



CHAPTER 3

Configuring Layer 2 Interfaces

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

This chapter includes the following sections:

- [Information About Access and Trunk Interfaces](#), page 3-1
- [Prerequisites for VLAN Trunking](#), page 3-3
- [Guidelines and Limitations](#), page 3-3
- [Default Settings](#), page 3-4
- [Configuring Access and Trunk Interfaces](#), page 3-4
- [Verifying the Interface Configuration](#), page 3-11
- [Monitoring the Interface Configuration](#), page 3-12
- [Configuration Examples for Access and Trunk Port Mode](#), page 3-12
- [Additional References](#), page 3-12
- [Feature History for Layer 2 Interface Parameters](#), page 3-13



Note

For information about configuring a Switched Port Analyzer (SPAN) destination interface, see the *Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(5.1)*.



Note

for information about VLANs, MAC address tables, and private VLANs, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(5.1)*.



Note

for information about configuring vEthernet interfaces, see the [“Configuring Virtual Ethernet Interfaces”](#) section on page 4-1.

Information About Access and Trunk Interfaces

This section includes the following topics:

- [Access and Trunk Interfaces](#), page 3-2
- [IEEE 802.1Q Encapsulation](#), page 3-2

Send document comments to nexus1k-docfeedback@cisco.com.

- [High Availability](#), page 3-3

Access and Trunk Interfaces

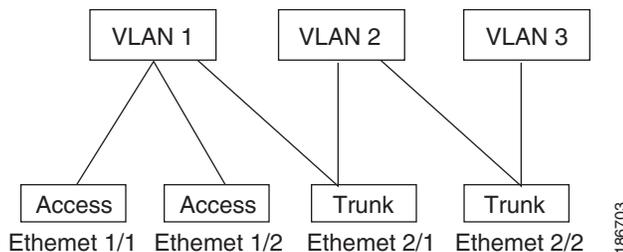
A Layer 2 port can be configured as an access or a trunk port as follows:

- 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 Getting Started Guide, Release 4.2(1)SV1(5.1)* for information about setting the default port mode.

[Figure 3-1](#) shows how you can use trunk ports in the network. The trunk port carries traffic for two or more VLANs.

Figure 3-1 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 (see the “[IEEE 802.1Q Encapsulation](#)” section on page 3-2 for more information).

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 [Figure 3-2](#) and [Figure 3-3](#)). 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.

Send document comments to nexus1k-docfeedback@cisco.com.

Figure 3-2 Header Without 802.1Q Tag

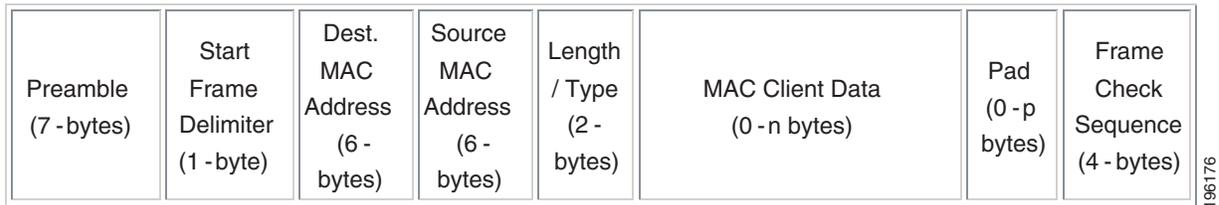
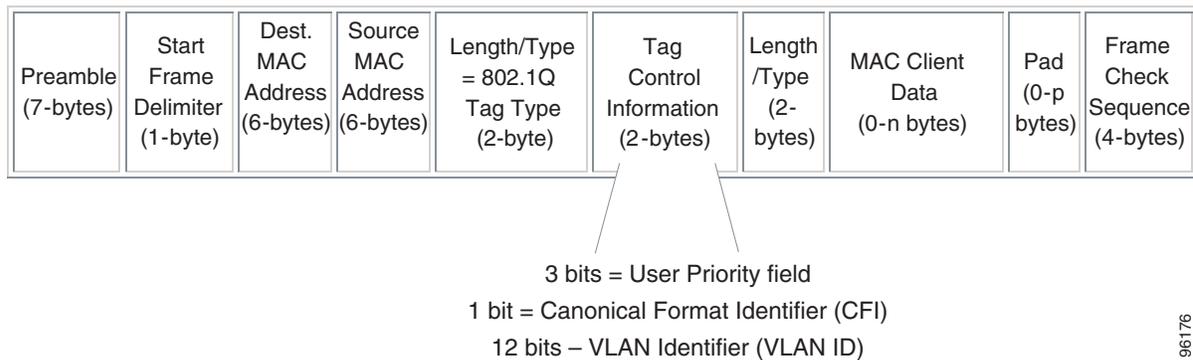


Figure 3-3 Header With 802.1Q Tag



High Availability

The software supports high availability for Layer 2 ports.

Prerequisites for VLAN Trunking

VLAN trunking has this prerequisite:

- You are logged into the CLI.

Guidelines and Limitations

VLAN trunking has the following 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.

Send document comments to nexus1k-docfeedback@cisco.com.

- 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

The following table lists the default settings for device access and trunk port mode parameters.

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

This section includes the following topics:

- [Configuring a LAN Interface as a Layer 2 Access Port, page 3-4](#)
- [Configuring Trunk Ports, page 3-6](#)
- [Configuring the Native VLAN for 802.1Q Trunking Ports, page 3-7](#)
- [Configuring the Allowed VLANs for Trunking Ports, page 3-8](#)
- [Configuring the Device to Tag Native VLAN Traffic, page 3-10](#)



Note

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

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

Before beginning this procedure, you must know or do the following:

- 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.

Send document comments to nexus1k-docfeedback@cisco.com.

SUMMARY STEPS

1. `config t`
2. `interface interface`
3. `switchport mode access`
4. `switchport access vlan vlan-id`
5. `show interface`
6. `copy running-config startup-config`

DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code> Example: n1000v# config t n1000v(config)#	Enters the global configuration mode.
Step 2	<code>interface interface</code> Example 1: n1000v(config)# interface ethernet 3/1 n1000v(config-if)#	Specifies the interface that you are configuring and places you in interface configuration mode. <ul style="list-style-type: none"> • For an Ethernet port, use ethernet <i>slot/port</i>, where <i>slot</i> is the module slot number and <i>port</i> is the port number. • For a vEthernet port, use vethernet <i>interface-number</i>, where <i>interface-number</i> is a number from 1 to 1048575.
Step 3	<code>switchport mode access</code> Example: n1000v(config-if)# switchport mode access	Sets the interface as a nontrunking nontagged, single-VLAN Layer 2 interface in the running configuration.
Step 4	<code>switchport access vlan vlan-id</code> Example: n1000v(config-if)# switchport access vlan 5	(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	<code>show interface</code> Example: n1000v(config)# show interface	(Optional) Displays the interface status and information.
Step 6	<code>copy running-config startup-config</code> Example: n1000v(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

EXAMPLES

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

Send document comments to nexus1k-docfeedback@cisco.com.

```
n1000v# config t
n1000v(config)# interface ethernet 3/1
n1000v(config-if)# switchport mode access
n1000v(config-if)# switchport access vlan 5
n1000v(config-if)#
```

Configuring Trunk Ports

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

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- Before you configure a trunk port, ensure that you are configuring a Layer 2 interface.
- The interface can be either Ethernet or vEthernet.
- A trunk port transmits untagged packets for one VLAN plus encapsulated, tagged, packets for multiple VLANs. (See the “[IEEE 802.1Q Encapsulation](#)” section on page 3-2 for information about encapsulation.)
- The device supports 802.1Q encapsulation only.

SUMMARY STEPS

1. **config t**
2. **interface *interface***
3. **switchport mode trunk**
4. **show interface**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Enters the global configuration mode.
Step 2	interface <i>interface</i> Example: n1000v(config)# interface ethernet 3/1 n1000v(config-if)#	Specifies the interface that you are configuring and places you in interface configuration mode. <ul style="list-style-type: none"> • For an Ethernet port, use ethernet <i>slot/port</i>, where <i>slot</i> is the module slot number and <i>port</i> is the port number. • For a vEthernet port, use vethernet <i>interface-number</i>, where <i>interface-number</i> is a number from 1 to 1048575.

Send document comments to nexus1k-docfeedback@cisco.com.

	Command	Purpose
Step 3	switchport mode trunk Example: n1000v(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	show interface Example: n1000v(config)# show interface	(Optional) Displays the interface status and information.
Step 5	copy running-config startup-config Example: n1000v(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

EXAMPLES

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

```
n1000v# config t
n1000v(config)# interface ethernet 3/1
n1000v(config-if)# switchport mode trunk
n1000v(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.

SUMMARY STEPS

1. **config t**
2. **interface *interface***
3. **switchport trunk native vlan *vlan-id***
4. **show vlan**
5. **copy running-config startup-config**

Send document comments to nexus1k-docfeedback@cisco.com.

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Enters the global configuration mode.
Step 2	interface interface Example: n1000v(config)# interface ethernet 3/1 n1000v(config-if)#	Specifies the interface that you are configuring and places you in interface configuration mode. <ul style="list-style-type: none"> For an Ethernet port, use ethernet slot/port, where <i>slot</i> is the module slot number and <i>port</i> is the port number. For a vEthernet port, use vethernet interface-number, where <i>interface-number</i> is a number from 1 to 1048575.
Step 3	switchport trunk native vlan vlan-id Example: n1000v(config-if)# switchport trunk native vlan 5	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	show vlan Example: n1000v(config)# show vlan	(Optional) Displays the status and information of VLANs.
Step 5	copy running-config startup-config Example: n1000v(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

EXAMPLES

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

```
n1000v# config t
n1000v(config)# interface ethernet 3/1
n1000v(config-if)# switchport trunk native vlan 5
n1000v(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 beginning this procedure, you must know or do the following:

- 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.

Send document comments to nexus1k-docfeedback@cisco.com.

SUMMARY STEPS

1. `config t`
2. `interface interface`
3. `switchport trunk allowed vlan {vlan-list | all | none | [add | except | | remove {vlan-list}]}`
4. `show vlan`
5. `copy running-config startup-config`

DETAILED STEPS

	Command	Purpose
Step 1	<p><code>config t</code></p> <p>Example: n1000v# config t n1000v(config)#</p>	Enters the global configuration mode.
Step 2	<p><code>interface interface</code></p> <p>Example: n1000v(config)# interface ethernet 3/1 n1000v(config-if)#</p>	<p>Specifies the interface that you are configuring and places you in interface configuration mode.</p> <ul style="list-style-type: none"> • For an Ethernet port, use ethernet slot/port, where <i>slot</i> is the module slot number and <i>port</i> is the port number. • For a vEthernet port, use vethernet interface-number, where <i>interface-number</i> is a number from 1 to 1048575.
Step 3	<p><code>switchport trunk allowed vlan {vlan-list all none [add except none remove {vlan-list}]}</code></p> <p>Example: n1000v(config-if)# switchport trunk allowed vlan add 15-20#</p>	<p>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.</p> <p>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.</p>
Step 4	<p><code>show vlan</code></p> <p>Example: n1000v# show vlan</p>	(Optional) Displays the status and information for VLANs.
Step 5	<p><code>copy running-config startup-config</code></p> <p>Example: n1000v(config)# copy running-config startup-config</p>	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Send document comments to nexus1k-docfeedback@cisco.com.

EXAMPLES

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:

```
n1000v# config t
n1000v(config)# interface ethernet 3/1
n1000v(config-if)# switchport trunk allowed vlan 15-20
n1000v(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

Before beginning this procedure, you must know or do the following:

- 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.



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.

SUMMARY STEPS

1. **config t**
2. **vlan dot1q tag native**
3. **show vlan**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Enters the global configuration mode.
Step 2	vlan dot1q tag native Example: n1000v(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.

Send document comments to nexus1k-docfeedback@cisco.com.

	Command	Purpose
Step 3	show vlan Example: n1000v# show vlan	(Optional) Displays the status and information for VLANs.
Step 4	copy running-config startup-config Example: n1000v# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

EXAMPLES

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# config t
n1000v(config)# vlan dot1q tag native
n1000v#
```

Verifying the Interface Configuration

You can display access and trunk interface configuration information.

Command	Purpose
show interface ethernet <i>slot/port</i> [brief capabilities counters mac-address status switchport trunk]	Displays the interface configuration
show interface ethernet <i>slot/port</i> counters [brief detailed errors snmp storm-control trunk]	Displays the counters for a specified Ethernet interface.
show interface ethernet <i>slot/port</i> 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 <i>module-number</i> vlan <i>vlan-id</i>]	Displays trunk configuration information.
show interface capabilities	Displays information on the capabilities of the interfaces.
show running-config interface ethernet <i>slot/port</i>	Displays configuration information about the specified interface.

[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

Monitoring the Interface Configuration

You can display access and trunk interface configuration information.

Command	Purpose
<code>clear counters [interface]</code>	Clears the counters.
<code>show interface counters [module module]</code>	Displays input and output octets unicast packets, multicast packets, and broadcast packets.
<code>show interface counters detailed [all]</code>	Displays input packets, bytes, and multicast as well as output packets and bytes.
<code>show interface counters errors [module module]</code>	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:

```
n1000v# configure terminal
n1000v(config)# interface ethernet 2/30
n1000v(config-if)# switchport
n1000v(config-if)# switchport mode access
n1000v(config-if)# switchport access vlan 5
n1000v(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:

```
n1000v# configure terminal
n1000v(config)# interface ethernet 2/35
n1000v(config-if)# switchport
n1000v(config-if)# switchport mode trunk
n1000v(config-if)# switchport trunk native vlan 10
n1000v(config-if)# switchport trunk allowed vlan 5, 10
n1000v(config-if)# exit
n1000v(config)# vlan dot1q tag native
n1000v(config)#
```

Additional References

For additional information related to implementing access and trunk port modes, see the following sections:

- [Related Documents, page 3-13](#)
- [Standards, page 3-13](#)

Send document comments to nexus1k-docfeedback@cisco.com.

Related Documents

Related Topic	Document Title
Complete command syntax, command modes, command history, defaults, usage guidelines, and examples for all Cisco Nexus 1000V commands.	<i>Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)</i>
Port channels	Chapter 5, “Configuring Port Channels”
VLANs, private VLANs, and STP	<i>Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(5.1)</i>
System management	<i>Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(5.1)</i>
Release Notes	<i>Cisco Nexus 1000V Release Notes, Release 4.2(1)SV1(5.1)</i>

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for Layer 2 Interface Parameters

This section provides the feature history for Layer 2 interface parameters.

Feature Name	Releases	Feature Information
Layer 2 interface parameters	4.0(4)SV1(1)	This feature was introduced.

Send document comments to nexus1k-docfeedback@cisco.com.