Configuring Layer 2 Interfaces

This chapter contains the following sections:

Information About Access and Trunk Interfaces

This section describes how to configure Layer 2 switching ports as access or trunk ports.

Note For information about configuring a Switched Port Analyzer (SPAN) destination interface, see the *Cisco Nexus 1000V for Microsoft Hyper-V System Management Configuration Guide*

Note For information about VLANs, MAC address tables, and private VLANs, see the *Cisco Nexus 1000V for Microsoft Hyper-V Layer 2 Switching Configuration Guide*.

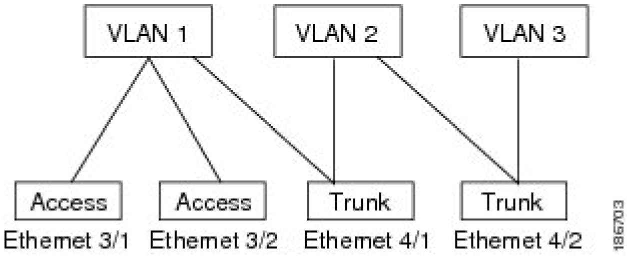
Access and Trunk Interfaces

A Layer 2 port can be configured as an access or a trunk port as follows:

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

By default, all ports on the Cisco Nexus 1000V are Layer 2 ports. You can change the default port mode (access or trunk). See the *Cisco Nexus 1000V for Microsoft Hyper-V Installation and Upgrade Guide* for information about setting the default port mode. The following figure shows how you can use trunk ports in the network. The trunk port carries traffic for two or more VLANs.

Figure 1: Trunk and Access Ports and VLAN Traffic



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.

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 that it takes the designated port to begin to forward packets.

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.

A Layer 2 interface can function as either an access port or a trunk port; it cannot function as both port types simultaneously.

IEEE 802.1Q Encapsulation

A trunk is a point-to-point link between the switch 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, or tagging, method that uses a tag that is inserted into the frame header (see the following figures). 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. Also, the encapsulated VLAN tag allows the trunk to move traffic end to end through the network on the same VLAN.

Figure 2: Header Without 802.1Q Tag

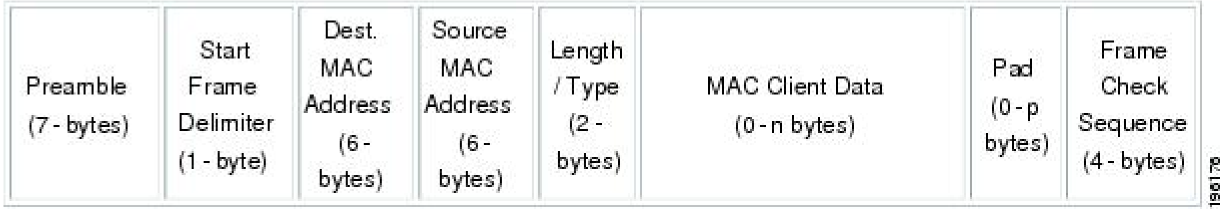
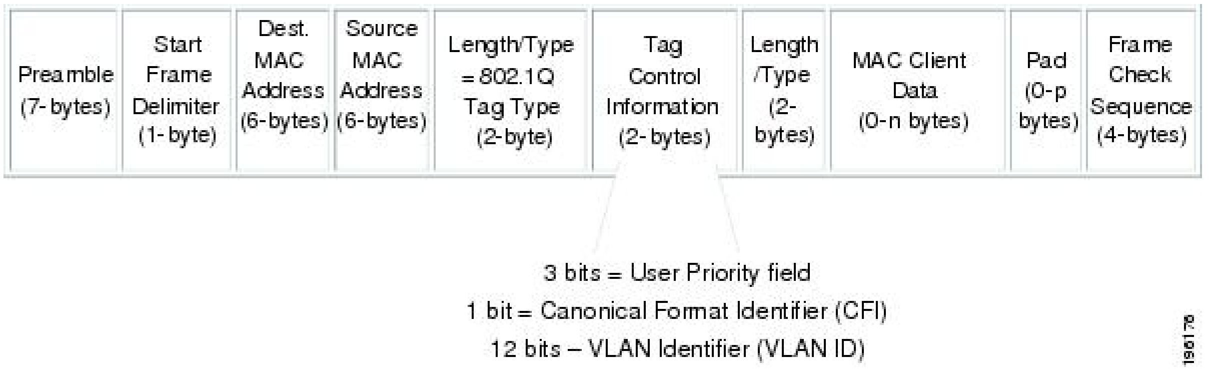

Preamble (7 - bytes)
Start Frame Delimiter (1 - byte)
Dest. MAC Address (6 - bytes)
Source MAC Address (6 - bytes)
Length / Type (2 - bytes)
MAC Client Data (0 - n bytes)
Pad (0 - p bytes)
Frame Check Sequence (4 - bytes)
196176

Figure 3: Header With 802.1Q Tag


Preamble (7- bytes)
Start Frame Delimiter (1- byte)
Dest. MAC Address (6-bytes)
Source MAC Address (6-bytes)
Length/Type = 802.1Q Tag Type (2-byte)
Tag Control Information (2- bytes)
Length /Type (2- bytes)
MAC Client Data (0-n bytes)
Pad (0-p bytes)
Frame Check Sequence (4-bytes)
3 bits = User Priority field
1 bit = Canonical Format Identifier (CFI)
12 bits – VLAN Identifier (VLAN ID)
196178

High Availability

The software supports high availability for Layer 2 ports.

Prerequisites for VLAN Trunking

VLAN trunking has the following prerequisite:

You are logged into the CLI.

Guidelines and Limitations

VLAN trunking has the following configuration guidelines and limitations:

- Do not connect devices with access links because access links may partition a VLAN.
- When connecting Cisco switches through an 802.1Q trunk, make sure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning tree loops might result.
- You can group trunk ports into port channel groups, but all trunks in the group must have the same configuration. When a group is first created, all ports follow the parameters set for the first port to be

added to the group. If you change the configuration of one of these parameters, the device propagates that setting to all ports in the group, such as the allowed VLANs and the trunk status. For example, if one port in a port group ceases to be a trunk, all ports cease to be trunks.

- If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled.
- If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.

Default Settings

Table 1: Default Settings for Access and Trunk Interfaces

Parameters	Default
Switchport mode	Access
Allowed VLANs	1 to 3967, 4048 to 4094
Access VLAN ID	VLAN1
Native VLAN ID	VLAN1
Native VLAN ID tagging	Disabled
Administrative state	Shut

Configuring Access and Trunk Interfaces

Configuring a LAN Interface as a Layer 2 Access Port

You can use this procedure to configure a Layer 2 port as an access port.

Before You Begin

- The interface can be either Ethernet or vEthernet.
- An access port transmits packets on only one, untagged VLAN. You specify which VLAN traffic that the interface carries, which becomes the access VLAN. If you do not specify a VLAN for an access port, that 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.
- Be aware that the Cisco Nexus 1000V commands may differ from the Cisco IOS commands.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *interface*	Specifies the interface that you are configuring and places you in interface configuration mode. • For an Ethernet port, use **ethernet** *slot/port*, where *slot* is the module slot number and *port* is the port number. • For a vEthernet port, use **vethernet** *interface-number*, where *interface-number* is a number from 1 to 1048575.
Step 3	switch(config-if)# **switchport mode access**	Sets the interface as a nontrunking nontagged, single-VLAN Layer 2 interface in the running configuration.
Step 4	switch(config-if)# **switchport mode access** *vlan-id*	(Optional) Specifies the VLAN for which this access port will carry traffic and saves the change in the running configuration. 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.
Step 5	switch(config-if)# **show interface** *interface*	(Optional) Displays the interface status and information.
Step 6	switch(config-if)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to set Ethernet 3/1 as a Layer 2 access port that carries traffic for VLAN 5 only:

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

Configuring Trunk Ports

You can use this procedure to configure a Layer 2 port as a trunk port.

Before You Begin

- Before you configure a trunk port, ensure that you are configuring a Layer 2 interface.
- You must use only an Ethernet interface.
- A trunk port transmits untagged packets for one VLAN plus encapsulated, tagged, packets for multiple VLANs.

- The device supports 802.1Q encapsulation only.
- Be aware that the Cisco Nexus 1000V commands may differ from the Cisco IOS commands.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *interface*	Specifies the interface that you are configuring and places you in the interface configuration mode. • For an Ethernet port, use **ethernet** *slot/port*, where *slot* is the module slot number and *port* is the port number.
Step 3	switch(config-if)# **switchport mode trunk**	Sets the interface as a Layer 2 trunk port in the running configuration. 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.
Step 4	switch(config-if)# **show interface***interface*	(Optional) Displays the interface status and information.
Step 5	switch(config-if)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to set Ethernet 3/1 as a Layer 2 trunk port:

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

Configuring the Native VLAN for 802.1Q Trunking Ports

You can use this procedure to configure the native VLAN for 802.1Q trunk ports. If you do not configure this parameter, the trunk port uses the default VLAN as the native VLAN ID.

Before You Begin

Be aware that the Cisco Nexus 1000V commands may differ from the Cisco IOS commands.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *interface*	Specifies the interface that you are configuring and places you in interface configuration mode. • For an Ethernet port, use **ethernet** *slot/port*, where *slot* is the module slot number and *port* is the port number. • For a vEthernet port, use **vethernet** *interface-number*, where *interface-number* is a number from 1 to 1048575.
Step 3	switch#(config-if) **switchport trunk native vlan***vlan-id*	Designates the native VLAN for the 802.1Q trunk in the running configuration. Valid values are from 1 to 4094, except those VLANs reserved for internal use. The default value is VLAN1.
Step 4	switch#(config-if) **show vlan**	(Optional) Displays the status and information of VLANs.
Step 5	switch(config-if)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to set the native VLAN for the Ethernet 3/1, Layer 2 trunk port to VLAN 5:

```
n1000v# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# switchport trunk native vlan 5
switch(config-if)#
```

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 Begin

- 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.
- Be aware that the Cisco Nexus 1000V commands may differ from the Cisco IOS commands.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *interface*	Specifies the interface that you are configuring and places you in interface configuration mode. • For an Ethernet port, use **ethernet** *slot/port*, where *slot* is the module slot number and *port* is the port number. • For a vEthernet port, use **vethernet** *interface-number*, where *interface-number* is a number from 1 to 1048575.
Step 3	switch(config-if)# **switchport trunk allowed vlan** {*vlan-list* **all** | **none** [**add** |**except** | **none** | **remove** {*vlan-list*}]}	Sets the allowed VLANs for the trunk interface in the running configuration. The default is to allow all VLANs on the trunk interface. The range is from 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. **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.
Step 4	switch(config-if)# **show vlan**	(Optional) Displays the status and information of VLANs.
Step 5	switch(config-if)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to add VLANs 15 to 20 to the list of allowed VLANs on the Ethernet 3/1, Layer 2 trunk port:

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

Configuring the Device to Tag Native VLAN Traffic

When working with 802.1Q trunked interfaces, you can maintain the tagging for all packets that enter with a tag that matches the native VLAN ID. Untagged traffic is dropped (you will still carry control traffic on that interface).

Before You Begin

- The vlan dot1q tag native global command changes the behavior of all native VLAN ID interfaces on all trunks on the device.

- This feature applies to the entire device; you cannot apply it to selected VLANs on a device.
- Be aware that the Cisco Nexus 1000V commands may differ from the Cisco IOS commands.

Note If you enable 802.1Q tagging on one device and disable it on another device, all traffic is dropped on the device with this feature disabled. You must configure this feature identically on each device.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch#(config) **vlan dot1q tag native**	Modifies the behavior of a 802.1Q trunked native VLAN ID interface in the running configuration. The interface maintains the taggings for all packets that enter with a tag that matches the value of the native VLAN ID and drops all untagged traffic. The control traffic is still carried on the native VLAN. The default is disabled.
Step 3	switch(config-if)# **show vlan**	(Optional) Displays the status and information of VLANs.
Step 4	switch(config-if)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to change the behavior of the native VLAN on an 802.1Q trunked interface to maintain the tagged packets and drop all untagged traffic (except control traffic):

```
n1000v# configure terminal
switch(config)# vlan dot1q tag native
switch(config-if)#
```

Verifying the Interface Configuration

Use one of the following commands to verify the access and trunk interface configuration information:

Command	Purpose
show interface ethernet *slot/port* [**brief** | **capabilities** | **counters** | **mac-address** | **status** | **switchport** | **trunk**]	Displays the interface configuration.
show interface ethernet *slot/port* **counters** [**brief** | **detailed** | **errors** | **snmp** | **storm-control** | **trunk**]	Displays the counters for a specified Ethernet interface.

Command	Purpose
show interface ethernet *slot/port* **status** [**err-disable**]	Displays the status for a specified Ethernet interface.
show interface brief	Displays interface configuration information, including the mode.
show interface switchport	Displays information, including access and trunk interface, information for all Layer 2 interfaces.
show interface trunk [**module** *module-number* | **vlan** *vlan-id*]	Displays trunk configuration information.
show interface capabilities	Displays information on the capabilities of the interfaces.
show running-config interface ethernet *slot/port*	Displays configuration information about the specified interface.

Monitoring the Interface Configuration

Use one of the following commands to display access and trunk interface configuration information:

Command	Purpose
clear counters [*interface*]	Clears the counters.
show interface counters [**module** *module*]	Displays input and output octets unicast packets, multicast packets, and broadcast packets.
show interface counters detailed [**all**]	Displays input packets, bytes, and multicast as well as output packets and bytes.
show interface counters errors [**module** *module*]	Displays information on the number of error packets.

Configuration Examples for Access and Trunk Port Mode

The following example shows how to configure a Layer 2 access interface and assign the access VLAN for that interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/30
switch(config-if)# switchport
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 5
switch(config-if)#
```

The following example shows how to configure a Layer 2 trunk interface, assign the native VLAN and the allowed VLANs, and configure the device to tag the native VLAN traffic on the trunk interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/35
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk native vlan 10
switch(config-if)# witchport trunk allowed vlan 5, 10
switch(config-if)# exit
switch(config-if)#
```

Feature History for Layer 2 Interface Parameters

Feature Name	Releases	Feature Information
Layer 2 interface parameters	5.2(1)SM1(5.1)	This feature was introduced