CHAPTER 18

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

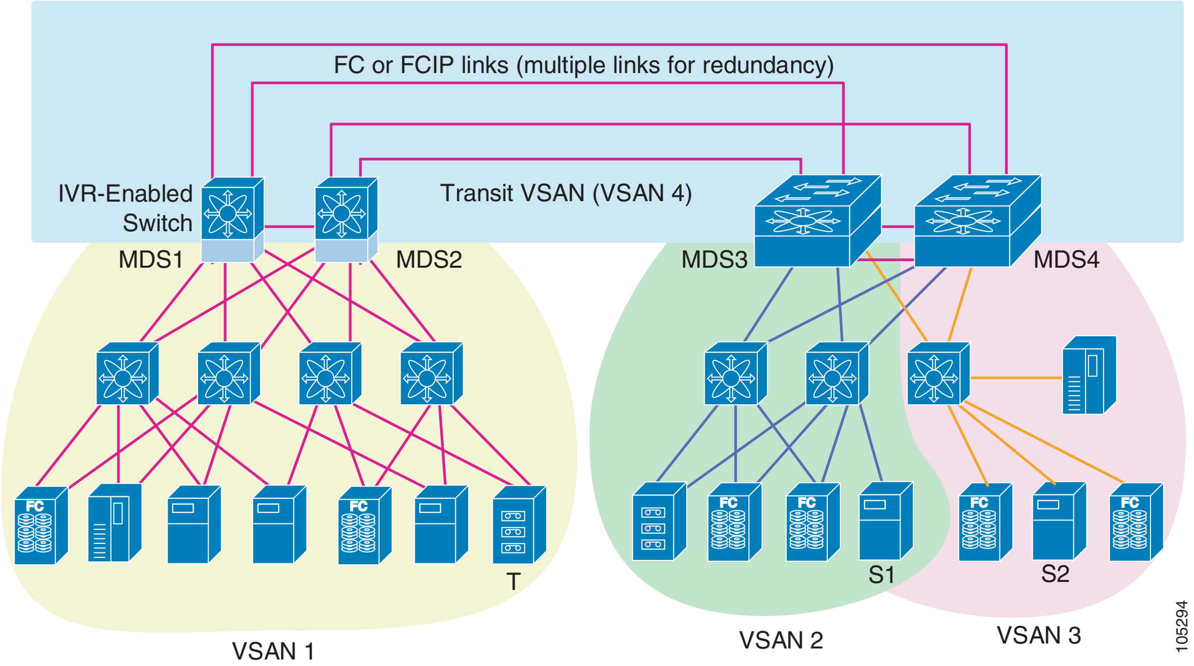
Virtual SANs (VSANs) improve storage area network (SAN) scalability, availability, and security by allowing multiple Fibre Channel SANs to share a common physical infrastructure of switches and ISLs. These benefits are derived from the separation of Fibre Channel services in each VSAN and isolation of traffic between VSANs. Data traffic isolation between the VSANs also inherently prevents sharing of resources attached to a VSAN, such as robotic tape libraries. Using IVR, you can access resources across VSANs 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. Fibre Channel control traffic does not flow between VSANs, and initiators cannot access any resource across VSANs other than the resources designated.

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 18-1).

Note See the "Example Configurations" section on page 18-31 for procedures to configure the sample scenario shown in Figure 18-1.

Figure 18-1 Traffic Continuity Using IVR and FCIP



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

IVR Features

IVR supports the following features:

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

IVR Terminology

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

- Native VSAN—The VSAN to which an end device logs on is the native VSAN for that end device.
- Current VSAN—The VSAN currently being configured for IVR.
- Inter-VSAN 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 the switches in the network. As of Cisco MDS SAN-OS Release 2.1(1a), you can configure up to 2000 IVZs and 10,000 IVZ members on the switches in the network.
- 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 an end device in one VSAN can reach another end device in another VSAN. Multiple paths can exist between two 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 can be adjacent to each other or they can be connected by one or more transit VSANs. In Figure 18-1, 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 a source edge VSAN to the destination edge VSAN. In Figure 18-1, 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, such as the IVR-enabled switch between VSAN 1 and VSAN 4 in Figure 18-1.
- Edge switch—A switch to which a member of an IVR zone has logged in. Edge switches are unaware of the IVR configurations in the border switches. Edge switches need not be IVR enabled.

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.
- Acquire a mandatory Enterprise License Package or, as of Cisco MDS SAN-OS Release 2.1(1a), a SAN Extension over IP License package for this feature.

Note IVR is bundled with the Cisco MDS 9216i switch and does not require a license.

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

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

Domain ID Guidelines

Prior to Cisco MDS SAN-OS Release 2.1(1a), unique domain IDs are required across inter-connected VSANs. Consider the following guidelines for unique domain IDs:

- 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.

Note As of Cisco MDS SAN-OS Release 2.1(1a), unique domain IDs are no longer required.

Note As of Cisco MDS SAN-OS Release 2.1(1a), in a configuration involving IVR without NAT, if one VSAN in the IVR topology is configured with static domain IDs, then the other VSANs (edge or transit) in the topology must be configured with static domain IDs.

Transit VSAN Guidelines

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 later.
- A border switch must be a member of two or more VSANs.
- A border switch that facilities IVR communications must be IVR enabled.
- IVR can (optionally) be enabled on additional border switches to provide redundant paths between active IVZ members.
- The VSAN topology configuration must be updated before a border switch is added or removed if the switch is running Cisco MDS SAN-OS Release 2.0(3) or earlier, or if IVR topology automatic mode is not enabled (available as of Cisco MDS SAN-OS Release 2.1(1a) or later).

IVR Configuration

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

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

Step 2 If you do not plan to use IVR NAT (supported as of Cisco MDS SAN-OS Release 2.1(1a)), verify that unique domain IDs are configured in all switches and VSANs participating in IVR.

Step 3 Enable IVR in the border switches.

Step 4 Configure the service group as required.

Step 5 Configure fabric distribution as required.

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

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

Step 8 Verify the IVR configuration.

Unique Domain ID Configuration Options

If you are not using IVR NAT, you must use unique domain IDs. You can configure unique domain IDs using one of two options:

- Configure the allowed-domains list so that the domains in different VSANs are non-overlapping on all participating switches and VSANs.
- Configure static, non-overlapping domains for each participating switch and VSAN (see Chapter 14, "Configuring Domain Parameters").

Note If you are using IVR NAT, you do not need unique domain IDs.

Enabling IVR

The IVR feature must be enabled in all border switches in the fabric that participate in the IVR. By default, this feature is disabled in all switches in the Cisco MDS 9000 Family. You can manually enable IVR on all required switches in the fabric or configure fabric-wide distribution of the IVR configuration ("IVR Configuration Distribution" section on page 18-6).

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 the switch.
	`switch(config)# no ivr enable`	Disables (default) IVR on the switch.

IVR Configuration Distribution

The IVR feature uses the Cisco Fabric Services (CFS) infrastructure to enable efficient configuration management and to provide a single point of configuration for the entire fabric in the VSAN (see Chapter 5, "Using the CFS Infrastructure").

The following configurations are distributed:

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

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

Database Implementation

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

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

Enabling Configuration Distribution

To enable IVR configuration distribution, follow these steps:

	Command	Purpose

Step 1	`switch# config t`
	`switch(config)#`
		Enters configuration mode.

Step 2	`switch(config)# ivr distribute`	Enables IVR distribution.
	`switch(config)# no ivr distribute`	Disables (default) IVR distribution.

Locking the Fabric

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

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

Committing the Changes

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

To commit IVR configuration changes, follow these steps:

	Command	Purpose

Step 1	`switch# config t`
	`switch(config)#`
		Enters configuration mode.

Step 2	`switch(config)# ivr commit`	Commits the IVR changes.

Discarding the Changes

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

To discard IVR configuration changes, follow these steps:

	Command	Purpose

Step 1	`switch# config t`
	`switch(config)#`
		Enters configuration mode.

Step 2	`switch(config)# ivr abort`	Discards the IVR changes and clears the pending configuration database.

Clearing a Locked Session

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

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

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

```
switch# clear ivr session
```

About IVR NAT

Prior to Cisco MDS SAN-OS Release 2.1(1a), IVR required unique domain IDs for all switches in the fabric. As of Cisco MDS SAN-OS Release 2.1(1a), you can enable IVR Network Address Translation (NAT) to allow non-unique domain IDs. This feature simplifies the deployment of IVR in an existing fabric where non-unique domain IDs might be present.

IVR NAT must be running on all border switches in the fabric IVR configuration distribution. IVR configuration distribution is supported by the CFS infrastructure (see the "IVR Configuration Distribution" section on page 18-6). By default, IVR NAT, and IVR configuration distribution are disabled in all switches in the Cisco MDS 9000 Family.

Note For IVR NAT to function correctly in the network, all IVR-enabled switches must run Cisco MDS SAN-OS Release 2.1(1a) or later.

Note You must enable NAT on all IVR-enabled switches.

Note Load balancing of IVR NAT traffic across equal cost paths from an IVR-enabled switch is not supported. However, load balancing of IVR NAT traffic over PortChannel links is supported.

IVR NAT virtualizes the switches in other VSANs by using local VSAN for the destination IDs in the Fibre Channel headers. In some Extended Link Service message types, the destinations IDs are part of the payload. In these cases, IVR NAT replaces the actual destination ID with the virtualized destination ID. IVR NAT supports destination ID replacement in the Extended Link Service messages described in Table 18-1.

Table 18-1 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
Read Exchange Concise	0x13 00 00 00	REC
Read Exchange Concise Accept	0x02 00 00 00	REC ACC
Read Exchange Status Block	0x08 00 00 00	RES
Read Exchange Status Block Accept	0x02 00 00 00	RES ACC
Read Link Error Status Block	0x0F 00 00 00	RLS
Read Sequence Status Block	0x09 00 00 00	RSS
Reinstate Recovery Qualifier	0x12 00 00 00	RRQ
Request Sequence Initiative	0x0A 00 00 00	RSI
Scan Remote Loop	0x7B 00 00 00	RSL
Third Party Process Logout	0x24 00 00 00	TPRLO
Third Party Process Logout Accept	0x02 00 00 00	TPRLO ACC

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

Enabling IVR NAT

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 configure IVR NAT, follow these steps:

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

About IVR Topologies

IVR must know about the topology of the IVR-enabled switches in the fabric to function properly. You can specify the topology two ways:

- Manual configuration

  If you manually configure the IVR topology, you must ensure that the IVR topology exists on every IVR-enabled switch in the fabric. You can configure the IVR topology manually on each IVR-enabled switch or you can use CFS to distribute the configuration automatically (see the "Database Merge Guidelines" section on page 18-29).

  If an IVR-enabled switch is removed from the network, the IVR topology database must be updated to reflect the change.

- Automatic mode

  As of Cisco MDS SAN-OS Release 2.1(1a), you can configure IVR topology automatic mode. Automatic mode uses CFS configuration distribution to dynamically learn and maintain up-to-date information about the topology of the IVR-enabled switches in the network.

  If a manually configured IVR topology database exists, automatic mode initially uses that topology information. This reduces disruption in the network by gradually migrating from a user-specified topology database to an automatically learned topology database. Then the user-configured topology entries that are not part of the network are aged out in about three minutes and new entries that are not part of user configured database are added as they are learned from the network.

Configuring IVR Topologies

This section describes how to manually configure an IVR topology or how to configure IVR topology automatic mode.

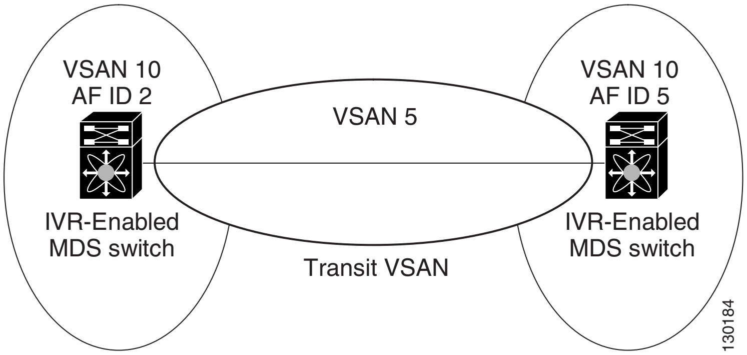
Manually Configuring the IVR Topology

You can have up to 64 VSANs (or 128 VSANs as of Cisco MDS SAN-OS Release 2.1(1a)) 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 (AFID), which distinguishes two VSANs that are logically and physically separate, but have the same VSAN number. Cisco MDS SAN-OS Releases 2.0(2b) supports only one default AFID (AFID 1) and thus does not support non-unique VSAN IDs in the network. As of Cisco MDS SAN-OS Release 2.1(1a), you can specify up to 64 AFIDs. See Figure 18-2.

Note If two VSANs in an IVR topology have the same VSAN ID and different AFIDs, they count as two VSANs for the 128-VSAN limit for IVR.

Figure 18-2 Example IVR Topology with Non-Unique VSAN IDs Using AFIDs



Note The use of a single AFID does not allow for VSANs that are logically and physically separate but have the same VSAN number in an IVR topology.

Caution You can only configure a maximum of 128 IVR-enabled switches and 64 distinct VSANs (or 128 distinct VSANs as of Cisco MDS SAN-OS Release 2.1(1a)) in an IVR topology (see the "Database Merge Guidelines" section on page 18-29).

Configuring an IVR Topology Database

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

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

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.

Step 2	`switch(config)# ivr vsan-topology database`
	`switch(config-ivr-topology-db)#`
		Enters the VSAN topology database configuration mode for the IVR feature.

Step 3	`switch(config-ivr-topology-db)# autonomous-fabric-id 1 switch 20:00:00:05:30:01:1b:b8 vsan-ranges 1-2,6`	Configures VSANs 1, 2, and 6 to participate in IVR for this switch.
	`switch(config-ivr-topology-db)# autonomous-fabric-id 1 switch 20:00:00:05:30:01:1b:c2 vsan-ranges 1-3`	Configures VSANs 1, 2 and 3 to participate in IVR for this switch.
	`switch(config-ivr-topology-db)# no autonomous-fabric-id 1 switch 20:00:00:05:30:01:1b:c2 vsan-ranges 1-2`	Removes VSANs 1 and 2 from IVR for this switch.

Step 4	`switch(config-ivr-topology-db)# end`
	`switch#`
		Reverts to EXEC mode.

View your configured IVR topology using the **show ivr vsan-topology** command. In the following example output, VSAN 2 is the transit VSAN between VSANs 1, 5, and 6.

```
switch# show ivr vsan-topology

AFID  SWITCH WWN                Active   Cfg. VSANS
--------------------------------------------------------------
   1  20:00:00:05:30:01:1b:c2 *   no      yes  1-2
   1  20:02:00:44:22:00:4a:05     no      yes  1-2,6
   1  20:02:00:44:22:00:4a:07     no      yes  2-5

Total:   3 entries in active and configured IVR VSAN-Topology

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

Note If CFS is not enabled, you must repeat this configuration in all IVR-enabled switches. See the "Database Merge Guidelines" section on page 18-29.

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

Activating a Manually Configured IVR Topology

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

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

To activate a manually 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.

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
```

Configuring IVR Topology Automatic Mode

As of Cisco MDS SAN-OS Release 2.1(1a), you can configure IVR topology automatic mode.

Note IVR configuration distribution must be enabled before configuring IVR topology automatic mode (see the "IVR Configuration Distribution" section on page 18-6). Once IVR topology automatic mode is enabled, you cannot disable IVR configuration distribution.

To configure IVR topology automatic mode, follow these steps:

	Command	Purpose

Step 1	`switch# config t`
	`switch(config)#`
		Enters configuration mode.

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

View automatically discovered IVR topology using the **show ivr vsan-topology** command.

```
switch# show ivr vsan-topology
AFID  SWITCH WWN                 Active   Cfg. VSANS
--------------------------------------------------------------
   1  20:00:00:05:30:01:1b:c2 *   yes     yes  1-2
   1  20:02:00:44:22:00:4a:05     yes     yes  1-2,6
   1  20:02:00:44:22:00:4a:07     yes     yes  2-5

Total:   3 entries in active and configured IVR VSAN-Topology

Current Status: Inter-VSAN topology is AUTO
Last activation time: Mon Mar 24 07:19:53 1980
```

Migrating from IVR Topology Automatic Mode to Manual Mode

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

	Command	Purpose
Step 1	`switch#` **`ivr copy auto-topology user-configured-topology`**	Copies the automatic IVR topology database to the user-configured IVR topology.

Step 2	`switch#` **`config t`**
	`switch(config)#`
		Enters configuration mode.

Step 3	`switch(config)#` **`ivr vsan-topology active`**	Disabled automatic mode for the IVR topology database and enables user-configuration mode.

Clearing the Configured IVR Topology Database

To clear the user-configured IVR VSAN topology database using, follow these steps:

	Command	Purpose

Step 1	`switch#` **`config t`**
	`switch(config)#`
		Enters configuration mode.

Step 2	`switch(config)#` **`no ivr vsan-topology database`**	Clears the previously created IVR topology.

Verifying the IVR Topology

You can verify the IVR topology by using the **show ivr vsan-topology** command. See Example 18-1 to Example 18-3.

Example 18-1 Displays the Configured IVR VSAN Topology

```
switch# show ivr vsan-topology
AFID    SWITCH WWN                 Active   Cfg. VSANS
--------------------------------------------------------------
   1    20:00:00:05:30:01:1b:c2 *   yes     yes  1-2
   1    20:02:00:44:22:00:4a:05     yes     yes  1-2,6
   1    20:02:00:44:22:00:4a:07     yes     yes  2-5

Total:   5 entries in active and configured IVR VSAN-Topology

Current Status: Inter-VSAN topology is ACTIVE
Last activation time: Sat Mar 22 21:46:15 1980
```

The asterisk (*) indicates the local switch.

Example 18-2 Displays the Active IVR VSAN Topology

```
switch# show ivr vsan-topology active
AFID   SWITCH WWN                 Active   Cfg. VSANS
--------------------------------------------------------------
    1  20:00:00:05:30:01:1b:c2 *   yes     yes  1-2
    1  20:02:00:44:22:00:4a:05     yes     yes  1-2,6
    1  20:02:00:44:22:00:4a:07     yes     yes  2-5

Total:   5 entries in active IVR VSAN-Topology

Current Status: Inter-VSAN topology is ACTIVE
Last activation time: Sat Mar 22 21:46:15
```

Example 18-3 Displays the Configured IVR VSAN Topology

```
switch# show ivr vsan-topology configured
AFID  SWITCH WWN                 Active   Cfg. VSANS
--------------------------------------------------------------
    1  20:00:00:05:30:01:1b:c2 *   yes     yes  1-2
    1  20:02:00:44:22:00:4a:05     yes     yes  1-2,6
    1  20:02:00:44:22:00:4a:07     yes     yes  2-5

Total:   5 entries in configured IVR VSAN-Topology
```

Non-Unique VSAN IDs Using AFIDs

As of Cisco MDS SAN-OS Release 2.1(1a), you can configure more than one AFID. This feature allows more than one VSAN in the network with the same VSAN ID. Using this feature you can avoid downtime when enabling IVR between fabrics that contain VSANs with the same ID. However, for VSANs with the same ID to communicate, there must be a transit VSAN with a different VSAN ID between the source and target VSANs.

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

Configuring the AFID Database

To configure the AFID database, follow these steps:

	Command	Purpose

Step 1	`switch# `**`config t`**
	`switch(config)#`
		Enters configuration mode.

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

	Command	Purpose
Step 4	`switch(config-afid-db)# switch-wwn 20:00:00:0c:91:90:3e:80 default-autonomous-fabric-id 5`	Configures the default AFID for all VSANs not explicitly associated with an AFID.
	`switch(config-afid-db)# no switch-wwn 20:00:00:0c:91:90:3e:80 default-autonomous-fabric-id 5`	Deletes the default AFID.

Verifying the AFID Database

View the contents of the AFID database using the **show autonomous-fabric-id database** command.

```
switch# show autonomous-fabric-id database

SWITCH WWN                    Default-AFID
--------------------------------------------------------------
20:00:00:0c:91:90:3e:80          5


Total:   1 entry in default AFID table

SWITCH WWN                    AFID      VSANS
--------------------------------------------------------------
20:00:00:0c:91:90:3e:80          10    1,2,5-8


Total:   1 entry in AFID table
```

Adding IVR Virtual Domain

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 Cisco SN5428 or Cisco MDS 9020 switches exist in the VSAN.

Tip 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.
	`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

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

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

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

Verifying the IVR Virtual Domain Configuration

View the status of the IVR virtual domain configuration using the **show ivr virtual-fcdomain-add-status** command.

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

Persistent FC IDs for IVR

As of Cisco MDS SAN-OS Release 2.1(2), you can configure persistent FC IDs for IVR. Persistent FC IDs across reboot improves IVR management by providing the following features:

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

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

- Host devices always see the same FC ID for targets.
- Helps you plan your SAN layout better by assigning virtual domains for IVR to use.
- Can make SAN monitoring and management easier. When you see the same domain or FC ID consistently assigned, you can readily determine the native VSAN or device to which it refers.

You can configure two types of database entries for IVR FC IDs:

- Virtual domain entries—Contain the virtual domain that should be used to represent a native VSAN in a specific VSAN (current VSAN). These entries contain the following information:
  - Native AFID
  - Native VSAN
  - Current AFID
  - Current VSAN
  - Virtual domain to be used for the native AFID and VSAN in current AFID and VSAN
- Virtual FC ID entries—Contain the virtual FC ID that should be used to represent a device in a specific VSAN (current VSAN). These entries contain the following information:
  - Port WWN
  - Current AFID
  - Current VSAN
  - Virtual FC ID to be used to represent a device for the given pWWN in the current AFID and VSAN

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

Note In an IVR-NAT configuration, if one VSAN in the IVR topology is configured with static domain IDs, then the IVR domains that can be exported to that VSAN must also be assigned static domains.

Configuring Persistent FC IDs for IVR

To configure persistent FC IDs for IVR in Cisco MDS SAN-OS Release 2.1(2) and later, follow these steps:

	Command	Purpose
Step 1	switch# **config t**	Enters configuration mode.
Step 2	switch(config)# **ivr fcdomain database autonomous-fabric-num 21 vsan 22** switch(config-fcdomain)#	Enters IVR fcdomain database configuration submode for current AFID 21 and VSAN 22.
	switch(config)# **no ivr fcdomain database autonomous-fabric-num 21 vsan 22**	Deletes all the database entries, including all the corresponding persistent FC ID entries, for current AFID 21 and VSAN 22.

	Command	Purpose

Step 3	`switch(config-fcdomain)# native-autonomous-fabric-num 20 native-vsan 11 domain 12`
	`switch(config-fcdomain-fcid)#`
		Adds or replaces a database entry for native AFID 20, native VSAN 11, and domain 12, and enters IVR fcdomain FC ID configuration submode. Domains of all the corresponding persistent FC ID entries, if any, are also changed to 12.

	`switch(config-fcdomain)# no native-autonomous-fabric-num 20 native-vsan 11`	Deletes the virtual domain entry native AFID 20 and native VSAN 11, and all corresponding FC ID entries.
Step 4	`switch(config-fcdomain-fcid)# pwwn 11:22:33:44:55:66:77:88 fcid 0x124466`	Adds or replaces a database entry for mapping the pWWN to the FC ID.
	`switch(config-fcdomain-fcid)# no pwwn 11:22:33:44:55:66:77:88`	Deletes the database entries for the pWWN.
Step 5	`switch(config-fcdomain-fcid)# device-alias SampleName fcid 0x123456`	Adds a database entry for mapping the device alias to the FC ID.
	`switch(config-fcdomain-fcid)# no device-alias SampleName`	Deletes the database entries for the device alias.

Clearing the IVR fcdomain Database

You might want to clear the IVR fcdomain database. You can do this using the following command:

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

Verifying the Persistent FC ID Configuration

Verify the persistent FC ID configuration using the **show ivr fcdomain database** command. See Example 18-4 and Example 18-5

Example 18-4 Displays All IVR fcdomain Database Entries

```
switch# show ivr fcdomain database
----------------------------------------------------
  AFID  Vsan  Native-AFID  Native-Vsan  Virtual-domain
----------------------------------------------------
    1     2        10           11         0xc(12)
   21    22        20           11         0xc(12)

Number of Virtual-domain entries: 2

----------------------------------------------------
  AFID  Vsan           Pwwn           Virtual-fcid
----------------------------------------------------
   21    22  11:22:33:44:55:66:77:88  0x114466
   21    22  21:22:33:44:55:66:77:88  0x0c4466
   21    22  21:22:33:44:55:66:78:88  0x0c4466

Number of Virtual-fcid entries: 3
```

Example 18-5 Displays the IVR fcdomain Database Entries for a Specific AFID and VSAN

```
switch# show ivr fcdomain database autonomous-fabric-num 21 vsan 22
----------------------------------------------------
  AFID  Vsan  Native-AFID  Native-Vsan  Virtual-domain
----------------------------------------------------
   21    22        20           11         0xc(12)

Number of Virtual-domain entries: 1

----------------------------------------------------
  AFID  Vsan           Pwwn           Virtual-fcid
----------------------------------------------------
   21    22  11:22:33:44:55:66:77:88  0x114466
   21    22  21:22:33:44:55:66:77:88  0x0c4466
   21    22  21:22:33:44:55:66:78:88  0x0c4466

Number of Virtual-fcid entries: 3
```

About 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* of the IVR-enabled switches.

Caution You can only configure a total number of 2000 zone members on all switches in a network. As of Cisco MDS SAN-OS Release 2.1(1a), the limit is increased to a total number of 10,000 zone members on all switches in a network. A zone member is counted twice if it exists in two zones. See the "Database Merge Guidelines" section on page 18-29.

IVZs Versus Zones

Table 18-2 identifies the key differences between IVZs and zones.

Table 18-2 Key Differences between IVZs and Zones

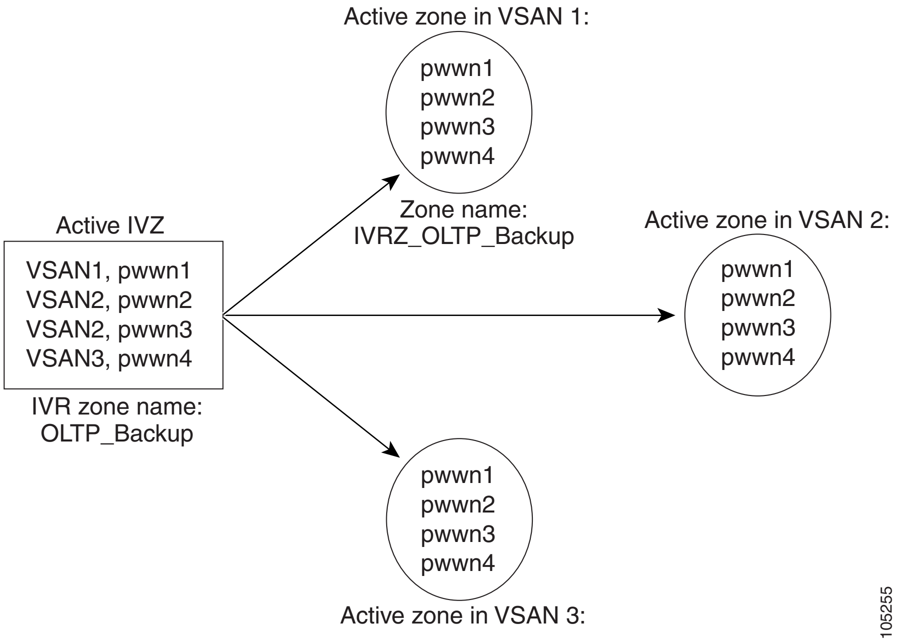
IVZs	Zones
IVZ membership is specified using the VSAN and pWWN combination.	Zone membership is specified using pWWN, fabric WWN, sWWN, or the fabric ID.
Default zone policy is always deny (not configurable).	Default zone policy is deny (configurable).

Automatic IVZ Creation

Figure 18-3 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 18-3 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 nondisruptively.

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.

IVZ and IVZS names are restricted to 64 alphanumeric characters.

Caution You can only configure a total of 200 zones and 32 zone sets on the switches in the network. As of Cisco MDS SAN Release 2.1(1a), you can configure up to 2000 zones on the switches in the network. See the "Database Merge Guidelines" section on page 18-29.

Configuring IVZs and IVZSs

This section describes how to configure IVZs and IVZSs.

Creating and Activating IVZs and IVZSs

When you activate an IVZS, IVR automatically adds an IVZ 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 IVZS using the force option, which causes IVR to create an active zone set called "nozoneset" and adds the IVZ to that active zone set.

Caution Regular zone set activation and deactivation is per VSAN where IVR zone set activation and deactivation is for a set of VSANs. If you deactivate the regular active zone set in a VSAN, the IVZs for the IVZS are removed, and all IVR traffic to and from that VSAN is stopped. This occurs because the IVZs in the regular active zone set of that VSAN are also removed and deactivated. IVR traffic between other VSANs continues to function. To reactivate the IVZS, you must reactivate the regular zone set.

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

To create and activate IVZs and IVZSs, follow these steps:

	Command	Purpose
Step 1	switch# **config t**	Enters configuration mode.
Step 2	switch(config)# **ivr zone name sample_vsan2-3** switch(config-ivr-zone)#	Creates an IVR zone named sample_vsan2-3.
Step 3	switch(config-ivr-zone)# **member pwwn 21:00:00:e0:8b:02:ca:4a vsan 3**	Adds the specified pWWN in VSAN 3 as an 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 sample_vsan4-5** switch(config-ivr-zone)#	Creates an IVZ named sample_vsan4-5.
Step 7	switch(config-ivr-zone)# **member pwwn** 21:00:00:e0:8b:06:d9:1d vsan 4	Adds the specified pWWN in VSAN 4 as an 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 IVZS named Ivr_zoneset1.

	Command	Purpose
Step 12	switch(config-ivr-zoneset)# **member sample_vsan2-3**	Adds the sample_vsan2-3 IVZ as an IVZS member.
Step 13	switch(config-ivr-zoneset)# **member sample_vsan4-5**	Adds the sample_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.

Configuring LUNs in IVR Zoning

LUN zoning can be used between members of active IVZs. Prior to Cisco MDS SAN-OS Release 2.1(1a), you can configure the service by creating and activating LUN zones between the desired IVZ members in all relevant edge VSANs using the zoning interface. As of Cisco MDS SAN-OS Release 2.1(1a), IVR directly supports LUN zoning. For more details on the advantages of LUN zoning, see the "About LUN Zoning" section on page 19-17.

To configure LUNs in IVR zoning in Cisco MDS SAN-OS Release 2.1(1a) or later, follow these steps:

	Command	Purpose
Step 1	switch# **config t** switch(config)#	Enters configuration mode.
Step 2	switch(config)# **ivr zone name IvrLunZone** switch(config-ivr-zone)#	Configures an IVZ called IvrLunZone.
Step 3	switch(config-ivr-zone)# **member pwwn 10:00:00:23:45:67:89:ab lun 0x64 vsan 10**	Configures an IVZ member based on the specified pWWN and LUN value. **Note** The CLI interprets the LUN identifier value as a hexadecimal value whether or not the **0x** prefix is included.
	switch(config-ivr-zone)# **member pwwn 10:00:00:23:45:67:89:ab lun 0x64 vsan 10 autonomous-fabric-id 20**	Configures an IVZ member based on the specified pWWN, LUN value, and AFID.
	switch(config-ivr-zone)# **no member pwwn 20:81:00:0c:85:90:3e:80 lun 0x32 vsan 13 autonomous-fabric-id 10**	Removes an IVZ member.

Note As of Cisco MDS SAN-OS Release 2.1(1a), you can configure LUN zoning in an IVZS setup.

Configuring the QoS Attribute

As of Cisco MDS SAN-OS Release 2.1(1a), you can configure a QoS attribute for an IVZ. To configure QoS for an IVZ, follow these steps:

	Command	Purpose

Step 1	`switch#` **`config t`**
	`switch(config)#`
		Enters configuration mode.

Step 2	`switch(config)#` **`ivr zone name IvrZone`**
	`switch(config-ivr-zone)#`
		Configures an IVZ called IvrZone.

Step 3	`switch(config-ivr-zone)#` **`attribute qos priority medium`**	Configures the QoS for IVZ traffic to medium.
	`switch(config-ivr-zone)#` **`no attribute qos priority medium`**	Reverts to the default QoS setting. The default is low.

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

Verifying the QoS Attribute Configuration

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

```
switch(config)# show ivr zone

zone name IvrZone
    attribute qos priority medium
```

Using the force Option

Use the **force** option to activate the specified IVZS. Table 18-3 lists the various scenarios with and without the **force** option.

Table 18-3 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 *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** 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`.

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.

Verifying IVZ and IVZS Configuration

Verify the IVZ and IVZS configurations using the **show ivr zone** and **show ivr zoneset** commands. See Example 18-6 to Example 18-14.

Example 18-6 Displays the IVZ Configuration

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

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

Example 18-7 Displays Information for a Specified IVZ

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

Example 18-8 Displays the Specified Zone in the Active IVZ

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

Example 18-9 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 sample_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

Example 18-10 Displays the Active IVZS Configuration

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

Example 18-11 Displays the Specified IVZS Configuration

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

Example 18-12 Displays Brief Information for All IVZSs

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

Example 18-13 Displays Brief Information for the Active IVZS

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

Example 18-14 Displays Status Information for the IVZS

```
switch# show ivr zoneset status
Zoneset Status
_______________
    name               : IVR_ZoneSet1
    state              : activation success
    last activate time : Sat Mar 22 21:38:46 1980
    force option       : off

status per vsan:
__________________
     vsan     status
     ____     ______
       1      active
       2      active
```

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

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

About IVR Service Groups

In a complex network topology, you might only have a few IVR-enabled VSANs. To reduce the amount of traffic to non-IVR-enabled VSANs, you can configure a service group that restricts the traffic to the IVR-enabled VSANs. Only one service group is allowed in a network. When a new IVR-enabled switch is added to the network, you must update the service group to include the new VSANs.

Note CFS distribution of IVR information is restricted within the service group only when IVR VSAN topology is in automatic mode. See the "About IVR Topologies" section on page 18-10.

Configuring IVR Service Groups

To configure an IVR service group, follow these steps:

	Command	Purpose

Step 1	`switch# `**`config t`**
	`switch(config)#`
		Enters configuration mode.

Step 2	`switch(config)# `**`ivr service-group name IVR-SG1`**
	`switch(config-ivr-sg)#`
		Configures the IVR service group called IVR-SG1.

	`switch(config)# `**`no ivr service-group name IVR-SG1`**	Deletes the IVR service group.

	Command	Purpose
Step 3	`switch(config-ivr-sg)# autonomous-fabric-id 10 vsan-ranges 1,2,6-10`	Configures AFID 10 for VSANs 1, 2, and 6 through 10.
	`switch(config-ivr-sg)# no autonomous-fabric-id 20 vsan-ranges 1,2,6-10`	Removes the association between AFID 20 and VSANs 1, 2, and 6 through 10.

Verifying IVR Service Group Configuration

Use the **show ivr service-group database** command to view the IVR service group database configuration.

```
switch# show ivr service-group database

SG-ID  SG-NAME                                                          AFID VSANS
-------------------------------------------------------------------------------
 1     IVR-SG1                                                            10 1-2,6-10
 1     IVR-SG1                                                            11 1


Total:   2 entries in service group table
```

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 "Switch Interoperability" section on page 25-9.

Configuring IVR Using Read-Only Zoning

Read-only zoning (with or without LUNs) can be used between members of active IVR zones. To configure this service, you must create and activate read-only zones between the desired IVZ members in all relevant edge VSANs using the zoning interface.

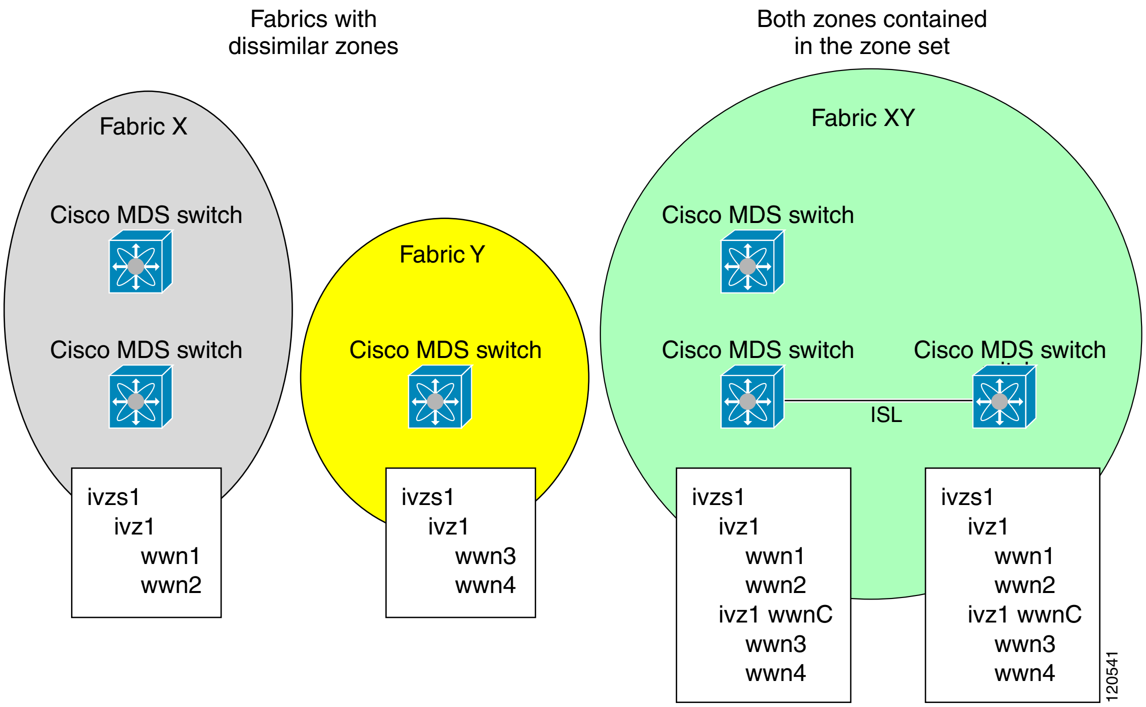
Note Read-only zoning cannot be configured in an IVZS setup.

Database Merge Guidelines

A database merge refers to a union of the configuration database and static (unlearned) entries in the active database. Refer to the "CFS Merge Support" section on page 5-7 for detailed concepts.

- Be aware of the following conditions when merging two IVR fabrics:
  - The IVR configurations are merged even if two fabrics contain different configurations.
  - If dissimilar zones exist in two merged fabrics, the zone from each fabric is cloned in the distributed zone set with appropriate names (see Figure 18-4).

Figure 18-4 Fabric Merge Consequences



- You can configure different IVR configurations in different Cisco MDS switches.
- Be aware that the merge follows more liberal approach in order to avoid traffic disruption. After the merge, the configuration will be a union of the configurations that were present on the two switches involved in the merge.
  - The configurations are merged even if both fabrics have different configurations.
  - A union of zones and zone sets are used to get the merged zones and zone sets. If a dissimilar zone exists in two fabrics, the dissimilar zones are cloned into the zone set with appropriate names so both zones are present.
  - The merged topology contains a union of the topology entries for both fabrics.
  - The merge will fail if the merged database contains more topology entries than the allowed maximum.
  - The total number of VSANs across the two fabrics cannot exceed 64. As of Cisco MDS SAN-OS Release 2.1(1a), 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 2000. As of Cisco MDS SAN-OS Release 2.1(1a), the total number of zone members across the two fabrics cannot exceed 10,000. A zone member is counted twice if it exists in two zones.
- The total number of zones across the two fabrics cannot exceed 200. As of Cisco MDS SAN-OS Release 2.1(1a), the total number of zones across the two fabrics cannot exceed 2000.
- The total number or zone sets across the two fabrics cannot exceed 32.

Table 18-4 describes the results of a CFS merge of two IVR-enabled fabrics under different conditions.

Table 18-4 Results of Merging Two IVR-Enabled Fabrics

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

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

Configuring IVR Logging Levels

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

	Command	Purpose

Step 1	`switch# config t`
	`switch(config)#`
		Enters configuration mode.

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

Verifying Logging Level Configuration

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

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

Example Configurations

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

- Manual Topology Configuration, page 18-31
- Auto-Topology Configuration, page 18-34

Manual Topology Configuration

This section provides the configuration steps to manually configure the example illustrated in Figure 18-1.

Step 1 Enable IVR.

```
mds# config 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 Enable CFS distribution.

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

Step 4 Manually configure the IVR VSAN-topology. In Figure 18-1, two of the four IVR-enabled switches (MDS1 and MDS2) are members of VSANs 1 and 4. The other two switches (MDS3 and MDS4) are members of VSANs 2, 3, and 4.

```
mds# 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 5 Verify the configured VSAN-topology.

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

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

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

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

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

Step 6 Activate the configured VSAN topology.

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

Step 7 Verify the activation.

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

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

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

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

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

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

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

```
mds(config)# ivr zoneset name tape_server1_server2

mds(config-ivr-zoneset)# zone name tape_server1
mds(config-ivr-zoneset-zone)# member pwwn 10:02:50:45:32:20:7a:52 vsan 1
mds(config-ivr-zoneset-zone)# member pwwn 10:02:66:45:00:20:89:04 vsan 2
mds(config-ivr-zoneset-zone)# exit

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

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

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

  zone name tape_server2
      pwwn 10:02:50:45:32:20:7a:52 vsan 1
      pwwn 10:00:ad:51:78:33:f9:86 vsan 3
```

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

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

  zone name $default_zone$ vsan 1
```

Step 11 Activate the configured IVR zone set.

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

Step 12 Verify the IVR zone set activation.

```
mds# show ivr zoneset active
zoneset name tape_server1_server2
  zone name tape_server1
      pwwn 10:02:50:45:32:20:7a:52 vsan 1
      pwwn 10:02:66:45:00:20:89:04 vsan 2

  zone name tape_server2
      pwwn 10:02:50:45:32:20:7a:52 vsan 1
      pwwn 10:00:ad:51:78:33:f9:86 vsan 3
```

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

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

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

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

  zone name $default_zone$ vsan 1

mds# show ivr zoneset status
Zoneset Status
______________
    name               : tape_server1_server2
    state              : activation success
    last activate time : Tue May 20 23:23:01 1980
    force option       : on

status per vsan:
__________________
     vsan     status
     ____     ______
     1        active
```

Auto-Topology Configuration

This section provides example configuration steps for configuring IVR auto-topology supported in Cisco SAN-OS Release 2.1(1a) and later.

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

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

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

```
switch# show ivr
Inter-VSAN Routing is enabled

Inter-VSAN enabled switches
---------------------------
No IVR-enabled VSAN is active. Check VSAN-Topology configuration.

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

```
Inter-VSAN zoneset status
-------------------------
    name               :
    state              : idle
    last activate time :

Fabric distribution status
-----------------------
fabric distribution disabled
Last Action                : None
Last Action Result         : None
Last Action Failure Reason : None

Inter-VSAN NAT mode status
--------------------------
FCID-NAT is disabled

License status
-----------------
IVR is running based on the following license(s)
ENTERPRISE_PKG
```

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

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

Step 4 Enable IVR auto-topology mode.

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

Step 5 Commit the change to the fabric.

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

Step 6 Verify the status of the commit request.

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

Step 7 Verify the active IVR topology.

```
switch# show ivr vsan-topology active

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

Default Settings

Table 18-5 lists the default settings for IVR parameters.

Table 18-5 Default IVR Parameters

Parameters	Default
IVR feature	Disabled.
IVR VSANs	Not added to virtual domains.
IVR NAT	Disabled.
QoS for IVZs	Low
Configuration Distribution	Disabled.