CHAPTER 29

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

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

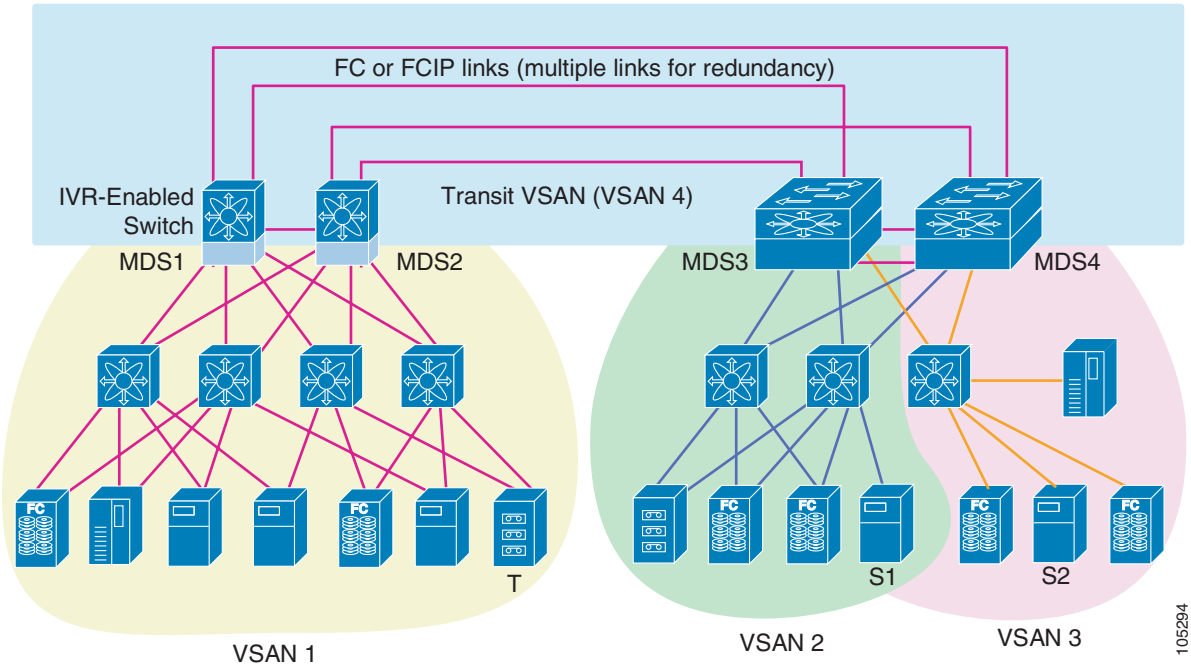
Note IVR is not supported on the Cisco MDS 9124 Fabric Switch, the Cisco MDS 9134 Fabric Switch, the Cisco Fabric Switch for HP c-Class BladeSystem, and the Cisco Fabric Switch for IBM BladeCenter.

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 29-1).

Figure 29-1 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 29-1, 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 29-1, 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 29-1, 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.

IVR Limits Summary

Table 29-1 summarizes the configuration limits for IVR. See Appendix 60, "Configuration Limits for Cisco MDS SAN-OS Release 3.1(x) and 3.2(x)," for a complete list of Cisco MDS SAN-OS feature configuration limits.

Table 29-1 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.

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 . 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:

- 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).

Note IVR NAT requires Cisco MDS SAN-OS Release 2.1(1a) or later on all switches in the fabric performing IVR. If you have isolated switches with an earlier release that are involved in IVR, you must remove any isolated fabrics from monitoring by Fabric Manager server and then re-open the fabric to use IVR NAT. See the "Selecting a Fabric to Manage Continuously" section on page 3-4.

- 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 29-2.

Table 29-2 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

Table 29-2 Extended Link Service Messages Supported by IVR NAT (continued)

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

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

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 SAN-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 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 29-8.

About the IVR Zone Wizard

The IVR Zone Wizard simplifies the steps required to configure IVR zones in a fabric. The IVR Zone Wizard checks the following conditions and prompts you for any issues:

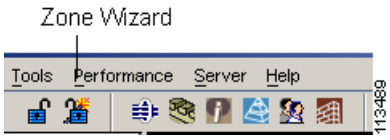
- Checks if all switches in the fabric are Cisco MDS SAN-OS Release 2.1(1a) or later and if so, asks if you want to migrate to using IVR NAT with auto-topology.
- Checks if any switches in the fabric are earlier than Cisco MDS SAN-OS Release 2.1(1a) and if so, asks you to upgrade the necessary switches or to disable IVR NAT or auto-topology if they are enabled.

Configuring IVR Using the IVR Zone Wizard

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

Step 1 Click the **IVR Zone Wizard** icon in the Zone toolbar (see Figure 29-2).

Figure 29-2 IVR Zone Wizard Icon

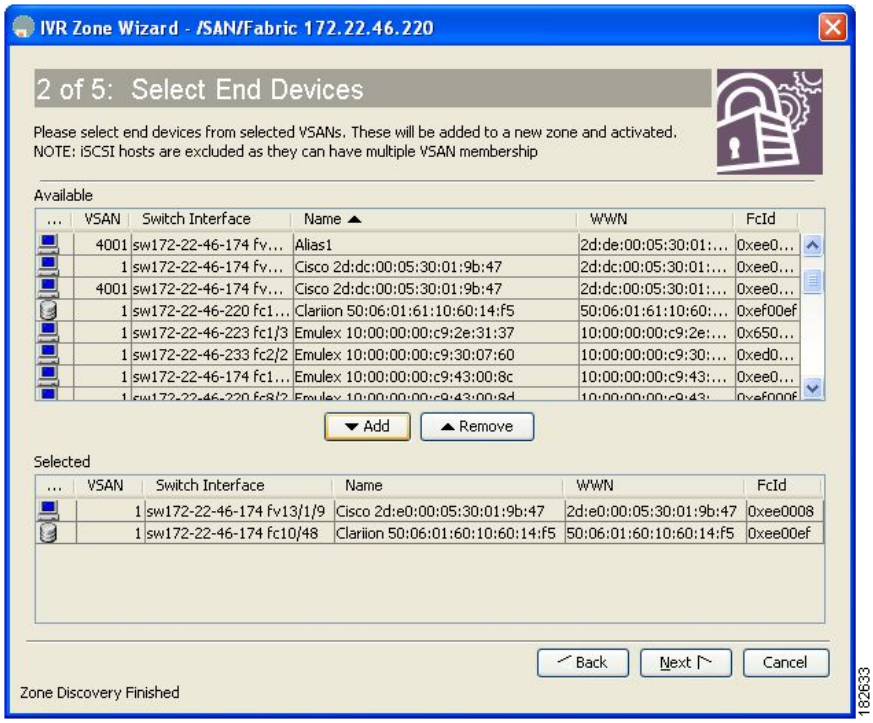


To migrate to IVR NAT mode click **Yes**, otherwise click **No**. You see the IVR Zone Wizard dialog box.

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

You see the Select End Devices dialog box shown in Figure 29-3.

Figure 29-3 Select End Devices Dialog Box



Step 3 Select the end devices that you want to communicate over IVR.

Note If you are not using IVR NAT, Fabric Manager may display an error message if all the switches participating in IVR do not have unique domain IDs. You must reconfigure those switches before configuring IVR. Go to Step 5.

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

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

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

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

Step 8 Set the IVR zone and IVR zone set.

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

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

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

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

Step 12 Click **Finish**.

Note IVR NAT and auto-topology can be configured independently if you configure these features outside the IVR Zone Wizard. See the "Manual IVR Configuration" section on page 29-9.

Manual IVR Configuration

You can configure IVR using the IVR tables in the Information pane in Fabric Manager. Use these tables only if you are familiar with all IVR concepts. We recommend you configure IVR using the IVR Wizard.

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

This section describes manually configuring IVR and includes the following topics:

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. You must first click the CFS tab in order for the other tabs on the dialog boxes to become available.
- Verify that all switches in the fabric are running Cisco MDS SAN-OS Release 2.1(1a) or later.
- Acquire a mandatory Enterprise License Package or SAN-EXTENSION license package if you have Cisco MDS SAN-OS Release2.1(1a) or later and one active IPS card for this feature (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.

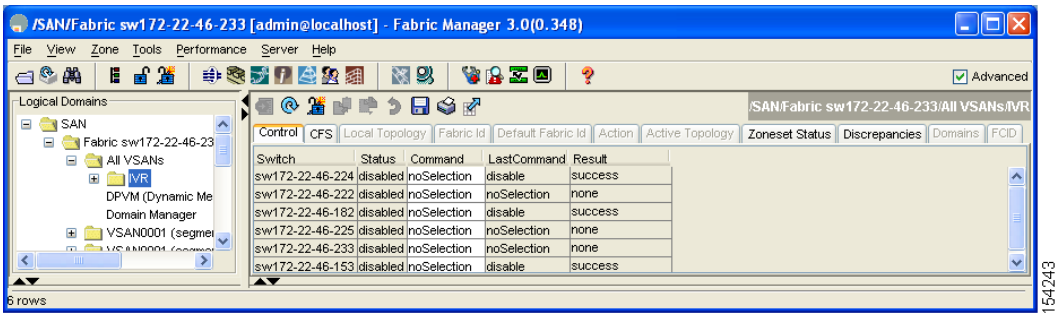
Configuring IVR NAT and IVR Auto Topology

To configure IVR in NAT mode and IVR topology in auto mode from Fabric Manager, follow these steps:

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

You see the inter-VSAN routing configuration in the Information pane shown in Figure 29-4.

Figure 29-4 IVR Routing Configuration Control Tab



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

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

Step 4 Click the **Action** tab.

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

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

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

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 default AFIDs using Fabric Manager, follow these steps:

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

You see the IVR configuration in the Information pane.

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

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

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

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

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

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

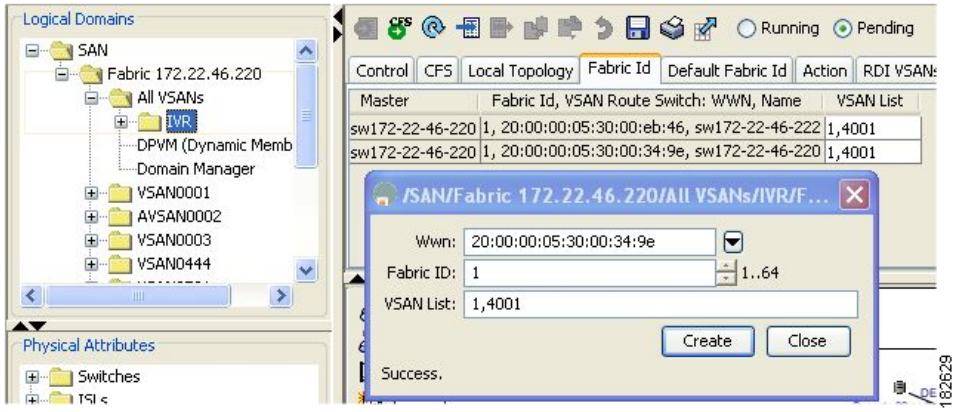
Configuring Individual AFIDs

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

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

You see the IVR configuration in the Information pane.

Figure 29-5 Fabric ID Tab



Step 2 Click the **Fabric ID** tab to display the existing AFIDs (see Figure 29-5).

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

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

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

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

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

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

About 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 should 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.

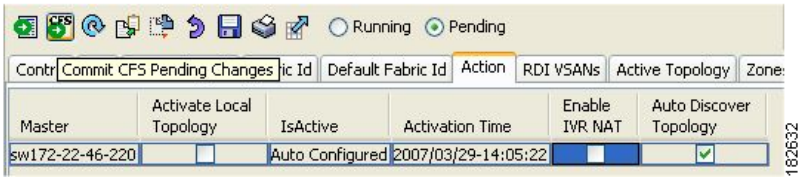
Configuring IVR Without NAT

To enable IVR in NAT mode from Fabric Manager, follow these steps:

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

You see the IVR configuration in the Information pane.

Figure 29-6 Action Tab



Step 2 Click the **Action** tab.

Step 3 Uncheck the **Enable IVR NAT** check box (see Figure 29-6).

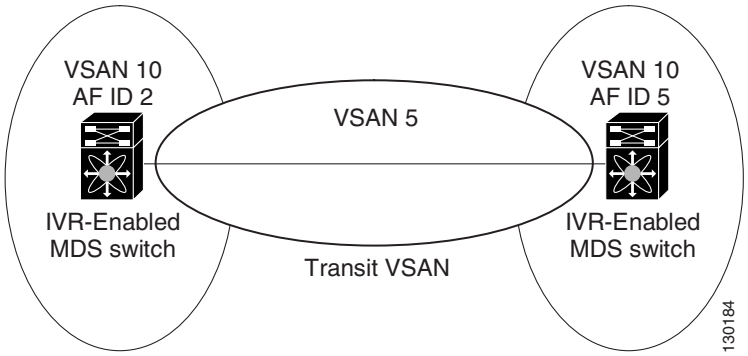
Step 4 Click the **Apply Changes** icon to distribute this change to all switches in the fabric.

Manually Creating the IVR Topology

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 29-7.

Figure 29-7 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.

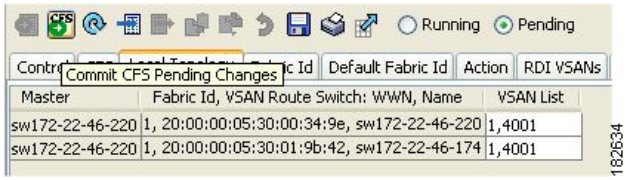
Caution You can only configure a maximum of 128 IVR-enabled switches and 128 distinct VSANs in an IVR topology (see the "Database Merge Guidelines" section on page 29-31).

To create the IVR topology using Fabric Manager, follow these steps:

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

You see the IVR configuration in the Information pane.

Figure 29-8 Local Topology Tab



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

Step 3 Click the **Create Row** icon to create rows in the IVR topology (see Figure 29-8).

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

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

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

Note Repeat this configuration in all IVR-enabled switches or distribute using CFS.

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

Activating a Manually Configured IVR Topology

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

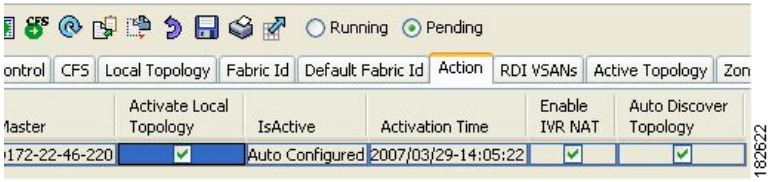
Caution Active IVR topologies cannot be deactivated. You can only switch to IVR topology automatic mode.

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

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

You see the IVR configuration in the Information pane.

Figure 29-9 Action Tab



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

Step 3 Check the **Activate Local Topology** check box (see Figure 29-9).

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

Clearing the Configured IVR Topology

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

To clear the IVR topology using Fabric Manager, follow these steps:

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

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

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

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

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

Migrating from IVR Auto Topology Mode to Manual Mode

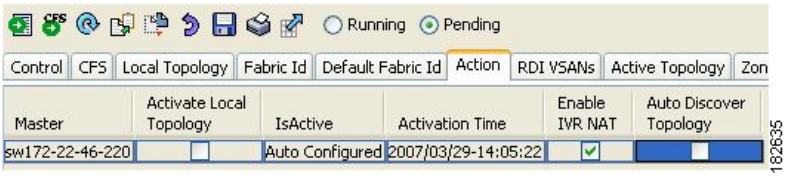
If you want to migrate the active IVR VSAN topology database from automatic mode to user-configured mode, first copy the active IVR VSAN topology database to the user-configured IVR VSAN topology database before switching modes.

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

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

You see the IVR configuration in the Information pane.

Figure 29-10 Action Tab



Step 2 Click the **Action** tab.

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

Step 4 Uncheck the **Auto Discover Topology** check box (see Figure 29-10).

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

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.

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

Configuring IVR Virtual Domains

To add IVR virtual domains using Fabric Manager, follow these steps:

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

You see the IVR configuration in the Information pane.

Figure 29-11 Domains Tab

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

Step 3 Click the **Create Row** icon to create rows in the IVR topology (see Figure 29-11).

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

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

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.

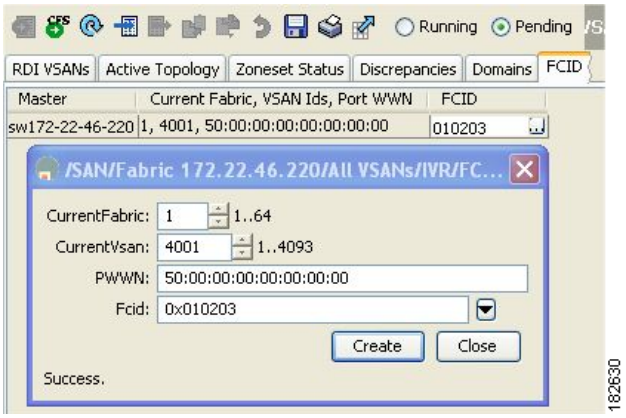
Configuring Persistent FC IDs for IVR

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

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

You see the IVR configuration in the Information pane.

Figure 29-12 FCID Tab



Step 2 Click the **FCID** tab.

Step 3 Click the **Create Row** icon to create an FC ID (see Figure 29-12).

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

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

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

Step 7 Enter the **pWWN.**

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

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

Configuring IVR Logging Levels

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

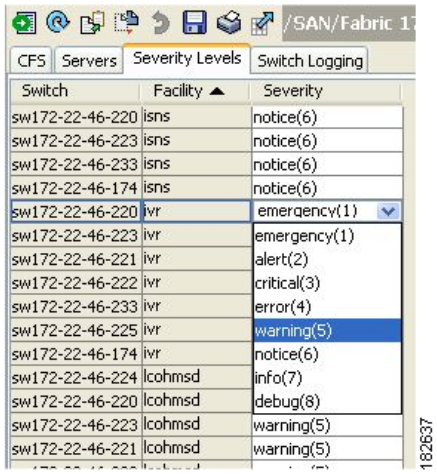
Step 1 Expand **Switches > Events** and then select **Syslog** from the Physical Attributes pane.

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

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

Step 4 Select the severity level at which the IVR logs system messages from the Severity drop-down menu (see Figure 29-13).

Figure 29-13 Syslog Severity Drop-Down Menu



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

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

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 29-31.

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

About IVR Zones

Table 29-3 identifies the key differences between IVR zones and zones.

Table 29-3 Key Differences Between IVR Zones and Zones

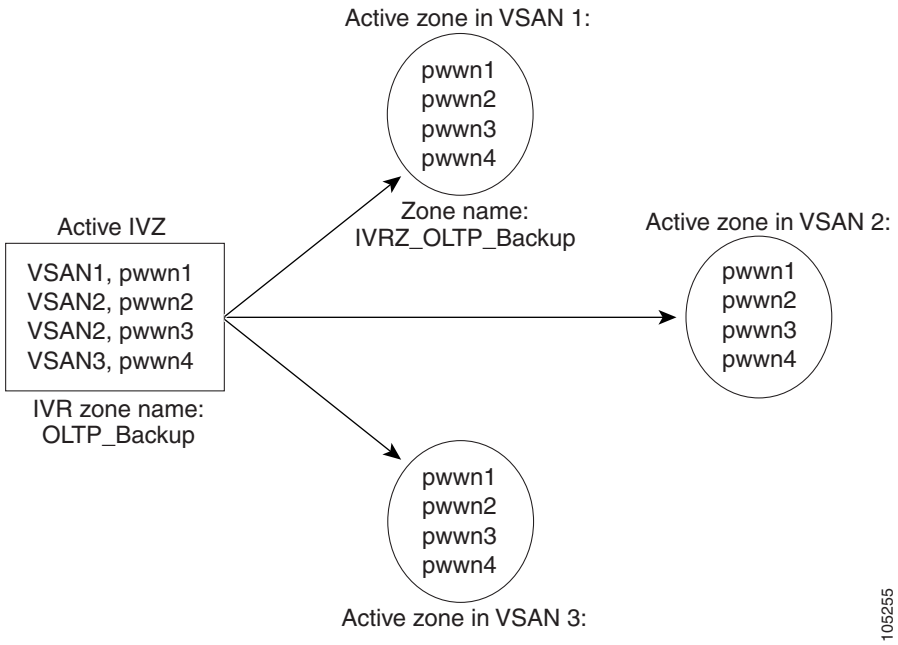
IVR Zones	Zones
IVR zone membership is specified using the VSAN and pWWN combination.	Zone membership is specified using pWWN, fabric WWN, sWWN, or the AFID.
Default zone policy is always deny (not configurable).	Default zone policy is deny (configurable).

Automatic IVR Zone Creation

Figure 29-14 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 29-14 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 29-31.

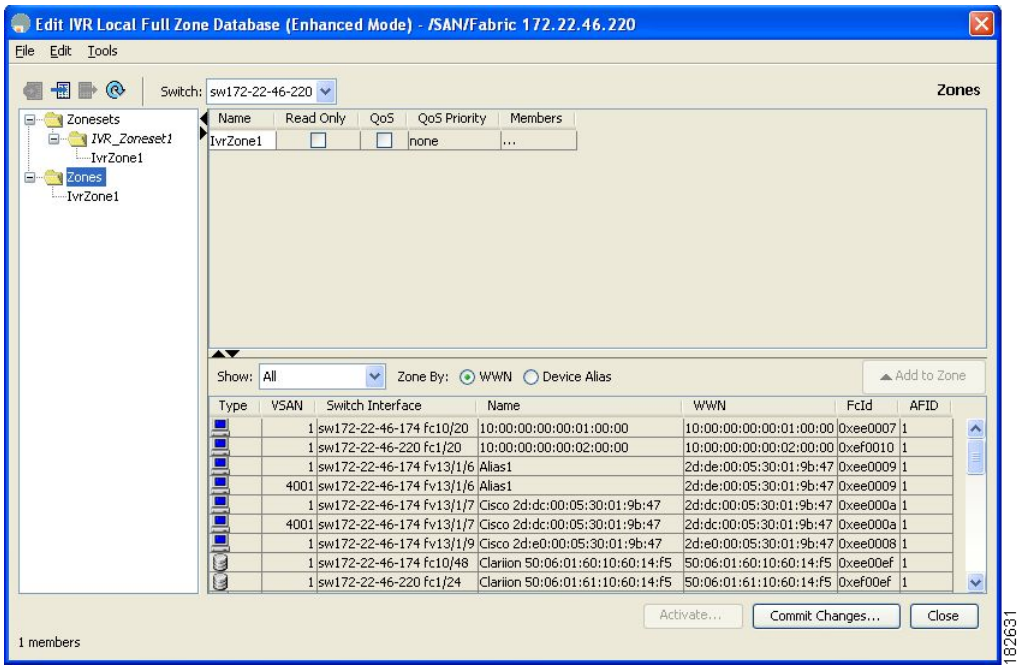
Configuring IVR Zones and IVR Zone Sets

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

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

You see the Edit IVR Local Full Zone Database dialog box for the selected VSAN (see Figure 29-15).

Figure 29-15 Edit IVR Local Full Zone Database Dialog Box

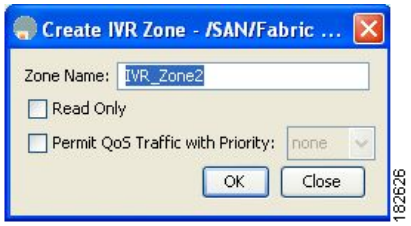


If you want to view zone membership information, right-click in the **Members** column, and then click **Show Details** for the current row or all rows from the pop-up menu.

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

You see the Create IVR Zone dialog box shown in Figure 29-16.

Figure 29-16 Create IVR Zone Dialog Box



Step 3 Enter an IVR zone name.

Step 4 Check one of the following check boxes:

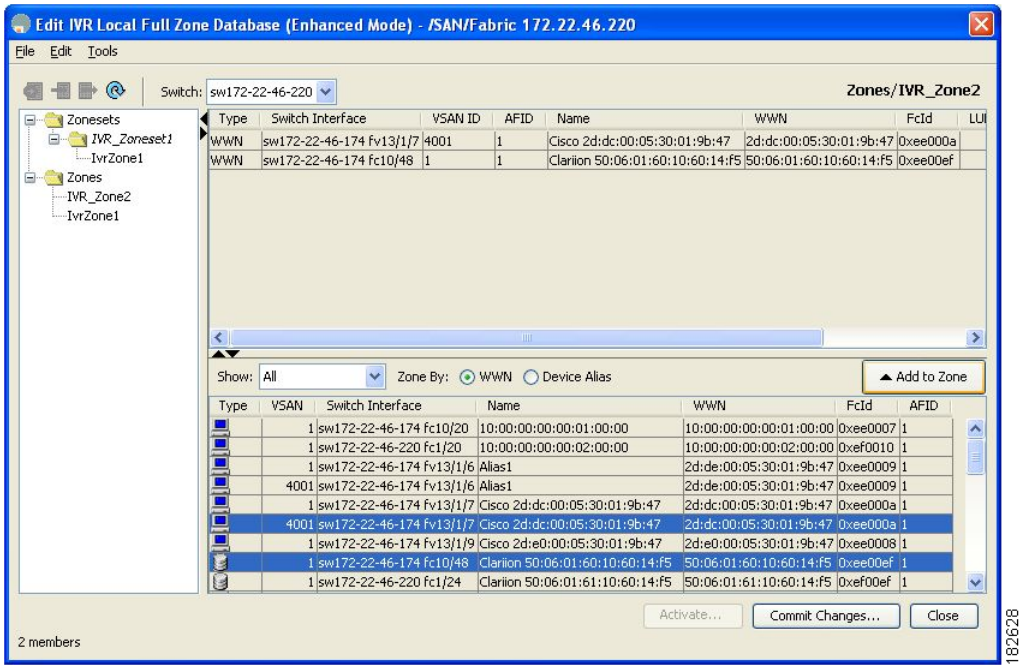
a. **Read Only**—The zone permits read and denies write.

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

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

Step 6 To add members to this zone, select the members you want to add from the Fabric pane (see Figure 29-17) and click **Add to Zone**.

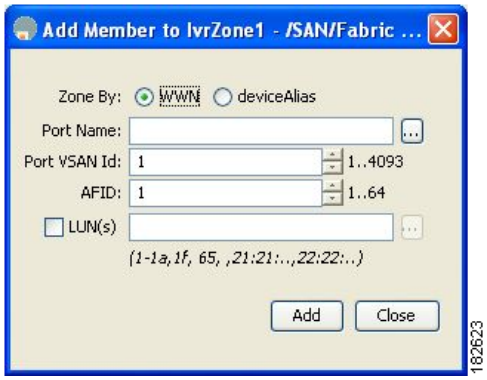
Figure 29-17 Edit IVR Local Full Zone Database Dialog Box



Step 7 Alternatively, click the zone where you want to add members and click the **Insert** icon.

You see the Add Member to Zone dialog box shown in Figure 29-18.

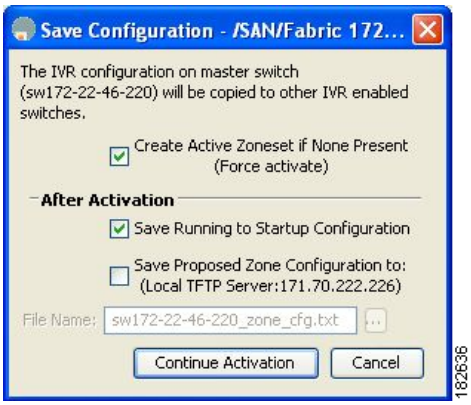
Figure 29-18 Add Member to IVR Zone Dialog Box



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

You see the Save Configuration dialog box shown in Figure 29-19.

Figure 29-19 Save Configuration Dialog Box



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

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

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

In the server.properties file, you can set the property zone.ignoreIVRZones to **true** or **false** to either hide or view IVR zones as part of regular active zones. See the "Fabric Manager Server Properties File" section on page 3-5 for more information on the server.properties file.

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

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

About Activating Zone Sets and Using the force Option

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

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

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

You can also use the force **activate** option to activate IVR zone sets. Table 29-4 lists the various scenarios with and without the force activate option.

Table 29-4 IVR Scenarios with and without the Force Activate Option.

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

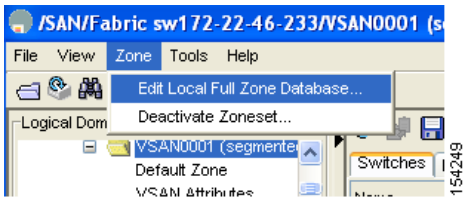
1. We recommend that you use the Case 3 scenario.

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

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

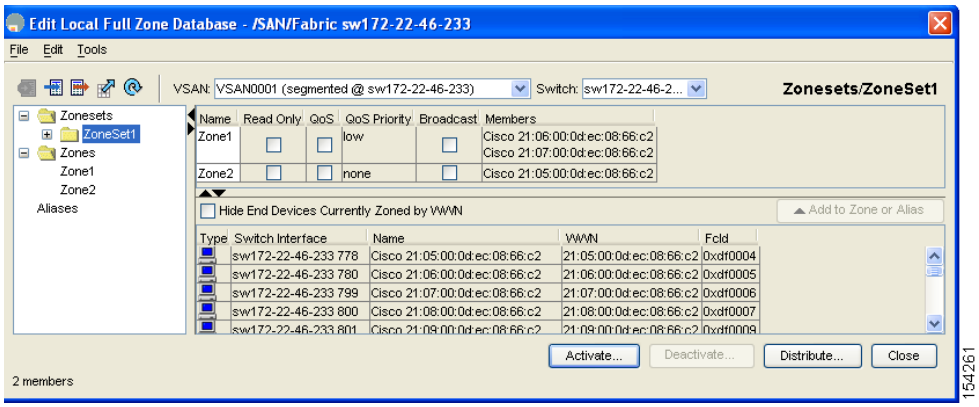
Step 1 Click **Zone** and then select **Edit Local Full Zone Database** as shown in Figure 29-20.

Figure 29-20 Zone Menu



You see the Edit Local Full Zone Database dialog box in Figure 29-21.

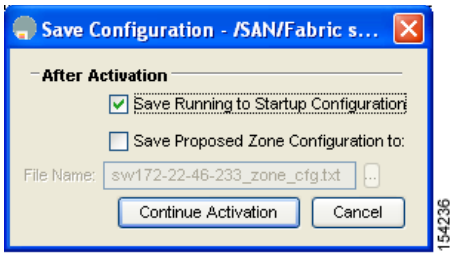
Figure 29-21 Edit Zone Database Dialog Box



Step 2 Select a **Zoneset** folder and then click **Activate** to activate the zone set (shown in Figure 29-21) or click **Deactivate** to deactivate an activated zone set.

You see the Save Configuration dialog box shown in Figure 29-22.

Figure 29-22 Save Configuration Options for a New Zone Set



Step 3 Optionally, check one of the **Save Running to Configuration** check boxes to save these changes to the startup configuration (see Figure 29-22).

Step 4 Click **Continue Activation** to activate the zone set (see Figure 29-22) or **Yes** if you are deactivating the zone set.

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

Recovering an IVR Full Zone Database

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

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

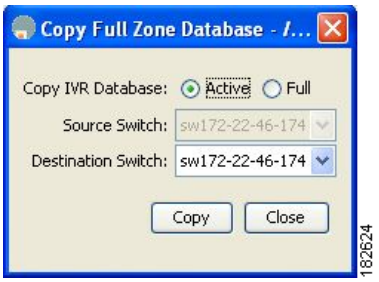
Step 1 Choose **Zone > IVR > Edit Local Full Zone Database**.

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

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

You see the Copy Full Zone Database dialog box shown in Figure 29-23.

Figure 29-23 Copy Full Zone Database Dialog Box



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

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

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

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

Recovering an IVR Full Topology

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

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

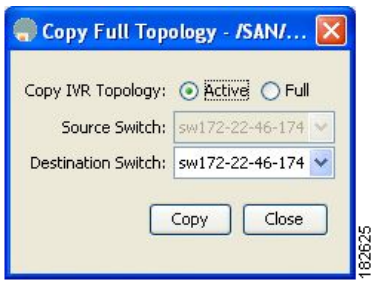
Step 1 Choose **Zone > IVR > Edit Local Full Zone Database**.

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

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

You see the Copy Full Topology dialog box shown in Figure 29-24.

Figure 29-24 Copy Full Topology Dialog Box



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

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

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

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

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 30-45.

Configuring LUNs in IVR Zoning

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

To configure LUNs in IVR zoning, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

About QoS in IVR Zones

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

Configuring QoS for IVR Zones

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

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

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

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

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

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

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

Renaming IVR Zones and IVR Zone Sets

You can rename IVR zones and IVR zone sets.

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

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

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

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

Step 3 Choose **Edit > Rename**.

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

Step 4 Enter a new name.

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

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, refer to the *Cisco MDS 9000 CLI Configuration Guide*.

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

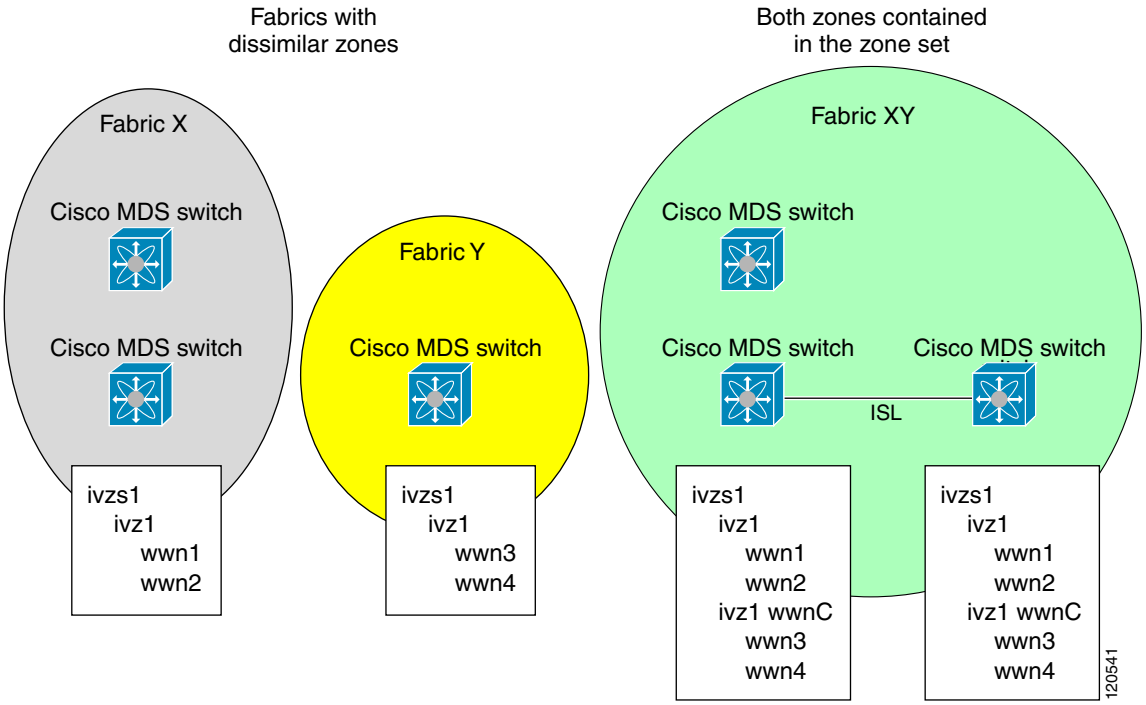
As of Cisco MDS SAN-OS Release 3.0(3), you can configure 8000 IVR zones and 20,000 IVR zone members. If you want to downgrade to a release prior to Cisco SAN-OS Release 3.0(3), the number of IVR zones cannot exceed 2000 and the number of IVR zone members cannot exceed 10,000.

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 13-9 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 29-25).

Figure 29-25 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 29-5 describes the results of a CFS merge of two IVR-enabled fabrics under different conditions.

Table 29-5 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 29-4).
- 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 29-12 and the"IVR Limits Summary" section on page 29-4).
- 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 29-13).

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

Default Settings

Table 29-6 lists the default settings for IVR parameters.

Table 29-6 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.