Configuring and Managing VSANs

Configuring and Managing VSANs

You can achieve higher security and greater stability in Fibre Channel fabrics by using virtual SANs (VSANs) on Cisco MDS 9000 Family switches and Cisco Nexus 5000 Series switches. VSANs provide isolation among devices that are physically connected to the same fabric. With VSANs you can create multiple logical SANs over a common physical infrastructure. Each VSAN can contain up to 239 switches and has an independent address space that allows identical Fibre Channel IDs (FC IDs) to be used simultaneously in different VSANs. This chapter includes the following sections:

Information About VSANs

A VSAN is a virtual storage area network (SAN). A SAN is a dedicated network that interconnects hosts and storage devices primarily to exchange SCSI traffic. In SANs, you use the physical links to make these interconnections. A set of protocols run over the SAN to handle routing, naming, and zoning. You can design multiple SANs with different topologies.

With the introduction of VSANs, the network administrator can build a single topology containing switches, links, and one or more VSANs. Each VSAN in this topology has the same behavior and property of a SAN. A VSAN has the following additional features:

- Multiple VSANs can share the same physical topology.
- The same Fibre Channel IDs (FC IDs) can be assigned to a host in another VSAN, thus increasing VSAN scalability.
- Every instance of a VSAN runs all required protocols such as FSPF, domain manager, and zoning.
- Fabric-related configurations in one VSAN do not affect the associated traffic in another VSAN.
- Events causing traffic disruptions in one VSAN are contained within that VSAN and are not propagated to other VSANs.

This section describes VSANs and includes the following topics:

VSANs Topologies

The switch icons shown in both Figure 1: Logical VSAN Segmentation , on page 2 and Figure 2: Example of Two VSANs , on page 3 indicate that these features apply to any switch in the Cisco MDS 9000 Family.

Figure 1: Logical VSAN Segmentation , on page 2 shows a fabric with three switches, one on each floor. The geographic location of the switches and the attached devices is independent of their segmentation into logical VSANs. No communication between VSANs is possible. Within each VSAN, all members can talk to one another.

Figure 1: Logical VSAN Segmentation

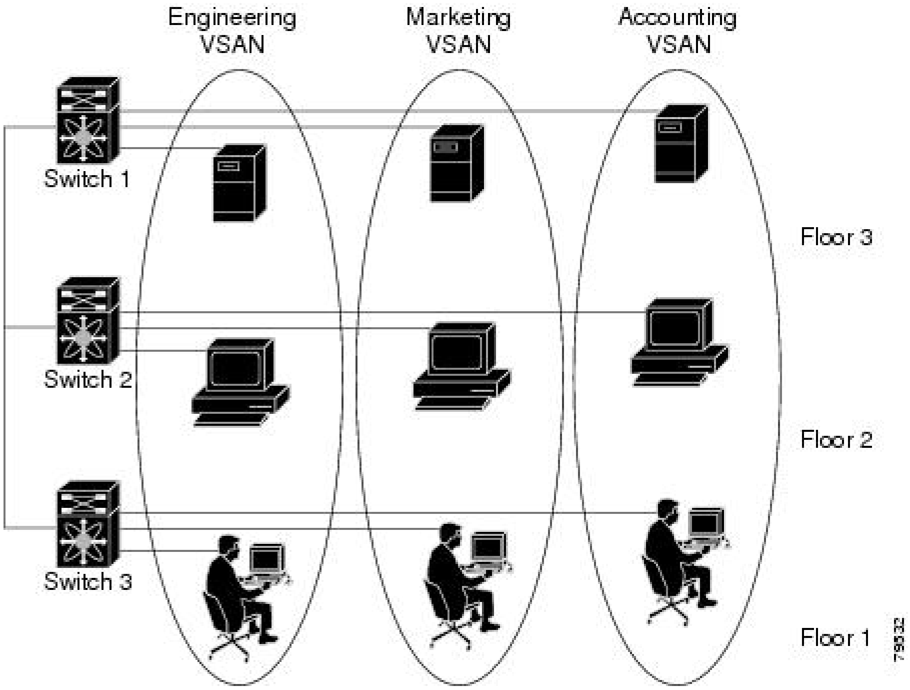
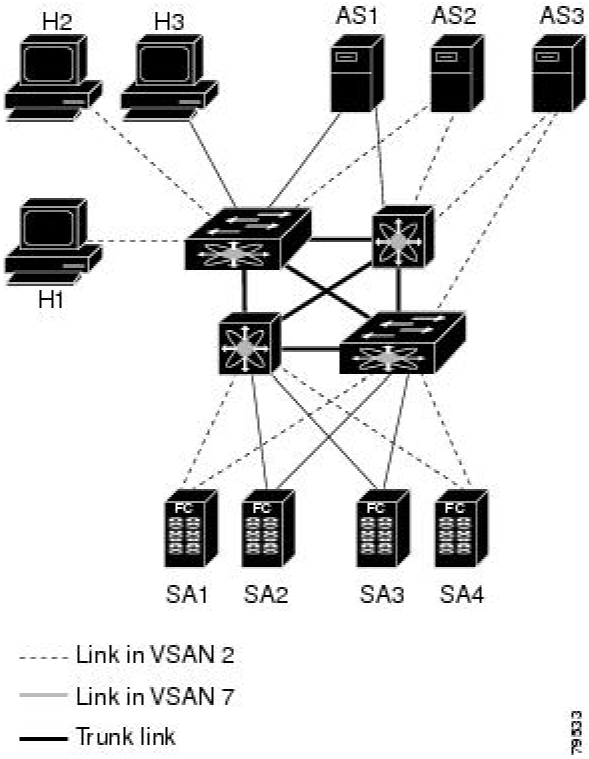


Figure 2: Example of Two VSANs , on page 3 shows a physical Fibre Channel switching infrastructure with two defined VSANs: VSAN 2 (dashed) and VSAN 7 (solid). VSAN 2 includes hosts H1 and H2, application servers AS2 and AS3, and storage arrays SA1 and SA4. VSAN 7 connects H3, AS1, SA2, and SA3.

Figure 2: Example of Two VSANs



The four switches in this network are interconnected by trunk links that carry both VSAN 2 and VSAN 7 traffic. The inter-switch topology of both VSAN 2 and VSAN 7 are identical. This is not a requirement and a network administrator can enable certain VSANs on certain links to create different VSAN topologies.

Without VSANs, a network administrator would need separate switches and links for separate SANs. By enabling VSANs, the same switches and links may be shared by multiple VSANs. VSANs allow SANs to be built on port granularity instead of switch granularity. Figure 2: Example of Two VSANs , on page 3 illustrates that a VSAN is a group of hosts or storage devices that communicate with each other using a virtual topology defined on the physical SAN.

The criteria for creating such groups differ based on the VSAN topology:

- VSANs can separate traffic based on the following requirements:
  - Different customers in storage provider data centers
  - Production or test in an enterprise network
  - Low and high security requirements
  - Backup traffic on separate VSANs
  - Replicating data from user traffic
- VSANs can meet the needs of a particular department or application.

VSAN Advantages

VSANs offer the following advantages:

- Traffic isolation—Traffic is contained within VSAN boundaries and devices reside only in one VSAN ensuring absolute separation between user groups, if desired.
- Scalability—VSANs are overlaid on top of a single physical fabric. The ability to create several logical VSAN layers increases the scalability of the SAN.
- Per VSAN fabric services—Replication of fabric services on a per VSAN basis provides increased scalability and availability.
- Redundancy—Several VSANs created on the same physical SAN ensure redundancy. If one VSAN fails, redundant protection (to another VSAN in the same physical SAN) is configured using a backup path between the host and the device.
- Ease of configuration—Users can be added, moved, or changed between VSANs without changing the physical structure of a SAN. Moving a device from one VSAN to another only requires configuration at the port level, not at a physical level.

Up to 256 VSANs can be configured in a switch. Of these, one is a default VSAN (VSAN 1), and another is an isolated VSAN (VSAN 4094). User-specified VSAN IDs range from 2 to 4093.

VSANs Versus Zones

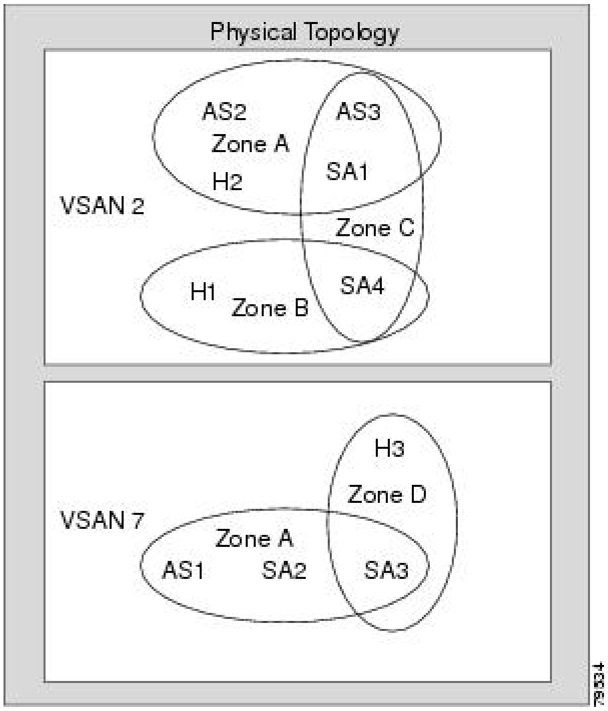
You can define multiple zones in a VSAN. Because two VSANs are equivalent to two unconnected SANs, zone A on VSAN 1 is different and separate from zone A in VSAN 2. Table 1: VSAN and Zone Comparison , on page 4 lists the differences between VSANs and zones.

Table 1: VSAN and Zone Comparison

VSAN Characteristic	Zone Characteristic
VSANs equal SANs with routing, naming, and zoning protocols.	Routing, naming, and zoning protocols are not available on a per-zone basis.
—	Zones are always contained within a VSAN. Zones never span two VSANs.
VSANs limit unicast, multicast, and broadcast traffic.	Zones limit unicast traffic.
Membership is typically defined using the VSAN ID to Fx ports.	Membership is typically defined by the pWWN.
An HBA or a storage device can belong only to a single VSAN—the VSAN associated with the Fx port.	An HBA or storage device can belong to multiple zones.
VSANs enforce membership at each E port, source port, and destination port.	Zones enforce membership only at the source and destination ports.
VSANs are defined for larger environments (storage service providers).	Zones are defined for a set of initiators and targets not visible outside the zone.
VSANs encompass the entire fabric.	Zones are configured at the fabric edge.

The following figure shows the possible relationships between VSANs and zones. In VSAN 2, three zones are defined: zone A, zone B, and zone C. Zone C overlaps both zone A and zone B as permitted by Fibre

Channel standards. In VSAN 7, two zones are defined: zone A and zone D. No zone crosses the VSAN boundary—they are completely contained within the VSAN. Zone A defined in VSAN 2 is different and separate from zone A defined in VSAN 7.



VSAN Configuration

VSANs have the following attributes:

- VSAN ID—The VSAN ID identifies the VSAN as the default VSAN (VSAN 1), user-defined VSANs (VSAN 2 to 4093), and the isolated VSAN (VSAN 4094).
- State—The administrative state of a VSAN can be configured to an active (default) or suspended state. Once VSANs are created, they may exist in various conditions or states.
    - The active state of a VSAN indicates that the VSAN is configured and enabled. By enabling a VSAN, you activate the services for that VSAN.
    - The suspended state of a VSAN indicates that the VSAN is configured but not enabled. If a port is configured in this VSAN, it is disabled. Use this state to deactivate a VSAN without losing the VSAN's configuration. All ports in a suspended VSAN are disabled. By suspending a VSAN, you can preconfigure all the VSAN parameters for the whole fabric and activate the VSAN immediately.
- VSAN name—This text string identifies the VSAN for management purposes. The name can be from 1 to 32 characters long and it must be unique across all VSANs. By default, the VSAN name is a concatenation of VSAN and a four-digit string representing the VSAN ID. For example, the default name for VSAN 3 is VSAN0003.

Note A VSAN name must be unique.

- Load balancing attributes—These attributes indicate the use of the source-destination ID (src-dst-id) or the originator exchange OX ID (src-dst-ox-id, the default) for load balancing path selection.

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 9000 Family switch should work. Generation 2 switching modules support OX ID based load balancing of IVR traffic from IVR-enabled switches.

About VSAN Creation

A VSAN is in the operational state if the VSAN is active and at least one port is up. This state indicates that traffic can pass through this VSAN. This state cannot be configured.

About Port VSAN Membership

Port VSAN membership on the switch is assigned on a port-by-port basis. By default, each port belongs to the default VSAN. You can assign VSAN membership to ports using one of two methods:

- Statically—By assigning VSANs to ports.

See the Assigning Static Port VSAN Membership, on page 10.

- Dynamically—By assigning VSANs based on the device WWN. This method is referred to as dynamic port VSAN membership (DPVM).

See Chapter 25, “Creating Dynamic VSANs.”

Trunking ports have an associated list of VSANs that are part of an allowed list (refer to the *Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide*).

About the Default VSAN

The factory settings for switches in the Cisco MDS 9000 Family have only the default VSAN 1 enabled. We recommend that you do not use VSAN 1 as your production environment VSAN. If no VSANs are configured, all devices in the fabric are considered part of the default VSAN. By default, all ports are assigned to the default VSAN.

Note VSAN 1 cannot be deleted, but it can be suspended.

Note Up to 256 VSANs can be configured in a switch. Of these, one is a default VSAN (VSAN 1), and another is an isolated VSAN (VSAN 4094). User-specified VSAN IDs range from 2 to 4093.

About the Isolated VSAN

VSAN 4094 is an isolated VSAN. All non-trunking ports are transferred to this VSAN when the VSAN to which they belong is deleted. This avoids an implicit transfer of ports to the default VSAN or to another configured VSAN. All ports in the deleted VSAN are isolated (disabled).

Note When you configure a port in VSAN 4094 or move a port to VSAN 4094, that port is immediately isolated.

Caution Do not use an isolated VSAN to configure ports.

Note Up to 256 VSANs can be configured in a switch. Of these, one is a default VSAN (VSAN 1), and another is an isolated VSAN (VSAN 4094). User-specified VSAN IDs range from 2 to 4093.

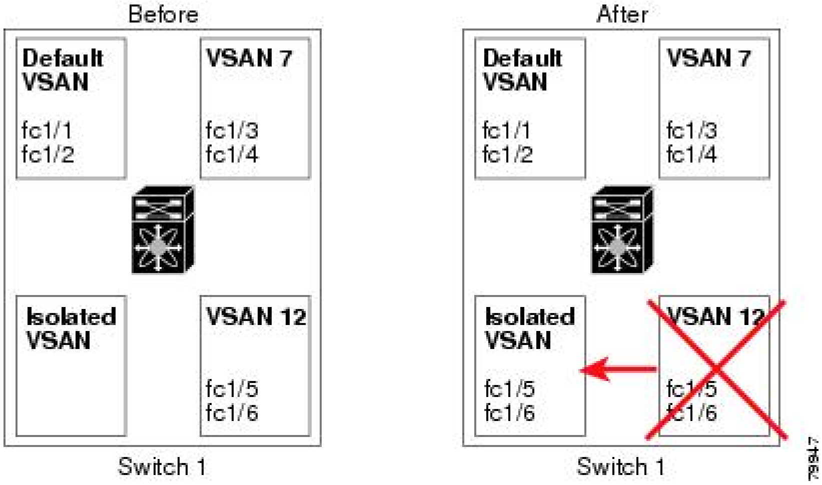
Operational State of a VSAN

A VSAN is in the operational state if the VSAN is active and at least one port is up. This state indicates that traffic can pass through this VSAN. This state cannot be configured.

About Static VSAN Deletion

When an active VSAN is deleted, all of its attributes are removed from the running configuration. VSAN-related information is maintained by the system software as follows:

- VSAN attributes and port membership details are maintained by the VSAN manager. This feature is affected when you delete a VSAN from the configuration. When a VSAN is deleted, all the ports in that VSAN are made inactive and the ports are moved to the isolated VSAN. If the same VSAN is recreated, the ports do not automatically get assigned to that VSAN. You must explicitly reconfigure the port VSAN membership.



- VSAN-based runtime (name server), zoning, and configuration (static routes) information is removed when the VSAN is deleted.
- Configured VSAN interface information is removed when the VSAN is deleted.

Note The allowed VSAN list is not affected when a VSAN is deleted (refer to the *Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide*).

Any commands for a nonconfigured VSAN are rejected. For example, if VSAN 10 is not configured in the system, then a command request to move a port to VSAN 10 is rejected.

About Load Balancing

Load balancing attributes indicate the use of the source-destination ID (src-dst-id) or the originator exchange OX ID (src-dst-ox-id, the default) for load balancing path selection.

About Interop Mode

Interoperability enables the products of multiple vendors to come into contact with each other. Fibre Channel standards guide vendors towards common external Fibre Channel interfaces. See the "Switch Interoperability" section on page 27-5 .

About FICON VSANs

You can enable FICON in up to eight VSANs. See the "FICON VSAN Prerequisites" section on page 24-6 .

Host Provisioning Wizard

The Host Provisioning wizard provides an intuitive way to commission a new host or decomission an existing host without requiring the use of multiple tools and features. The wizard allows you to create a device alias, and configure DPVM, zoning, and flow creation.

Licensing Requirements for VSAN

The following table shows the licensing requirements for this feature:

License	License Description
ENTERPRISE_PKG	The enterprise license is required to enable VSAN. For a complete explanation of the licensing scheme, see the *Cisco MDS 9000 Family NX-OS Licensing Guide* .

Default Settings

Table 2: Default VSAN Parameters , on page 8 lists the default settings for all configured VSANs.

Table 2: Default VSAN Parameters

Parameters	Default
Default VSAN	VSAN 1.
State	Active state.
Name	Concatenation of VSAN and a four-digit string representing the VSAN ID. For example, VSAN 3 is VSAN0003.
Load-balancing attribute	OX ID (src-dst-ox-id).

Configuring VSANs

This section includes the following topics:

Multi-tenancy with MDS9000 and DCNM for SAN

Cisco DCNM is capable of providing users a partial view of the installed devices. To ensure that you have a clear understanding for multi-tenancy functionality on DCNM. Following is an example of multi-tenancy applied to a Fiber Channel fabric.

Imagine to have two users configured on your fabric. The first one is the SAN administrator, with full privileges. The second user, called vsanUser, has limited privileges enforced by the Role Based Access Control capabilities of MDS9000 devices and DCNM for SAN. In our example, the user vsanUser is only allowed to see and work on VSAN 2 and 444. He is not allowed to act upon all other VSANs in the fabric. In other words, the user vsanUser has read-write capabilities on VSAN 2 and 444 but he has not even read-only access to other VSANs. This user was configured with the custom role vsanRole as indicated below:

```
sw172-22-46-182# sh role name vsanRole

Role: vsanRole

vsan policy: deny

Permitted vsans: 2,444

-------------------------------------------

Rule Type Command-type Feature

-------------------------------------------

1. permit show *

2. permit config *

3. permit exec *

sw172-22-46-182#

vsanUser md5 des(no) vsanRole
```

When user vsanUser belonging to role vsanRole opens a fabric with multiple VSAN via DCNM SAN client, he will only see vsans 2 and 444. Instead, the SAN administrator would see all VSANs configured on switches.

Note DCNM SAN is not doing any of this filtering; MDS9000 switch is the filtering point enforced by roles.

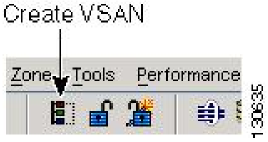
Creating VSANs

You cannot configure any application-specific parameters for a VSAN before creating the VSAN.

To create and configure VSANs, follow these steps:

Procedure

Step 1 Click the Create VSAN icon.



Note As of Cisco SAN-OS Release 3.1(2) and later, if you check the Static Domain IDs check box, DCNM-SAN creates the VSAN in suspended mode and then automatically activates the VSAN.

Step 2 Check the switches that you want in this VSAN.

Step 3 Fill in the VSAN Name and VSAN ID fields.

Step 4 Set the **LoadBalancing** value and the **InterOperValue**.

Step 5 Set the Admin State to active or suspended.

Step 6 Check the **Static Domain Ids** check box to assign an unused static domain ID to the VSAN.

Step 7 (Optional) Select the **FICON** and **Enable Fabric Binding for Selected Switches** options if you want these features enabled.

See the *Configuring FICON* section and refer to the *Cisco MDS 9000 Family NX-OS Security Configuration Guide* for details.

Step 8 Complete the fields in this dialog box and click Create to add the VSAN or click **Close**.

Assigning Static Port VSAN Membership

To statically assign VSAN membership for an interface, follow these steps:

Procedure

Step 1 Choose FC Interfaces > Physical from the Physical Attributes pane. You see the interface configuration in the Information pane.

Step 2 Click the General tab.

You see the Fibre Channel general physical information. Double-click and complete the PortVSAN field.

Step 3 Click **Apply Changes** to save these changes, or click **Undo Changes to** discard any unsaved changes.

Deleting Static VSANs

To delete a VSAN and its attributes, follow these steps:

Procedure

Step 1 Select **All VSANs** from the Logical Domains pane.

The VSANs in the fabric are listed in the Information pane.

Step 2 Right-click the VSAN that you want to delete and select **Delete Row** from the drop-down menu.

You see a confirmation dialog box.

Step 3 Click **Yes** to confirm the deletion or **No** to close the dialog box without deleting the VSAN.

Configuring Load Balancing

To configure load balancing on an existing VSAN, follow these steps:

Procedure

Step 1 Choose Fabric xx > All **VSANs** from the Logical Domains pane.

You see the VSAN configuration in the Information pane.

Step 2 Select a VSAN and complete the LoadBalancing field.

Step 3 Click **Apply Changes** to save these changes, or click **Undo Changes** to discard any unsaved changes.

Commissioning a Host

To commission a new host, follow these steps:

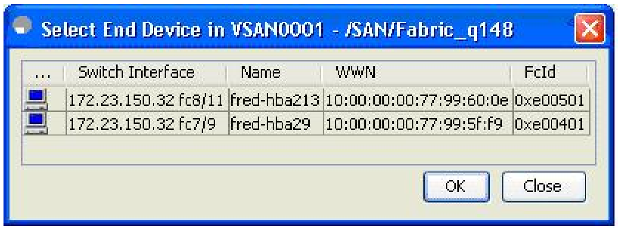
Procedure

Step 1 From the DCNM-SAN window, select **Tools > Host Provisioning**.

The Host Provisioning wizard window is displayed.

Step 2 Click the **Commission** radio button.

Step 3 Click **[...]** and select the host from the existing configurations or VSAN, or enter the WWN of a host that is not in VSAN or not configured yet.



...	Switch Interface	Name	WWN	FcId
	172.23.150.32 fc8/11	fred-hba213	10:00:00:00:77:99:60:0e	0xe00501
	172.23.150.32 fc7/9	fred-hba29	10:00:00:00:77:99:5f:f9	0xe00401

If the host configuration already exists, the switch, device alias, and VSAN information are populated in the window.

If the configuration does not exist already, enter a device alias for the WWN, enter a switch where the configuration will be initiated, and select a VSAN to which the host should belong. The entries are created and saved when you click Next in the Host Provisioning wizard window.

Step 4 Uncheck the **Skip Zoning** check box.

Step 5 Click Next. The Select Targets and the Select Zone windows appear.

Step 6 Uncheck the **Skip DPVM** check box.

Step 7 Click Next. The DPVM entries are created.

Step 8 Click **Next**.

The Select Targets window appears.

Note The Host Provisioning wizard requires that basic and enhanced device alias, DPVM, and CFS to be enabled in all switches in the selected VSAN.

Step 9 Select the target with which the host needs to communicate, and click **Add**.

The target entry is moved to the bottom of the window.

Step 10 Click **Next**.

The Select Zone window appears.

Step 11 Select a zone and check the **Create Flow after Activation** check box.

The host and storage are added to a zone and the zone is activated, and a flow between host and storage is created when you click Finish.

Step 12 Click **Finish**.

The device alias and DPVM entries are created, a zone is created and activated, and the flow is created based on the check boxes you checked.

Decommissioning a Host

To decommission an existing host, follow these steps:

Procedure

Step 1 From the DCNM-SAN window, select **Tools > Host Provisioning**.

The Select Host window appears.

Step 2 Click the **Decommission** radio button.

Step 3 Click **[...]** and select the host from the existing configurations or VSAN, or enter the WWN of a host that is not in VSAN.

The device alias and DPVM state from all of the switches in the selected VSAN are populated if device alias with CFS and CFS DPVM are enabled and if the WWN is an eight-byte number.

Step 4 Click Finish. The device aliases are removed.

Step 5 Uncheck the **Skip Zoning** check box.

The WWN zone member is removed from all zones. If the zones without a WWN member become single member zones, these zones also are removed.

Step 6 Click Finish. If there is a local active zone set change due to the removal of zones, the appropriate zone set is activated.

Step 7 Uncheck the **Skip DPVM** check box.

Step 8 Click Finish. The DPVM entry is removed.

Step 9 Click **Next**.

The Decommission Zones window appears.

Step 10 Check the **Remove Flow after Deactivation** check box.

The flow entry associated with the host is removed when you click Finish.

Step 11 Click **Finish**.

The device alias and DPVM entries are deleted, the zone is deactivated and deleted (if it has only one member after removing the host), and the flow is deleted depending on the check boxes you checked.

Displaying Isolated VSAN Membership

The **show vsan 4094 membership** command displays all ports associated with the isolated VSAN.

To display interfaces that exist in the isolated VSAN, follow these steps:

Procedure

Step 1 Expand Fabric xx, and then select All VSANs in the Logical Domains pane.

You see the VSAN configuration in the Information pane.

Step 2 Click the Isolated Interfaces tab.

You see the interfaces that are in the isolated VSAN.

Field Descriptions for VSAN

The following are the field descriptions for VSAN.

VSAN General

Field	Description
Name	The name of the VSAN. Note that default value will be the string VSANxxxx where xxxx is value of vsanIndex expressed as 4 digits. For example, if vsanIndex is 23, the default value is VSAN0023.
Mtu	The MTU of the VSAN. Normally, this is 2112.
LoadBalancing	The type of load balancing used on this VSAN. • srcdst— use source and destination ID for path selection • srcdst 0xld— use source, destination, and exchange IDs

Field	Description
InterOp	The interoperability mode of the local switch on this VSAN. • standard • interop-1 • interop-2 • interop-3
AdminState	The state of this VSAN.
OperState	The operational state of the VSAN.
InOrderDelivery	The InorderDelivery guarantee flag of device. If true, then the inorder delivery is guaranteed. If false, it is not guaranteed.
DomainId	Specifies an insistent domain ID.
FICON	True if the VSAN is FICON-enabled.
Network Latency	Network latency of this switch on this VSAN. This is the time interval after which the frames are dropped if they are not delivered in the order they were transmitted.

VSAN Membership

Field	Description
Switch	Name of the switch
Ports	FC ports in VSAN
Channels	PortChannels in VSAN
FCIP	FCIP Interfaces in VSAN
iSCSI	iSCSI Interfaces in VSAN
FICON	Interfaces in VSAN by FICON
FC Virtual Interface	Virtual FC interfaces in VSAN

VSAN Interop-4 WWN

Field	Description
VSAN ID	The ID of the VSAN containing the McData switch.
WWN	The WWN of the McData switch.

VSAN Timers

Field	Description
VSAN Id	The ID of the VSAN.
R_A_TOV	The Resource_Allocation_Timeout Value used for FxPorts as the timeout value for determining when to reuse an NxPort resource such as a Recovery_Qualifier. It represents E_D_TOV plus twice the maximum time that a frame may be delayed within the fabric and still be delivered. Note that all switches in a fabric should be configured with the same value of this timeout.
D_S_TOV	The Distributed_Services_Timeout Value which indicates that how long a distributed services requestor will wait for a response.
E_D_TOV	The Error_Detect_Timeout Value used for FxPorts as the timeout value for detecting an error condition. Note that all switches in a fabric should be configured with the same value of this timeout. Note that value must be less than value of D_S_TOV.
NetworkDropLatency	Network latency of this switch on this VSAN.

VSAN Default Zone Policies

Field	Description
Zone Behavior	Represents the initial value for default zone behavior on a VSAN when it is created. If a VSAN were to be deleted and re-created again, the default zone behavior will be set to the value specified for this object.
Propagation Mode	Represents the initial value for zone set propagation mode on a VSAN when it is created. If a VSAN were to be deleted and re-created again, the zone set propagation mode will be set to the value specified for this object.