



IVR

- [Information About IVR, on page 1](#)
- [Default Settings, on page 4](#)
- [Guidelines and Limitations, on page 5](#)
- [Configuring IVR, on page 5](#)
- [Verifying IVR Configuration, on page 9](#)
- [Feature History, on page 10](#)

Information 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 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 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.
- Establishes proper interconnected routes that traverse 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.
- 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.

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)

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

Inter-VSAN routing zone sets (IVR zone sets)

Inter-VSAN routing zone sets (IVR zone sets)-One or more IVR zones make up an IVR zone set.

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.



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.



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.

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.

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 Database Merge

A database merge refers to the combination of the configuration database and static (unlearned) entries in the active database.

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.
- You can configure different IVR configurations in different Cisco SAN 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, as follows:

- 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 following total number of items across the two fabrics cannot exceed the maximum allowed in one fabric:

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

- IVR-enabled switches.
- Zone members. A zone member is counted twice if it exists in two zones.
- Zones.
- Zone sets.

Table 1: Results of Merging Two IVR-Enabled Fabrics

IVR Fabric 1	IVR Fabric 2	Merged Fabric
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
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.

Related Topics

[IVR Configuration Limits](#)

[Resolving IVR Merge Failures](#), on page 8

Default Settings

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

Guidelines and Limitations

IVR has the following guidelines and limitations:

- All border switches in the fabric must be Cisco SAN switches. Other switches in the fabric can be non-Cisco switches.
- IVR must be enabled in the storage VDC.

Configuring IVR

SUMMARY STEPS

1. Enable IVR on all border switches.
2. Enable IVR distribution on all IVR-enabled switches.
3. Enable IVR NAT on a single IVR-enabled switch.
4. Enable IVR auto topology on a single IVR-enabled switch.
5. Configure and activate Zone sets.
6. Commit the IVR configuration.

DETAILED STEPS

-
- | | |
|---------------|--|
| Step 1 | Enable IVR on all border switches. |
| Step 2 | Enable IVR distribution on all IVR-enabled switches. |
| Step 3 | Enable IVR NAT on a single IVR-enabled switch. |
| Step 4 | Enable IVR auto topology on a single IVR-enabled switch. |
| Step 5 | Configure and activate Zone sets. |
| Step 6 | Commit the IVR configuration. |
-

Related Topics

- [Enabling IVR](#), on page 5
- [Distributing IVR](#), on page 6
- [Enabling IVR NAT](#)
- [Enabling IVR Auto Topology](#)
- [Committing IVR Changes](#), on page 7

Enabling IVR

By default, the IVR feature is disabled on the device. You must explicitly enable the IVR feature to access the configuration and verification commands.

Before you begin

- You must enable the IVR feature from the storage VDC.
- You must enable the IVR feature in all border switches in the fabric that participate in the IVR.

SUMMARY STEPS

1. **switchto vdc** *vdc-name*
2. **configure terminal**
3. **feature ivr**
4. (Optional) **show feature**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switchto vdc <i>vdc-name</i> Example: <pre>switch(config)# switchto vdc fcoe switch-fcoe#</pre>	Switch to the storage VDC to enable the IVR feature. The <i>vdc-name</i> can be any case-sensitive alphanumeric string up to 32 characters.
Step 2	configure terminal Example: <pre>switch-fcoe# configure terminal switch-fcoe(config)#</pre>	Enters global configuration mode.
Step 3	feature ivr Example: <pre>switch-fcoe(config)# feature ivr</pre>	Enables the IVR feature. You must enable this feature on all border switches in the fabric.
Step 4	(Optional) show feature Example: <pre>switch-fcoe(config)# show feature</pre>	Displays the enable or disable state for all features.

Distributing IVR

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.

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

Before you begin

- You must enable IVR distribution on all IVR-enabled switches in the fabric.

SUMMARY STEPS

1. **configure terminal**
2. **ivr distribute**
3. (Optional) **show cfs application**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	ivr distribute Example: <pre>switch(config)# ivr distribute</pre>	Enables CFS distribution for IVR configuration. You must enable IVR distribution on all IVR-enabled switches in the fabric.
Step 3	(Optional) show cfs application Example: <pre>switch(config)# show cfs application</pre>	Displays information about CFS enabled features, such as IVR.
Step 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Committing IVR 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.

Before you begin

- Ensure you have enabled CFS distribution for IVR.

SUMMARY STEPS

1. **configure terminal**
2. **ivr commit**
3. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	ivr commit Example: <pre>switch(config)# ivr commit</pre>	Commits all pending IVR changes into the active IVR database.
Step 3	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Related Topics

[Distributing IVR](#), on page 6

Resolving IVR Merge Failures

Step 1 Display error conditions.

Example:

```
switch# show ivr merge status
switch# show cfs merge status name ivr
switch# show logging last 100
```

Review the information from these show commands. Look for MERGE failures in the log output.

Step 2 For failures because the merged fabric exceeded the maximum configuration limits (VSANs, IVR-enabled switches, zone members, zones, or zone sets) where you have a different versions of NX-OS running on Cisco SAN switches, upgrade to the most recent Cisco NX-OS version for all switches, or reduce the configuration below the maximum limits.

Step 3 For failures because the merged fabric exceeded the maximum configuration limits (VSANs, IVR-enabled switches, zone members, zones, or zone sets) and all switches are at the same release for their platform, identify the switch that has the correct configuration and perform a CFS commit to distribute the IVR configuration

Step 4 For other failures, resolve the error causing the merge failure on the switch that has the correct configuration and perform a CFS commit to distribute the IVR configuration.

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

Related Topics

[Committing IVR Changes](#), on page 7

Verifying IVR Configuration

To display the IVR configuration, perform one of the following tasks:

Command	Purpose
show ivr	Displays the status for the IVR configuration.
show ivr diagnostics	Displays information about IVR diagnostics.
show ivr merge status	Displays information the last IVR merge event.
show ivr pending	Displays information about the IVR pending database.
show ivr pending-diff	Displays the differences between the pending database and the config database.
show ivr vsan-topology [active configured]	Displays the IVR VSAN topology.
show ivr session status	Displays information about IVR CFS session.
show ivr virtual-domains	Displays information about IVR virtual domains for all local VSANs.
show ivr zone	Displays information about IVR zones.
show ivr zoneset	Displays information about IVR zone sets.
show ivr service-group active	Displays information about the active service group.
show ivr service-group configured	Displays information about the configured service group.
show autonomous-fabric-id database	Displays information about the AFIDs.
show ivr virtual-fcdomain-add-status	Displays the status of the IVR virtual domain configuration.

Related Topics

[Information about IVR Zones and Zonesets](#)

[Configuring IVR Zones](#)

[Configuring IVR Zone Sets](#)

Feature History

Table 2: Feature History IVR

Feature Name	Releases	Feature Information
IVR	5.2(1)	This feature was introduced.