Send feedback to nx5000-docfeedback@cisco.com

CHAPTER 1

# Configuring Access and Trunk Interfaces

Ethernet interfaces can be configured either as access ports or trunk ports. Trunks carry the traffic of multiple VLANs over a single link and allow you to extend VLANs across the network.

This chapter includes the following sections:


- Information About Access and Trunk Interfaces, page 1-1
- Configuring Access and Trunk Interfaces, page 1-4
- Verifying Interface Configuration, page 1-8


## Information About Access and Trunk Interfaces

This section includes the following topics:


- Understanding Access and Trunk Interfaces, page 1-1
- Understanding IEEE 802.1Q Encapsulation, page 1-2
- Understanding Access VLANs, page 1-3
- Understanding the Native VLAN ID for Trunk Ports, page 1-3
- Understanding Allowed VLANs, page 1-4


**Note** Cisco NX-OS supports only IEEE 802.1Q-type VLAN trunk encapsulation.

### Understanding Access and Trunk Interfaces

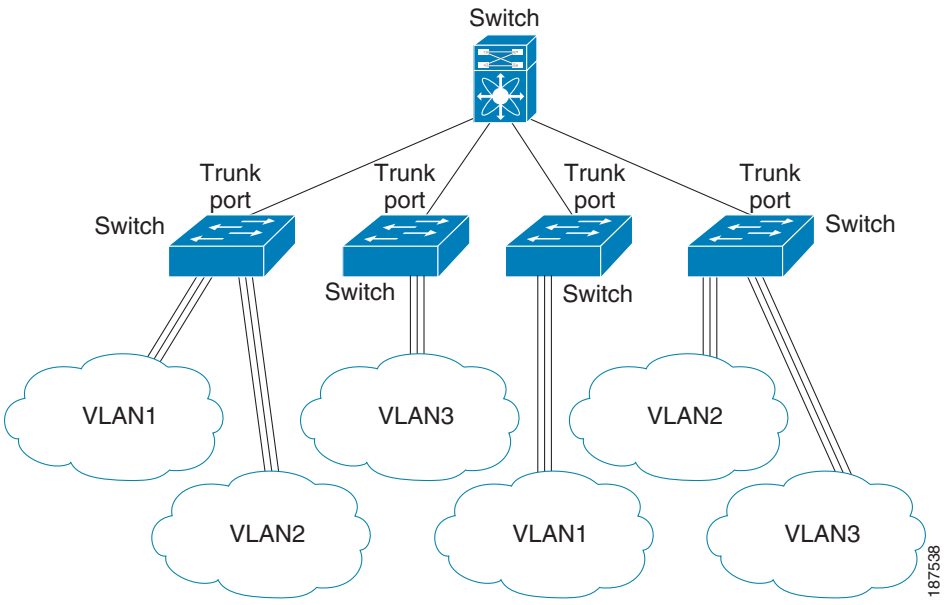
Ethernet interfaces can be configured either as access ports or a trunk ports, as follows:

- An access port can have only one VLAN configured on the interface; it can carry traffic for only one VLAN.
- A trunk port can have two or more VLANs configured on the interface; it can carry traffic for several VLANs simultaneously.

Figure 1-1 show how you can use trunk ports in the network. The trunk port carries traffic for two or more VLANs.

Send feedback to nx5000-docfeedback@cisco.com

*Figure 1-1 Devices in a Trunking Environment*




In order to correctly deliver the traffic on a trunk port with several VLANs, the device uses the IEEE 802.1Q encapsulation or tagging method (see the "Understanding IEEE 802.1Q Encapsulation" section on page 1-2 for more information on this subject).

To optimize the performance on access ports, you can configure the port as a host port. Once the port is configured as a host port, it is automatically set as an access port, and channel grouping is disabled. Use the host designation to decrease the time it takes the designated port to begin to forward packets.

**Note** Only an end station can be set as a host port; you will receive an error message if you attempt to configure other ports as hosts.

If an access port receives a packet with an 802.1Q tag in the header other than the access VLAN value, that port drops the packet without learning its MAC source address.

**Note** An Ethernet interface can function as either an access port or a trunk port; it cannot function as both port types simultaneously.

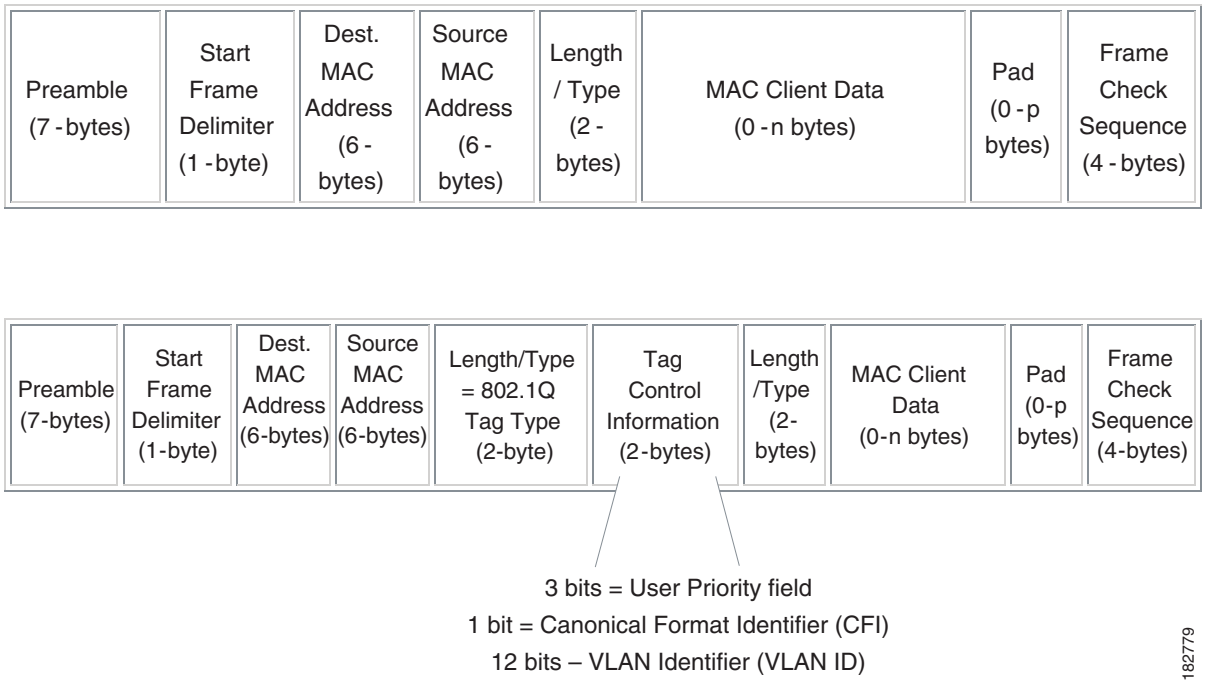
# Understanding IEEE 802.1Q Encapsulation

A trunk is a point-to-point link between the device and another networking device. Trunks carry the traffic of multiple VLANs over a single link and allow you to extend VLANs across an entire network.

To correctly deliver the traffic on a trunk port with several VLANs, the device uses the IEEE 802.1Q encapsulation (tagging) method that uses a tag that is inserted into the frame header. This tag carries information about the specific VLAN to which the frame and packet belong. This method allows packets that are encapsulated for several different VLANs to traverse the same port and maintain traffic separation between the VLANs. The encapsulated VLAN tag also allows the trunk to move traffic end-to-end through the network on the same VLAN.

Send feedback to nx5000-docfeedback@cisco.com

*Figure 1-2 Header without and with 802.1Q Tag Included*




# Understanding Access VLANs

**Note** If you assign an access VLAN that is also a primary VLAN for a private VLAN, all access ports with that access VLAN will also receive all the broadcast traffic for the primary VLAN in the private VLAN mode.

When you configure a port in access mode, you can specify which VLAN will carry the traffic for that interface. If you do not configure the VLAN for a port in access mode, or an access port, the interface carries traffic for the default VLAN (VLAN1).

You can change the access port membership in a VLAN by specifying the new VLAN. You must create the VLAN before you can assign it as an access VLAN for an access port. If you change the access VLAN on an access port to a VLAN that is not yet created, the system will shut that access port down.

If an access port receives a packet with an 802.1Q tag in the header other than the access VLAN value, that port drops the packet without learning its MAC source address.

# Understanding the Native VLAN ID for Trunk Ports

**Note** Native VLAN ID numbers *must* match on both ends of the trunk.

Send feedback to nx5000-docfeedback@cisco.com

A trunk port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default port VLAN ID to the trunk port, all untagged traffic travels on the default port VLAN ID for the trunk port, and all untagged traffic is assumed to belong to this VLAN. This VLAN is referred to as the native VLAN ID for a trunk port. The native VLAN ID is the VLAN that carries untagged traffic on trunk ports.

The trunk port sends an egressing packet with a VLAN that is equal to the default port VLAN ID as untagged; all the other egressing packets are tagged by the trunk port. If you do not configure a native VLAN ID, the trunk port uses the default VLAN.

## Understanding Allowed VLANs

By default, a trunk port sends traffic to and receives traffic from all VLANs. All VLAN IDs are allowed on each trunk. However, you can remove VLANs from this inclusive list to prevent traffic from the specified VLANs from passing over the trunk. You can add any specific VLANs later that you may want the trunk to carry traffic for back to the list.

To partition spanning tree protocol (STP) topology for the default VLAN, you can remove VLAN1 from the list of allowed VLANs. Otherwise, VLAN1, which is enabled on all ports by default, will have a very big STP topology, which can result in problems during STP convergence. When you remove VLAN1, all data traffic for VLAN1 on this port is blocked, but the control traffic continues to move on the port.

# Configuring Access and Trunk Interfaces

This section includes the following topics:


- Configuring a LAN Interface as an Ethernet Access Port, page 1-4
- Configuring Access Host Ports, page 1-5
- Configuring Trunk Ports, page 1-6
- Configuring the Native VLAN for 802.1Q Trunking Ports, page 1-6
- Configuring the Allowed VLANs for Trunking Ports, page 1-7


## Configuring a LAN Interface as an Ethernet Access Port

You can configure an Ethernet port as an access port. An access port transmits packets on only one, untagged VLAN. You specify which VLAN traffic that the interface carries. If you do not specify a VLAN for an access port, the interface carries traffic only on the default VLAN. The default VLAN is VLAN1.

The VLAN must exist before you can specify that VLAN as an access VLAN. The system shuts down an access port that is assigned to an access VLAN that does not exist.

To configure an Ethernet access port, perform this task:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `switch# configure terminal` | Enters configuration mode. |
| **Step 2** | `switch(config)# interface {{type slot/port} \| {port-channel number}}` | Specifies an interface to configure, and enters interface configuration mode. |

Send feedback to nx5000-docfeedback@cisco.com

| | Command | Purpose |
|---|---|---|
| Step 3 | `switch(config-if)# switchport mode {access \| trunk}` | Sets the interface as a nontrunking nontagged single-VLAN Ethernet interface. An access port can carry traffic in one VLAN only. By default, an access port carries traffic for VLAN1; to set the access port to carry traffic for a different VLAN, use the **switchport access vlan** command. |
| Step 4 | `switch(config-if)# switchport access vlan vlan-id` | Specifies the VLAN for which this access port will carry traffic. If you do not enter this command, the access port carries traffic on VLAN1 only; use this command to change the VLAN for which the access port carries traffic. |

This example shows how to set Ethernet 1/10 as an Ethernet access port that carries traffic for VLAN 5 only:

```
switch# configure terminal
switch(config)# interface ethernet 1/10
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 5
```

# Configuring Access Host Ports

**Note** You should apply the **switchport host** command only to interfaces connected to an end station.

You can optimize performance on access ports that are connected to end stations by simultaneously setting that port as an access port. An access host port handles the Spanning Tree Protocol (STP) like an edge port and immediately moves to the forwarding state without passing through the blocking and learning states. Configuring an interface as an access host port also disables port channeling on that interface.

**Note** See Chapter 1, "Configuring EtherChannels" for information on port channel interfaces and Chapter 1, "Configuring Rapid PVST+" for complete information on the Spanning Tree Protocol.

Ensure that you are configuring the correct interface to an interface that is an end station.

To configure an access host port, perform this task:

| | Command | Purpose |
|---|---|---|
| Step 1 | `switch# configure terminal` | Enters configuration mode. |
| Step 2 | `switch(config)# interface type slot/port` | Specifies an interface to configure, and enters interface configuration mode. |
| Step 3 | `switch(config-if)# switchport host` | Sets the interface to be an access host port, which immediately moves to the spanning tree forwarding state and disables port channeling on this interface.<br>**Note** Apply this command only to end stations. |

Send feedback to nx5000-docfeedback@cisco.com

This example shows how to set Ethernet 1/10 as an Ethernet access port with **PortFast enabled** and port channel disabled:

```
switch# configure terminal
switch(config)# interface ethernet 1/10
switch(config-if)# switchport host
```

# Configuring Trunk Ports

You can configure an Ethernet port as a trunk port; a trunk port transmits untagged packets for the native VLAN plus encapsulated, tagged, packets for multiple VLANs. (See "Understanding IEEE 802.1Q Encapsulation" section on page 1-2 for information about encapsulation.)

**Note** Cisco NX-OS supports only 802.1Q encapsulation.

To configure a trunk port, perform this task:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `switch# configure terminal` | Enters configuration mode. |
| **Step 2** | `switch(config)# interface {type slot/port \| port-channel number}` | Specifies an interface to configure, and enters interface configuration mode. |
| **Step 3** | `switch(config-if)# switchport mode {access \| trunk}` | Sets the interface as an Ethernet trunk port. A trunk port can carry traffic in one or more VLANs on the same physical link (VLANs are based on the trunk-allowed VLANs list). By default, a trunk interface can carry traffic for all VLANs. To specify that only certain VLANs are allowed on the specified trunk, use the **switchport trunk allowed vlan** command. |

This example shows how to set Ethernet 3/1 as an Ethernet trunk port:

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# switchport mode trunk
```

# Configuring the Native VLAN for 802.1Q Trunking Ports

If you do not configure this parameter, the trunk port uses the default VLAN as the native VLAN ID.

To configure native VLAN for a 802.1Q trunk port, perform this task:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `switch# configure terminal` | Enters configuration mode. |

Send feedback to nx5000-docfeedback@cisco.com

| | Command | Purpose |
|---|---|---|
| Step 2 | `switch(config)# interface {type slot/port \| port-channel number}` | Specifies an interface to configure, and enters interface configuration mode. |
| Step 3 | `switch(config-if)# switchport trunk native vlan vlan-id` | Sets the native VLAN for the 802.1Q trunk. Valid values are from 1 to 4094, except those VLANs reserved for internal use. The default value is VLAN1. |

This example shows how to set the native VLAN for Ethernet 3/1 Ethernet trunk port to VLAN 5:

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# switchport trunk native vlan 5
```

# Configuring the Allowed VLANs for Trunking Ports

You can specify the IDs for the VLANs that are allowed on the specific trunk port.

Before you configure the allowed VLANs for the specified trunk ports, ensure that you are configuring the correct interfaces and that the interfaces are trunks.

To configure the allowed VLAN for a trunk port, perform this task:

| | Command | Purpose |
|---|---|---|
| Step 1 | `switch# configure terminal` | Enters configuration mode. |
| Step 2 | `switch(config)# interface {type slot/port \| port-channel number}` | Specifies an interface to configure, and enters interface configuration mode. |
| Step 3 | `switch(config-if)# switchport trunk allowed vlan {vlan-list all \| none [add \|except \| none \| remove {vlan-list}]}` | Sets allowed VLANs for the trunk interface. The default is to allow all VLANs on the trunk interface: 1 to 3967 and 4048 to 4094. VLANs 3968 to 4047 are the default VLANs reserved for internal use by default; this group of VLANs is configurable. By default, all VLANs are allowed on all trunk interfaces.<br>**Note** You cannot add internally allocated VLANs as allowed VLANs on trunk ports. The system returns a message if you attempt to list an internally allocated VLAN as an allowed VLAN. |

This example shows how to add VLANs 15 to 20 to the list of allowed VLANs on the Ethernet 3/1 Ethernet trunk port:

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# switchport trunk allow vlan 15-20
```

Send feedback to nx5000-docfeedback@cisco.com

# Verifying Interface Configuration

To display access and trunk interface configuration information, perform one of these tasks:

| Command | Purpose |
|---|---|
| `switch# show interface` | Displays the interface configuration |
| `switch# show interface switchport` | Displays information for all Ethernet interfaces, including access and trunk interfaces. |
| `switch# show interface brief` | Displays interface configuration information. |