C H A P T E R **26**

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:

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.

This section describes VSANs and includes the following topics:

VSANs 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.

The switch icons shown in both Figure 26-1 and Figure 26-2 indicate that these features apply to any switch in the Cisco MDS 9000 Family.

Figure 26-1 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 26-1   Logical VSAN Segmentation
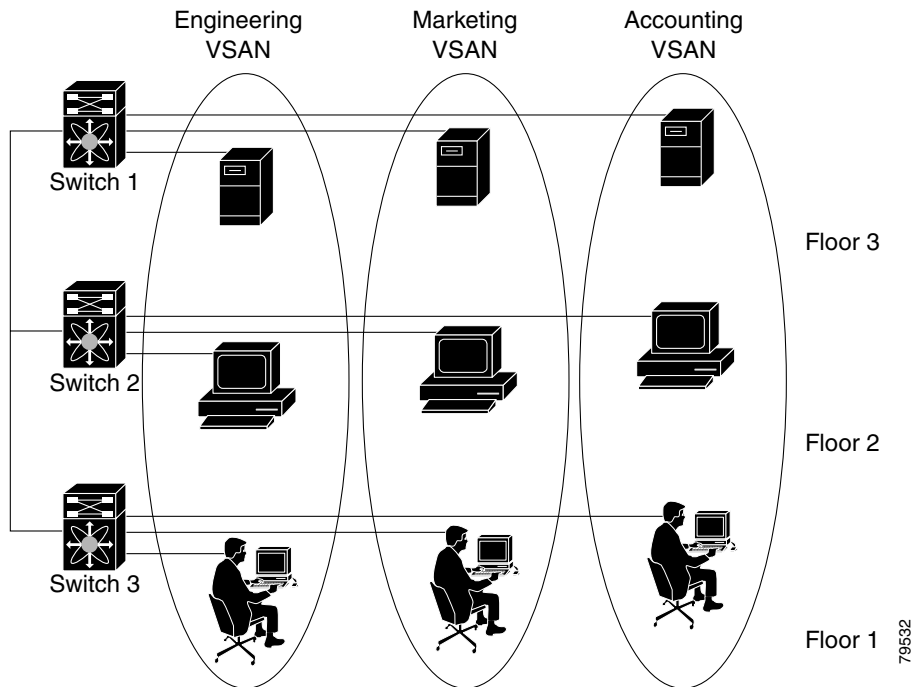
Figure 26-2 shows a physical Fibre Channel switching infrastructure with two defined VSANs: VSAN 2 (dashed) and VSAN 7 (solid). VSAN 2 includes hosts H1 and H2, application servers AS2 and AS3, and storage arrays SA1 and SA4. VSAN 7 connects H3, AS1, SA2, and SA3.

Figure 26-2   Example of Two VSANs
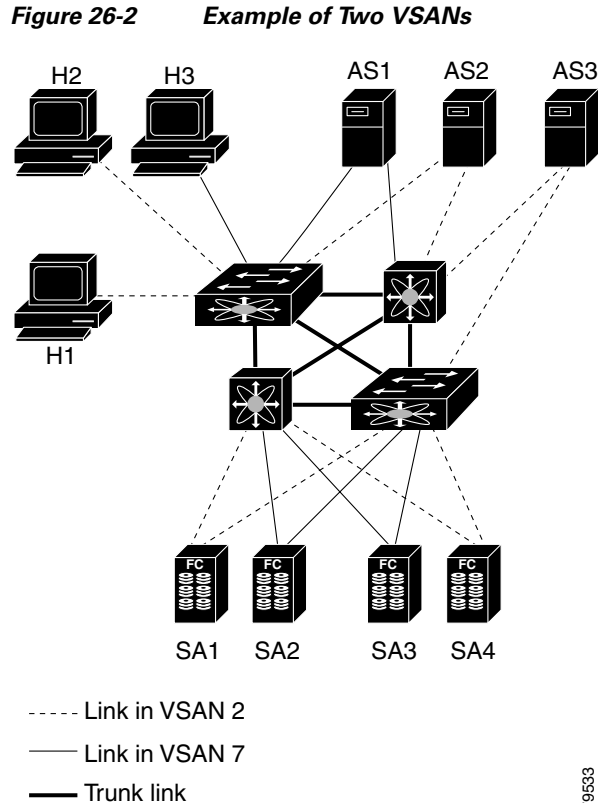
The four switches in this network are interconnected by trunk links that carry both VSAN 2 and VSAN 7 traffic. The inter-switch topology of both VSAN 2 and VSAN 7 are identical. This is not a requirement and a network administrator can enable certain VSANs on certain links to create different VSAN topologies.

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 26-2 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 1024 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 26-1 lists the differences between VSANs and zones.

Table 26-1   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.

Figure 26-3 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.

Figure 26-3   VSANS with Zoning
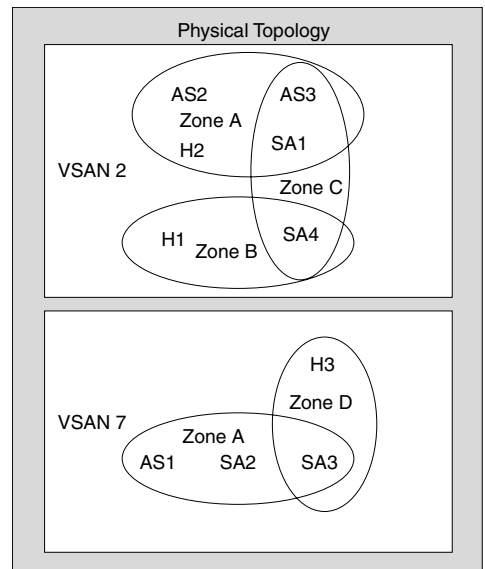
VSAN Configuration

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

This section describes how to create and configure VSANs and includes the following topics:

- About VSAN Creation, page 26-6
- Creating VSANs Statically, page 26-6
- About Port VSAN Membership, page 26-8
- Assigning Static Port VSAN Membership, page 26-8
- About the Default VSAN, page 26-8
- About the Isolated VSAN, page 26-8
- Displaying Isolated VSAN Membership, page 26-9
- Operational State of a VSAN, page 26-9
- Mapping VSANs to VLANs, page 26-9
- About Static VSAN Deletion, page 26-12
- Deleting Static VSANs, page 26-13
- About Load Balancing, page 26-13
- Configuring Load Balancing, page 26-13
- About Interop Mode, page 26-14
- About FICON VSANs, page 26-14

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.

Creating VSANs Statically

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

To create and configure VSANs using Fabric Manager, follow these steps:

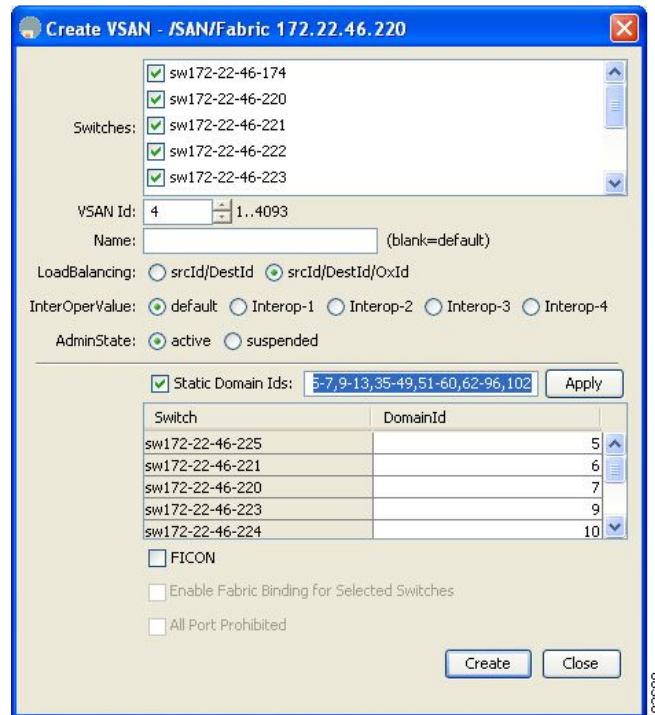**Step 1** Click the **Create VSAN** icon (see Figure 26-4).

Figure 26-4   Create VSAN Icon
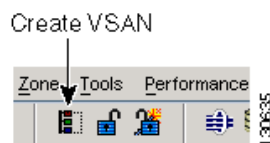
You see the Create VSAN dialog box in Figure 26-5.

Figure 26-5   Create VSAN Dialog Box

> ✎
> **Note**   As of Cisco SAN-OS Release 3.1(2) and later, if you check the Static Domain IDs check box,
> Fabric Manager 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 on page 36-1 and Configuring Fabric Binding, page 47-1 for
details.

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

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" section on page 26-8.

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

  See Chapter 28, "Creating Dynamic VSANs."

Trunking ports have an associated list of VSANs that are part of an allowed list (see Chapter 24, "Configuring Trunking").

Assigning Static Port VSAN Membership

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

Step 1   Choose **Interfaces > FC 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.

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 1024 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 1024 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.

Displaying Isolated VSAN Membership

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

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.

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.

Mapping VSANs to VLANs

> **Note** This section applies to Cisco Nexus 5000 Series switches only.

A VSAN-VLAN mapping indicates the VLAN that is used to transport Fibre Channel traffic for a specific VSAN. Each virtual Fibre Channel interface is associated with only one VSAN. Any VSAN with associated virtual Fibre Channel interfaces must be mapped to a dedicated Fibre Channel over Ethernet (FCoE)-enabled VLAN. FCoE is not supported on private VLANs.

This section provides information about how to configure a virtual Fibre Channel interface and includes the following topics:

- Mapping VSANs to VLANs Using Fabric Manager, page 26-10
- Mapping VSANs to VLANs Using Device Manager, page 26-11

Mapping VSANs to VLANs Using Fabric Manager

To create a mapping between a VSAN and its associated VLAN using Fabric Manager, follow these steps:

✎
Note   You must have a Cisco Nexus 5000 Series switch in the fabric to map a VSAN to a VLAN using the VSAN-VLAN Mapping tab in the Information pane.

Step 1   In the Logical Domains pane, choose **All VSANs**.

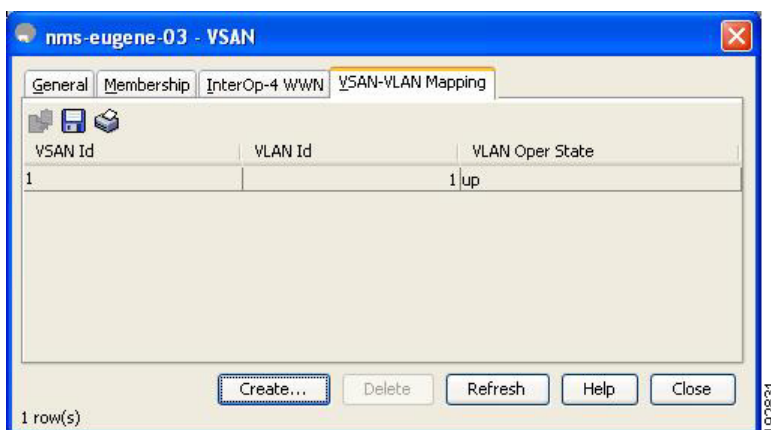You see the VSAN information pane, as shown in Figure 26-6.

Figure 26-6   VSAN Information Pane
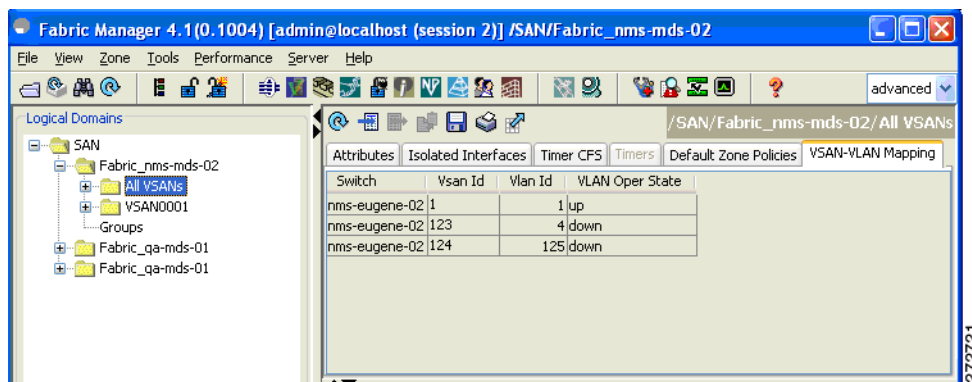
Step 2   In the Information pane, click the **VSAN-VLAN Mapping** tab.

You see the VSAN-VLAN Mapping tab, as shown in Figure 26-7.

Figure 26-7   VSAN-VLAN Mapping Tab

The table shows the existing VSAN-VLAN mappings and the operational state of each VLAN.
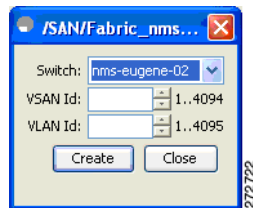
✎
Note   You cannot modify an existing VSAN-VLAN mapping.

Step 3   Click **Create Row** to create a new mapping.

You see the Create dialog box appears, as shown in Figure 26-8.

Figure 26-8   Insert VSAN-VLAN Mapping

Step 4   From the Switch drop-down list, choose a Cisco Nexus 5000 Series switch.

Step 5   In the VSAN Id and VLAN Id fields, enter the VSAN ID and the VLAN ID that will be mapped together.

Step 6   Click **Create** to create the mapping.

Mapping VSANs to VLANs Using Device Manager

To create a mapping between a VSAN and its associated VLAN using Device Manager, follow these steps:

Step 1   Launch Device Manager from the Cisco Nexus 5000 Series switch, as described in the "Launching Device Manager" section on page 6-2.

Step 2   Choose **FC > VSANs**.

You see the VSAN dialog box. In the dialog box, the Membership tab displays the virtual Fibre Channel interfaces associated with a VSAN.

Step 3   Click the **VSAN-VLAN Mapping** tab.

In the VSAN-VLAN Mapping tab, the table lists the existing VSAN-VLAN mappings and the operational state of each VLAN.
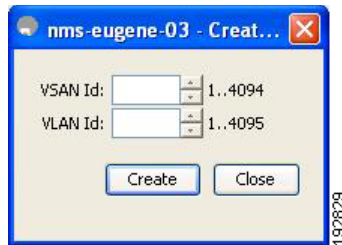
> **Note**   You cannot modify an existing VSAN-VLAN mapping.

Step 4   Click **Create** to create a new mapping.

You see the Create VSAN-VLAN Mapping dialog box as shown in Figure 26-9.

Figure 26-9　　Create VSAN-VLAN Mapping

Step 5　In the VSAN Id and VLAN Id fields, enter the VSAN ID and the VLAN ID that will be mapped together.

Step 6　Click **Create** to create the mapping.

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 (see Figure 26-10).

Figure 26-10　　VSAN Port Membership Details
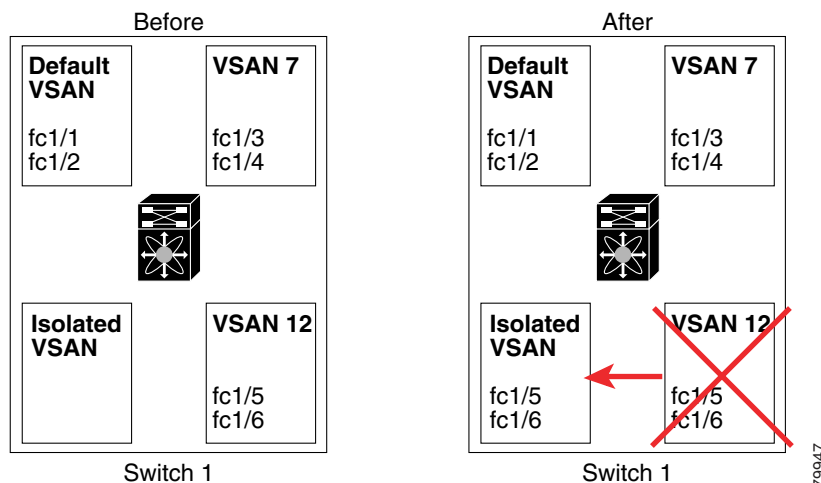
- VSAN-based runtime (name server), zoning, and configuration (static routes) information is removed when the VSAN is deleted.
- Configured VSAN interface information is removed when the VSAN is deleted.

**Note**　The allowed VSAN list is not affected when a VSAN is deleted (see Chapter 24, "Configuring Trunking").

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.

Deleting Static VSANs

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

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 (see Figure 26-11).

Figure 26-11   Deleting a VSAN
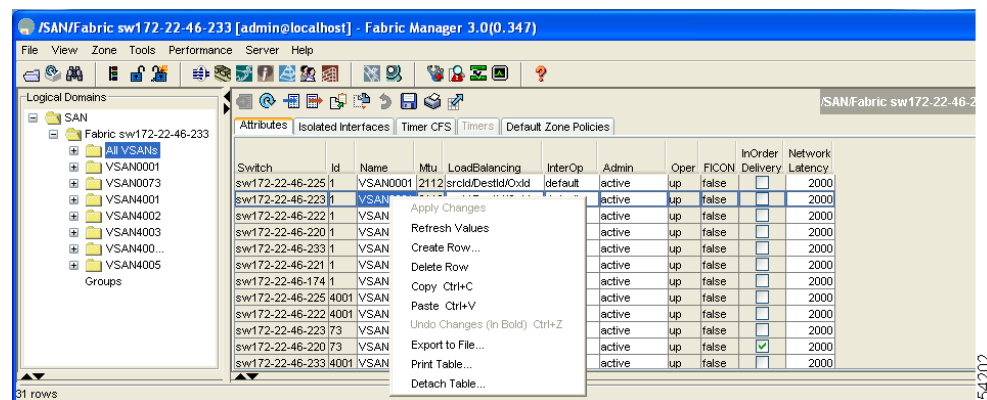
You see a confirmation dialog box.

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

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.
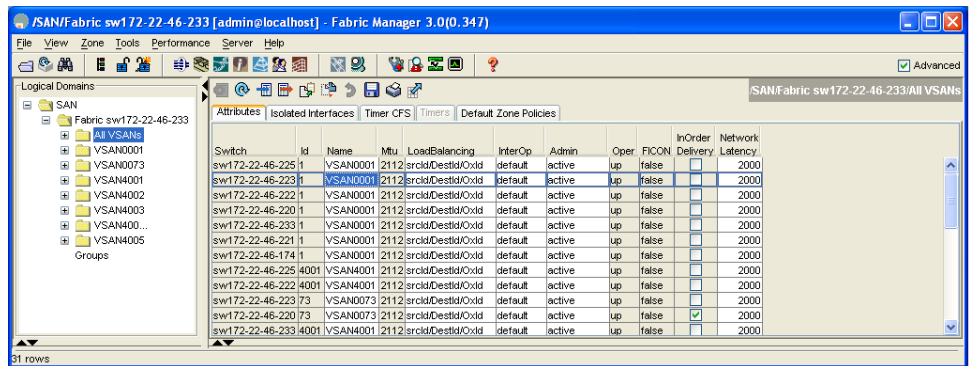
Configuring Load Balancing

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

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

You see the VSAN configuration in the Information pane shown in Figure 26-12.

Figure 26-12   All VSAN Attributes

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.

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 37-8.

About FICON VSANs

You can enable FICON in up to eight VSANs. See the "FICON VSAN Prerequisites" section on page 36-7.

Default Settings

Table 26-2 lists the default settings for all configured VSANs.

Table 26-2   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).