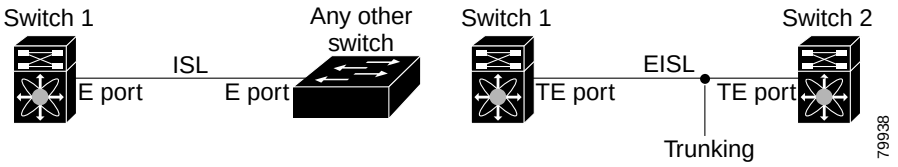
Configuring Trunking

This chapter describes the trunking feature provided in Cisco MDS 9000 switches. It includes the following sections:

About Trunking

Trunking, also known as VSAN trunking, is a feature specific to switches in the Cisco MDS 9000 Family. Trunking enables interconnect ports to transmit and receive frames in more than one VSAN, over the same physical link, using Extended ISL (EISL) frame format (see Figure 10-1).

Figure 10-1 Trunking



The 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 (see the "Configuring Trunk Modes" section on page 10-3).
- 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 (see the "Configuring Trunk-Allowed VSAN List" section on page 10-4).
- If a trunking enabled E port is connected to a third-party switch, the trunking protocol ensures seamless operation as an E port (see the "About Trunking Protocol" section on page 10-2).

About Trunking Protocol

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

- Dynamic negotiation of operational trunk mode (see the "Configuring Trunk Modes" section on page 10-3).
- Selection of a common set of trunk-allowed VSANs (see the "Configuring Trunk-Allowed VSAN List" section on page 10-4).
- Detection of a VSAN mismatch across an ISL (see the "Trunking Configuration Guidelines" section on page 10-6).

By default, the 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 will not be affected—the TE port continues to function in trunk mode, but only supports traffic in VSANs that it negotiated previously (when the trunking protocol was enabled). Also, other switches that are directly connected to this switch are similarly affected on the connected interfaces. In some cases, you may need to merge traffic from different port VSANs across a non-trunking ISL. If so, you need to disable the trunking protocol.

Tip To avoid inconsistent configurations, ensure to shut all E ports before enabling or disabling the trunking protocol.

To enable or disable the trunking protocol, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# no trunk protocol enable` `switch(config)#`	Disables the trunking protocol.
	`switch(config)# trunk protocol enable` `switch(config)#`	Enables trunking protocol (default).

Configuring Trunk Modes

By default, the trunk mode is enabled in all Fibre Channel interfaces. However, the trunk mode configuration takes effect only in E-port mode. You can configure the trunk mode as **on** (enabled), **off** (disabled), or **auto** (automatic). The default trunk mode is **on**. The trunk mode configuration at the two ends of an ISL, between two switches, determine the trunking state of the link and the port modes at both ends (see Table 10-1).

Table 10-1 Trunk Mode Status Between Switches

Switch 1 Trunk Mode	Switch 2 Trunk Mode	Trunking State of ISL	Port Mode
On	Auto or on	Trunking is enabled on both sides.	TE port
Off	Auto, on, or off	Trunking is disabled.	E port
Auto	Auto	Trunking is disabled.	E port

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

To configure the trunk mode, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# interface fc1/1` `switch(config-if)#`	Configures the specified interface.
Step 3	`switch(config-if)# switchport trunk mode on` `switch(config-if)#`	Enables the trunk mode for the specified interface.
	`switch(config-if)# switchport trunk mode off` `switch(config-if)#`	Disables the trunk mode for the specified interface.
	`switch(config-if)# switchport trunk mode auto` `switch(config-if)#`	Configures the trunk mode for the specified interface. The **auto** option provides automatic sensing for the interface.

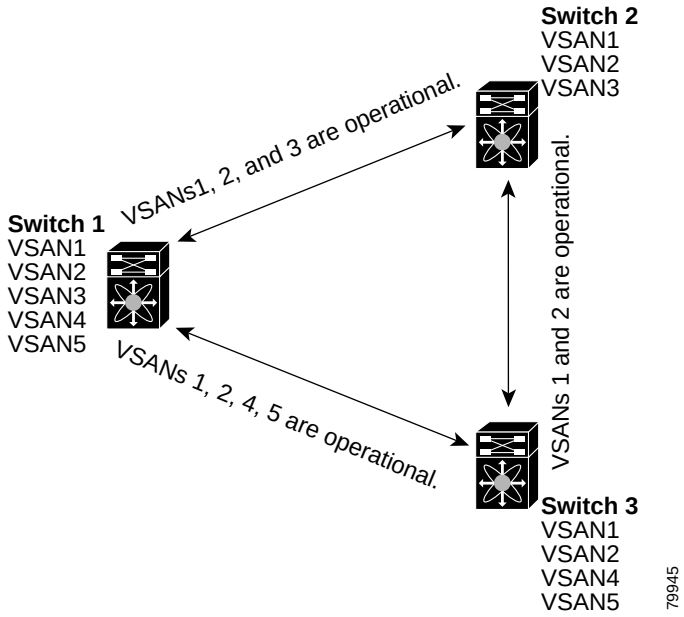
Configuring Trunk-Allowed VSAN List

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 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.

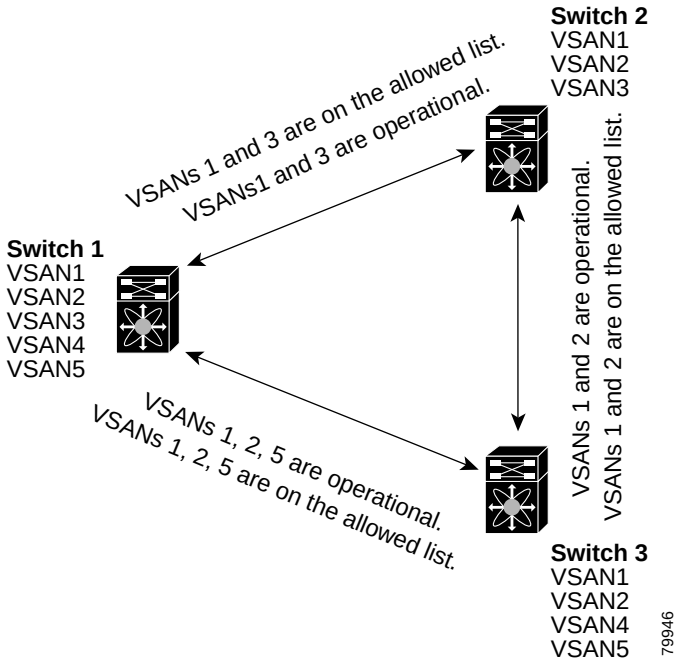
In Figure 10-2, switch 1 has VSANs 1 through 5, switch 2 has VSANs 1 through 3, and switch 3 has VSANs 1, 2, 4, and 5 with a default configuration of trunk-allowed VSANs. All VSANs configured in all three switches are allowed-active. However, only the common set of allowed-active VSANs at the ends of the ISL become operational as shown in Figure 10-2.

Figure 10-2 Default Allowed -Active VSAN Configuration



You can configure a select set of VSANs (from the allowed-active list) to control access to those VSANs in a trunking ISL. Using Figure 10-2 as an example, you can configure the list of allowed VSANs on a per-interface basis (see Figure 10-3).

Figure 10-3 Operational and Allowed VSAN Configuration



In Figure 10-3, the operational allowed list of VSANs between switches is as follows:

- Switch 1 and switch 2 include VSAN 1 and VSAN 3.
- Switch 2 and switch 3 include VSAN 1 and VSAN 2.
- Switch 3 and switch 1 include VSAN 1, 2, and 5.

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

To configure an allowed-active list of VSANs for an interface, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# interface fc1/1` `switch(config-if)#`	Configures the specified interface.
Step 3	`switch(config-if)# switchport trunk allowed vsan 2-4` `switch(config-if)#`	Changes the allowed list for the specified VSANs.

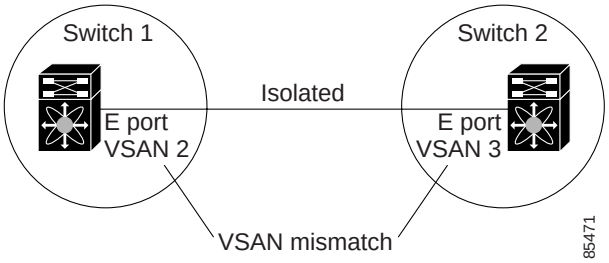
	`switch(config-if)# switchport trunk allowed vsan add 5`
	`updated trunking membership`
	`switch(config-if)#`
		Expands the specified VSAN (5) to the new allowed list.

	`switch(config-if)# no switchport trunk allowed vsan 2-4` `switch(config-if)#`	Deletes VSANs 2, 3, and 4.
	`switch(config-if)# no switchport trunk allowed vsan add 5` `switch(config-if)#`	Deletes the expanded allowed list.

Trunking Configuration Guidelines

If you misconfigure VSAN configurations across E ports, you could face consequences such as merging the traffic in two VSANs. The trunking protocol validates the VSAN interfaces at both ends of an ISL to avoid VSANs merging (see Figure 10-4).

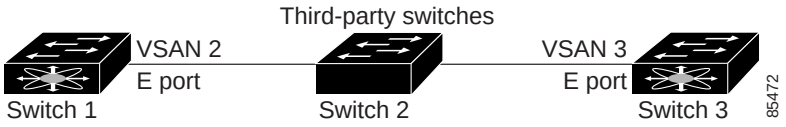
Figure 10-4 VSAN Mismatch



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 MDS 9000 Family switches (see Figure 10-5).

Figure 10-5 Third-Party Switch VSAN Mismatch



VSANs 2 and 3 get effectively merged with overlapping entries in the name server and the zone applications. The Cisco MDS 9000 Fabric Manager helps detect such topologies (see the *Cisco MDS 9000 Family Fabric Manager User Guide)*.

Displaying Trunking Information

The **show interface** command is invoked from the EXEC mode and displays trunking configurations for a TE port. Without any arguments, this command displays the information for all of the configured interfaces in the switch. See Examples 10-1 to 10-3.

Example 10-1 Displays a Trunked Fiber Channel Interface

```
switch# show interface fc1/13
fc1/13 is trunking
    Hardware is Fibre Channel
    Port WWN is 20:0d:00:05:30:00:58:1e
    Peer port WWN is 20:0d:00:05:30:00:59:1e
    Admin port mode is auto, trunk mode is on
    Port mode is TE
    Port vsan is 1
    Speed is 2 Gbps
    Receive B2B Credit is 255
    Beacon is turned off
    Trunk vsans (admin allowed and active) (1)
    Trunk vsans (up)                       (1)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             ()
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      233996 frames input, 14154208 bytes, 0 discards
        0 CRC,  0 unknown class
        0 too long, 0 too short
      236 frames output, 13818044 bytes, 0 discards
      11 input OLS, 12 LRR, 10 NOS, 28 loop inits
      34 output OLS, 19 LRR, 17 NOS, 12 loop inits
```

Example 10-2 Displays Trunking Protocol

```
switch# show trunk protocol
Trunk protocol is enabled
```

Example 10-3 Displays Per VSAN Information on Trunk Ports

```
switch# show interface trunk vsan 1-1000
fc3/1 is not trunking

fc3/7 is trunking
    Vsan 1000 is down (Isolation due to vsan not configured on peer)

fc3/10 is trunking
    Vsan 1 is up, FCID is 0x760001
    Vsan 2 is up, FCID is 0x6f0001

fc3/11 is trunking
    Belongs to port-channel 6
    Vsan 1 is up, FCID is 0xef0000
    Vsan 2 is up, FCID is 0xef0000

port-channel 6 is trunking
    Vsan 1 is up, FCID is 0xef0000
    Vsan 2 is up, FCID is 0xef0000
```

Default Settings

Table 10-2 lists the default settings for trunking parameters.

Table 10-2 Default Trunk Configuration Parameters

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