activate IVR zone sets in *all* of the IVR-enabled border switches, either manually or using fabric distribution.

Step 8 Verify the IVR configuration.

Configuring IVR

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

- Enabling IVR, page 23-9
- Distributing the IVR Configuration using CFS, page 23-10
- About IVR NAT and Auto Topology, page 23-12
- Configuring IVR Topology Automatic Mode, page 23-13
- Enabling IVR NAT, page 23-14
- About IVR Service Groups, page 23-14
- Configuring IVR Service Groups, page 23-14

- Copying the Active IVR Service Group Database, page 23-15
- Clearing IVR Service Group Database, page 23-15
- Verifying IVR Service Group Configuration, page 23-15
- About AFIDs, page 23-16
- Configuring Default AFIDs, page 23-16
- Configuring Individual AFIDs, page 23-17
- Verifying the AFID Database Configuration, page 23-17
- Activating a Manually Configured IVR Topology, page 23-20
- Adding an IVR-Enabled Switch to an Existing IVR Topology, page 23-21
- Copying the Active IVR Topology, page 23-22
- Clearing the Configured IVR Topology Database, page 23-22
- Migrating from IVR Auto Topology Mode to Manual Mode, page 23-23
- About IVR Virtual Domains, page 23-23
- Configuring IVR Virtual Domains, page 23-24
- Verifying the IVR Virtual Domain Configuration, page 23-24
- Clearing the IVR fcdomain Database, page 23-24
- About Persistent FC IDs for IVR, page 23-25
- Configuring Persistent FC IDs for IVR, page 23-26
- Verifying the Persistent FC ID Configuration, page 23-26
- Configuring IVR Logging Levels, page 23-27
- Verifying Logging Level Configuration, page 23-27

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 switches in the Cisco MDS 9000 Family. You can manually enable IVR on all required switches in the fabric or configure fabric-wide distribution of the IVR configuration ("Distributing the IVR Configuration using CFS" section on page 23-10).

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:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# feature ivr`	Enables IVR on the switch.
	`switch(config)# no feature ivr`	Disables (default) IVR on the switch.

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 (see Chapter 7, "Using the CFS Infrastructure").

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).
- IVR service groups.
- 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.

This section includes the following topics:

- Database Implementation, page 23-10
- Enabling Configuration Distribution, page 23-10
- Locking the Fabric, page 23-11
- Committing the Changes, page 23-11
- Discarding the Changes, page 23-11
- Clearing a Locked Session, page 23-11

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:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ivr distribute`	Enables IVR distribution.
	`switch(config)# no ivr distribute`	Disables (default) IVR distribution.

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:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ivr commit`	Commits the IVR changes.

Discarding the Changes

If you discard (abort) 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:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ivr abort`	Discards the IVR changes and clears the pending configuration database.

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 are 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 Auto Topology

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

- 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 Release2.1(1a) or later and one active IPS card for this feature (see Chapter 10, "Obtaining and Installing Licenses").

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).

Transit VSAN Guidelines

Consider the following guidelines for transit VSANs:

- 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:

- 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 facilities 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.

Service Group Guidelines

If you use service groups with IVR auto topology, you should enable IVR and configure your service groups first, then distribute them with CFS before setting the IVR topology in auto mode.

Configuring IVR Topology Automatic Mode

Note IVR configuration distribution must be enabled before configuring IVR topology automatic mode (see the "Distributing the IVR Configuration using CFS" section on page 23-10). Once IVR topology automatic mode is enabled, you cannot disable IVR configuration distribution.

To configure IVR topology automatic mode, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ivr vsan-topology auto`	Configures IVR topology automatic mode.
	`switch(config)# ivr vsan-topology activate`	Disables IVR topology automatic mode and reverts to user-configuration mode.

View automatically discovered 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 AUTO
Last activation time: Mon Mar 24 07:19:53 1980
```

Note The asterisk (*) indicates the local switch.

Enabling IVR NAT

To configure IVR NAT, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# ivr nat`	Enables IVR NAT on the switch.
	`switch(config)# no ivr nat`	Disables (default) IVR NAT on the switch.

About IVR Service Groups

In a complex network topology, you might have only 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.

CFS distribution of IVR information is restricted within the service group only when IVR VSAN topology is in automatic mode. See the "IVR VSAN Topology" section on page 23-6.

Configuring IVR Service Groups

To configure an IVR service group, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ivr service-group name IVR-SG1` `switch(config-ivr-sg)#`	Configures the IVR service group called IVR-SG1 and enters IVR server group configuration mode.
	`switch(config)# no ivr service-group name IVR-SG1` `Successfully erased service group IVR-SG1`	Deletes the IVR service group.
Step 3	`switch(config-ivr-sg)# autonomous-fabric-id 10 vsan-ranges 1,2,6-10`	Configures AFID 10 for VSANs 1, 2, and 6 through 10.
	`switch(config-ivr-sg)# autonomous-fabric-id 11 vsan-ranges 1`	Configures AFID 11 for VSAN 1.
	`switch(config-ivr-sg)# autonomous-fabric-id 12 vsan-ranges 3-5`	Configures AFID 12 for VSANs 3 through 5.
	`switch(config-ivr-sg)# no autonomous-fabric-id 12 vsan-ranges 3-5`	Removes the association between AFID 12 and VSANs 3 through 5.
	`switch(config-ivr-sg)# exit` `switch(config)#`	Returns to configuration mode.
	`switch(config)# ivr service-group name IVR-SG2` `switch(config-ivr-sg)#`	Configures the IVR service group called IVR-SG2 and enters IVR server group configuration mode.
	`switch(config-ivr-sg)# autonomous-fabric-id 20 vsan-ranges 3-5`	Configures AFID 20 for VSANs 3 through 5.

	Command	Purpose
Step 4	`switch(config-ivr-sg)# exit` `switch(config)#`	Returns to configuration mode.
Step 5	`switch(config)# ivr service-group activate`	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 default-sg-deny`	Activates the service group configuration and sets the communication policy between switches in the default service group to deny. **Note** To change the communication policy back to allow, you must issue the **ivr service-group activate** command again.
	`switch(config)# no ivr service-group activate`	Deactivates (default) the service group configuration.
Step 6	`switch(config)# ivr vsan-topology activate`	Activates the VSAN topology.
Step 7	`switch(config)# ivr distribute`	Enables CFS distribution for the IVR configuration.
Step 8	`switch(config)# ivr commit`	Commits the IVR configuration to the fabric.

Copying the Active IVR Service Group Database

You cannot modify the active IVR service group database. However, you can modify the configured IVR service group database. To copy the active IVR service group database to the manually configure 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 using the **clear ivr service-group database** 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
```

About AFIDs

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. IVR supports a maximum of 64 AFIDs.

Note You can only use AFID configuration when the VSAN topology mode is automatic. In user-configured VSAN topology mode, the AFIDs are specified in the VSAN topology configuration itself and a separate AFID configuration is not needed.

Configuring Default AFIDs

To configure the default AFID, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# autonomous-fabric-id database`	Enters AFID database configuration submode.
Step 3	`switch(config-afid-db)# switch-wwn 20:00:00:0c:91:90:3e:80 default-autonomous-fabric-id 5`	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)# no switch-wwn 20:00:00:0c:91:90:3e:80 default-autonomous-fabric-id 5`	Reverts to the default value (1) for the default AFID.

Configuring Individual AFIDs

To configure individual AFIDs, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# autonomous-fabric-id database`	Enters AFID database configuration submode.
Step 3	`switch(config-afid-db)# switch-wwn 20:00:00:0c:91:90:3e:80 autonomous-fabric-id 10 vsan-ranges 1,2,5-8`	Configures an AFID and VSAN range for a switch. The valid range for AFIDs is 1 to 64.
	`switch(config-afid-db)# no switch-wwn 20:00:00:0c:91:90:3e:80 autonomous-fabric-id 10 vsan-ranges 2`	Deletes VSAN 2 from AFID 10.

Verifying the AFID Database Configuration

View the contents of the AFID database using 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
```

Configuring IVR Without IVR NAT or Auto Topology

Before configuring an IVR SAN fabric without IVR in NAT mode or IVR topology in auto mode, 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
- Configure IVR only in the relevant border switches.
- Acquire a mandatory Enterprise License Package or SAN-EXTENSION license package and one active IPS card for this feature.

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).

Domain ID Guidelines

Domain IDs must be unique across inter-connected VSANs when not using IVR NAT. To ensure unique domain IDs across inter-connected VSANs, consider these guidelines:

- 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:

- 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 facilities IVR communications must be IVR enabled.
- IVR can (optionally) be enabled on additional border switches to provide redundant paths between active IVR zone members.

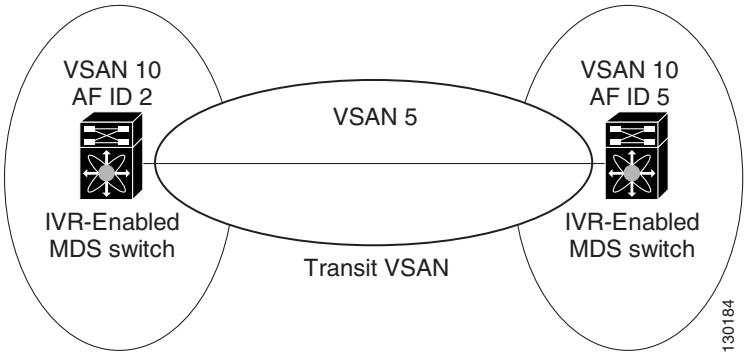
- The VSAN topology configuration must be updated before a border switch is added or removed.

Configuring IVR Without NAT

You must create the IVR topology in every IVR-enabled switch in the fabric if you have not configured IVR topology in auto mode. You can have up to 128 VSANs in an IVR topology. Specify the IVR topology using the following information:

- The switch WWNs of the IVR-enabled switches.
- A minimum of two VSANs to which the IVR-enabled switch belongs.
- The AFID, which distinguishes two VSANs that are logically and physically separate, but have the same VSAN number. You can specify up to 64 AFIDs. See Figure 23-2.

Figure 23-2 Example IVR Topology with Non-Unique VSAN IDs Using AFIDs



Note 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.

Note The use of a single AFID does not allow for segmented VSANs in an inter-VSAN routing topology.

Caution You can only configure a maximum of 128 IVR-enabled switches and 128 distinct VSANs in an IVR topology (see the "Database Merge Guidelines" section on page 23-36).

Manually Configuring the IVR Topology

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

To configure a user-defined IVR topology database, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# ivr vsan-topology database` `switch(config-ivr-topology-db)#`	Enters the VSAN topology database configuration mode for the IVR feature.
Step 3	`switch(config-ivr-topology-db)# autonomous-fabric-id 1 switch 20:00:00:05:30:01:1b:b8 vsan-ranges 1-2,6`	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:c2 vsan-ranges 1-3`	Configures VSANs 1, 2 and 3 to participate in 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`	Removes VSANs 1 and 2 from IVR for this switch.
Step 4	`switch(config-ivr-topology-db)# end` `switch#`	Reverts to EXEC mode.

View your configured 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
```

Note If CFS is not enabled, you must repeat this configuration in all IVR-enabled switches. See the "Database Merge Guidelines" section on page 23-36.

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 database, you must activate it.

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

To activate the manually configured IVR topology database, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ivr vsan-topology activate`	Activates the configured IVR topology.

View your 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 1980
```

Note The asterisk (*) indicates the local switch.

Adding an IVR-Enabled Switch to an Existing IVR Topology

Before adding an IVR-enabled switch to an existing fabric with manual IVR topology and CFS distribution enabled (see the "Distributing the IVR Configuration using CFS" section on page 23-10), 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 the existing IVR topology on the IVR-enabled switch where you update the IVR configuration, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 1	`mds(config)# ivr vsan-topology database` `mds(config-ivr-topology-db)#`	Enters IVR VSAN topology database configuration submode.
Step 2	`mds(config-ivr-topology-db)# autonomous-fabric-id 1 switch-wwn 20:00:00:05:40:01:1b:c2 vsan-ranges 1,4`	Adds the new IVR-enabled switch to the topology.
Step 3	`switch(config-ivr-topology-db)# exit` `switch(config)#`	Returns to configuration mode.
Step 4	`switch(config)# ivr vsan-topology activate`	Activates the IVR VSAN topology.
Step 5	`switch(config)# ivr commit`	Commits the IVR configuration change to the fabric.
Step 6	`switch(config)# exit` `switch#`	Returns to EXEC mode.
Step 7	`switch# copy running-config startup-config`	Saves the running configuration.

After adding the switch to the IVR topology, you then enable IVR and CFS for the IVR application on the new switch (see the"Enabling IVR" section on page 23-9 and the "Distributing the IVR Configuration using CFS" section on page 23-10).

Copying the Active IVR Topology

You cannot edit the active IVR topology. However, you can edit the manually configured topology. To copy the active IVR topology database to the manually configure topology, use the following command in EXEC mode:

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

Clearing the Configured IVR Topology Database

You can only clear manually created IVR VSAN topology entries from the configured database.

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

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# no ivr vsan-topology database`	Clears the previously created IVR topology.

Verifying the IVR Topology

You can verify the IVR topology by using the **show ivr vsan-topology** command. See Example 23-1 to Example 23-3.

Example 23-1 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.

Example 23-2 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
```

Example 23-3 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 Manual Mode

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

To migrate from automatic mode to manual mode, follow these steps:

	Command	Purpose
Step 1	`switch# ivr copy auto-topology user-configured-topology`	Copies the automatic IVR topology database to the user-configured IVR topology.
Step 2	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 3	`switch(config)# ivr vsan-topology active`	Disabled automatic mode for the IVR topology database and enables user-configuration mode.

About 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) 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(s) 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 domain 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 so, 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.

Configuring IVR Virtual Domains

To configure an IVR virtual domain in a specified VSAN, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ivr virtual-fcdomain-add vsan-ranges 1`	Adds the IVR virtual domains in VSAN 1.
	`switch(config)# no ivr virtual-fcdomain-add vsan-ranges 1`	Reverts to the factory default of not adding IVR virtual domains and removes the currently active virtual domains for that VSAN from the fcdomain manger list.

Note To configure FCS with IVR virtual domains, configure the IVR virtual domains, discover the FCS virtual devices using the **fcs virtual-device-add vsan-ranges** command, and then activate the IVR zone set. For more information, see the "About FCS" section on page 63-1.

Verifying the IVR Virtual Domain Configuration

View the status of the IVR virtual domain configuration using 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 the IVR fcdomain Database

You can clear the IVR fcdomain database by using the following command:

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

About Persistent FC IDs for IVR

You can configure persistent FC IDs for IVR. FC ID persistence across reboot improves IVR management by providing the following features:

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

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

- Host devices always see the same FC ID for targets.
- It helps you plan your SAN layout better by assigning virtual domains for IVR to use.
- It 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.

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). These 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). These 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

Note If you use persistent FC IDs for IVR, we recommend that you use them for all the devices in the IVR zoneset. We do not recommend using persistent FC IDs for some of the IVR devices while using automatic allocation for others.

Note IVR NAT must be enabled to use IVR persistent FC IDs.

Note 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:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# ivr fcdomain database autonomous-fabric-num 21 vsan 22` `switch(config-fcdomain)#`	Enters IVR fcdomain database configuration submode for current AFID 21 and VSAN 22.
	`switch(config)# no ivr fcdomain database autonomous-fabric-num 21 vsan 22`	Deletes all the database entries, including all the corresponding persistent FC ID entries, for current AFID 21 and VSAN 22.
Step 3	`switch(config-fcdomain)# native-autonomous-fabric-num 20 native-vsan 11 domain 12` `switch(config-fcdomain-fcid)#`	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)# no native-autonomous-fabric-num 20 native-vsan 11`	Deletes the virtual domain entry native AFID 20 and native VSAN 11, and all corresponding FC ID entries.
Step 4	`switch(config-fcdomain-fcid)# pwwn 11:22:33:44:55:66:77:88 fcid 0x114466`	Adds or replaces a database entry for mapping the pWWN to the FC ID.
	`switch(config-fcdomain-fcid)# no pwwn 11:22:33:44:55:66:77:88`	Deletes the database entries for the pWWN.
Step 5	`switch(config-fcdomain-fcid)# device-alias SampleName fcid 0x123456`	Adds a database entry for mapping the device alias to the FC ID.
	`switch(config-fcdomain-fcid)# no device-alias SampleName`	Deletes the database entries for the device alias.

Verifying the Persistent FC ID Configuration

Verify the persistent FC ID configuration using the **show ivr fcdomain database** command. See Example 23-4 and Example 23-5.

Example 23-4 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
```

Example 23-5 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
```

Configuring IVR Logging Levels

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

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# logging level ivr 4`	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.

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)
```

IVR Zones and IVR Zone Sets

As part of the IVR configuration, you need to configure one or more IVR zone 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.

Caution Prior to Cisco SAN-OS Release 3.0(3) you can only configure a total of 10,000 zone members on all switches in a network. As of Cisco SAN-OS Release 3.0(3) you can only configure a total of 20,000 zone members on all switches in a network. A zone member is counted twice if it exists in two zones. See the "Database Merge Guidelines" section on page 23-36.

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

- About IVR Zones, page 23-28
- Configuring IVR Zones and IVR Zone Sets, page 23-30
- About Activating Zone Sets and Using the force Option, page 23-31
- Activating or Deactivating IVR Zone Sets, page 23-32
- Verifying IVR Zone and IVR Zone Set Configuration, page 23-32
- About LUNs in IVR Zoning, page 23-34
- Configuring LUNs in IVR Zoning, page 23-34
- About QoS in IVR Zones, page 23-35
- Configuring the QoS Attribute, page 23-35
- Verifying the QoS Attribute Configuration, page 23-35
- Clearing the IVR Zone Database, page 23-36
- Configuring IVR Using Read-Only Zoning, page 23-36
- System Image Downgrading Considerations, page 23-36

About IVR Zones

Table 23-3 identifies the key differences between IVR zones and zones.

Table 23-3 Key Differences Between IVR Zones and Zones

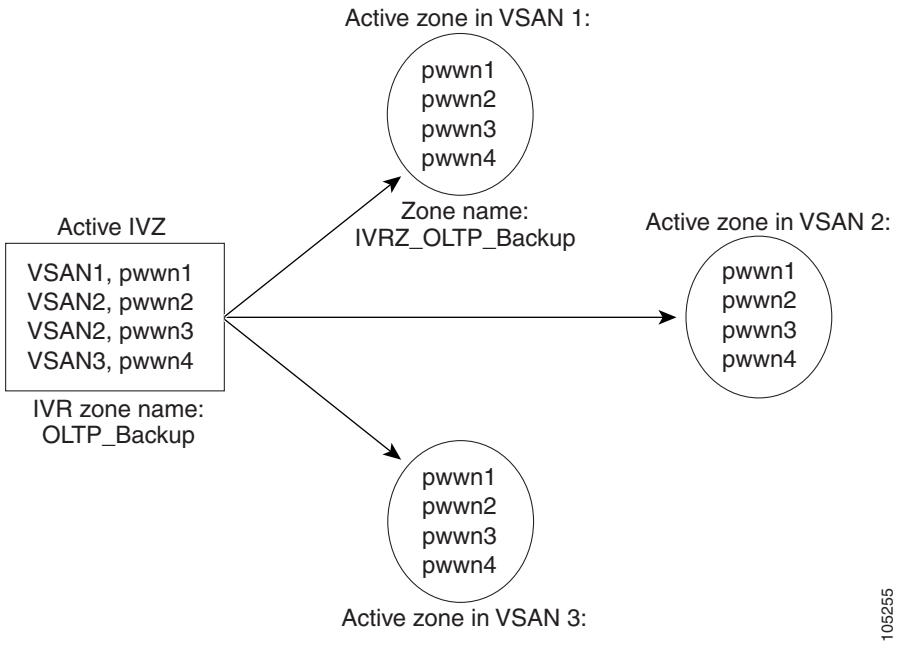
IVR Zones	Zones
IVR zone membership is specified using the VSAN and pWWN combination.	Zone membership is specified using pWWN, fabric WWN, sWWN, or the AFID.
Default zone policy is always deny (not configurable).	Default zone policy is deny (configurable).

Automatic IVR Zone Creation

Figure 23-3 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 23-3 Creating Zones Upon IVR Zone Activation



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

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

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

Caution Prior to Cisco SAN-OS Release 3.0(3) you can only configure a total of 2000 IVR zones and 32 IVR zone sets on the switches in the network. As of Cisco SAN-OS Release 3.0(3) you can only configure a total of 8000 IVR zones and 32 IVR zone sets on the switches in the network. See the "Database Merge Guidelines" section on page 23-36.

Configuring IVR Zones and IVR Zone Sets

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

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ivr zone name sample_vsan2-3` `switch(config-ivr-zone)#`	Creates an IVR zone named sample_vsan2-3.
Step 3	`switch(config-ivr-zone)# member pwwn 21:00:00:e0:8b:02:ca:4a vsan 3`	Adds the specified pWWN in VSAN 3 as an IVR zone member.
Step 4	`switch(config-ivr-zone)# member pwwn 21:00:00:20:37:c8:5c:6b vsan 2`	Adds the specified pWWN in VSAN 2 as an IVR zone member.
Step 5	`switch(config-ivr-zone)# exit` `switch(config)#`	Reverts to configuration mode.
Step 6	`switch(config)# ivr zone name sample_vsan4-5` `switch(config-ivr-zone)#`	Creates an IVR zone named sample_vsan4-5.
Step 7	`switch(config-ivr-zone)# member pwwn 21:00:00:e0:8b:06:d9:1d vsan 4`	Adds the specified pWWN in VSAN 4 as an IVR zone member.
Step 8	`switch(config-ivr-zone)# member pwwn 21:01:00:e0:8b:2e:80:93 vsan 4`	Adds the specified pWWN in VSAN 4 as an IVR zone member.
Step 9	`switch(config-ivr-zone)# member pwwn 10:00:00:00:c9:2d:5a:dd vsan 5`	Adds the specified pWWN in VSAN 5 as an IVR zone member.
Step 10	`switch(config-ivr-zone)# exit` `switch(config)#`	Reverts to configuration mode.
Step 11	`switch(config)# ivr zoneset name Ivr_zoneset1` `switch(config-ivr-zoneset)#`	Creates an IVR zone set named Ivr_zoneset1.
Step 12	`switch(config-ivr-zoneset)# member sample_vsan2-3`	Adds the sample_vsan2-3 IVR zone as an IVR zone set member.
Step 13	`switch(config-ivr-zoneset)# member sample_vsan4-5`	Adds the sample_vsan4-5 IVR zone as an IVR zone set member.
Step 14	`switch(config-ivr-zoneset)# exit` `switch(config)`	Returns to configuration mode.

	Command	Purpose
Step 15	`switch(config)# ivr zoneset activate name IVR_ZoneSet1`	Activates the newly created IVR zone set.
	`switch(config)# ivr zoneset activate name IVR_ZoneSet1 force`	Forcefully activates the specified IVR zone set.
	`switch(config)# no ivr zoneset activate name IVR_ZoneSet1`	Deactivates the specified IVR zone set.
Step 16	`switch(config)# end` `switch#`	Returns to EXEC mode.

About Activating Zone Sets and Using the force Option

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

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

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

You can also use the **force** option to activate IVR zone sets. Table 23-4 lists the various scenarios with and without the **force** option.

Table 23-4 IVR Scenarios with and without theforce Option

Case	Default Zone Policy	Active Zone Set before IVR Zone Activation	force 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	No	Failure	No	No
5		or Active zone set present	Yes	Success	Yes	Yes

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

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

Activating or Deactivating IVR Zone Sets

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

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ivr zoneset activate name IVR_ZoneSet1`	Activates the newly created IVR zone set.
	`switch(config)# ivr zoneset activate name IVR_ZoneSet1 force`	Forcefully activates the specified IVR zone set.
	`switch(config)# no ivr zoneset activate name IVR_ZoneSet1`	Deactivates the specified IVR zone set.

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. See Example 23-6 to Example 23-14.

Example 23-6 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
```

Example 23-7 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
```

Example 23-8 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
```

Example 23-9 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
```

Example 23-10 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
```

Example 23-11 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
```

Example 23-12 Displays Brief Information for All IVR Zone Sets

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

Example 23-13 Displays Brief Information for the Active IVR Zone Set

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

Example 23-14 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 Using the Cisco MDS Fabric Manager, you can distribute IVR zone configurations to all IVR-capable switches in the interconnected VSAN network. Refer to the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.

About 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, see the "About LUN Zoning" section on page 30-48.

Configuring LUNs in IVR Zoning

To configure LUNs in IVR zoning, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ivr zone name IvrLunZone` `switch(config-ivr-zone)#`	Configures an IVR zone called IvrLunZone.

	Command	Purpose
Step 3	`switch(config-ivr-zone)# member pwwn 10:00:00:23:45:67:89:ab lun 0x64 vsan 10`	Configures an IVR zone member based on the specified pWWN and LUN value. **Note** The CLI interprets the LUN identifier value as a hexadecimal value whether or not the **0x** prefix is included.
	`switch(config-ivr-zone)# member pwwn 10:00:00:23:45:67:89:ab lun 0x64 vsan 10 autonomous-fabric-id 20`	Configures an IVR zone member based on the specified pWWN, LUN value, and AFID.
	`switch(config-ivr-zone)# no member pwwn 20:81:00:0c:85:90:3e:80 lun 0x32 vsan 13 autonomous-fabric-id 10`	Removes an IVR zone member.

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

About QoS in IVR Zones

You can configure a QoS attribute for an IVR zone. The default QoS attribute setting is low.

Configuring the QoS Attribute

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

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

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

Verifying the QoS Attribute Configuration

Verify the QoS attribute configuration for an IVR zone using the **show ivr zone** command.

```
switch(config)# show ivr zone

zone name IvrZone
    attribute qos priority medium
```

Renaming IVR Zones and IVR Zone Sets

You can rename 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 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** to ensure that the running configuration is used when you next start the switch.

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.

System Image Downgrading Considerations

As of Cisco MDS SAN-OS Release 3.0(3), you can configure 8000 IVR zones and 20,000 IVR zone members. 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.

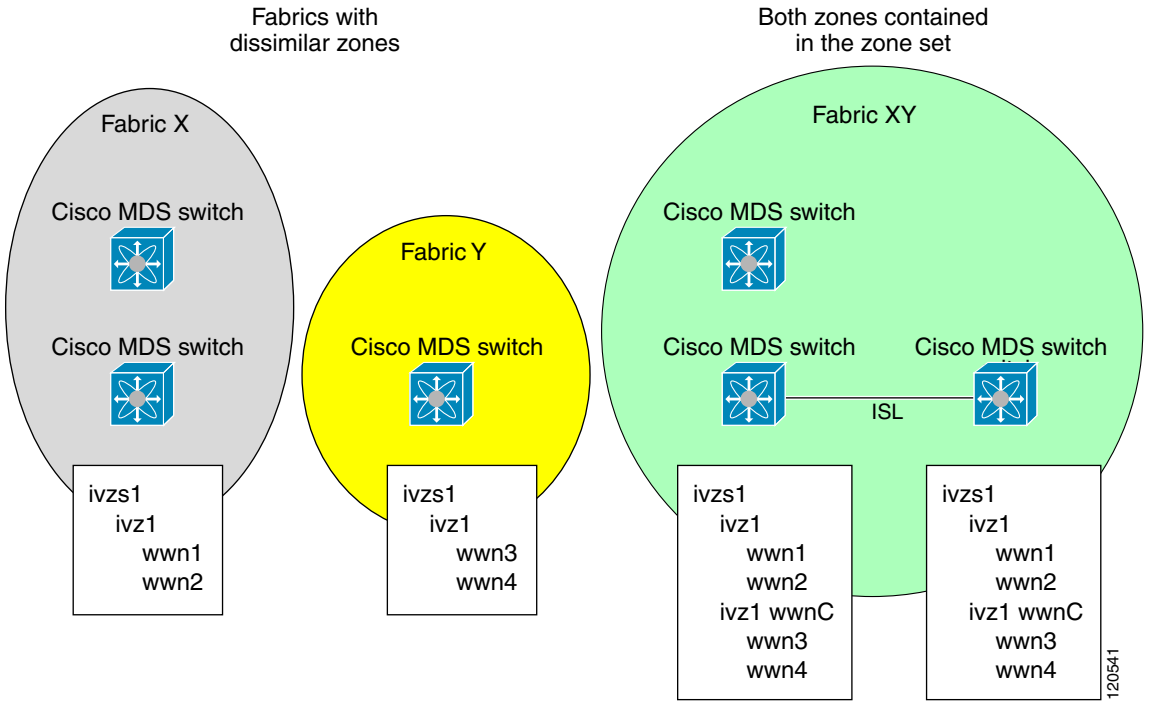
Database Merge Guidelines

A database merge refers to a union of the configuration database and static (unlearned) entries in the active database. See the "CFS Merge Support" section on page 7-9 for detailed concepts.

- Be aware of the following conditions when merging two IVR fabrics:
  - The IVR configurations are merged even if two fabrics contain different configurations.

- If dissimilar zones exist in two merged fabrics, the zone from each fabric is cloned in the distributed zone set with appropriate names (see Figure 23-4).

Figure 23-4 Fabric Merge Consequences



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

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

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

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

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

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

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

Table 23-5 describes the results of a CFS merge of two IVR-enabled fabrics under different conditions.

Table 23-5 Results of Merging Two IVR-Enabled Fabrics

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

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

Resolving Database Merge Failures

If a merge failure occurs, use the following 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)

Depending on the failure indicated in the **show** command outputs, you can perform the following:

- If the failure is due to exceeding the maximum configuration limits in a fabric where the switches are running more than one Cisco SAN-OS release, then either upgrade the switches running the earlier release or reduce the number of IVR zones and IIVR zone members on the switches running the more recent release to the earlier release limit (see the"IVR Limits Summary" section on page 23-4).
- If the failure is due to exceeding maximum limits in a fabric where all switches are running the same Cisco SAN-OS release, identify the switch that has the correct configuration and perform a CFS commit to distribute the IVR configuration (see the "Configuring Default AFIDs" section on page 23-16 and the"IVR Limits Summary" section on page 23-4).
- For other failures, resolve the error causing the merge failure on the switch that has the correct configuration and perform a CFS commit to distribute the IVR configuration (see the "Configuring Individual AFIDs" section on page 23-17).

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

Example Configurations

This section provides IVR configurations examples and includes the following topics:

- Manual Topology Configuration, page 23-39
- Auto-Topology Configuration, page 23-42

Manual Topology Configuration

This section provides the configuration steps to manually configure the example illustrated in Figure 23-1.

Step 1 Enable IVR.

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

Step 2 Verify that IVR is enabled.

```
mds# 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.

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

Step 4 Manually configure the IVR VSAN-topology. In Figure 23-1, two of the four IVR-enabled switches (MDS1 and MDS2) are members of VSANs 1 and 4. The other two switches (MDS3 and MDS4) are members of VSANs 2, 3, and 4.

```
mds(config)# ivr vsan-topology database
mds(config-ivr-topology-db)# autonomous-fabric-id 1 switch-wwn 20:00:00:05:40:01:1b:c2
vsan-ranges 1,4
mds(config-ivr-topology-db)# autonomous-fabric-id 1 switch-wwn 20:02:00:44:22:00:4a:08
vsan-ranges 1,4
mds(config-ivr-topology-db)# autonomous-fabric-id 1 switch-wwn 20:00:00:44:22:02:8a:04
vsan-ranges 2-4
mds(config-ivr-topology-db)# autonomous-fabric-id 1 switch-wwn 20:00:00:44:22:40:aa:16
vsan-ranges 2-4
mds(config-ivr-topology-db)# exit
mds(config)#
```

Step 5 Verify the configured VSAN topology.

Note The configured topology has not yet been activated—as indicated by the `no` status displayed in the `Active` column.

```
mds(config)# do show ivr vsan-topology

AFID  SWITCH WWN                 Active   Cfg. VSANS
------------------------------------------------------------
   1  20:00:00:05:40:01:1b:c2 *    no     yes  1,4
   1  20:00:00:44:22:00:4a:08      no     yes  1,4
   1  20:00:00:44:22:02:8a:04      no     yes  2-4
   1  20:00:00:44:22:40:aa:16      no     yes  2-4

Total:   4 entries in active and configured IVR VSAN-Topology

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

Step 6 Activate the configured VSAN topology.

```
mds(config)# ivr vsan-topology activate
```

Step 7 Verify the activation.

```
mds(config)# do show ivr vsan-topology
```

```
AFID  SWITCH WWN                 Active   Cfg. VSANS
-----------------------------------------------------------
   1  20:00:00:05:40:01:1b:c2 *   yes     yes  1,4
   1  20:00:00:44:22:00:4a:08     yes     yes  1,4
   1  20:00:00:44:22:02:8a:04     yes     yes  2-4
   1  20:00:00:44:22:40:aa:16     yes     yes  2-4

Total:   4 entries in active and configured IVR VSAN-Topology

Current Status: Inter-VSAN topology is ACTIVE
Last activation time: Tue May 20 23:14:59 1980
```

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.

```
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.

```
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.

```
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.

```
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.

```
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.

```
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
```

Auto-Topology Configuration

This section provides example configuration steps for configuring IVR auto-topology.

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

```
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.

```
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.

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

Step 4 Enable IVR auto-topology mode.

```
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.

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

Step 6 Verify the status of the commit request.

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

Step 7 Verify the active IVR topology.

```
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
```

Default Settings

Table 23-6 lists the default settings for IVR parameters.

Table 23-6 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.