



CHAPTER 16

Configuring Trunking

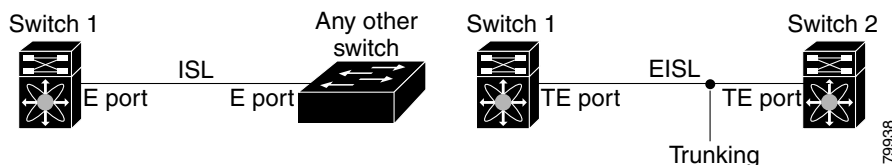
This chapter describes the trunking feature provided in Cisco MDS 9000 switches. It includes the following sections:

- [About Trunking, page 16-1](#)
- [Trunking Protocol, page 16-2](#)
- [Displaying Trunking Information, page 16-6](#)
- [Default Settings, page 16-7](#)

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 enhanced ISL (EISL) frame format (see [Figure 16-1](#)).

Figure 16-1 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.



Note

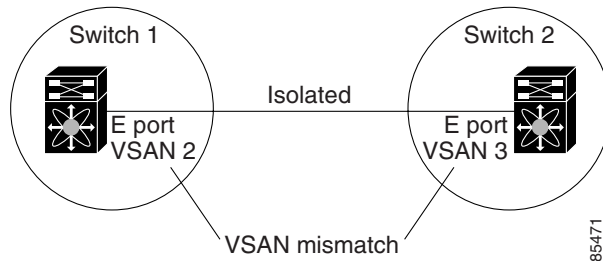
Trunking is not supported by internal ports on both the Cisco Fabric Switch for HP c_Class BladeSystem and the Cisco Fabric Switch for IBM BladeCenter.

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

Trunking Configuration Guidelines

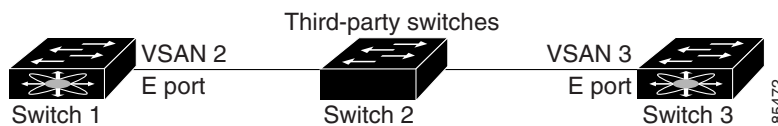
If you misconfigure VSAN configurations across E ports, you could face consequences such as merging the traffic in two VSANs (thus causing both VSANs to mismatch). The trunking protocol validates the VSAN interfaces at both ends of an ISL to avoid merging VSANs (see [Figure 16-2](#)).

Figure 16-2 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 MDS 9000 Family switches (see [Figure 16-3](#)).

Figure 16-3 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. Refer to the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.

Trunking Protocol

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

- 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 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.

Send documentation comments to mdsfeedback-doc@cisco.com

**Note**

We recommend that both ends of a trunking ISL belong to the same port VSAN. On certain platforms or fabric switches where the port VSANs are different, one end returns an error, and the other is not connected.

**Tip**

To avoid inconsistent configurations, disable all E ports with a **shutdown** command before enabling or disabling the trunking protocol.

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

- [Enabling or Disabling the Trunking Protocol, page 16-3](#)
- [About Trunk Mode, page 16-3](#)
- [Configuring Trunk Mode, page 16-4](#)
- [About Trunk-Allowed VSAN Lists, page 16-4](#)
- [Configuring an Allowed-Active List of VSANs, page 16-6](#)

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).

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 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 16-1](#)).

Table 16-1 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

Send documentation comments to mdsfeedback-doc@cisco.com

**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 Trunk Mode

To configure 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	Enables (default) the trunk mode for the specified interface.
	switch(config-if)# switchport trunk mode off	Disables the trunk mode for the specified interface.
	switch(config-if)# switchport trunk mode auto	Configures the trunk mode to auto mode, which provides automatic sensing for the interface.

About Trunk-Allowed VSAN Lists

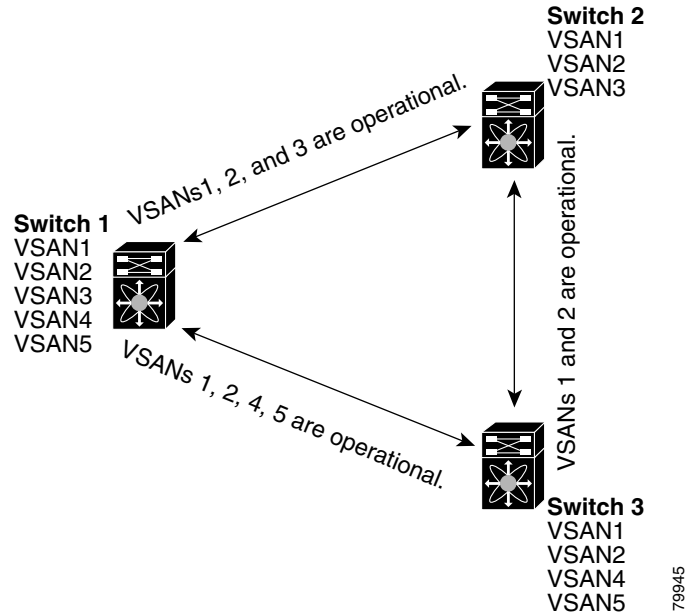
Each Fibre Channel interface has an associated trunk-allowed VSAN list. In TE-port mode, frames are transmitted and received in one or more VSANs specified in this list. By default, the VSAN range (1 through 4093) is included in the trunk-allowed list.

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 16-4](#), 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 16-4](#).

Send documentation comments to mdsfeedback-doc@cisco.com

Figure 16-4 Default Allowed-Active VSAN Configuration



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

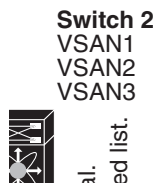
Using [Figure 16-4](#) as an example, you can configure the list of allowed VSANs on a per-interface basis (see [Figure 16-5](#)). For example, if VSANs 2 and 4 are removed from the allowed VSAN list of ISLs connecting to switch 1, the operational allowed list of VSANs for each ISL would be as follows:

- 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.

Send documentation comments to mdsfeedback-doc@cisco.com

Figure 16-5 Operational and Allowed VSAN Configuration



Configuring an Allowed-Active List of VSANs

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	Changes the allowed list for the specified VSANs.
	switch(config-if)# switchport trunk allowed vsan add 5 updated trunking membership	Expands the specified VSAN (5) to the new allowed list.
	switch(config-if)# no switchport trunk allowed vsan 2-4	Deletes VSANs 2, 3, and 4.
	switch(config-if)# no switchport trunk allowed vsan add 5	Deletes the expanded allowed list.

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 16-1 to 16-3.

Example 16-1 Displays a Trunked Fibre Channel Interface

```
switch# show interface fc1/13
fc1/13 is trunking
```

Send documentation comments to mdsfeedback-doc@cisco.com

```

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 16-2 Displays the Trunking Protocol

```

switch# show trunk protocol
Trunk protocol is enabled

```

Example 16-3 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 16-2 lists the default settings for trunking parameters.

Send documentation comments to mdsfeedback-doc@cisco.com

Table 16-2 **Default Trunk Configuration Parameters**

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