



Configuring Trunking

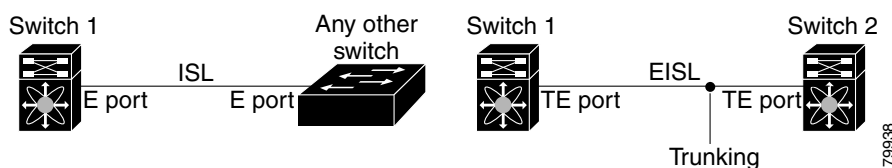
This chapter describes the trunking feature provided in Cisco MDS 9000 switches. It includes the following sections:

- [About Trunking, page 12-1](#)
 - [About the Trunking Protocol, page 12-2](#)
 - [Configuring Trunk Mode, page 12-2](#)
 - [Trunk-Allowed VSAN Configuration, page 12-3](#)
 - [Trunking Configuration Guidelines, page 12-6](#)
 - [Displaying Trunking Information, page 12-7](#)
 - [Default Settings, page 12-8](#)

About Trunking

Family. 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 12-1](#)).

Figure 12-1 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.

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.

About the Trunking Protocol

-
-
-

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 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). 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, disable the trunking protocol.



Tip

shutdown

Enabling or Disabling the Trunking Protocol

	Command	Purpose
Step 1	switch# config t	
Step 2	switch(config)# no trunk protocol enable	
	trunk protocol enable	

Configuring Trunk Mode

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 resulting trunking state of the link and the port modes at both ends (see [Table 12-2](#)).

Table 12-2 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 MDS 9000 Family switches is one side of the trunk set to auto and the other 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 the Trunk Mode

To configure the trunk mode, follow these steps:

	Command	Purpose
Step 1		Enters configuration mode.
Step 2	<code>switch(config-if)# fc1/1</code>	
Step 3	<code>switch(config-if)# switchport trunk mode on</code>	
	<code>switch(config-if)# switchport trunk mode off</code>	
	<code>switch(config-if)# switchport trunk mode auto</code>	auto

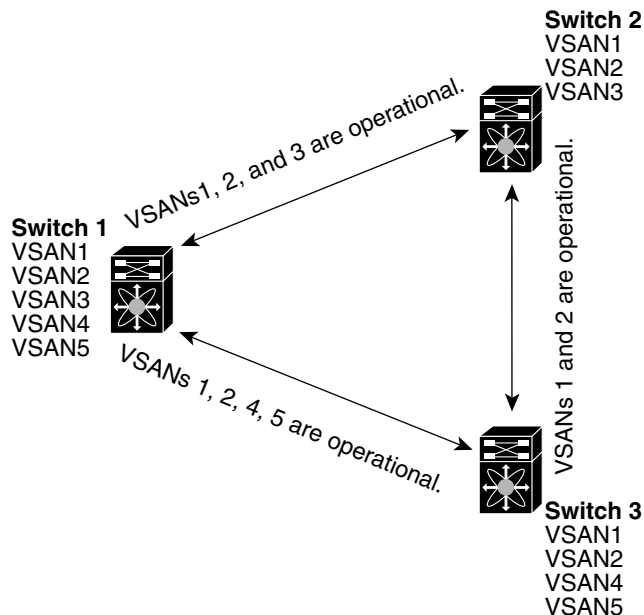
Trunk-Allowed VSAN Configuration

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 12-1](#), 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 12-1](#).

Default Allowed-Active VSAN Configuration



Using [Figure 12-1](#) as an example, you can configure the list of allowed VSANs on a per-interface basis (see [Figure 12-2](#)). 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:

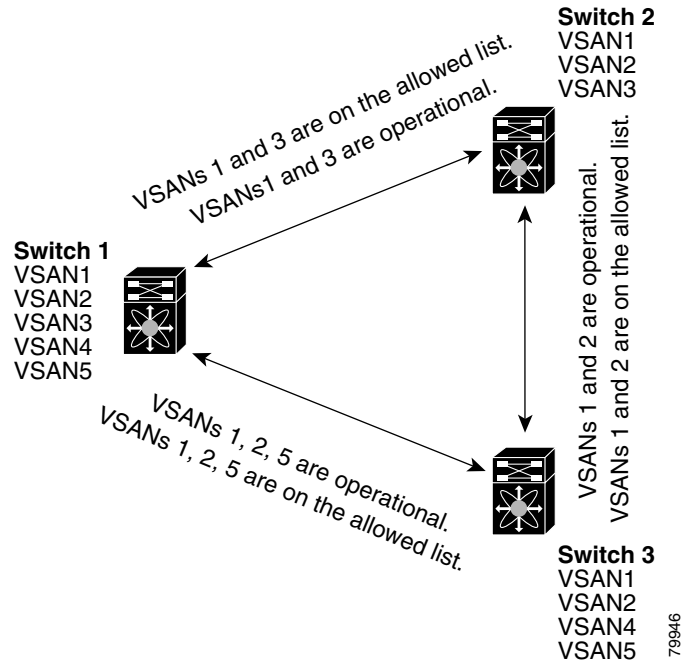
The ISL between switch 1 and switch 2 shall include VSAN 1 and VSAN 3.

The ISL between switch 2 and switch 3 shall include VSAN 1 and VSAN 2.

The ISL between switch 3 and switch 1 shall include VSAN 1, 2, and 5.

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

Operational and Allowed VSAN Configuration



Configuring an Allowed-Active List of VSANs

	Command	Purpose
Step 1	switch#	
Step 2	switch(config)# switch(config-if)#	
Step 3	switch(config-if)# switchport trunk allowed vsan 2-4	
	switch(config-if)# switchport trunk allowed vsan add 5 updated trunking membership	
	switch(config-if)# no switchport trunk allowed vsan 2-4	
	switch(config-if)# no switchport trunk allowed vsan add 5	

Trunking Configuration Guidelines

Figure 12-3 VSAN Mismatch

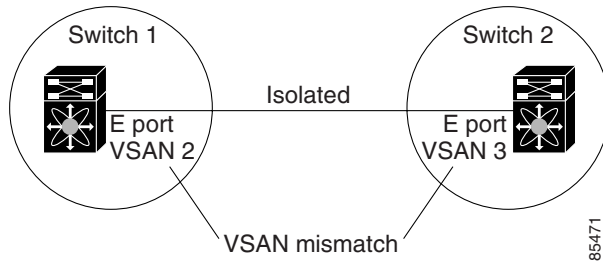
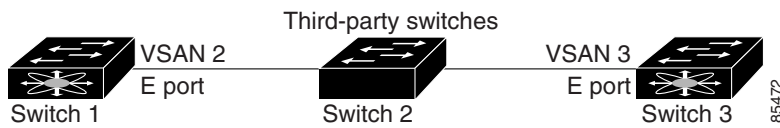


Figure 12-4 Third-Party Switch VSAN Mismatch



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. Refer to the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.

Displaying Trunking Information

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 12-1 to 12-3.

Example 12-1 Displays a Trunked Fibre 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

switch# show trunk protocol
Trunk protocol is enabled

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

```

Table 12-3 lists the default settings for trunking parameters.

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