# Switch Trunking Operation

The purpose of a switch trunk is to forward multiple VLANs between switches. The switch port must be configured for trunk mode to enable forwarding of multiple VLANs. That allows communication between hosts assigned to the same VLAN that span switches. Forwarding multiple VLANs across a switch link requires trunk mode to enable the VLAN tagging feature.

### Static vs Dynamic

There is a choice to configure either static trunking or dynamic trunking. When static trunking is configured, you are telling the switch to explicitly turn up a trunk. There is no negotiation, however the same static trunk configuration must be enabled on the neighbor switch port. The other option is a dynamic (negotiated) trunk that is conditional based on how connected switches are configured.

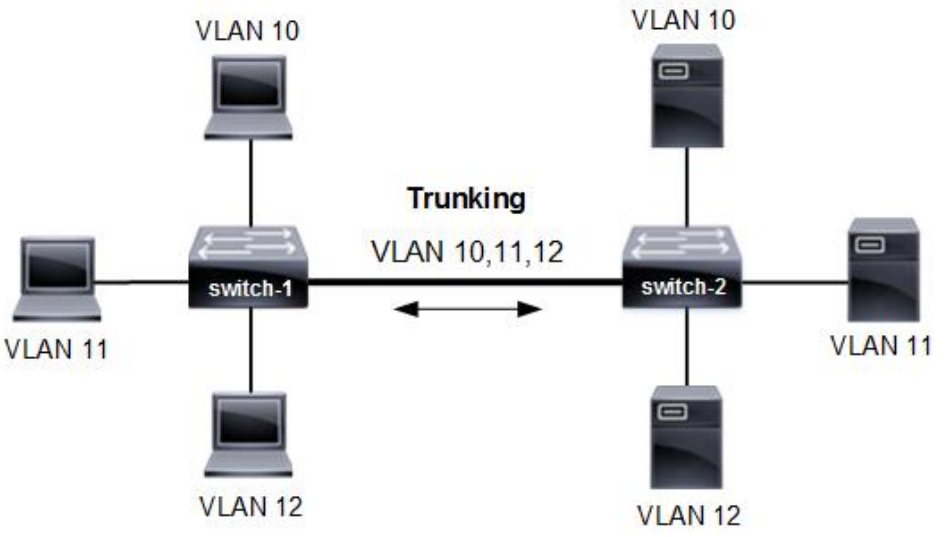
The following interface level IOS commands enables static trunking on a switch interface. The switchport nonegotiate command turns off DTP frames as a recommended best practice. There is optional command **switchport access vlan 10** as well. It assigns VLAN 10 to what is an access port if trunking fails.

```
switch(config)# interface fastethernet0/1
switch(config-if)# switchport mode trunk
switch(config-if)# switchport nonegotiate
switch(config-if)# end
```

## 802.1q Encapsulation

The purpose of 802.1q is to enable forwarding of multiple VLANs to a neighbor switch. That is accomplished by tagging each frame with 4-byte tag for VLAN membership. The tagging and forwarding of Ethernet frames starts after Layer 2 convergence has occurred with STP. The Ethernet frame header is modified as a result of adding the VLAN tag. That requires recalculation of the FCS value used for CRC. Access ports will drop any frame that has an 802.1q tag. The open standard for multi-vendor switch connectivity is 802.1q encapsulation. It is the current Cisco default setting as well for a trunk mode interface.

**Figure 1** Trunking Operation




# Native VLAN

The switch management VLAN 1 forwards management frames between switches and cannot be deleted. The default configuration is to assign all switch ports to VLAN 1. As a result, all management and user traffic use VLAN 1. Some examples of management frames include CDP, LACP, VTP, STP and DTP. The purpose of management frames are to provide control plane communication between switches. Cisco recommends you separate management and user traffic for security purposes.

The native VLAN is used to forward untagged packets across a switch trunk. Cisco default trunk configuration assigns VLAN 1 to the native VLAN. Ethernet frame sent across a trunk, are tagged with the VLAN membership of that frame. Management frames however are sent untagged across native VLAN.

## Nondefault Native VLAN

The default native VLAN is assigned to VLAN 1. That is the same as the default management VLAN for switches. Cisco recommends that you assign native VLAN to a nondefault VLAN instead of VLAN 1. It is a security best practice and minimizes STP issues. Layer 2 control plane traffic such as DTP and STP protocols are always sent across native VLAN. That occurs even when native VLAN is modified from VLAN 1.

The following statements describes proper operation for the native VLAN.

- Native VLAN must match between connected switches.
- Native VLAN forwards untagged packets across a switch trunk.
- Native VLAN should not be assigned the default VLAN 1.

The following command configures a nondefault native VLAN 999 instead of the default VLAN 1. It is configured on all switch port interfaces assigned as trunk ports.

switch(config-if)# **switchport trunk native vlan 999**

The recommendation is to modify the native VLAN from default VLAN 1 to any available nondefault VLAN.

The following IOS interface command configure the default native VLAN setting for a trunk interface.

switch(config-if)# **switchport trunk native vlan 1**

There are known security vulnerabilities when implementing the default native VLAN. STP issues are minimized as well by selecting a nondefault VLAN. DTP and STP control traffic are always assigned to VLAN 1. That is true as well where the native VLAN for trunk is changed from VLAN. The native VLAN must match between neighbor switches. VLAN hopping is a well-known security vulnerability caused by mismatches. CDP, STP and DTP can detect native VLAN mismatch.

## Add/Remove VLANs

Cisco default configuration is to allow **all** VLANs from 1 - 4094 across the trunk. The purpose of VLAN pruning is to permit or deny VLANs across a trunk interface. That will permit or deny all traffic originating from specific VLAN/s. It is a recommended security practice to only permit traffic from VLANs that must traverse a trunk and remove everything else.

Each switch alerts neighbor switch of all VLANs that are not active. Any VLANs not configured are automatically removed from the trunk by the neighbor switch. That is done to minimize all unicast, broadcast and multicast traffic across the trunk. The administrator can also add or remove VLANs manually **after** trunk mode is enabled. The following command displays default trunking operation. It displays operational status of all trunk interfaces on a switch.

```
switch# show interfaces trunk

Port        Mode         Encapsulation  Status        Native vlan
Gi1/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gi1/1       1-4094

Port        Vlans allowed and active in management domain
Gi1/1       1-4094

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/1       1-4094
```

**Example 1**

The network administrator has configured a trunk between two switches. The configuration must allow only VLAN 10, 11 and 12 across the trunk. What is the correct IOS command to accomplish that?

The default trunk configuration allows all VLAN traffic from range 1-4094 across the trunk. The following IOS interface command will **only allow** VLAN 10, VLAN 11 and VLAN 12 across the trunk.

To allow a range of consecutive VLANs such as VLAN 1 to VLAN 100 for example, use hyphen (1-100). For a non-consecutive list such as VLAN 9 and 100 to 200 use commas and hyphens (9,100-200).

```
switch(config-if)# switchport trunk allowed vlan 10-12
```

The previous command is issued first on a default trunk configuration to limit the number of VLANs. The network administrator can add or remove VLANs after that based on requirements. Configure IOS command **switchport trunk allowed vlan all** to reset and allow all VLANs.

**Example 2**

The following IOS interface command will add VLAN 9 and VLAN range 100-200 to the trunk interface. The **add** | **remove** keyword only applies after the default VLAN range has been initially modified.

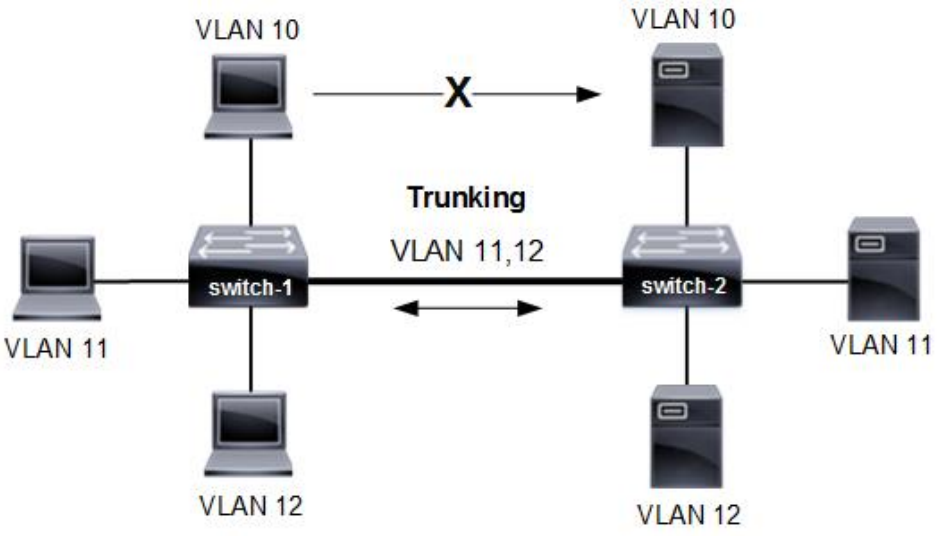
```
switch(config-if)# switchport trunk allowed vlan add 9,100-200
```

**Example 3**

The following command will remove VLAN 10 from a trunk interface.

switch(config-if)# **switchport trunk allowed vlan remove 10**

**Figure 2** Remove VLAN 10 From Trunk Interface




## Trunk Operational Status

The following displays the operational status of switch-1 for example 3. The operational status has default settings except VLANs allowed.

switch# **show interfaces trunk**

| Port | Mode | Encapsulation | Status | Native vlan |
|---|---|---|---|---|
| Gi1/1 | **on** | 802.1q | trunking | **1** |

| Port | Vlans allowed on trunk |
|---|---|
| Gi1/1 | **11-12** |

| Port | Vlans allowed and active in management domain |
|---|---|
| Gi1/1 | 1,11,12 |

| Port | Vlans in spanning tree forwarding state and not pruned |
|---|---|
| Gi1/1 | 1,11,12 |

## Interface Switchport Command

Cisco IOS command **show interface switchport** displays both the operational and administrative status for all trunk interfaces. That includes switch ports assigned, allowed VLANs, trunking mode, encapsulation type and native VLAN.

switch# **show interface gigabitethernet 1/2 switchport**

Name: Gig1/2
Switchport: Enabled
**Administrative Mode: trunk**
**Operational Mode: trunk**
Administrative Trunking Encapsulation: **dot1q**
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: **1** (default)
Voice VLAN: none
**Trunking VLANs Enabled: 11-12**
Pruning VLANs Enabled: 2-1001

The administrative mode (trunk) is how the switch port is configured and operational mode (trunk) is the switch interface status. The trunk is not formed unless administrative and operational mode is trunk. Cisco switch ports support access mode or trunk mode. The network administrator would configure a port mode when enabling an interface.

## Trunking Best Practices

The following are Cisco recommended best practices for trunking between switches. They will optimize network operation and security for the switching infrastructure.

- Native VLAN configured on a trunk interface must match neighbor switch. That is required to forward untagged packets across the trunk and prevent VLAN hopping.

- Change the native VLAN from default VLAN 1 for security purposes. Layer 2 loops are minimized as well when STP control frames are sent across the native VLAN.

- Configure an SVI on the switch for management purposes instead of the default VLAN 1.
- VLAN 1 is used to forward control frames (CDP, DTP, STP, LACP) between switches and should not be assigned to data traffic.
- Remove PortFast from any trunk interfaces. It is only recommended on switch access ports.