CHAPTER 14

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:

About IVR

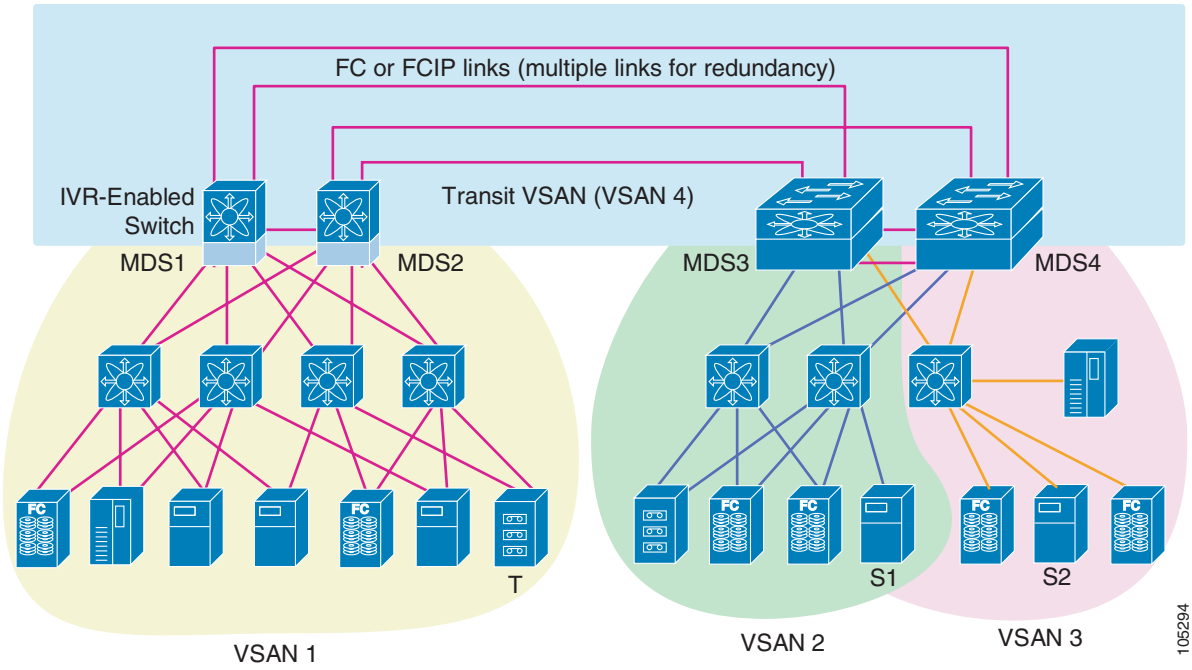
Virtual SANs (VSANs) improve storage area network (SAN) scalability, availability, and security by allowing multiple Fibre Channel SANs to share a common physical infrastructure of switches and ISLs. These benefits are derived from the separation of Fibre Channel services in each VSAN and isolation of 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 such as 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 (see Figure 14-1).

The procedure to configure this example is provided at the end of this chapter.

Figure 14-1 Traffic Continuity Using IVR and FCIP



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

- Native VSAN—The VSAN to which an end device logs on is the native VSAN for that end device.
- Inter-VSAN Zone (IVZ)—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. 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 through 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—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 14-1, 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 14-1, 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, as identified in Figure 14-1.
- 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.

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 Prior to Cisco MDS SAN-OS Release 1.3(4a), IVR-enabled VSANs can only be configured in no interop (default) mode or in interop mode 1. As of Cisco MDS SAN-OS Release 1.3(4a), IVR-enabled VSANs can be configured in no interop (default) mode or in any interop 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 VSAN 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 Cisco MDS 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.
- IVR can (optionally) be enabled on additional border switches to provide redundant paths between active IVZ members.
- 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 Configure 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 the 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 (see Chapter 24, “Configuring Domain Parameters”).

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.

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

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

Configuring 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. Cisco MDS SAN-OS Release 1.3(1) supports only one AF ID.

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

Creating an IVR Topology

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

To create an IVR topology, 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 in this switch.
Step 4	`switch(config-ivr-topology-db)# autonomous-fabric-id 1 switch 20:00:00:05:30:01:1b:c2 vsan-ranges 1-2`	Configures VSANs 1 and 2 to participate in IVR in this switch.
Step 5	`switch(config-ivr-topology-db)# end` `switch#`	Reverts to EXEC mode.

View your configured IVR topology using the **show ivr vsan-topology** command (see Example 14-1).

Example 14-1 Displays the Configured IVR Topology

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

Tip Transit VSANs are deduced based on your configuration The IVR feature does not have an explicit transit-VSAN configuration. In Example 14-1, VSAN 2 is the transit VSAN between VSANs 1 and 3.

Activating an IVR Topology

After configuring the IVR topology, you must activate it.

To activate a configured IVR topology, 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.

Caution Active IVR topologies cannot be deactivated.

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
```

Clearing the IVR Topology

You can clear a configured IVR topology using the **no ivr vsan-topology database** command in configuration mode.

Note You can replace the active IVR topology with another IVR topology configuration by issuing the **ivr vsan-topology activate** command. Active IVR topologies cannot be deactivated.

To clear a previously-created IVR topology, 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.

Adding IVR Virtual Domains

In a remote VSAN, the IVR application does not automatically add the virtual domain to the assigned domain list. Some switches (for example, the Cisco SN5428) do not query the remote name server until the remote domain appears in the assigned domain list in the fabric. In such cases, add the IVR virtual domains in a specific VSAN(s) to the assigned domain 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 the following conditions apply:
—If an IVR zone set is not active.
—If Cisco SN5428 or Qlogic SANBox switches exist in the VSAN.

Tip As of Cisco MDS SAN-OS Release1.3(4), only add IVR domains in the edge VSANs and not in transit VSANs.

To add an IVR virtual domain to 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.
Step 3	`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

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)
```

When you enable the **ivr virtual-fcdomain-add** command, links may fail to come up due to overlapping virtual domain identifiers. If so, temporarily withdraw the overlapping virtual domain from that VSAN using the **ivr withdraw domain** command in EXEC mode.

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

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 IVR zone. You can define several IVZSs and activate only one of the defined IVZSs.

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

IVZs Versus Zones

Table 14-1 identifies the key differences between IVZs and zones.

Table 14-1 Key Differences between IVZs and Zones

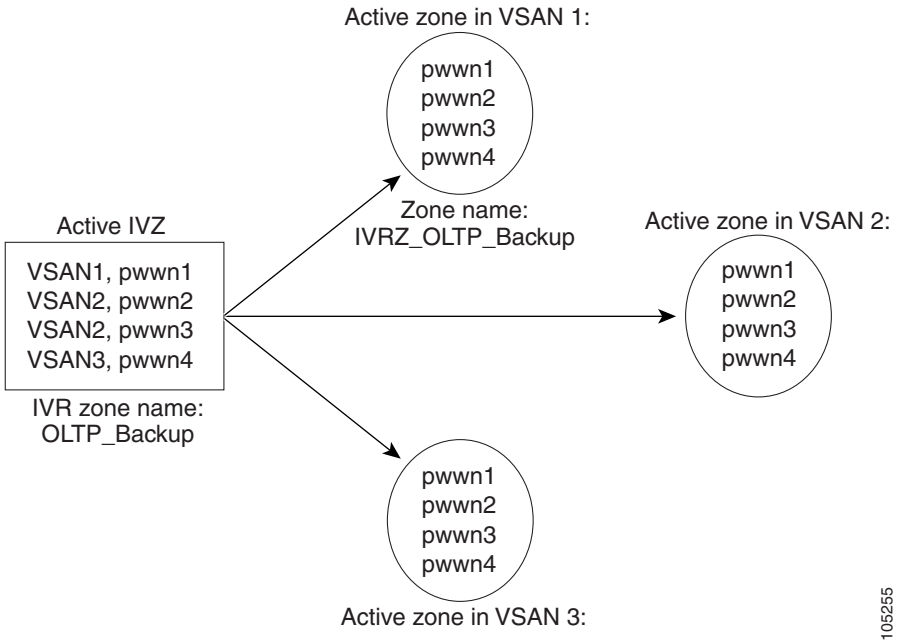
IVZs	Zones
IVZ membership is specified using the VSAN and pWWN combination.	Zone membership is specified using pWWN, fabric WWN, sWWN, or the fabric ID.
Default zone policy is always deny (not configurable).	Default zone policy is deny (configurable).

Automatic IVZ Creation

Figure 14-2 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.

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.

Figure 14-2 Creating Zones on IVZ Activation



The zones are created automatically by the IVR process when an IVZS is activated. They are not stored in 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.

Note 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.

To configure IVZs and IVZSs, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# ivr zone name Ivz_vsan2-3` `switch(config-ivr-zone)#`	Creates an IVR zone named Ivz_vsan2-3.

	Command	Purpose
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 IVZ 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 IVZ member.
Step 5	`switch(config-ivr-zone)# exit` `switch(config)#`	Reverts to configuration mode.
Step 6	`switch(config)# ivr zone name Ivz_vsan4-5` `switch(config-ivr-zone)#`	Creates an IVR zone named Ivz_vsan2-3.
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 IVZ 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 IVZ 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 IVZ 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_zone set1.
Step 12	`switch(config-ivr-zoneset)# member Ivz_vsan2-3`	Adds the Ivz_vsan2-3 IVZ as an IVZS member.
Step 13	`switch(config-ivr-zoneset)# member Ivz_vsan4-5`	Adds the Ivz_vsan4-5 IVZ as an IVZS member.
Step 14	`switch(config-ivr-zoneset)# exit` `switch(config)`	Returns to configuration mode.
Step 15	`switch(config)# ivr zoneset activate name IVR_ZoneSet1`	Activates the newly created IVZS.
	`switch(config)# ivr zoneset activate name IVR_ZoneSet1 force`	Forcefully activates the specified IVZS.
	`switch(config)# no ivr zoneset activate name IVR_ZoneSet1`	Deactivates the specified IVZS.
Step 16	`switch(config-ivr-zoneset)# end` `switch#`	Returns to EXEC mode.

Using the force Option

Use the **force** option to activate the specified IVZS. Table 14-2 lists the various scenarios with and without the **force** option.

Table 14-2 IVR Scenarios with and without the force Option.

Case	Default Zone Policy	Active Zone Set before IVR Zone Activation	`force` Option Used?	IVZS 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 you use the Case 3 scenario.

Caution 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. Because 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`.

Displaying IVZ Configurations

View your IVZ configuration using the **show ivr zone** command.

```
switch# show ivr zone

zone name Ivz_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 Ivz_vsan4-5
    pwwn 21:00:00:e0:8b:06:d9:1d vsan 4
    pwwn 21:01:00:e0:8b:2e:80:93 vsan 4
    pwwn 10:00:00:00:c9:2d:5a:dd vsan 5
```

View your IVZS configuration using the **show ivr zoneset** command.

```
switch# show ivr zoneset

zoneset name ivr_qa_zs_all
   zone name Ivz_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 Ivz_vsan4-5
        pwwn 21:00:00:e0:8b:06:d9:1d vsan 4
        pwwn 21:01:00:e0:8b:2e:80:93 vsan 4
        pwwn 10:00:00:00:c9:2d:5a:dd vsan 5
```

Use the **show ivr zoneset active** command to view your active IVZS status (see Example 14-2).

Example 14-2 Displays the Active IVZS Status

```
switch# show ivr zoneset active
zoneset name ivr_qa_zs_all
   zone name Ivz_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 Ivz_vsan4-5
      pwwn 21:00:00:e0:8b:06:d9:1d vsan 4
    * pwwn 21:01:00:e0:8b:2e:80:93 vsan 4
                  pwwn 10:00:00:00:c9:2d:5a:dd vsan 5
```

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

Note 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 Configuration Guide*.

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 one of the **interop** modes is enabled.

See the "Configuring the Switch for Interoperability" section on page 29-21.

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.

Clearing the IVZ Database

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

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

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

This command clears all configured IVZ 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.

Specifying 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.

Use the **show logging level** command to view the configured logging level for the IVR feature (see Example 14-3).

Example 14-3 Displays IVR Logging Levels

```
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)
```

Displaying IVR Information

You can verify IVR information by using the **show ivr** set of commands. If you request information for a specific object (for example, a specific zone, zone set, VSAN, alias, or even a keyword like **brief** or **active**), only information for the specified object is displayed. If you do not request specific information, all available information is displayed. See Examples 14-4 to 14-15.

Example 14-4 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
```

The * indicates the local switch.

Example 14-5 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 14-6 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
```

Example 14-7 Displays the IVZ Configuration

```
switch# show ivr zone
zone name Ivz_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 14-8 Displays the Active IVZS Configuration

```
switch# show ivr zoneset active
zoneset name IVR_ZoneSet1
  zone name Ivz_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 14-9 Displays Information for a Specified IVZ

```
switch# show ivr zone name Ivz_vsan2-3
zone name Ivz_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 14-10 Displays the Specified Zone in the Active IVZS

```
switch# show ivr zone name Ivz_vsan2-3 active
zone name Ivz_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 14-11 Displays the IVZS 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 Ivz_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 14-12 Displays Brief Information for an IVR VSAN Topology

```
switch# show ivr zoneset brief Active
zoneset name IVR_ZoneSet1
  zone name Ivz_vsan2-3
```

Example 14-13 Displays Brief Information for the Active IVZS

```
switch# show ivr zoneset brief Active
zoneset name IVR_ZoneSet1
  zone name Ivz_vsan2-3
```

Example 14-14 Displays Status Information for the IVZ

```
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
```

Example 14-15 Displays the Specified Zone Set

```
switch# show ivr zoneset name IVR_ZoneSet1
zoneset name IVR_ZoneSet1
  zone name Ivz_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

Sample Configuration

This section provides the configuration steps to configure the example illustrated in Figure 14-1.

Step 1 Enable IVR.

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

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 :
```

Step 3 Configure the IVR VSAN-topology. In Figure 14-1, two of the four IVR-enabled switches are members of VSANs 1 and 4. The other two switches are members of VSANs 2, 3, and 4.

```
mds# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
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
```

Step 4 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 5 Activate the configured VSAN topology.

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

Step 6 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 7 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 taepe_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 8 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 9 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 10 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
```

Step 11 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 12 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
```

Default Settings

Table 14-3 lists the default settings for IVR parameters.

Table 14-3 Default IVR Parameters

Parameters	Default
IVR feature	Disabled.
IVR VSANs	Not added to virtual domains.