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 contains the following topics:

About IVR

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, like robotic tape libraries. Using IVR, resources across VSANs are accessed without compromising other VSAN benefits.

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

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.

IVR Features

IVR has 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.
- Compliant with Fibre Channel standards compliant.
- Incorporates with third-party switches--if the IVR-enabled VSANs are configured in **interop 1** mode.

IVR Terminology

The terms used in this chapter are explained in this section.

- Native VSAN—The VSAN to which an end device logs on is called a native VSAN for that end device.
- Inter-VSAN zone (IVZ)—Defines a set of end devices s 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 association. You can configure up to 200 IVZs and 2000 IVZ members on any switch in the Cisco MDS 9000 Family.
- Inter-VSAN zone sets (IVZS)—One or more IVZs make up an IVZS. You can configure up to 32 IVZSs on any switch in the Cisco MDS 9000 Family. Only one IVZS can be active at any time.
- IVR path—An IVR path is a set of switches and inter-switch links via which a frame from one 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 in which the IVR feature is enabled.
- Edge VSAN—An edge VSAN refers to a VSAN which 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 16-1, VSANs 1, 2, and 3 are edge VSANs.

  An edge VSAN for one IVR path can be a transit VSAN for another IVR path.
- Transit VSAN—Transit VSAN is a VSAN that exists along an IVR path from the source edge VSAN of that path to the destination edge VSAN of that path.

  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.
- Edge switch—A switch to which a member of an IVR zone has logged in. Edge switches are oblivious to the IVR configurations in the border switches. Edge switches need not be IVR enabled.

IVR Guidelines

Before configuring an IVR SAN fabric, consider the following guidelines:

- Configure unique domain IDs across all VSANs and switches participating in IVR operations. 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.
- An Enterprise License Package is required for this feature.

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.

IVR-enabled VSANs must be configured in **no interop** (default) mode or **interop 1** mode.

Domain ID Guidelines

Domain IDs must be unique across inter-connected VSANs. To ensure unique domain IDs across inter-connected VSAN, follow 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.

Transit VSANs Guidelines

Consider the following guidelines for transit VSANs:

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

Border Switch Guidelines

Before configuring border switches, consider the following guidelines:

- Border switches require SAN-OS Release 1.3(1) or higher.
- A border switch must be a member of two or more VSANs.
- A border switch that facilities IVR communications must be IVR enabled.

- To provide redundant paths between active IVZ members, IVR can (optionally) be enabled on additional border switches.
- The VSAN topology configuration must be updated before a border switch is added or removed.

Configuring IVR

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

Step 1 Verify that unique domain IDs are configured in all switches and VSANs participating in IVR.

Step 2 Enable IVR in the border switches.

Step 3 Create and activate the required IVR topology in all the IVR-enabled border switches.

Step 4 Create and activate IVZSs in all the IVR-enabled border switches.

Step 5 Verify the IVR configuration.

Unique Domain ID Configuration Options

You can configure domain IDs using one of two options:

- Configure allowed-domains list using the Domain Manager MIBs so that the domains in different VSANs are non-overlapping on all participating switches and VSANs.
- Configure static, non-overlapping domains (using the CLI) for each participating switch and VSAN.

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. To begin configuring the IVR feature, you must explicitly enable IVR on the required switches in the fabric.

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.

Configuring an IVR Topology

This section explains the process used to create an IVR topology.

Creating an IVR Topology

You must create the IVR topology in every IVR-enabled switch in the fabric. You can have up to 64 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 autonomous fabric ID (AF ID) which distinguishes two VSANs that are logically and physically separate, but have the same VSAN number. SAN-OS Release 1.3(1) supports only one AF ID.

The use of a single AF ID does not allow for segmented VSANs in an inter-VSAN topology.

Ensure to repeat this configuration in all IVR-enabled switches.

Transit VSANs are deduced based on your configuration The IVR feature does not have an explicit transit-VSAN configuration. In the example used above, VSAN 2 is the transit VSAN between VSANs 1 and 3.

Creating IVR Zones and Zone Sets

To create IVR zones or zone sets, perform the following steps:

Step 1 From the Fabric Manager, choose **Zone > IVR (Inter VSAN Routing) > Edit Full Database on Switch**.

The Edit VSANxxx Local Full Zones window displays for the VSAN you selected.

Step 2 Right-click the zone set or zone for that VSAN and choose **Insert** to add a zone set or zone.

If you are adding a zone set, you can activate it by clicking the **Activate** button. This configuration is distributed to the other switches in the network fabric.

Note When you confirm the activate operation, the current running configuration is saved to the startup configuration. This permanently saves any changes made to the running configuration (not just zoning changes).

Note Some time zones beginning with prefix ‘IVRZ’ and a zone set with name ‘nozoneset’ appear in logical view. The zones with prefix ‘IVRZ’ are IVR zones which get appended to regular active zones. The prefix ‘IVRZ’ is appended to active IVR zones by the system. Similarly the zone set with name ‘nozonset’ is an IVR active zone set created by system if no active zone set is available for that VSAN and if ‘ivrZoneSetActivateForce’ flag is enabled on switch. In 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.

Note Do not create a zone with prefix ‘IVRZ’ or a zone set with name ‘nozonset’. These names are used by the system for identifying IVR zones.

Creating Additional IVR Zones and Zone Sets

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

Step 1 With the Zone > IVR (Inter VSAN Routing) > Edit Full Database on Switch dialog open, right-click the Zones folder and choose **Insert** from the pop-up menu.

Step 2 Enter the zone name in the dialog box that appears and click **OK** to add the zone.

The zone is automatically added to the zone database.

Step 3 To create a zone set, right-click the ZoneSets folder in the Edit Full Database on Switch dialog, and choose **Insert**.

Step 4 Enter the zone set name in the dialog box that appears and click **OK** to add the zone set.

The zone set is automatically added to the zone database.

Activating IVR Zone Sets

Once the zone sets have been created and populated, you must activate the zone set.

To activate an IVR zone set, follow these steps:

Step 1 Right-click the zone set in the Zone > IVR (Inter VSAN Routing) > Edit Full Database on Switch dialog.

Step 2 Click **Activate**.

Note The active zone set in Edit Zone is always shown in bold, even after successful activation. This is because a member of this VSAN must be participating in IVR zoning. Since the IVR zones get added to active zones, the active zone set configuration is always different from local zone set configuration with same name.

Deactivating IVR Zone Sets

To activate a zone set, follow these steps:

Step 1 Right-click the zone set in the Zone > IVR (Inter VSAN Routing) > Edit Full Database on Switch dialog.

Step 2 Click **Deactivate**.

Recovering an IVR Full Zone Database

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

To recover an IVR zone database, perform these steps.

Step 1 From the Fabric Manager, choose **Zone > IVR (Inter VSAN Routing) > Recover Full Zone Database**. You see the Recover Full Zone Database dialog.

Step 2 Click the **Copy Active** or the **Copy Full** radio button, depending on which type of database you want to copy.

Step 3 Choose the source VSAN from which to copy the information from the drop-down list.

Step 4 If you selected Copy Full, choose the source switch and the destination VSAN from those drop-down lists.

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

Step 6 Click **Copy** to copy the database, or click **Close** to close the dialog without copying.

Recovering an IVR Full Topology

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

To recover a zone database, perform these steps.

Step 1 From the Fabric Manager, choose **Zone > IVR (Inter VSAN Routing) > Recover FullTopology**. You see the Recover Full Topology dialog box.

Step 2 Click the **Copy Full** radio button.

Step 3 Choose the source VSAN from which to copy the information from the drop-down list.

Step 4 Choose the source switch and the destination VSAN from those drop-down lists.

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

Step 6 Click **Copy** to copy the topology, or click **Close** to close the dialog without copying.

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 IVZS 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 the **interop-mode 1** option is enabled.

IVR Using LUN Zoning or Read-Only Zoning

LUN-zoning and read-only zoning can be used between members of active IVR zones. To configure this service, you need to create and activate LUN-zones and/or read-only zones between the desired IVZ members in all relevant edge VSANs using the zoning interface.

The LUN zoning and read-only zoning features cannot be configured in a IVZS setup.

Creating IVZs and IVZSs

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

The same IVZS must be activated on all the IVR-enabled switches.

Zones versus IVZs

Table 16-1 identifies the key differences between IVZs and Zones.

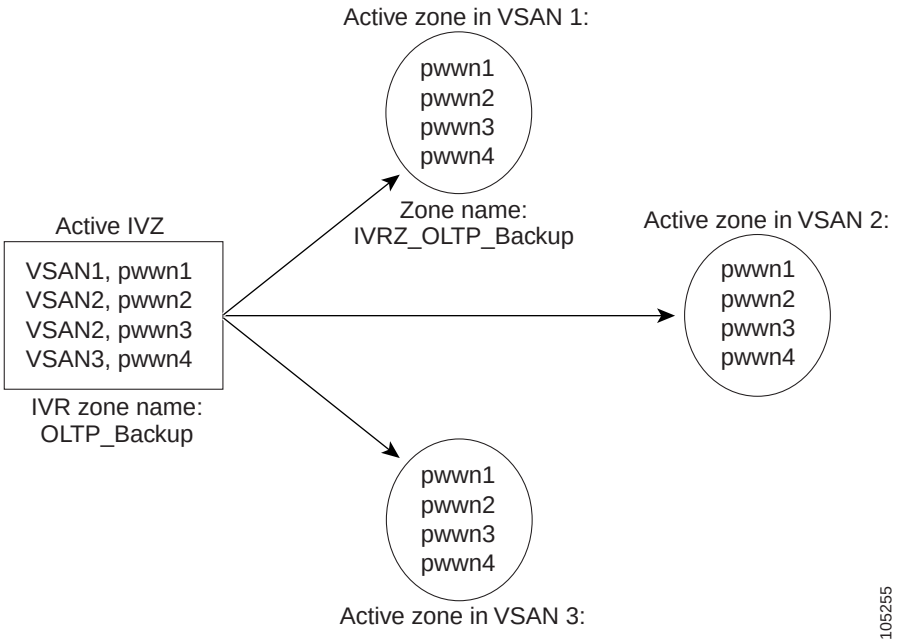
Table 16-1 Key Differences between IVZs and Zones

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

Automatic IVZ Creation

Figure 16-1 depicts an IVZ 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.

Figure 16-1 IVZ



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

The zones are created automatically by the IVR process when an IVZS 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 IVZS configuration when a new zone set is activated. Like zone sets, IVR zone sets are also activated non-disruptively.

If pwwn1 and pwwn2 are in an IVZ in the current as well as the new IVZS then activation of the new IVZS does not cause any traffic disruption between them.

Configuring and Activating IVZs and IVZSs

IVZ and IVZS names are restricted to 64 alphanumeric characters.

Using the force Option

Use the **force** option to activate the specified IVZS. Table 16-2 lists the various scenarios with and without the force option.

Table 16-2 Using the force Option

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

Using the **force** option of IVZS 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 IVZS activation will fail. However, IVZS activation will go through if the **force** option is used. Since zones are created in the edge VSANs corresponding to each IVZ, traffic may be disrupted in edge VSANs where the default zone policy is permit.

Be sure to repeat this configuration in all border switches participating in the IVR configuration.

Using the Cisco MDS Fabric Manager, you can distribute IVZ configurations to all IVR-capable switches in the interconnected VSAN network. Refer to the *Cisco MDS 9000 Family Fabric Manager User Guide* for more information.

Clearing the IVZ Database

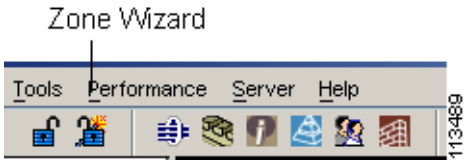
Clearing a zone set only erases the configured zone database, not the active zone database.

Using the Zone Wizard

Use the Zone Wizard to configure zones, read-only zones, and IVR zones.

Step 1 From the Fabric Manager, click the **Zone Wizard** icon in the Fabric Manager Zone toolbar.

Figure 16-2 Zone Wizard icon



The Zone Wizard displays.

Step 2 Follow the prompts in the wizard to migrate the database.