



CHAPTER 20

Configuring and Managing VSANs

You can achieve higher security and greater stability in Fibre Channel fabrics by using virtual SANs (VSANs). 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, page 20-1](#)
- [VSAN Configuration, page 20-5](#)
- [Displaying Static VSAN Configuration, page 20-11](#)
- [Default Settings, page 20-12](#)

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, page 20-1](#)
- [VSAN Advantages, page 20-3](#)
- [VSANs Versus Zones, page 20-4](#)

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.

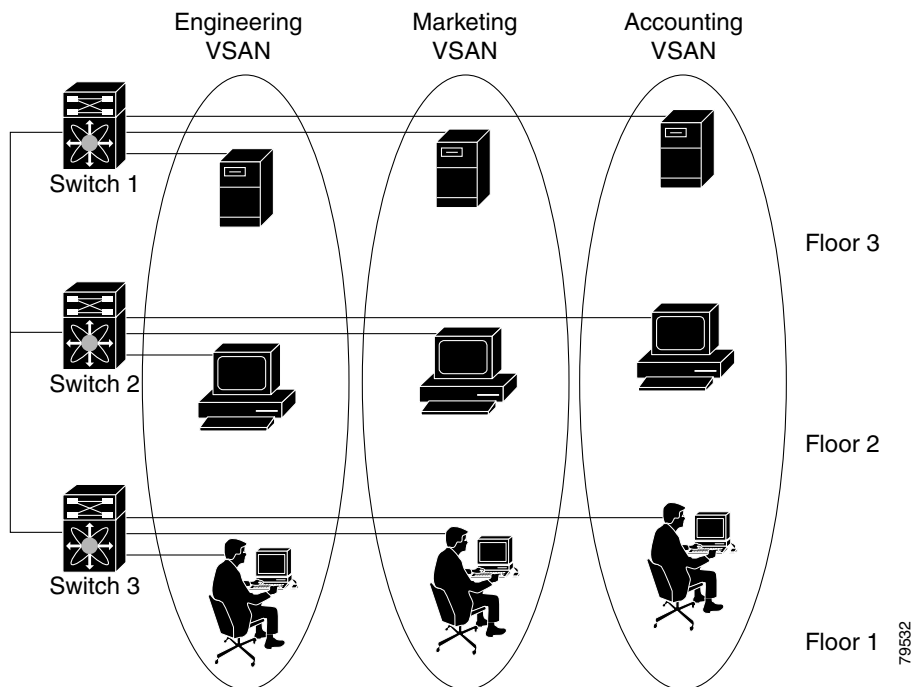
Send documentation comments to mdsfeedback-doc@cisco.com

- 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 20-1](#) and [Figure 20-2](#) indicate that these features apply to any switch in the Cisco MDS 9000 Family.

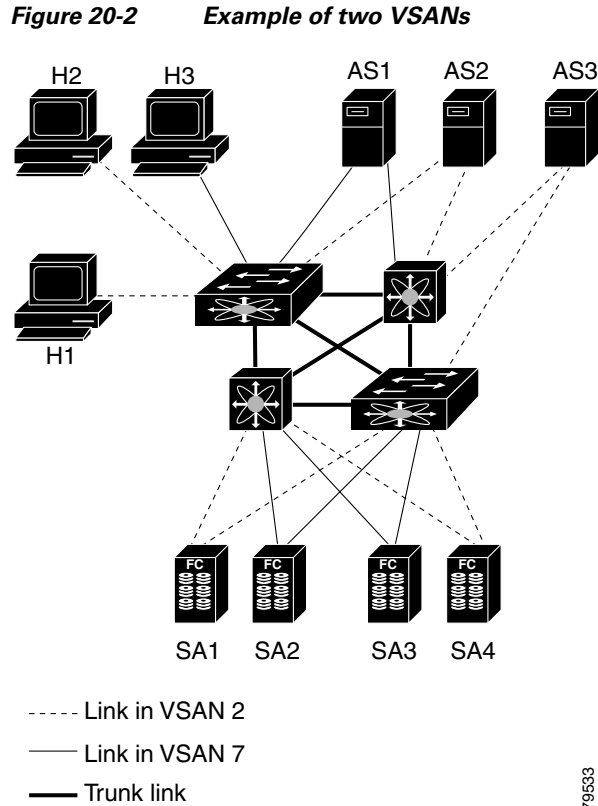
[Figure 20-1](#) shows a fabric with three switches, one on each floor. The geographic location of the switches and the attached devices is independent of their segmentation into logical VSANs. No communication between VSANs is possible. Within each VSAN, all members can talk to one another.

Figure 20-1 Logical VSAN Segmentation



[Figure 20-2](#) 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.

Send documentation comments to mdsfeedback-doc@cisco.com



The four switches in this network are interconnected by trunk links that carry both VSAN 2 and VSAN 7 traffic. Thus 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 20-2](#) 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:

Send documentation comments to mdsfeedback-doc@cisco.com

- 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 20-1](#) lists the differences between VSANs and zones.

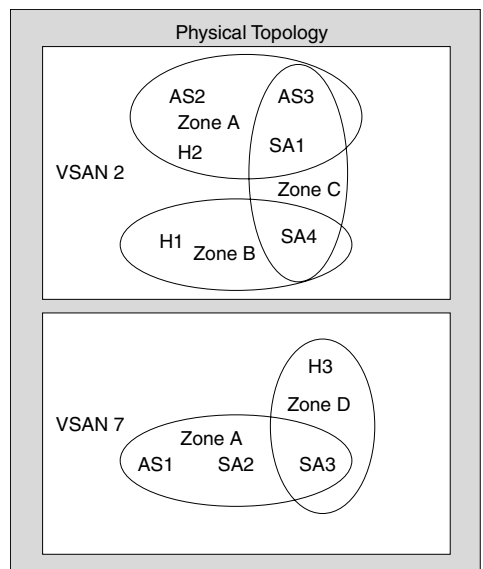
Table 20-1 VSAN and Zone Comparison

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 20-3](#) 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.

Send documentation comments to mdsfeedback-doc@cisco.com

Figure 20-3 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.

Send documentation comments to mdsfeedback-doc@cisco.com

**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 20-6](#)
- [Creating VSANs Statically, page 20-6](#)
- [About Port VSAN Membership, page 20-7](#)
- [Assigning Static Port VSAN Membership, page 20-7](#)
- [Displaying VSAN Static Membership, page 20-8](#)
- [About the Default VSAN, page 20-8](#)
- [About the Isolated VSAN, page 20-9](#)
- [Displaying Isolated VSAN Membership, page 20-9](#)
- [Operational State of a VSAN, page 20-9](#)
- [About Static VSAN Deletion, page 20-9](#)
- [Deleting Static VSANs, page 20-10](#)
- [About Load Balancing, page 20-10](#)
- [Configuring Load Balancing, page 20-11](#)
- [About Interop Mode, page 20-11](#)
- [About FICON VSANs, page 20-11](#)

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 VSANs, follow these steps:

	Command	Purpose
Step 1	switch# config t	Enters configuration mode.
Step 2	switch(config)# vsan database switch(config-vsan-db)#	Configures the database for a VSAN. Application specific VSAN parameters cannot be configured from this prompt.
Step 3	switch(config-vsan-db)# vsan 2	Creates a VSAN with the specified ID (2) if that VSAN does not exist already.

Send documentation comments to mdsfeedback-doc@cisco.com

	Command	Purpose
Step 4	switch(config-vsan-db) # vsan 2 name TechDoc updated vsan 2	Updates the VSAN with the assigned name (TechDoc).
Step 5	switch(config-vsan-db) # vsan 2 suspend	Suspends the selected VSAN.
Step 6	switch(config-vsan-db) # no vsan 2 suspend	Negates the suspend command issued in the previous step.
Step 7	switch(config-vsan-db) # end switch#	Returns you to EXEC mode.

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 20-7.
- Dynamically—by assigning VSANs based on the device WWN. This method is referred to as dynamic port VSAN membership (DPVM).
See [Chapter 22, “Creating Dynamic VSANs.”](#)

Trunking ports have an associated list of VSANs that are part of an allowed list (see [Chapter 16, “Configuring Trunking”](#)).

Assigning Static Port VSAN Membership

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

	Command	Purpose
Step 1	switch# config t	Enters configuration mode.
Step 2	switch(config) # vsan database switch(config-vsan-db) #	Configures the database for a VSAN.
Step 3	switch(config-vsan-db) # vsan 2	Creates a VSAN with the specified ID (2) if that VSAN does not exist already.
Step 4	switch(config-vsan-db) # vsan 2 interface fc1/8	Assigns the membership of the fc1/8 interface to the specified VSAN (VSAN 2).
Step 5	switch(config-vsan-db) # vsan 7	Creates another VSAN with the specified ID (7) if that VSAN does not exist already.
Step 6	switch(config-vsan-db) # vsan 7 interface fc1/8	Updates the membership information of the interface to reflect the changed VSAN.
	switch(config-vsan-db) # vsan 1 interface fc1/8	Removes the interface fc1/8 from VSAN 7 to VSAN 1 (the default VSAN). To remove the VSAN membership of interface fc1/8 from VSAN 7, you should define the VSAN membership of fc1/8 to another VSAN. The best practice is to assign it back to VSAN 1.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Displaying VSAN Static Membership

To display the VSAN static membership information, use the **show vsan membership** command (see [Example 20-1](#) through [Example 20-3](#)).

Example 20-1 Displays Membership Information for the Specified VSAN

```
switch # show vsan 1 membership
vsan 1 interfaces:
    fc1/1   fc1/2   fc1/3   fc1/4   fc1/5   fc1/6   fc1/7   fc1/9
    fc1/10  fc1/11  fc1/12  fc1/13  fc1/14  fc1/15  fc1/16  port-channel 99
```



Note

Interface information is not displayed if interfaces are not configured on this VSAN.

Example 20-2 Displays Static Membership Information for All VSANs

```
switch # show vsan membership
vsan 1 interfaces:
    fc2/16  fc2/15  fc2/14  fc2/13  fc2/12  fc2/11  fc2/10  fc2/9
    fc2/8   fc2/7   fc2/6   fc2/5   fc2/4   fc2/3   fc2/2   fc2/1
    fc1/16  fc1/15  fc1/14  fc1/13  fc1/12  fc1/11  fc1/10  fc1/9
    fc1/7   fc1/6   fc1/5   fc1/4   fc1/3   fc1/2   fc1/1
vsan 2 interfaces:
    fc1/8
vsan 7 interfaces:
vsan 100 interfaces:
vsan 4094(isolated vsan) interfaces:
```

Example 20-3 Displays Static Membership Information for a Specified Interface

```
switch # show vsan membership interface fc1/1
fc1/1
    vsan:1
    allowed list:1-4093
```

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.

Displaying Isolated VSAN Membership

The `show vsan 4094 membership` command displays all ports associated with 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.

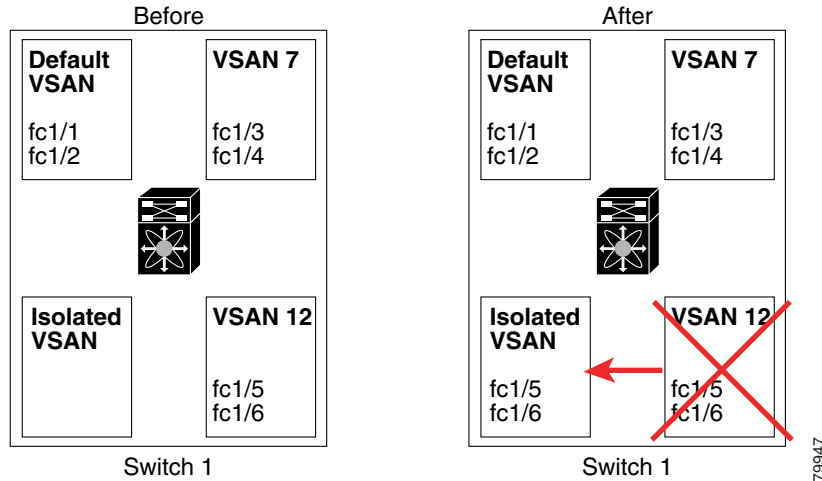
About Static VSAN Deletion

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 20-4](#)).

Send documentation comments to mdsfeedback-doc@cisco.com

Figure 20-4 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 16, “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 various attributes, follow these steps:

	Command	Purpose
Step 1	switch# config t	Enters configuration mode.
Step 2	switch(config)# vsan database switch(config-db)#	Configures the VSAN database.
Step 3	switch-config-db# vsan 2 switch(config-vsan-db)#	Places you in VSAN configuration mode.
Step 4	switch(config-vsan-db)# no vsan 5 switch(config-vsan-db)#	Deletes VSAN 5 from the database and switch.
Step 5	switch(config-vsan-db)# end switch#	Places you in EXEC mode.

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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Configuring Load Balancing

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

	Command	Purpose
Step 1	switch# config t	Enters configuration mode.
Step 2	switch(config)# vsan database switch(config-vsan-db)#	Enters VSAN database configuration submode
Step 3	switch(config-vsan-db)# vsan 2	Specifies an existing VSAN.
Step 4	switch(config-vsan-db)# vsan 2 loadbalancing src-dst-id	Enables the load balancing guarantee for the selected VSAN and directs the switch to use the source and destination ID for its path selection process.
	switch(config-vsan-db)# no vsan 2 loadbalancing src-dst-id	Negates the command issued in the previous step and reverts to the default values of the load balancing parameters.
	switch(config-vsan-db)# vsan 2 loadbalancing src-dst-ox-id	Changes the path selection setting to use the source ID, the destination ID, and the OX ID (default).
Step 5	switch(config-vsan-db)# vsan 2 suspend	Suspends the selected VSAN.
Step 6	switch(config-vsan-db)# no vsan 2 suspend	Negates the suspend command issued in the previous step.
Step 7	switch(config-vsan-db)# end switch#	Returns you to EXEC mode.

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 30-12.

About FICON VSANs

You can enable FICON in up to eight VSANs. See the [“FICON VSAN Prerequisites”](#) section on page 29-7.

Displaying Static VSAN Configuration

Use the **show vsan** command to display information about configured VSANs (see Examples 20-4 to 20-6).

Example 20-4 Displays the Configuration for a Specific VSAN

```
switch# show vsan 100
vsan 100 information
  name:VSAN0100 state:active
  in-order guarantee:no interoperability mode:no
  loadbalancing:src-id/dst-id/oxid
```

Send documentation comments to mdsfeedback-doc@cisco.com

Example 20-5 Displays the VSAN Usage

```
switch# show vsan usage
4 vsan configured
configured vsans:1-4
vsans available for configuration:5-4093
```

Example 20-6 Displays All VSANs

```
switch# show vsan
vsan 1 information
    name:VSAN0001 state:active
    in-order guarantee:no interoperability mode:no
    loadbalancing:src-id/dst-id/oxid
vsan 2 information
    name:VSAN0002 state:active
    in-order guarantee:no interoperability mode:no
    loadbalancing:src-id/dst-id/oxid
vsan 7 information
    name:VSAN0007 state:active
    in-order guarantee:no interoperability mode:no
    loadbalancing:src-id/dst-id/oxid
vsan 100 information
    name:VSAN0100 state:active
    in-order guarantee:no interoperability mode:no
    loadbalancing:src-id/dst-id/oxid
vsan 4094:isolated vsan
```

Default Settings

Table 20-2 lists the default settings for all configured VSANs.

Table 20-2 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).