Configuring VSAN Trunking

This chapter contains the following sections:

Configuring VSAN Trunking

Information About VSAN Trunking

VSAN trunking enables interconnected ports to transmit and receive frames in more than one VSAN. Trunking is supported on E ports and F ports.

Beginning in Cisco NX-OS Release 5.0(2)N1(1), VSAN trunking is supported on native Fibre Channel interfaces and virtual Fibre Channel interfaces.

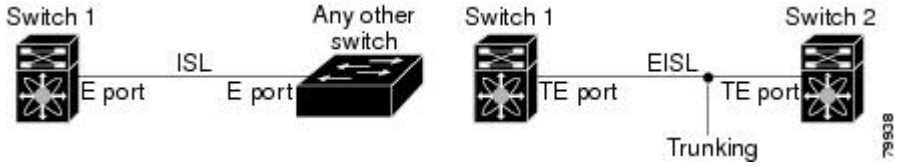
The VSAN trunking feature includes the following restrictions:

- 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.

Trunking E Ports

Trunking E ports enables interconnected ports to transmit and receive frames in more than one VSAN, over the same physical link, using enhanced ISL (EISL) frame format.

Figure 1: Trunking E Ports



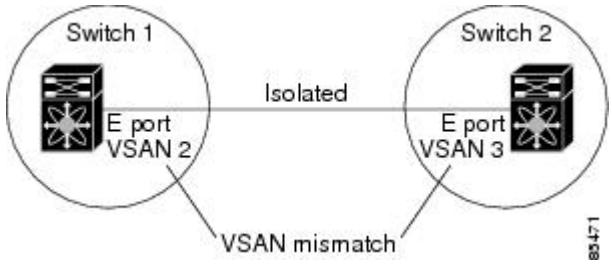
Trunking F Ports

Trunking F ports allows interconnected ports to transmit and receive tagged frames in more than one VSAN, over the same physical link.

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 the following figure).

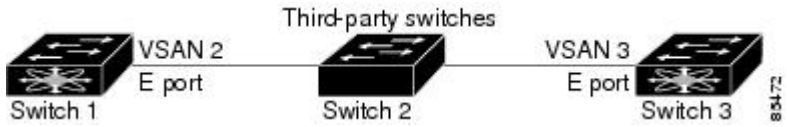
Figure 2: VSAN Mismatch



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 the following figure).

Figure 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

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, disable all E ports with a **shutdown** command before enabling or disabling the VSAN trunking protocol.

Difference Between TE Ports and TF-TNP Ports

In case of TE ports, the VSAN will in be initializing state when VSAN is coming up on that interface and when peers are in negotiating phase. Once the handshake is done, VSAN will be moved to up state in the successful case, and isolated state in the case of failure. Device Manager will show the port status as amber during initializing state and it will be green once VSANs are up.

In case of TF ports, after the handshake, one of the allowed VSAN will be moved to up state. And all other VSAN will be in initializing state even though the handshake with the peer is completed and successful. Each VSAN will be moved from initializing state to up state when a server or target logs in through the trunked F or NP ports in the corresponding VSAN.

Enabling or Disabling the VSAN Trunking Protocol

To enable or disable the VSAN trunking protocol, perform this task:

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **no trunk protocol enable**
3. switch(config)# **trunk protocol enable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configuration terminal**	Enters configuration mode.
Step 2	switch(config)# **no trunk protocol enable**	Disables the trunking protocol.
Step 3	switch(config)# **trunk protocol enable**	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 configurations at the two ends of the link determine the trunking state of the link and the port modes at both ends (see the following table).

Table 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

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, perform this task:

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **interface** {**fc** *slot/port* | **vfc** *vfc-id*}
3. switch(config-if)# **switchport trunk mode on**
4. switch(config-if)# **switchport trunk mode off**
5. switch(config-if)# **switchport trunk mode auto**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configuration terminal**	Enters configuration mode.
Step 2	switch(config)# **interface** {**fc** *slot/port* | **vfc** *vfc-id*}	Configures the specified Fibre Channel or virtual Fibre Channel interface.
Step 3	switch(config-if)# **switchport trunk mode on**	Enables (default) the trunk mode for the specified interface.
Step 4	switch(config-if)# **switchport trunk mode off**	Disables the trunk mode for the specified interface. **Note** Trunk mode cannot be turned off for virtual Fibre Channel interfaces.
Step 5	switch(config-if)# **switchport trunk mode auto**	Configures the trunk mode to **auto** mode, which provides automatic sensing for the interface.

The following example shows how to configure a vFC interface in trunk mode.

```
switch# config t
switch#(config)# vfc 200
switch(config-if)# switchport trunk mode on
```

The following example shows the output for the vFC interface 200 in trunk mode.

```
switch(config-if)# show interface vfc200
vfc200 is trunking (Not all VSANs UP on the trunk)
    Bound interface is Ethernet1/3
    Hardware is Virtual Fibre Channel
    Port WWN is 20:c7:00:0d:ec:f2:08:ff
    Peer port WWN is 00:00:00:00:00:00:00:00
    Admin port mode is E, trunk mode is on
    snmp link state traps are enabled
    Port mode is TE
    Port vsan is 1
    Trunk vsans (admin allowed and active) (1-6,10,22)
    Trunk vsans (up)                       ()
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             (1-6,10,22)
    5 minute input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minute output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
```

```
  0 frames input, 0 bytes
    0 discards, 0 errors
  0 frames output, 0 bytes
    0 discards, 0 errors
last clearing of "show interface" counters never
Interface last changed at Mon Jan 18 10:01:27 2010
```

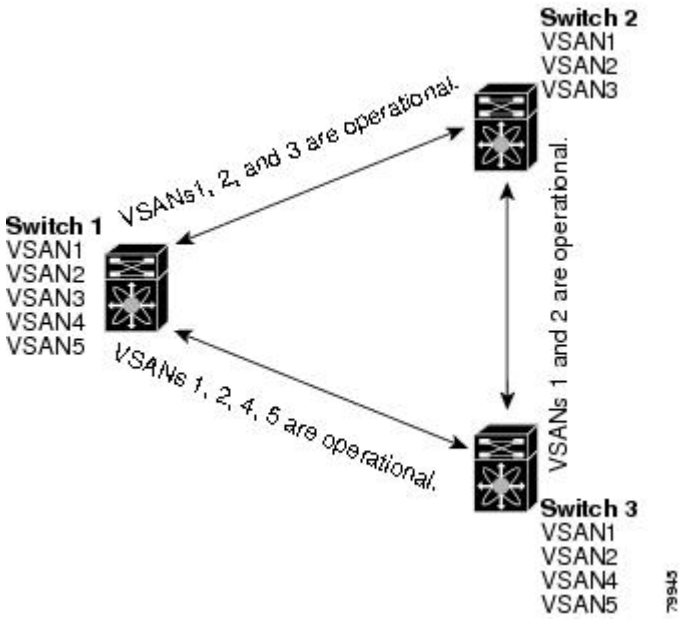
About Trunk-Allowed VSAN Lists

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 the following figure, 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 below.

Figure 4: 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.

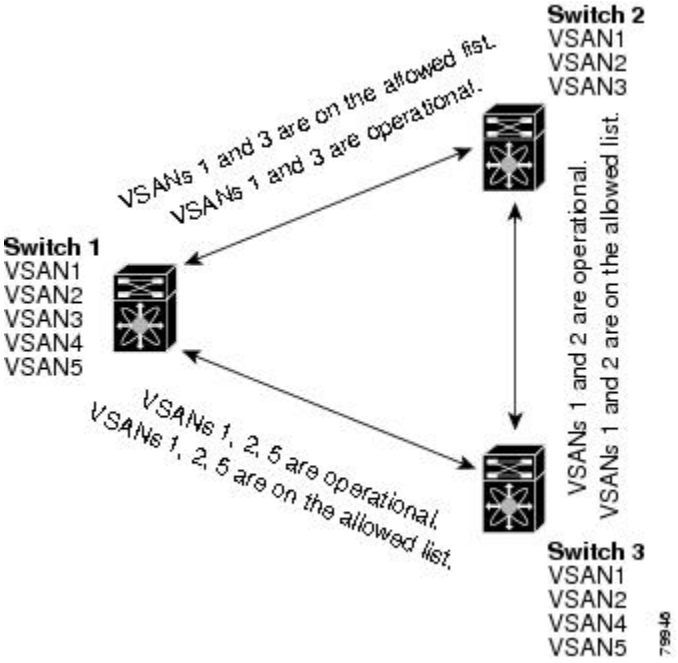
Using the figure above as an example, you can configure the list of allowed VSANs on a per-interface basis (see the following figure). For example, if VSANs 2 and 4 are removed from the allowed VSAN list of ISLs connecting to switch 1, the operational allowed list of VSANs for each ISL would be as follows:

- 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 5: Operational and Allowed VSAN Configuration



Configuring an Allowed-Active List of VSANs

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

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **interface fc** *slot/port*
3. switch(config-if)# **switchport trunk allowed vsan** *vsan-id* **-** *vsan-id*
4. switch(config-if)# **switchport trunk allowed vsan add** *vsan-id*
5. switch(config-if)# **no switchport trunk allowed vsan** *vsan-id* **-** *vsan-id*
6. switch(config-if)# **no switchport trunk allowed vsan add** *vsan-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configuration terminal**	Enters configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# **interface fc** *slot/port*	Configures the specified interface.
Step 3	switch(config-if)# **switchport trunk allowed vsan** *vsan-id* **-** *vsan-id*	Changes the allowed list for the specified VSAN range.
Step 4	switch(config-if)# **switchport trunk allowed vsan add** *vsan-id*	Expands the specified VSAN to the new allowed list.
Step 5	switch(config-if)# **no switchport trunk allowed vsan** *vsan-id* **-** *vsan-id*	Deletes the specified VSAN range.
Step 6	switch(config-if)# **no switchport trunk allowed vsan add** *vsan-id*	Deletes the expanded allowed list.

Displaying VSAN Trunking Information

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

The following example shows how to display the trunk mode of a Fibre Channel interface:

```
switch# show interface fc3/3
fc3/3 is up
    Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:83:00:0d:ec:6d:78:40
    Peer port WWN is 20:0c:00:0d:ec:0d:d0:00
    Admin port mode is auto, trunk mode is on
...
```

The following example shows how to display the trunk protocol of a Fibre Channel interface:

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

The following example shows how to display the VSAN information for all trunk interfaces:

```
switch# show interface trunk vsan 1-1000
fc3/1 is not trunking
...
fc3/11 is trunking
    Belongs to san-port-channel 6
    Vsan 1 is up, FCID is 0xef0000
    Vsan 2 is up, FCID is 0xef0000
...
san-port-channel 6 is trunking
    Vsan 1 is up, FCID is 0xef0000
    Vsan 2 is up, FCID is 0xef0000
```

Default Trunk Configuration Settings

The following table lists the default settings for trunking parameters.

Table 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