CHAPTER 13

Configuring VSAN Trunking

This chapter describes the VSAN trunking feature provided in Cisco Nexus 5000 Series switches.

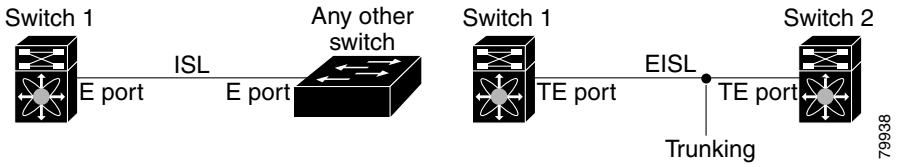
This chapter includes the following sections:

Information About VSAN Trunking

VSAN trunking enables interconnect ports to transmit and receive frames in more than one VSAN, over the same physical link, using enhanced ISL (EISL) frame format (see Figure 13-1).

VSAN trunking is supported on native Fibre Channel interfaces, but not on virtual Fibre Channel interfaces.

Figure 13-1 VSAN Trunking



The VSAN trunking feature includes the following restrictions:

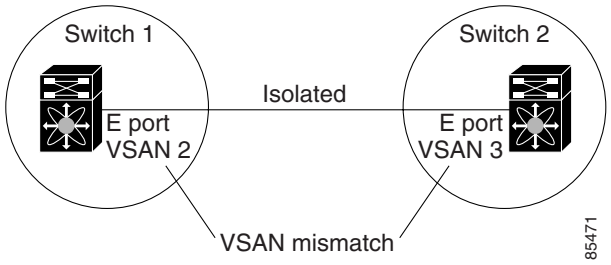
- Trunking configurations are only applicable to E ports. If trunk mode is enabled in an E port and that port becomes operational as a trunking E port, it is referred to as a TE port.
- The trunk-allowed VSANs configured for TE ports are used by the trunking protocol to determine the allowed-active VSANs in which frames can be received or transmitted.
- If a trunking-enabled E port is connected to a third-party switch, the trunking protocol ensures seamless operation as an E port.

Additional information about VSAN trunking is covered in the following topics:

VSAN Trunking Mismatches

If you misconfigure VSAN configurations across E ports, issues can occur such as the merging of traffic in two VSANs (causing both VSANs to mismatch). The VSAN trunking protocol validates the VSAN interfaces at both ends of an ISL to avoid merging VSANs (see Figure 13-2).

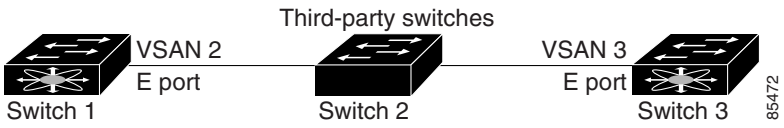
Figure 13-2 VSAN Mismatch



In this example, the trunking protocol detects potential VSAN merging and isolates the ports involved.

The trunking protocol cannot detect merging of VSANs when a third-party switch is placed in between two Cisco Nexus 5000 Series switches (see Figure 13-3).

Figure 13-3 Third-Party Switch VSAN Mismatch



VSAN 2 and VSAN 3 are effectively merged with overlapping entries in the name server and the zone applications. The Cisco MDS 9000 Fabric Manager helps detect such topologies.

VSAN Trunking Protocol

The trunking protocol is important for E-port and TE-port operations. It supports the following capabilities:

- Dynamic negotiation of operational trunk mode.
- Selection of a common set of trunk-allowed VSANs.
- Detection of a VSAN mismatch across an ISL.

By default, the VSAN trunking protocol is enabled. If the trunking protocol is disabled on a switch, no port on that switch can apply new trunk configurations. Existing trunk configurations are not affected: the TE port continues to function in trunk mode, but only supports traffic in VSANs that it negotiated with previously (when the trunking protocol was enabled). Other switches that are directly connected to this switch are similarly affected on the connected interfaces. If you need to merge traffic from different port VSANs across a nontrunking ISL, disable the trunking protocol.

Configuring VSAN Trunking

This section explains how to configure VSAN trunking and includes the following topics:

Guidelines and Restrictions

When configuring VSAN trunking, note the following guidelines:

- We recommend that both ends of a VSAN trunking ISL belong to the same port VSAN. On platforms or fabric switches where the port VSANs are different, one end returns an error, and the other is not connected.
- To avoid inconsistent configurations, shut all E ports before enabling or disabling the VSAN trunking protocol.

About Trunk Mode

By default, trunk mode is enabled in all Fibre Channel interfaces. However, trunk mode configuration takes effect only in E-port mode. You can configure trunk mode as on (enabled), off (disabled), or auto (automatic). The default trunk mode is on. The trunk mode configurations at the two ends of the link determine the trunking state of the link and the port modes at both ends (see Table 13-1).

Table 13-1 Trunk Mode Status Between Switches

Your Trunk Mode Configuration		Resulting State and Port Mode	
Switch 1	**Switch 2**	**Trunking State**	**Port Mode**
On	Auto or on	Trunking (EISL)	TE port
Off	Auto, on, or off	No trunking (ISL)	E port
Auto	Auto	No trunking (ISL)	E port

Tip The preferred configuration on the Cisco Nexus 5000 Series switches is that one side of the trunk is set to auto and the other is set to on.

Note When connected to a third-party switch, the trunk mode configuration has no effect. The ISL is always in a trunking disabled state.

Configuring Trunk Mode

To configure trunk mode using Fabric Manager, perform this task:

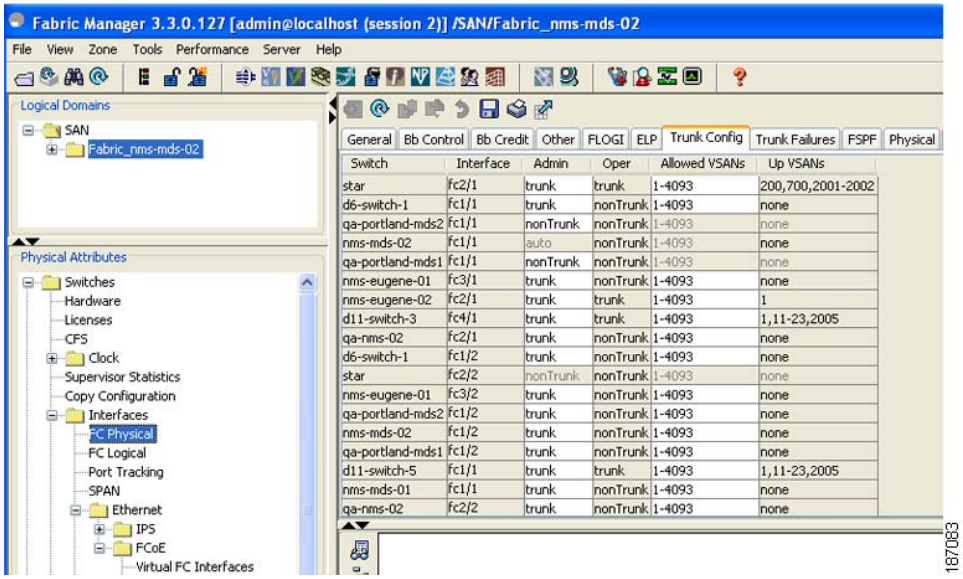
Step 1 In the Physical Attributes pane, expand **Switches > Interfaces**, and then choose **FC Physical**.

You see the interface configuration in the Information pane.

Step 2 Click the **Trunk Config** tab to modify the trunking mode for the selected interface.

You see the information shown in Figure 13-4.

Figure 13-4 Trunking Configuration

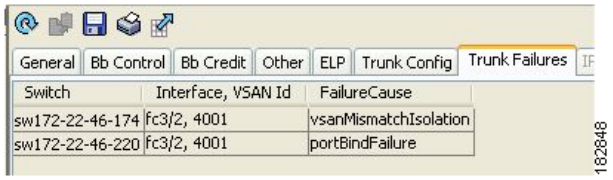


Step 3 Make changes to the Admin and Allowed VSANs values.

Step 4 Click the **Trunk Failures** tab to check the failure state of an ISL.

You see the reason listed in the FailureCause column (see Figure 13-5).

Figure 13-5 Trunk Failures Tab



Step 5 Click the **Apply Changes** icon.

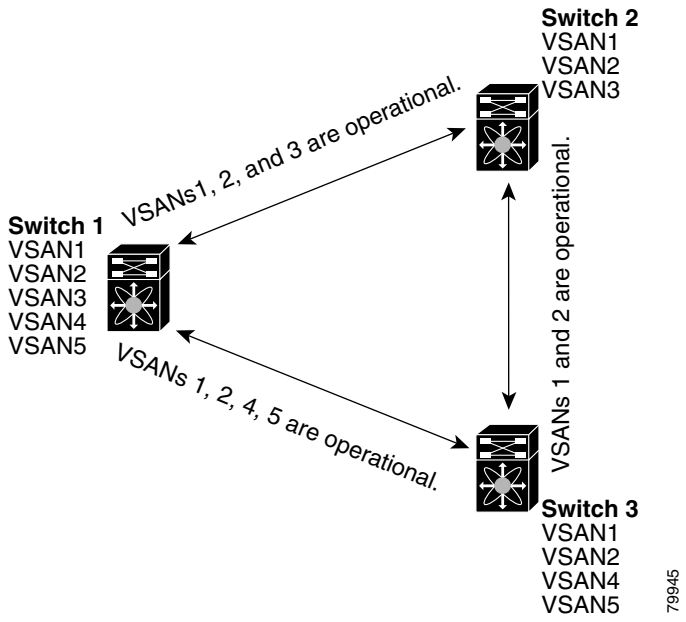
About Trunk-Allowed VSAN Lists

Each Fibre Channel interface has an associated trunk-allowed VSAN list. In TE-port mode, frames are transmitted and received in one or more VSANs specified in this list. By default, the complete VSAN range (1 through 4093) is included in the trunk-allowed list.

The common set of VSANs that are configured and active in the switch are included in the trunk-allowed VSAN list for an interface, and they are called *allowed-active VSANs*. The trunking protocol uses the list of allowed-active VSANs at the two ends of an ISL to determine the list of operational VSANs in which traffic is allowed.

In Figure 13-6, switch 1 has VSANs 1 through 5, switch 2 has VSANs 1 through 3, and switch 3 has VSANs 1, 2, 4, and 5 with a default configuration of trunk-allowed VSANs. All VSANs configured in all three switches are allowed-active. However, only the common set of allowed-active VSANs at the ends of the ISL become operational as shown in Figure 13-6.

Figure 13-6 Default Allowed-Active VSAN Configuration



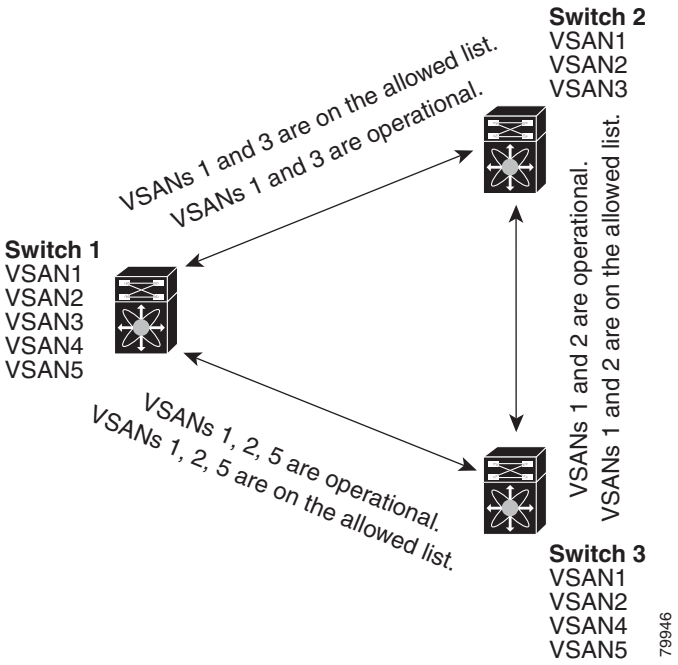
You can configure a selected set of VSANs (from the allowed-active list) to control access to the VSANs specified in a trunking ISL.

Using Figure 13-6 as an example, you can configure the list of allowed VSANs on a per-interface basis (see Figure 13-7). For example, if VSANs 2 and 4 are removed from the allowed VSAN list of ISLs connecting to switch 1, the operational allowed list of VSANs for each ISL would be as follows:

- The ISL between switch 1 and switch 2 includes VSAN 1 and VSAN 3.
- The ISL between switch 2 and switch 3 includes VSAN 1 and VSAN 2.
- The ISL between switch 3 and switch 1 includes VSAN 1, 2, and 5.

Consequently, VSAN 2 can only be routed from switch 1 through switch 3 to switch 2.

Figure 13-7 Operational and Allowed VSAN Configuration



Configuring an Allowed-Active List of VSANs

To configure an allowed-active list of VSANs for an interface using Fabric Manager, perform this task:

Step 1 In the Physical Attributes pane, expand **Interfaces**, and then choose **FC Physical**.

You see the interface configuration in the Information pane.

Step 2 Click the **Trunk Config** tab.

You see the current trunk configuration.

Step 3 Set Allowed VSANs to the list of allowed VSANs for each interface that you want to configure.

Step 4 Click **Apply Changes** to save these changes or click **Undo Changes** to discard any unsaved changes.

Default Settings

Table 13-2 lists the default settings for trunking parameters.

Table 13-2 Default Trunk Configuration Parameters

Parameters	Default
Switch port trunk mode	On
Allowed VSAN list	1 to 4093 user-defined VSAN IDs
Trunking protocol	Enabled