

Basic Inter-VSAN Routing Configuration

This chapter describes the Inter-VSAN Routing (IVR) feature and provides basic instructions on sharing resources across VSANs using IVR management interfaces. After setting up a basic IVR configuration, see Advanced Inter-VSAN Routing Configuration if you need to set up an advanced IVR configuration.

- About Inter-VSAN Routing, on page 1
- Basic IVR Configuration Task List, on page 4
- Basic IVR Configuration, on page 5
- IVR Virtual Domains, on page 13
- IVR Zones and IVR Zone Sets, on page 15
- IVR Logging, on page 22
- Database Merge Guidelines, on page 23
- IVR Auto Topology Mode Configuration Example, on page 25
- Default Settings , on page 29

About Inter-VSAN Routing

Virtual SANs (VSANs) improve storage area network (SAN) scalability, availability, and security by allowing multiple Fibre Channel SANs to share a common physical infrastructure of switches and ISLs. These benefits are derived from the separation of Fibre Channel services in each VSAN and the isolation of traffic between VSANs. Data traffic isolation between the VSANs also inherently prevents sharing of resources attached to a VSAN, such as robotic tape libraries. Using IVR, you can access resources across VSANs without compromising other VSAN benefits.

IVR Features

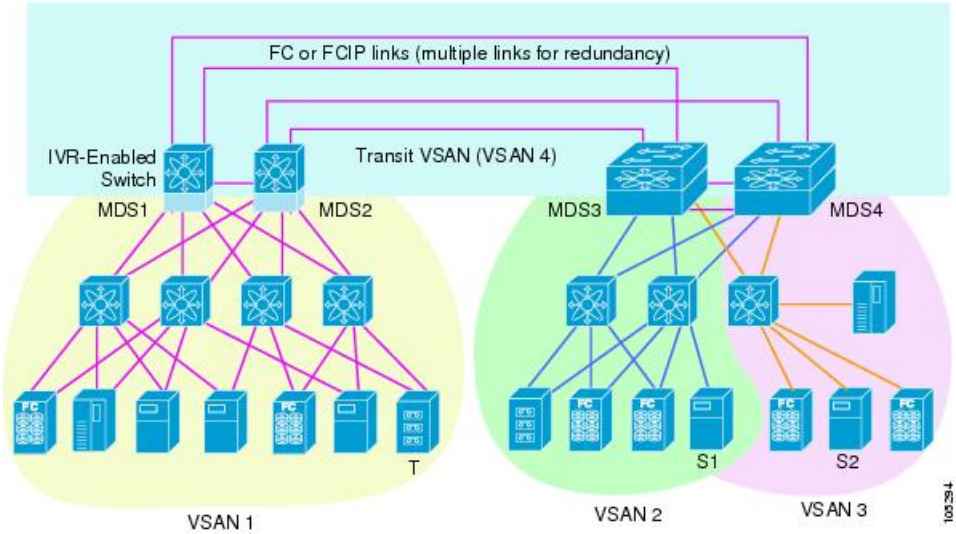
IVR supports the following features:

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

- Provides efficient business continuity or disaster recovery solutions when used in conjunction with FCIP. See the figure, Traffic Continuity Using IVR and FCIP.
- Is in compliance with Fibre Channel standards.
- Incorporates third-party switches, however, IVR-enabled VSANs may need to be configured in one of the interop modes.

Note To configure the sample scenario shown in the following figure, follow the steps in IVR Auto Topology Mode Configuration Example.

Figure 1: Traffic Continuity Using IVR and FCIP



IVR Terminology

The following IVR-related terms are used in the IVR documentation:

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

- Edge VSAN—A VSAN that initiates (source edge-VSAN) or terminates (destination edge-VSAN) an IVR path. Edge VSANs may be adjacent to each other or they may be connected by one or more transit VSANs. VSANs 1, 2, and 3 (see Figure 1: Traffic Continuity Using IVR and FCIP, on page 2), are edge VSANs.

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

- Transit VSAN—A VSAN that exists along an IVR path from the source edge VSAN of that path to the destination edge VSAN of that path. VSAN 4 is a transit VSAN(see Figure 1: Traffic Continuity Using IVR and FCIP, on page 2).

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

- Border switch—An IVR-enabled switch that is a member of two or more VSANs. Border switches, such as the IVR-enabled switch between VSAN 1 and VSAN 4(see Figure 1: Traffic Continuity Using IVR and FCIP, on page 2), span two or more different color-coded VSANs.
- Edge switch—A switch to which a member of an IVR zone has logged in to. Edge switches are unaware of the IVR configurations in the border switches. Edge switches do not need to be IVR-enabled.
- Autonomous Fabric Identifier (AFID)—Allows you to configure more than one VSAN in the network with the same VSAN ID and avoid downtime when configuring IVR between fabrics that contain VSANs with the same ID.
- Service group—Allows you to reduce the amount of IVR traffic to non-IVR-enabled VSANs by configuring one or more service groups that restrict the traffic to the IVR-enabled VSANs.

IVR Configuration Limits

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

Fibre Channel Header Modifications

IVR virtualizes the remote end devices in the native VSAN using a virtual domain. When IVR is configured to link end devices in two disparate VSANs, the IVR border switches are responsible for modifying the Fibre Channel headers for all communication between the end devices. The sections of the Fibre Channel frame headers that are modified include:

- VSAN number
- Source FCID
- Destination FCID

When a frame travels from the initiator to the target, the Fibre Channel frame header is modified such that the initiator VSAN number is changed to the target VSAN number. If IVR Network Address Translation (NAT) is enabled, then the source and destination FCIDs are also translated at the edge border switch. If IVR NAT is not enabled, then you must configure unique domain IDs for all switches involved in the IVR path.

IVR Network Address Translation

To use IVR NAT, it must be enabled on all IVR-enabled switches in the fabric. For information on distributing the IVR configuring using CFS, see Distributing the IVR Configuration Using CFS, on page 6. By default, IVR NAT and IVR configuration distributions are disabled on all switches in the Cisco MDS 9000 Family.

See About IVR NAT and IVR Auto Topology Mode, on page 8 for information on IVR requirements and guidelines as well as configuration information.

IVR VSAN Topology

IVR uses a configured IVR VSAN topology to determine how to route traffic between the initiator and the target across the fabric.

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

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

When IVR auto topology mode is enabled, it starts with the previously active IVR manual topology if it exists, and then the discovery process begins. New, alternate, or better paths my be discovered. If the traffic is switched to an alternate or better path, there may be temporary traffic disruptions that are normally associated with switching paths.



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

IVR Interoperability

When using the IVR feature, all border switches in a fabric must be Cisco MDS switches. However, other switches in the fabric may be non-MDS switches. For example, end devices that are members of the active IVR zone set may be connected to non-MDS switches. Non-MDS switches may also be present in the transit VSAN(s) or in the edge VSANs if one of the interop modes is enabled.

For additional information on switch interoperability, refer to the *Cisco Data Center Interoperability Support Matrix* .

Basic IVR Configuration Task List

To configure IVR, follow these steps:

Procedure

Step 1 See Enabling IVR NAT, on page 11

Enable IVR NAT.

Step 2 See Enabling IVR , on page 5.

Enable IVR on all border switches.

Step 3 See Distributing the IVR Configuration Using CFS, on page 6.

Enable IVR distribution.

Step 4 See About IVR NAT and IVR Auto Topology Mode, on page 8 .

Enable IVR auto topology mode.

Step 5 Configure IVR virtual domains.

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

Configure and activate zone sets.

Step 7 See Committing the Changes, on page 7.

Commit the IVR configuration.

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

Verify the IVR configuration.

Basic IVR Configuration

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

Enabling IVR

The IVR feature must be enabled in all border switches in the fabric that participate in the IVR. By default, this feature is disabled in all Cisco MDS 9000 Series switches. You can manually enable IVR on all required switches in the fabric or configure fabric-wide distribution of the IVR configuration. See Distributing the IVR Configuration Using CFS, on page 6.

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

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

Procedure

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Enables IVR NAT on the switch.

switch(config)# **ivr nat**

Step 3 Enables IVR on the switch.

switch(config)# **feature ivr**

Step 4 Disables (default) IVR on the switch.

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

Distributing the IVR Configuration Using CFS

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

The following configurations are distributed:

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



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

Database Implementation

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

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

Enabling Configuration Distribution

To enable IVR configuration distribution, follow these steps:

Procedure

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Enables IVR distribution.

switch(config)# **ivr distribute**

Step 3 Disables (default) IVR distribution.

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

Locking the Fabric

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

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

Committing the Changes

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

To commit IVR configuration changes, follow these steps:

Procedure

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Commits the IVR changes.

switch(config)# **ivr commit**

Discarding the Changes

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

To discard IVR configuration changes, follow these steps:

Procedure

Step 1 Enters configuration mode.

switch# **config t**

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

switch(config)# **ivr abort**

Clearing a Locked Session

If you have performed an IVR task and have forgotten to release the lock by either committing or discarding the changes, an administrator can release the lock from any switch in the fabric. If the administrator performs this task, your changes to the pending database are discarded and the fabric lock is released.

Tip The pending database is only available in the volatile directory and is subject to being discarded if the switch is restarted.

To use administrative privileges and release a locked DPVM session, use the **clear ivr session** command in EXEC mode.

```
switch# clear ivr session
```

About IVR NAT and IVR Auto Topology Mode

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

- Configure IVR only in the relevant switches.
- Enable CFS for IVR on all switches in the fabric.
- Verify that all switches in the fabric are running Cisco MDS SAN-OS Release 2.1(1a) or later.
- Acquire a mandatory Enterprise License Package or SAN-EXTENSION license package if you have Cisco MDS SAN-OS Release 2.1(1a) or later and one active IPS card for this feature. For information on licensing, refer to the *Cisco MDS 9000 Series Licensing Guide* .

Note The IVR over FCIP feature is bundled with the Cisco MDS 9216i Switch and does not require the SAN extension over IP package for the fixed IP ports on the supervisor module.

Tip If you change any FSPF link cost, ensure that the FSPF path distance (that is, the sum of the link costs on the path) of any IVR path is less than 30,000.

Note IVR-enabled VSANs can be configured when the interop mode is enabled (any interop mode) or disabled (no interop mode).

IVR NAT Requirements and Guidelines

The requirements and guidelines for using IVR NAT are listed below:

- IVR NAT port login (PLOGI) requests that are received from hosts are delayed a few seconds to perform the rewrite on the FC ID address. If the host's PLOGI timeout value is set to a value less than five seconds, it may result in the PLOGI being unnecessarily terminated and the host being unable to access the target. We recommend that you configure the host bus adapter for a timeout of at least ten seconds (most HBAs default to a value of 10 or 20 seconds).
- IVR NAT requires Cisco MDS SAN-OS Release 2.1(1a) or later on all IVR switches in the fabric.
- IVR non-NAT mode is not supported from Cisco NX-OS Release 5.2(x) and later releases. If you have IVR non-NAT mode configured, see the Migrate to IVR NAT section for instructions on how to migrate to IVR NAT mode.
- IVR NAT allows you to set up IVR in a fabric without needing unique domain IDs on every switch in the IVR path. IVR NAT virtualizes the switches in other VSANs by using local VSAN for the destination IDs in the Fibre Channel headers. In some Extended Link Service message types, the destination IDs are included in the packet data. In these cases, IVR NAT replaces the actual destination ID with the virtualized destination ID. IVR NAT supports destination ID replacement in the Extended Link Service messages described in the following table.

Table 1: Extended Link Service Messages Supported by IVR NAT

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

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

- If you have a message that is not recognized by IVR NAT and contains the destination ID in the packet data, you cannot use IVR with NAT in your topology.



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

Transit VSAN Guidelines

Consider the following guidelines for transit VSANs:

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

Border Switch Guidelines

Before configuring border switches, consider the following guidelines:

- Border switches require Cisco MDS SAN-OS Release 2.1(1a) or later.
- A border switch must be a member of two or more VSANs.
- A border switch that facilitates IVR communications must be IVR-enabled.
- IVR can (optionally) be enabled on additional border switches to provide redundant paths between active IVR zone members.
- The VSAN topology configuration updates automatically when a border switch is added or removed.

Enabling IVR NAT

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

To enable IVR NAT, follow these steps:

Procedure

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Enables IVR NAT on the switch.

switch(config)# **ivr nat**

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

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

Enabling IVR Auto Topology Mode



Note IVR configuration distribution must be enabled before configuring IVR auto topology mode (see Distributing the IVR Configuration Using CFS, on page 6). Once IVR auto topology mode is enabled, you cannot disable IVR configuration distribution.

To enable IVR auto topology mode, follow these steps:

Procedure

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Enables IVR auto topology mode.

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

What to do next

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

```
switch# show ivr vsan-topology

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


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

Note The asterisk (*) indicates the local switch.

Migrate to IVR NAT mode

The purpose of this task is to enable and distribute Inter-VSAN Routing (IVR) configurations across all IVR-enabled switches using Cisco Fabric Services (CFS), ensuring consistent and efficient fabric-wide configuration for seamless inter-VSAN communication.

This task is performed to configure and enable the Interactive Voice Response (IVR) system, which allows automated voice interactions and announcements within the network environment, ensuring proper setup and integration with dependent applications and services.

Procedure

Step 1 Enter the configuration mode.

Example:

```
switch# config t
```

Step 2 Deactivate IVR zoneset.

Example:

```
switch(config)# no ivr zoneset activate name IVR_Zoneset force
```

Step 3 Enable IVR NAT.

Example:

```
switch(config)# ivr nat
```

Step 4 Activate IVR zoneset.

Example:

```
switch(config)# ivr zoneset activate name IVR_Zoneset force
```

Step 5 Commit changes across the IVR fabric.

Example:

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

This task ensures proper migration to IVR NAT mode, which is required since IVR non-NAT mode is deprecated and not supported from NX-OS Release 5.2(x) onwards. The update also includes guidance on stopping dependent applications and using CFS distribution for configuration consistency across switches.

IVR Virtual Domains

In a remote VSAN, the IVR application does not automatically add the virtual domain to the assigned domains list. Some switches (for example, the Cisco SN5428 switch) do not query the remote name server until the remote domain appears in the assigned domains list in the fabric. In such cases, add the IVR virtual domains in a specific VSAN to the assigned domains list in that VSAN. When adding IVR domains, all IVR virtual domains that are currently present in the fabric (and any virtual domain that is created in the future) will appear in the assigned domains list for that VSAN.

Tip Be sure to add IVR virtual domains if Cisco SN5428 or MDS 9020 switches exist in the VSAN.

When you enable the IVR virtual domains, links may fail to come up due to overlapping virtual domain identifiers. If this occurs, temporarily withdraw the overlapping virtual domain from that VSAN.

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

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

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

Manually Configuring IVR Virtual Domains

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

Procedure

Step 1 Enters configuration mode.

switch# **config t**

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

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

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

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

Manually Configuring Fabric-wide IVR Virtual Domains



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

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

Procedure

Step 1 Enters configuration mode.

switch# **config t**

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

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

Step 3 Commits the fabric-wide configuration.

switch(config)# **ivr commit**

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

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

Verifying an IVR Virtual Domain Configuration

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

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

Clearing an IVR fcdomain Database

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

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

IVR Zones and IVR Zone Sets

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

About IVR Zones

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

Note The same IVR zone set must be activated on all of the IVR-enabled switches.

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

Table 2: Key Differences Between IVR Zones and Zones

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

IVR Zone Limits and Image Downgrading Considerations

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

Table 3: IVR Zone Limits

Cisco Release	IVR Zone Limit	IVR Zone Member Limit	IVR Zone Set Limit
SAN-OS Release 3.0(3 or later	8000	20,000	32
SAN-OS Release 3.0(2b) or earlier	2000	10,000	32

Note A zone member is counted twice if it exists in two zones. See Database Merge Guidelines, on page 23.

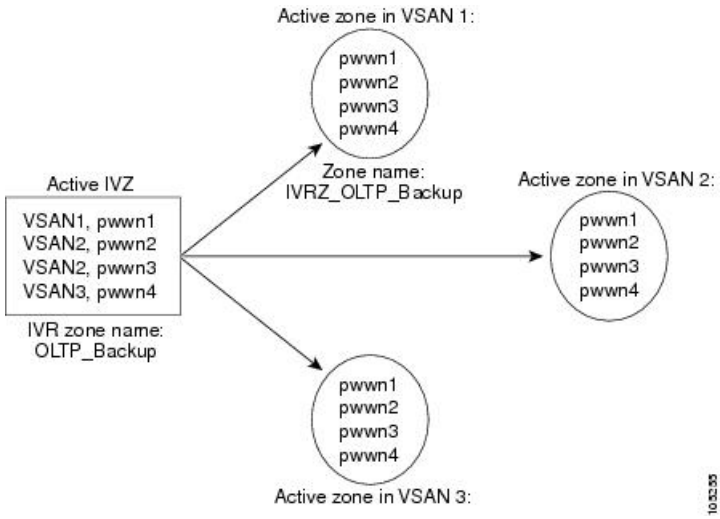
Caution If you want to downgrade to a release prior to Cisco SAN-OS Release 3.0(3), the number of IVR zones cannot exceed 2000 and the number of IVR zone members cannot exceed 10,000.

Automatic IVR Zone Creation

The following figure depicts an IVR zone consisting of four members. To allow pwwn1 to communicate with pwwn2, they must be in the same zone in VSAN 1, as well as in VSAN 2. If they are not in the same zone, then the hard-zoning ACL entries will prohibit pwwn1 from communicating with pwwn2.

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

Figure 2: Creating Zones Upon IVR Zone Activation



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

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

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

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

Configuring IVR Zones and IVR Zone Sets

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

Procedure

Step 1 Enters configuration mode.
switch# **config t**

Step 2 Creates an IVR zone named sample_vsan2-3.
switch(config)# **ivr zone name sample_vsan2-3**

Step 3 Adds the specified pWWN in VSAN 3 as an IVR zone member.
switch(config-ivr-zone)# **member pwwn 21:00:00:e0:8b:02:ca:4a vsan 3**

Step 4 Adds the specified pWWN in VSAN 2 as an IVR zone member.
switch(config-ivr-zone)# **member pwwn 21:00:00:20:37:c8:5c:6b vsan 2**

Step 5 Returns to configuration mode.
switch(config-ivr-zone)# **exit**

Step 6 Creates an IVR zone named sample_vsan4-5.
switch(config)# **ivr zone name sample_vsan4-5**

Step 7 Adds the specified pWWN in VSAN 4 as an IVR zone member.
switch(config-ivr-zone)# **member pwwn 21:00:00:e0:8b:06:d9:1d vsan 4**

Step 8 Adds the specified pWWN in VSAN 4 as an IVR zone member.
switch(config-ivr-zone)# **member pwwn 21:01:00:e0:8b:2e:80:93 vsan 4**

Step 9 Adds the specified pWWN in VSAN 5 as an IVR zone member.
switch(config-ivr-zone)# **member pwwn 10:00:00:00:c9:2d:5a:dd vsan 5**

Step 10 Returns to configuration mode.
switch(config-ivr-zone)# **exit**

Step 11 Creates an IVR zone set named Ivr_zoneset1.
switch(config)# **ivr zoneset name Ivr_zoneset1**

Step 12 Adds the sample_vsan2-3 IVR zone as an IVR zone set member.
switch(config-ivr-zoneset)# **member sample_vsan2-3**

Step 13 Adds the sample_vsan4-5 IVR zone as an IVR zone set member.
switch(config-ivr-zoneset)# **member sample_vsan4-5**

Step 14 Returns to configuration mode.

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

Step 15 Activates the newly created IVR zone set.

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

Step 16 Forcefully activates the specified IVR zone set.

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

Step 17 Deactivates the specified IVR zone set.

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

Step 18 Returns to EXEC mode.

switch(config)# **end**

About Activating Zone Sets and Using the force Option

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

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

Note

- If IVR and iSLB are enabled in the same fabric, at least one switch in the fabric must have both features enabled. Any zoning-related configuration or activation operation (for normal zones, IVR zones, or iSLB zones) must be performed on this switch. Otherwise, traffic might be disrupted in the fabric.
- If a segmented VSAN is present in an IVR topology, then the IVR zone set will not be activated.

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

Table 4: IVR Scenarios with and without the force Command

Case	Default Zone Policy	Active Zone Set before IVR Zone Activation	force command Option Used?	IVR Zone Set Activation Status	Active IVR Zone Created?	Possible Traffic Disruption
1	Deny	No active zone set	No	Failure	No	No
2			Yes	Success	Yes	No

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

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

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

Activating or Deactivating IVR Zone Sets

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

Procedure

Step 1 Enters configuration mode.

switch# **config t**

Step 2 Activates the newly created IVR zone set.

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

Step 3 Forcefully activates the specified IVR zone set.

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

Step 4 Deactivates the specified IVR zone set.

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

What to do next

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

Verifying IVR Zone and IVR Zone Set Configuration

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

Displays the IVR Zone Configuration

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

Displays Information for a Specified IVR Zone

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

Displays the Specified Zone in the Active IVR Zone

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

Displays the IVR Zone Set Configuration

```
switch# show ivr zoneset
zoneset name ivr_qa_zs_all
  zone name ivr_qa_z_all
    pwwn 21:00:00:e0:8b:06:d9:1d vsan 1
    pwwn 21:01:00:e0:8b:2e:80:93 vsan 4
    pwwn 10:00:00:00:c9:2d:5a:dd vsan 1
    pwwn 10:00:00:00:c9:2d:5a:de vsan 2
    pwwn 21:00:00:20:37:5b:ce:af vsan 6
    pwwn 21:00:00:20:37:39:6b:dd vsan 6
    pwwn 22:00:00:20:37:39:6b:dd vsan 3
```

```
    pwwn 22:00:00:20:37:5b:ce:af vsan 3
    pwwn 50:06:04:82:bc:01:c3:84 vsan 5
zoneset name IVR_ZoneSet1
  zone name sample_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

Displays the Active IVR Zone Set Configuration

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

Displays the Specified IVR Zone Set Configuration

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

Displays Brief Information for All IVR Zone Sets

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

Displays Brief Information for the Active IVR Zone Set

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

Displays Status Information for the IVR Zone Set

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

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

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

Clearing the IVR Zone Database

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

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

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

This command clears all configured IVR zone information.

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

IVR Logging

You can configure Telnet or SSH logging for the IVR feature. For example, if you configure the IVR logging level at level 4 (warning), then messages with a severity level of 4 or above are displayed. Use the instructions in this section to configure and verify the logging levels:

Configuring IVR Logging Severity Levels

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

Procedure

Step 1 Enters configuration mode.

switch# **config t**

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

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

Verifying Logging Level Configuration

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

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

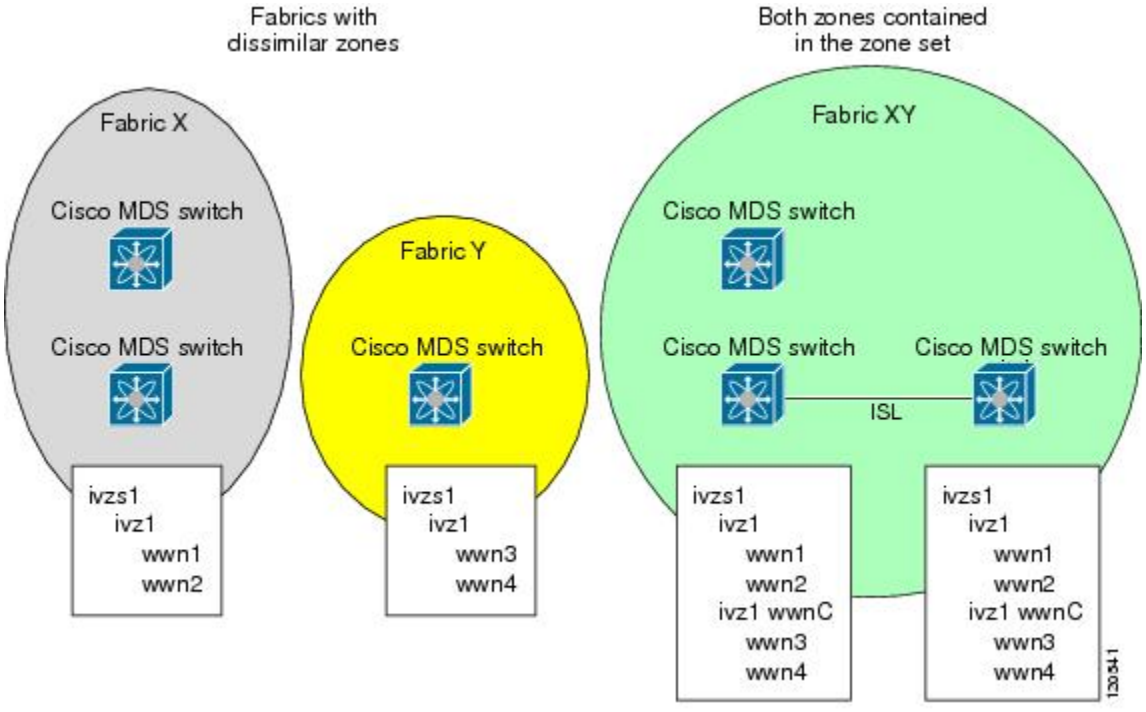
Database Merge Guidelines

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

Consider the following when merging two IVR fabrics:

- The IVR configurations are merged even if two fabrics contain different configurations.
- If dissimilar zones exist in two merged fabrics, the zone from each fabric is cloned in the distributed zone set with appropriate names.

Figure 3: Fabric Merge Consequences



- You can configure different IVR configurations in different Cisco MDS switches.

- To avoid traffic disruption, after the database merge is complete, the configuration is a combination of the configurations that were present on the two switches involved in the merge.
  - The configurations are merged even if both fabrics have different configurations.
  - A combination of zones and zone sets are used to get the merged zones and zone sets. If a dissimilar zone exists in two fabrics, the dissimilar zones are cloned into the zone set with appropriate names so both zones are present.
  - The merged topology contains a combination of the topology entries for both fabrics.
  - The merge will fail if the merged database contains more topology entries than the allowed maximum.
  - The total number of VSANs across the two fabrics cannot exceed 128.



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

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



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

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



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

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

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

Table 5: Results of Merging Two IVR-Enabled Fabrics

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

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

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

Resolving Database Merge Failures

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

- **show ivr merge status**
- **show cfs merge status name ivr**
- **show logging last** *lines* (and look for MERGE failures)

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

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

IVR Auto Topology Mode Configuration Example

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

Procedure

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

Example:

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

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

Example:

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

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

Example:

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

Step 4 Enable IVR auto topology mode.

Example:

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

Step 5 Commit the change to the fabric.

Example:

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

Step 6 Verify the status of the commit request.

Example:

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

Step 7 Verify the active IVR auto topology.

Example:

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

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

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

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

Example:

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

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

Example:

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

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

Example:

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

```
  zone name $default_zone$ vsan 1
```

Step 11 Activate the configured IVR zone set.

Example:

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

Step 12 Verify the IVR zone set activation.

Example:

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

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

Example:

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

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

  zone name IVRZ_tape_server2 vsan 1
    pwwn 10:02:50:45:32:20:7a:52
    pwwn 10:00:ad:51:78:33:f9:86

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

__________________
     vsan     status
     ____     ______
     1        active
```

Default Settings

The following table lists the default settings for IVR parameters.

Table 6: Default IVR Parameters

Parameters	Default
IVR feature	Disabled
IVR VSANs	Not added to virtual domains
IVR NAT	Disabled
QoS for IVR zones	Low
Configuration distribution	Disabled