CHAPTER 13

Troubleshooting IVR

This chapter describes how to troubleshoot and resolve inter-VSAN routing (IVR) configuration issues in the Cisco MDS 9000 Family of multilayer directors and fabric switches. It includes the following sections:

Overview

IVR allows resources to be shared across VSANs without compromising other VSAN benefits. Troubleshooting IVR involves checking the configuration of domain IDs, VSANs, border switches, and zone sets. Configuration problems with IVR can prevent devices from communicating properly.

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.

Note By default, IVR-NAT is not enabled.

Configuration Guidelines

This section provides guidelines for configuring components that can affect IVR, and includes the following topics:

Transit VSANs

Follow these guidelines when configuring transit VSANs:

- Besides 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 traverses only the shortest IVR path.
- Transit VSAN information is common to all IVR zones. Sometimes a transit VSAN can also be an edge VSAN in another IVR zone.

Border Switches

Always follow these guidelines when configuring border switches:

- Border switches require Cisco SAN-OS Release 1.3(1) or higher.
- A border switch must be a member of two or more VSANs.
- A border switch that facilities IVR communications must be IVR enabled.
- For redundant paths between active IVR zone members, IVR can (optionally) be enabled on additional border switches.
- The VSAN topology configuration must be updated before a border switch is added or removed.

Limitations and Restrictions

The following limitations apply to IVR:

- IVR is not supported on the Cisco MDS 9124 Fabric Switch, the Cisco Fabric Switch for HP c-Class BladeSystem, and the Cisco Fabric Switch for IBM BladeCenter.
- OX ID based load balancing of IVR traffic from IVR- enabled switches is not supported on Generation1 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.
- You cannot configure IVR NAT and preferred Fibre Channel routes on Generation 1 module interfaces.
- You cannot run SANTap and IVR together. IVR and SANTap both perform straddling across VSANs and cannot be used together.

Table 13-1 describes the configuration limits for IVR. (See Appendix C, “Configuration Limits for Cisco MDS SAN-OS Release 3.x” for complete limitations to the IVR configuration based on the Cisco SAN-OS release.)

Table 13-1 IVR Configuration Limits

IVR Feature	Maximum Limit
IVR zone members	• 20,000 IVR zone members per physical fabric as of Cisco SAN-OS Release 3.0(3). • 10,000 IVR zone members per physical fabric prior to Cisco SAN-OS Release 3.0(3).
IVR zones	• 8000 IVR zones per physical fabric as of Cisco SAN-OS Release 3.0(3). • 2000 IVR zones per physical fabric prior to Cisco SAN-OS Release 3.0(3).
IVR zone sets	32 IVR zone sets per physical fabric.

Initial Troubleshooting Checklist

Begin troubleshooting IVR issues by checking the following issues:

Checklist	Check off
Verify licensing requirements. See *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.	❑
Verify that IVR is enabled on all border switches involved in IVR.	❑
Verify that you have the correct license installed (SAN_EXTENSION for IVR over FCIP or ENTERPRISE_PKG for IVR over Fibre Channel).	❑
Verify that the IVR configuration is the same on all IVR-enabled switches.	❑
Verify that the IVR zone is part of the active IVR zone set.	❑
Verify that you have an active zone set or that you activate the IVR zone set using the **force** option.	❑
Verify that you have added IVR virtual domains to the allowed domain ID list if you have a Cisco SN5428 storage router or a Cisco MDS 9020 switch in your fabric.	❑

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

This section includes the following topics:

Verifying IVR Configuration Using Fabric Manager

To verify your IVR configuration using Fabric Manager, follow these steps:

Step 1 Choose **Fabric*xx* > All VSANs > IVR** to verify your IVR configuration.

Step 2 Select the **CFS** tab to verify that the Oper column is enabled and the Global column is enabled for CFS distribution. Check the LastResult column for the status of the last CFS action.

Step 3 Select the **Action** tab to determine if auto topology and IVR NAT are enabled.

Step 4 Select the **Local Topology** and **Active Topology** tabs to verify your IVR VSAN topology.

Step 5 Choose **Fabric*xx* > All VSANs > Domain Manager** to verify unique domain IDs if IVR NAT is not enabled.

Step 6 Choose **Zone > IVR > Edit Local Full Zone Database** to verify your IVR zones and zone sets and to verify that you have activated your IVR zone set. The active IVR zone set name appears in bold.

Verifying IVR Configuration Using the CLI

Several commands involving multiple configuration tasks can be used to verify the IVR configuration.

Table 13-1 CLI Commands for Verification of IVR

CLI Command	Description
show fcdomain domain-list	Verifies unique domain ID assignment. If a domain overlap exists, edit and verify the allowed-domains list or manually configure static, non-overlapping domains for each participating switch and VSAN.
show interface brief	Verifies if the ports are operational, VSAN membership, and other configuration settings covered previously.
show fcns database	Verifies the name server registration for all devices participating in the IVR.
show zoneset active	Displays zones in the active zone set. This should include configured IVR zones.
show ivr fcdomain	Displays the IVR persistent fcdomain database.
show ivr internal	Shows the IVR internal troubleshooting information.
show ivr pending-diff	Shows the IVR pending configuration.
show ivr service-group	Shows the difference between the IVR pending and configured databases.
show ivr tech-support	Shows information that is used by your customer support representative to troubleshoot IVR issues.
show ivr virtual-domains	Shows IVR virtual domains for all local VSANs.
show ivr virtual-fcdomain-add-status	Shows IVR virtual fcdomain status.
show ivr vsan-topology	Verifies the configured IVR topology.
show ivr zoneset	Verifies the IVR zone set configuration.

Table 13-1 CLI Commands for Verification of IVR (continued)

CLI Command	Description
show ivr zone	Verifies the IVR zone configuration.
clear ivr zone database	Clears all configured IVR zone information. **Note** Clearing a zone set erases only the configured zone database, not the active zone database.

The following **show internal** commands can be useful for troubleshooting IVR issues.

```
add-rw                  Show ivr fcid rewrite fsm internals
  adv_vsans               Show IVR advertise VSANs for a native VSAN and domain
  area-port-allocation    Show IVR area-port allocation
  capability-fsm          Show IVR capability fsm internal debug information
  commit-rw               Show ivr fcid rewrite fsm internals
  debug-log-buffer1       Show IVR debug-log buffer
  del-rw                  Show ivr fcid rewrite fsm internals
  dep                     Show ivr dep internals
  device-list             Show ivr device list
  distribution            Show ivr distribution internals
  domain-capture-list     Show ivr domain controller capture list
  drav-fsm                Show DRAV FSM details
  event-history           Show ivr internal event history
  fcid-rewrite-fsm        Show ivr fcid rewrite fsm internals
  fcid-rewrite-list       Show ivr fcid rewrite entries
  fsmtca                  Show IVR FSM transition statistics
  global-data             Show ivr global data
  mem-stats               Show memory statistics
  nhvsan-change           Show ivr fcid rewrite fsm internals
  plogi-captured-list     Show ivr PLOGI captured
  pnat                    Show IVR payload NAT internal information
  pvm                     Show IVR PV Master internal information
  tu-fsm                  Show TU FSM internal debug information
  vdri-fsm                Show VDRI FSM internal debug information
  virtual-domains         Show IVR capability fsm internal debug information
  vsan-rewrite-list       Show ivr vsan rewrite list
  vsan-topology           Show internal information on IVR VSAN topology
  vsan-topology-graph     Show IVR VSAN Topology graph internal debug information
  zone-fsm                Show ivr zone fsm internals
```

IVR Enhancements by Cisco SAN-OS Release

Table 13-2 lists the IVR enhancements by Cisco SAN-OS release.

Table 13-2 IVR Enhancements by Cisco SAN-OS Release

Cisco SAN-OS Release	IVR Enhancement
Release 3.3(1)	Support for read-only LUN attribute in IVR zone configuration.
Release 2.1(2)	Persistent FC IDs and domains for IVR

Table 13-2 IVR Enhancements by Cisco SAN-OS Release

Cisco SAN-OS Release (continued)	IVR Enhancement
Release 2.1(1a)	• IVR NAT • AFIDs • Auto-topology • Virtual domains added to remote domain lists • IVR LUN zoning • IVR QoS zoning • Service group
Release 2.0(1)	IVR with CFS support
Release 1.3(4a)	Virtual domains added to remote domain lists
Release 1.3(1)	IVR introduced

IVR Issues

This section describes the problems associated with IVR. This section includes the following topics:

IVR allows device discovery across VSANs. IVR also supports FC ping and FC traceroute across VSANs using the following criteria:

- Either FC ID or pWWN can be used.
- Must be initiated from a switch with an active IVR zone member.

IVR Licensing Issues

To use IVR, you must obtain the correct licenses for the IVR features you are using and install those licenses on every IVR-enabled switch in your fabric. Table 13-3 shows which license to purchase based on the IVR feature you are using and the module or chassis you have enabled IVR on.

Table 13-3 License Requirements for IVR

IVR Feature	Chassis or Module Type	License Required	Number of Licenses
IVR over Fibre Channel and IVR NAT over Fibre Channel	All	ENTERPRISE_PKG	One per IVR-enabled chassis
IVR over FCIP	MDS 9216i [1]	None	None
	MPS-14/2	SAN_EXTN_OVER_IPS2	One per module running IVR over FCIP
	MPS-18/4 or MPS-18/4 FIPS	SAN_EXTN_OVER_MPS_184_FIPS	
	IPS-8	SAN_EXTN_OVER_IP	
	IPS-4	SAN_EXTN_OVER_IPS4	

1. Cisco MDS 9216i enables the SAN_EXTENSION features without a license for the two Gigabit Ethernet ports on the integrated supervisor card.

Note If you are using IVR over FCIP and Fibre Channel, you need the ENTERPRISE_PKG as well as the appropriate SAN extension license as shown in Table 13-3.

Tip Be sure to enter the correct chassis serial number when purchasing your license packages. Choose **Switches > Hardware** and check the SerialNo Primary for the switch chassis in Fabric Manager or use the **show license host-id** CLI command to obtain the chassis serial number for each switch that requires a license. Your license will not operate if the serial number used does not match the serial number of the chassis you are installing the license on.

See Chapter 6, "Troubleshooting Licensing," for complete details on troubleshooting licensing issues.

Cannot Enable IVR

Symptom Cannot enable IVR.

Table 13-4 Cannot Enable IVR

Symptom	Possible Cause	Solution
Cannot enable IVR.	License not installed and grace period has expired.	Purchase and install the appropriate licenses. See the "IVR Licensing Issues" section on page 13-6.
	Switch not running Cisco SAN-OS Release 1.3(1) or later.	Upgrade to the Cisco SAN-OS release required for the IVR features you want to use. See Table 13-1 and Chapter 2, "Troubleshooting Installs, Upgrades, and Reboots."
	Using IVR auto topology but CFS distribution is not enabled.	Choose **Fabric*xx* > All VSANs > IVR**, set the Global drop-down menu to **enable**, and click **Apply Changes** in Fabric Manager. Or use the **ivr distribute** CLI command before enabling IVR.

IVR Network Address Translation Fails

Symptom IVR NAT fails.

Table 13-5 IVR NAT Fails

Symptom	Possible Cause	Solution
IVR NAT fails.	Internal message payload uses destination ID.	IVR NAT modifies the destination ID in the Fibre Channel header. If this same destination ID appears inside the message payload, Cisco SAN-OS may not detect it and IVR NAT fails. Disable IVR NAT and ensure that all domain IDs are unique. Refer to the Cisco MDS 9000 Family configuration guides at the following website for a list of payloads that work with IVR NAT when the payload includes the destination ID: http://www.cisco.com/en/US/products/ps5989/products_installation_and_configuration_guides_list.html
	Some switches are running IVR without NAT.	You cannot combine IVR and IVR NAT in the same VSAN. Use the same IVR configuration on all switches. Deactivate the active zone set before converting to IVR or IVR NAT.

IVR Zone Set Activation Fails

If zone set activation fails, you may see the following system messages:

Error Message `IVR-2-IVZS_ACTIVATION_FAILED_RETRYING: Inter-VSAN zoneset activation failed in VSAN [dec] : [chars]. retrying after [dec] seconds.`

Explanation Inter-VSAN zone set activation failed in the listed VSAN. This could be an intermittent, regular zone set activation error. The activation will be retried after the number of seconds listed in the message.

Recommended Action No action is required.

Introduced Cisco MDS SAN-OS Release 2.1(2).

Error Message `IVR-3-IVZ_ACTIVATION_FAILED: Inter-VSAN zoneset [chars] activation failed.`

Explanation Inter-VSAN zone set activation failed.

Recommended Action No action is required.

Introduced Cisco MDS SAN-OS Release 1.3(1).

Error Message `IVR-3-IVZ_ACTIVATION_FAILED_VSAN: Inter-VSAN zoneset [chars] activation failed in VSAN [dec].`

Explanation Inter-VSAN zone set activation failed in the VSAN.

Recommended Action No action is required.

Introduced Cisco MDS SAN-OS Release 1.3(1).

Error Message `IVR-5-IVZS_ACTIVATION_RETRYING: Inter-VSAN zoneset activation failed with error [hex] in VSAN [dec]. retrying after [dec] seconds.`

Explanation Inter-VSAN zone set activation failed with VSAN shown in the error message. This could be an intermittent regular zone set activation error. The activation retried in the number of seconds shown in the error message.

Recommended Action No action is required.

Introduced Cisco MDS SAN-OS Release 1.3(3).

Error Message `IVR-5-IVZS_WAITING_FOR_LOWEST_SWWN: Waiting for lowest switch WWN Inter-VSAN enabled switch in VSAN [dec].`

Explanation This switch does not have the lowest switch world wide name (sWWN) in the VSAN. Only the inter-VSAN (IVR) enabled switch with the lowest sWWN can add the IVR zones to the regular active zone set in a VSAN. This switch is waiting until the IVR switch with the lowest sWWN adds the IVR zone and reactivates the zone set.

Recommended Action No action is required.

Introduced Cisco MDS SAN-OS Release 2.0(1b).

Symptom IVR zone set activation fails.

Table 13-6 IVR Activation Fails

Symptom	Possible Cause	Solution
IVR zone set activation fails.	Overlapping domain IDs.	Use static domain IDs to assign unique domain IDs to each switch in the VSAN or use IVR NAT. Choose **Fabric*xx* > All VSANs > Domain Manager** in Fabric Manager or use the **fcdomain domain** *domain-id* **[static | preferred] vsan** *vsan-id* CLI command
	Default zone policy is permit.	Choose **Zone > IVR > Edit Local Full Zone Database** in Fabric Manager. Right-click the IVR zone set that you want to activate and select **Activate**. Check the **Create Active Zone Set if none Present** check box or use the **force** option with the **ivr zoneset activate** CLI command.
	Default zone policy is deny and no active zone set present.	
	No active zone set.	No zone set has been activated. See the "Troubleshooting Zone Set Activation" section on page 14-8 to activate a zone set on an IVR-enabled switch, or use the **force** option when activating the IVR zone set.

Border Switch Fails

If an IVR-enabled switch fails, you must update the IVR topology to reflect this change if you are not using auto topology.

Symptom Border switch fails.

Table 13-7 Border Switch Fails

Symptom	Possible Causes	Solutions
Border switch fails.	IVR topology incorrect.	Choose **Fabricxx > All VSANs > IVR** and select the **Action** tab in Fabric Manager. Check the **Auto Discover Topology** check box and click **Apply Changes.** Select the **CFS** tab and set ConfigAction to **commit** and click **Apply Changes**. Or use the **ivr vsan topology auto** CLI command to automatically reconfigure the IVR topology, or use the **ivr vsan topology database** CLI command to manually reconfigure the IVR topology.

Traffic Does Not Traverse IVR Path

Symptom Traffic does not traverse the IVR path.

Table 13-8 Traffic Does Not Traverse IVR Path

Symptom	Possible Cause	Solution
Traffic does not traverse the IVR path.	Fabric includes an SN5428 or MDS 9020 switch and you have not added the IVR virtual domains to the remote VSAN domain lists.	Choose **Fabric*xx* > All VSANs > IVR** and select the **Action** tab in Fabric Manager.Fill in the Create Virtual Domains for VSAN field and click **Apply Changes.** Select the **CFS** tab, and set ConfigAction to **commit**, and click **Apply Changes.** Or use the i**vr virtual-fcdomain-add vsan-ranges** CLI command to add existing and future virtual domains to the domain list for the selected VSANs. Repeat this on all edge VSANs.
	Internal message payload uses destination ID.	See the "IVR Network Address Translation Fails" section on page 13-8.
	Devices are in different IVR service groups.	Verify the IVR service groups. Choose **Fabric*xx* > All VSANs > IVR and** select the **Service Group** tab in Fabric Manager. Or use the **show ivr service-group** CLI command. Move the VSANs into the same IVR service group. Choose **Fabric*xx* > All VSANs > IVR** and select the **Service Group** tab in Fabric Manager. Or use the **ivr service-group** CLI command. Use the **ivr service-group activate** CLI command to activate this change. If CFS is enabled, use the **ivr commit** CLI command to commit this change.

Link Isolated

Symptom Link isolated.

Table 13-9 Link Isolated

Symptom	Possible Cause	Solution
Link isolated.	Virtual domain overlap.	Choose **Fabric*xx* > All VSANs > Domain Manager** in Fabric Manager to verify a domain overlap. Choose **Fabric*xx* > All VSANs > IVR** and select the **Action** tab in Fabric Manager.Fill in the Create Virtual Domains for VSAN field and click **Apply Changes.** Select the **CFS** tab and set ConfigAction to **commit,** and click **Apply Changes.** Or use the **show fcdomain domain-list** CLI command to verify a domain overlap. Use the **ivr widthdraw domain** CLI command to remove the overlapped domain. Use persistent FC IDs to reassign the overlapped domain. Use the **ivr virtual-fcdomain-add vsan-ranges** CLI command to add existing and future virtual domains to the domain list for the selected VSANs. Repeat this on all edge VSANs.
	Internal message payload uses destination ID.	See the "IVR Network Address Translation Fails" section on page 13-8.

Persistent FC ID for IVR Failed

Symptom Persistent FC ID for IVR failed.

Table 13-10 Persistent FC ID for IVR Failed

Symptom	Possible Cause	Solution
Persistent FC ID for IVR failed.	Selected virtual FC ID does not match the assigned virtual domain.	Use the **show ivr fcdomain database** CLI command to verify the virtual domain ID. Use the **native-autonomous-fabric-num** CLI command to assign the virtual domain and then use the **pwwn** CLI command to map the pWWN to an appropriate FC ID that matches the virtual domain ID. Refer to the Cisco MDS 9000 Family configuration guides for the related procedure to configure Persistent FC IDs for IVR.

LUN Configuration Failure in IVR Zoning

Symptom LUN configuration failed in IVR zoning.

Table 13-11 LUN Configuration Failure in IVR Zoning

Symptom	Possible Cause	Solution
LUN configuration failed in IVR zoning.	One or more switches in the VSAN are not running Cisco MDS SAN-OS Release 2.1(1a) or later.	Upgrade to the Cisco SAN-OS release required for the IVR features you want to use. See Table 13-1 and Chapter 2, "Troubleshooting Installs, Upgrades, and Reboots."

Host Does Not Have Write Access to Storage

Symptom Host does not have write access to storage.

Table 13-12 Host Does Not Have Write Access to Storage

Symptom	Possible Cause	Solution
Host does not have write access to storage.	Host is a member of a read-only zone.	If a host is a member of a read-only zone, the host has no write access to any IVR zone it may be a member of. Remove the host from the read-only zone.

Locked IVR CFS Session

IVR uses CFS to distribute the IVR configuration. If you enable IVR auto topology, it also uses CFS to distribute and update the IVR VSAN topology on all switches. In rare cases, you may encounter problems where CFS locks IVR so that you cannot modify the configuration.

Symptom Locked IVR CFS session.

Table 13-13 Locked IVR CFS Session

Symptom	Possible Cause	Solution
Locked IVR CFS session.	CFS did not give up the session lock for IVR after the last commit or an IVR configuration change is pending and has not been committed.	Choose **Fabric*xx* > All VSANs > IVR** and select the **CFS** tab in Fabric Manager. Set the ConfigView As drop-down menu to **pending** and verify the pending configuration changes. Set the ConfigAction drop-down menu to **commit** to save these changes, **abort** to discard the changes, or **clear** to clear the session lock. Click **Apply Changes**. Or use the **show ivr pending-diff** CLI command to determine if you have a pending configuration change. Use **ivr commit** to commit this change or **ivr abort** to discard the changes and free up the session lock. If you do not have pending configuration changes, use the **clear ivr session** CLI command to free the session lock.

CFS Merge Failed

If a CFS merge fails, you may see the following system messages:

Error Message `IVR-2-CFS_PEER_LOST_WITHIN_SESSION: CFS peer with switch wwn [chars] was lost in the middle of an active CFS session. Abort the CFS session and re-enter the configuration changes.`

Explanation Due to port flaps (enable and disable of the VSAN), link outages, switch restarts and so on, a CFS peer switch of IVR was lost. The current configuration changes would not be applied to this peer until the peer merges with this switch. The CFS merge may fail if the configuration at the lost peer conflicts with the changes made in this session. Also, IVR auto topology could be out of sync. with this peer. We recommend that you discard this CFS session using **ivr abort** command and then re-enter the configuration changes. You can alternatively use Fabric Manager and/or Device Manager instead of the command line method.

Recommended Action No action is required.

Introduced Cisco MDS SAN-OS Release 2.0(1b).

Error Message `IVR-3-MERGE_FAILED: [chars].`

Explanation An error occurred while merging the configuration. The reason for the failure is shown in the error message.

Recommended Action If you purchased Cisco support through a Cisco reseller, contact the reseller directly. If you purchased support directly from Cisco Systems, contact Cisco Technical Support.

Introduced Cisco MDS SAN-OS Release 2.0(1b).

Symptom CFS merge failed.

Table 13-14 CFS Merge Failed

Symptom	Possible Cause	Solution
CFS merge failed.	IVR topology incorrect.	Choose **Fabric*xx* > All VSANs > IVR** and select the **Action** tab in Fabric Manager. Check the **Auto Discover Topology** check box and click **Apply Changes.** Select the **CFS** tab and set ConfigAction to **commit** and click **Apply Changes.** Or use either the **ivr vsan topology auto** CLI command to automatically reconfigure the IVR topology, or the **ivr vsan topology database** CLI command to manually reconfigure the IVR topology.
	Maximum number of VSANs or IVR VSAN topology entries reached.	Reconfigure your fabric before merging to reduce the number of VSANs or topology entries. See Appendix C, "Configuration Limits for Cisco MDS SAN-OS Release 3.x."
	Conflicting entries in the AFID database.	Modify the conflicting entries in the AFID database.
	Conflicting user-configured IVR VSAN topology database entries.	Enable IVR auto topology on both fabrics before the merge and remove any user-configured IVR VSAN topology database entries.

Troubleshooting the IVR Wizard

The IVR wizard in Fabric Manager simplifies the process of configuring IVR across your fabric. The IVR wizard automatically checks for the appropriate Cisco SAN-OS version across the switches in the VSAN and determines which IVR features the switches are capable of. (See Table 13-1.)

This section describes the following warning or error dialog boxes that display when you configure IVR using the Fabric Manager IVR wizard:

- Warning: Not All Switches Are IVR NAT Capable or Are Unmanageable, page 13-16
- Error: The Following Switches Do Not Have Unique Domain IDs, page 13-16
- Error: Pending Action/ Pending Commits, page 13-17
- Error: Fabric Is Changing. Please Retry the Request Later, page 13-17

Warning: Not All Switches Are IVR NAT Capable or Are Unmanageable

Symptom Warning: Not all switches are IVR NAT capable or are unmanageable.

Table 13-15 Not All Switches Are IVR NAT Capable or Are Unmanageable

Symptom	Possible Cause	Solution
Warning: Not all switches are IVR NAT capable or are unmanageable.	One or more switches in the fabric are not running Cisco MDS SAN-OS Release 2.1(1a) or later.	Upgrade to the Cisco SAN-OS release required for the IVR features you want to use. See Table 13-1 and Chapter 2, "Troubleshooting Installs, Upgrades, and Reboots."
	One or more switches in the fabric cannot communicate with Fabric Manager or are not Cisco SAN-OS switches.	Determine if any of the problem switches are required in the IVR topology. If not, ignore this message and proceed with the IVR configuration. If they are required, choose **Switches** and check the Status column to determine the cause and address the problem.

Error: The Following Switches Do Not Have Unique Domain IDs

Symptom The following switches do not have unique domain IDs.

Table 13-16 The Following Switches Do Not Have Unique Domain IDs

Symptom	Possible Cause	Solution
The following switches do not have unique domain IDs.	The listed switches have duplicate domain IDs in two or more VSANs in your proposed IVR configuration.	Choose **Fabric*xx* > All VSANS > Domain Manager** and set the ConfigDomainId to a unique number and set the Config Type drop-down menu to **static** in Fabric Manager. Set the Restart drop-down menu to **disruptive** and click **Apply Changes**. This triggers a disruptive restart to make the running domain ID match the configured domain ID.
		Use IVR NAT. This may require upgrading to Cisco MDS SAN-OS Release 2.1(1a) or later.

Error: Pending Action/ Pending Commits

Symptom Pending action on pending commit error displays.

Table 13-17 Pending Action/Pending Commits

Symptom	Possible Cause	Solution
Pending action on pending commit error displays.	A separate IVR configuration change that was not committed.	IVR has pending changes that were not committed. Choose **Fabric*xx* > All VSANS > IVR** and select the **CFS** tab in Fabric Manager. Set the View Config As drop-down menu to **pending** and verify the pending configuration changes. Set the ConfigAction drop-down menu to **commit** to save these changes or **abort** to discard the changes**.** Click **Apply Changes**.
	The IVR CFS session was not unlocked after the last commit.	Choose **Fabric*xx* > All VSANS > IVR** and select the **CFS** tab in Fabric Manager. Set the ConfigAction drop-down menu to **clear** to remove the session lock. Click **Apply Changes**.

Error: Fabric Is Changing. Please Retry the Request Later

This error may occur if there are different versions of Cisco SAN-OS on the IVR-enabled switches. You should upgrade all IVR-enabled switches to the same version of Cisco SAN-OS.