



CHAPTER 3

Configuring Layer 2 Interfaces



Note

This chapter describes how to configure Layer 2 switching ports as access or trunk ports. A Layer 2 port can function as either a trunk port, an access port, or a private VLAN port. See the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.0* for more information on private VLANs.

This chapter includes the following topics:

- [Information About Access and Trunk Interfaces, page 3-2](#)
- [Licensing Requirements for Layer 2 Port Modes, page 3-6](#)
- [Prerequisites for VLAN Trunking, page 3-6](#)
- [Guidelines and Limitations, page 3-6](#)
- [Configuring Access and Trunk Interfaces, page 3-7](#)
- [Verifying Interface Configuration, page 3-18](#)
- [Displaying and Clearing Statistics, page 3-18](#)
- [Access and Trunk Port Mode Example Configurations, page 3-18](#)
- [Additional References, page 3-19](#)



Note

See the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.0* for information on configuring a SPAN destination interface.

You can configure Layer 2 switching ports as access or trunk ports. Trunks carry the traffic of multiple VLANs over a single link and allow you to extend VLANs across an entire network. All Layer 2 switching ports maintain media access control (MAC) address tables.



Note

See the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.0* for information on VLANs, MAC address tables, private VLANs, and the Spanning Tree Protocol.



Note

A Layer 2 port can function as either a trunk port, an access port, or a private VLAN port. See the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.0* for more information on private VLANs.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Information About Access and Trunk Interfaces



Note

See the *Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 4.0* for complete information on high-availability features.

This section includes the following topics:

- [Information About Access and Trunk Interfaces, page 3-2](#)
- [IEEE 802.1Q Encapsulation, page 3-3](#)
- [Access VLANs, page 3-4](#)
- [Native VLAN IDs for Trunk Ports, page 3-5](#)
- [Tagging Native VLAN Traffic, page 3-5](#)
- [Allowed VLANs, page 3-5](#)
- [High Availability, page 3-5](#)
- [Virtualization Support, page 3-6](#)



Note

The device supports only IEEE 802.1Q-type VLAN trunk encapsulation.

Information About 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 device are Layer 3 ports.

You can make all ports Layer 2 ports using the setup script or by entering the **system default switchport** command. See the *Cisco NX-OS Fundamentals Configuration Guide* for information on using the setup script. To configure the port as a Layer 2 port using the CLI, use the **switchport** command,

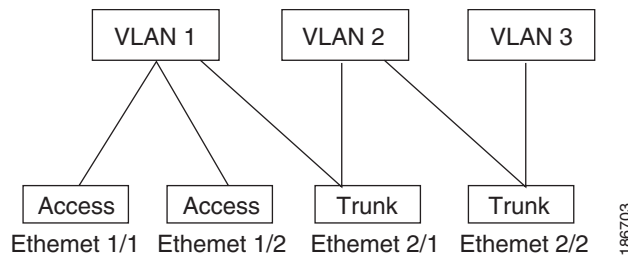
All ports in one trunk must be in the same virtual device context (VDC). See the *Cisco Virtual Device Context Configuration Guide* for information on VDCs.

All ports in the same trunk must be in the same VDC, and trunk ports cannot carry VLANs from different VDCs.

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

Send document comments to nexus7k-docfeedback@cisco.com

Figure 3-1 Trunk and Access Ports and VLAN Traffic



Note

See the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.0* for information on VLANs.

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 3-3 for more information).



Note

See the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0* for information on subinterfaces on Layer 3 interfaces.

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.

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.

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

When you change a Layer 2 interface back to a Layer 3 interface, that interface loses all the Layer 2 configuration and resumes the default VLAN configurations.

IEEE 802.1Q Encapsulation



Note

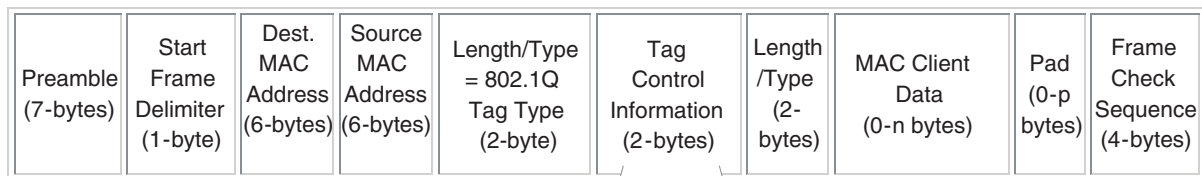
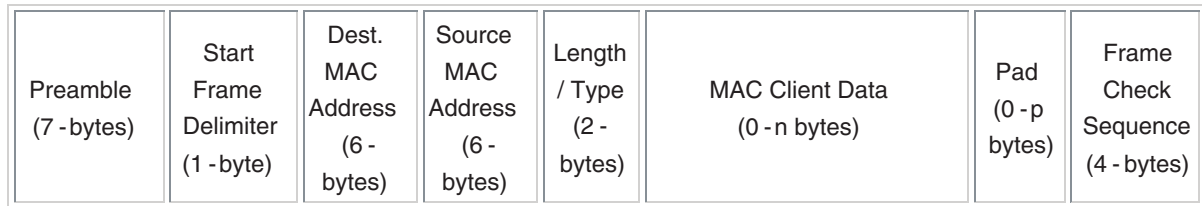
For information about VLANs, see the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.0*.

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, or tagging, method that uses a tag that is inserted into the frame header (see [Figure 3-2](#)). 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 nexus7k-docfeedback@cisco.com

Figure 3-2 Header Without and With 802.1Q Tag



3 bits = User Priority field
1 bit = Canonical Format Identifier (CFI)
12 bits – VLAN Identifier (VLAN ID)

182779

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.



Note

See the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.0* for complete information on private VLANs.

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 shuts 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.

Send document comments to nexus7k-docfeedback@cisco.com

Native VLAN IDs for Trunk Ports

A trunk port can carry nontagged 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. That is, the native VLAN ID is the VLAN that carries untagged traffic on trunk ports.

**Note**

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

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.

Tagging Native VLAN Traffic

The NX-OS software supports the IEEE 802.1Q standard on trunk ports. In order to pass untagged traffic through the trunk ports, you must create a VLAN that does not tag any packets (or you can use the default VLAN). Untagged packets can pass through trunk ports and access ports.

However, all packets that enter the device with an 802.1Q tag that matches the value of the native VLAN on the trunk are stripped of any tagging and egress the trunk port as untagged packets. This can cause problems because you may want to retain the tagging on packets on the native VLAN for the trunk port.

You can configure the device to drop all untagged packets on the trunk ports and to retain the tagging of packets entering the device with 802.1Q values that are equal to that of the native VLAN ID. All control traffic still passes on the native VLAN. This is a global configuration; trunk ports on the device either do or do not retain the tagging for the native VLAN.

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. Later, you can add any specific VLANs that you may want the trunk to carry traffic for back to the list.

To partition the 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.

**Note**

See the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.0* for more information about STP.

High Availability

The software supports high availability for Layer 2 ports.

Send document comments to nexus7k-docfeedback@cisco.com



Note

See the *Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 4.0* for complete information on high availability features.

Virtualization Support

The device supports virtual device contexts (VDCs).

All ports in the same trunk must be in the same VDC, and trunk ports cannot carry VLANs from different VDCs.



Note

See the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.0* for complete information on VDCs and assigning resources.

Licensing Requirements for Layer 2 Port Modes

The following table shows the licensing requirements for this feature:

Product	License Requirement
NX-OS	Layer 2 port modes require no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the <i>Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0</i> .

However, using VDCs requires an Advanced Services license.

Prerequisites for VLAN Trunking

To set the port in either an access or trunk switchport mode, you must have the following prerequisites:

- You are logged onto the device.
- You must configure the port as a Layer 2 port before you can use the **switchport mode** command. By default, all ports on the device are Layer 3 ports.

Guidelines and Limitations

The following configuration guidelines and restrictions apply when using 802.1Q trunks and impose some limitations on the trunking strategy for a network. Consider these restrictions when using 802.1Q trunks:

- A port can be either a Layer 2 or a Layer 3 interface; it cannot be both simultaneously.
- When you change a Layer 3 port to a Layer 2 port or a Layer 2 port to a Layer 3 port, all layer-dependent configuration is lost. When you change an access or trunk port to a Layer 3 port, all information about the access VLAN, native VLAN, allowed VLANs, and so forth, is lost.

Send document comments to nexus7k-docfeedback@cisco.com

- 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.
- Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can cause spanning tree loops. You must leave spanning tree enabled on the native VLAN of an 802.1Q trunk. If you cannot leave spanning tree enabled, you must disable spanning tree on every VLAN in the network. Make sure that your network has no physical loops before you disable spanning tree.
- When you connect two Cisco switches through 802.1Q trunks, the switches exchange spanning tree bridge protocol data units (BPDUs) on each VLAN allowed on the trunks. The BPDUs on the native VLAN of the trunk are sent untagged to the reserved IEEE 802.1D spanning tree multicast MAC address (01-80-C2-00-00-00). The BPDUs on all other VLANs on the trunk are sent tagged to the reserved Cisco Shared Spanning Tree (SSTP) multicast MAC address (01-00-0c-cc-cc-cd).
- Non-Cisco 802.1Q switches maintain only a single instance of spanning tree (the Mono Spanning Tree) that defines the spanning tree topology for all VLANs. When you connect a Cisco device to a non-Cisco device through an 802.1Q trunk, the Mono Spanning Tree of the non-Cisco device and the native VLAN spanning tree of the Cisco device combine to form a single spanning tree topology known as the Common Spanning Tree (CST).
- Because Cisco switches transmit BPDUs to the SSTP multicast MAC address on VLANs other than the native VLAN of the trunk, non-Cisco switches do not recognize these frames as BPDUs and flood them on all ports in the corresponding VLAN. Other Cisco switches connected to the non-Cisco 802.1Q cloud receive these flooded BPDUs. This BPDU reception allows Cisco switches to maintain a per-VLAN spanning tree topology across a cloud of non-Cisco 802.1Q switches. The non-Cisco 802.1Q cloud that separates the Cisco switches is treated as a single broadcast segment between all switches connected to the non-Cisco 802.1Q cloud through 802.1Q trunks.
- Make certain that the native VLAN is the same on all of the 802.1Q trunks that connect the Cisco switches to the non-Cisco 802.1Q cloud.
- If you are connecting multiple Cisco switches to a non-Cisco 802.1Q cloud, all of the connections must be through 802.1Q trunks. You cannot connect Cisco switches to a non-Cisco 802.1Q cloud through access ports because doing so places the access port on the Cisco device into the spanning tree “port inconsistent” state and no traffic will pass through the port.
- 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.

Configuring Access and Trunk Interfaces

This section includes the following topics:

- [Guidelines for Configuring Access and Trunk Interfaces, page 3-8](#)
- [Configuring a LAN Interface as a Layer 2 Access Port, page 3-8](#)
- [Configuring Access Host Ports, page 3-9](#)

Send document comments to nexus7k-docfeedback@cisco.com

- [Configuring Trunk Ports, page 3-11](#)
- [Configuring the Native VLAN for 802.1Q Trunking Ports, page 3-12](#)
- [Configuring the Allowed VLANs for Trunking Ports, page 3-13](#)
- [Configuring the Device to Tag Native VLAN Traffic, page 3-15](#)
- [Changing the System Default Port Mode to Layer 2, page 3-16](#)

**Note**

If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Guidelines for Configuring Access and Trunk Interfaces

All VLANs on a trunk must be in the same VDC.

Configuring a LAN Interface as a Layer 2 Access Port

You can configure a Layer 2 port as an access port. 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.

BEFORE YOU BEGIN

Ensure that you are configuring a Layer 2 interface.

SUMMARY STEPS

1. **config t**
2. **interface** *{{type slot/port} | {port-channel number}}*
3. **switchport mode** *{access | trunk}*
4. **switchport access vlan** *vlan-id*
5. **exit**
6. **show interface**
7. **copy running-config startup-config**

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code> Example: switch# config t switch(config)#	Enters configuration mode.
Step 2	<code>interface {{type slot/port} {port-channel number}}</code> Example: switch(config)# interface ethernet 3/1 switch(config-if)#	Specifies an interface to configure, and enters interface configuration mode.
Step 3	<code>switchport mode {access trunk}</code> Example: switch(config-if)# switchport mode access	Sets the interface as a nontrunking nontagged, single-VLAN Layer 2 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	<code>switchport access vlan vlan-id</code> Example: switch(config-if)# switchport access vlan 5	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 <i>change</i> the VLAN for which the access port carries traffic.
Step 5	<code>exit</code> Example: switch(config-if)# exit switch(config)#	Exits the configuration mode.
Step 6	<code>show interface</code> Example: switch# show interface	(Optional) Displays the interface status and information.
Step 7	<code>copy running-config startup-config</code> Example: switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

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

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

Configuring Access Host Ports



Note

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

Send document comments to nexus7k-docfeedback@cisco.com

You can optimize the performance of access ports that are connected to end stations by simultaneously setting that port as an access port. An access host port handles the 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 5, “Configuring Port Channels”](#) for information on port-channel interfaces and the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.0* for complete information on the Spanning Tree Protocol.

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. **config t**
2. **interface** *type slot/port*
3. **switchport host**
4. **exit**
5. **show interface**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: switch# config t switch(config)#	Enters configuration mode.
Step 2	interface <i>type slot/port</i> Example: switch(config)# interface ethernet 3/1 switch(config-if)#	Specifies an interface to configure, and enters interface configuration mode.
Step 3	switchport host Example: 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. Note Apply this command only to end stations.
Step 4	exit Example: switch(config-if)# exit switch(config)#	Exits the interface mode.

Send document comments to nexus7k-docfeedback@cisco.com

	Command	Purpose
Step 5	show interface Example: switch# show interface	(Optional) Displays the interface status and information.
Step 6	copy running-config startup-config Example: switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

This example shows how to set Ethernet 3/1 as a Layer 2 access port with PortFast enabled and port channel disabled:

```
switch# config t
switch(config)# interface ethernet 3/1
switch(config-if)# switchport host
switch(config-if)#
```

Configuring Trunk Ports

You can configure a Layer 2 port as a trunk port. 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 3-3 for information about encapsulation.)



Note

The device supports 802.1Q encapsulation only.

BEFORE YOU BEGIN

Before you configure a trunk port, ensure that you are configuring a Layer 2 interface.

SUMMARY STEPS

1. **config t**
2. **interface** {*type slot/port* | **port-channel number**}
3. **switchport mode** {**access** | **trunk**}
4. **exit**
5. **show interface**
6. **copy running-config startup-config**

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: switch# config t switch(config)#	Enters configuration mode.
Step 2	interface { <i>type slot/port</i> port-channel number } Example: switch(config)# interface ethernet 3/1 switch(config-if)#	Specifies an interface to configure, and enters interface configuration mode.
Step 3	switchport mode { access trunk } Example: switch(config-if)# switchport mode trunk	Sets the interface as a Layer 2 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.
Step 4	exit Example: switch(config-if)# exit switch(config)#	Exits the interface mode.
Step 5	show interface Example: switch# show interface	(Optional) Displays the interface status and information.
Step 6	copy running-config startup-config Example: switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

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

```
switch# config t
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 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** {*type slot/port* | **port-channel number**}
3. **switchport trunk native vlan** *vlan-id*

Send document comments to nexus7k-docfeedback@cisco.com

4. `exit`
5. `show vlan`
6. `copy running-config startup-config`

DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code> Example: switch# <code>config t</code> switch(config)#	Enters configuration mode.
Step 2	<code>interface {type slot/port port-channel number}</code> Example: switch(config)# <code>interface ethernet 3/1</code> switch(config-if)#	Specifies an interface to configure, and enters interface configuration mode.
Step 3	<code>switchport trunk native vlan vlan-id</code> Example: switch(config-if)# <code>switchport trunk native vlan 5</code>	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.
Step 4	<code>exit</code> Example: switch(config-if)# <code>exit</code> switch(config)#	Exits the interface mode.
Step 5	<code>show vlan</code> Example: switch# <code>show vlan</code>	(Optional) Displays the status and information of VLANs.
Step 6	<code>copy running-config startup-config</code> Example: switch(config)# <code>copy running-config startup-config</code>	(Optional) Copies the running configuration to the startup configuration.

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

```
switch# config t
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.

Send document comments to nexus7k-docfeedback@cisco.com

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.

SUMMARY STEPS

1. **config t**
2. **interface** { *ethernet slot/port* | **port-channel number**}
3. **switchport trunk allowed vlan** { *vlan-list* | **all** | **none** | [**add** | **except** | | **remove** { *vlan-list* }]}
4. **exit**
5. **show vlan**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: switch# config t switch(config)#	Enters configuration mode.
Step 2	interface { <i>ethernet slot/port</i> port-channel number } Example: switch(config)# interface ethernet 3/1	Specifies an interface to configure, and enters interface configuration mode.
Step 3	switchport trunk allowed vlan { <i>vlan-list</i> all none [add except none remove { <i>vlan-list</i> }]} Example: switch(config-if)# switchport trunk allowed vlan add 15-20#	Sets the 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. 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	exit Example: switch(config-if)# exit switch(config)#	Exits the interface mode.

Send document comments to nexus7k-docfeedback@cisco.com

	Command	Purpose
Step 5	show vlan Example: switch# show vlan	(Optional) Displays the status and information for VLANs.
Step 6	copy running-config startup-config Example: switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

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

```
switch# config t
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 you are working with 802.1Q trunked interfaces, you can maintain the tagging for all packets that enter with a tag that matches the value of the native VLAN ID and drops all untagged traffic (you will still carry control traffic on that interface). This feature applies to the entire device; you cannot apply it to selected VLANs on a device.

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

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command). You can repeat VLAN names and IDs in different VDCs, so you must confirm that you are working in the correct VDC.

SUMMARY STEPS

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

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: switch# config t switch(config)#	Enters configuration mode.
Step 2	vlan dot1q tag native Example: switch(config)# vlan dot1q tag native	Modifies the behavior of a 802.1Q trunked native VLAN ID interface. The interface <i>maintains</i> the taggings for all packets that enter with a tag that matches the value of the native VLAN ID and <i>drops</i> all untagged traffic. The control traffic is still carried on the native VLAN. The default is disabled.
Step 3	exit Example: switch(config)# exit switch#	Exits the configuration mode.
Step 4	show vlan Example: switch# show vlan	(Optional) Displays the status and information for VLANs.
Step 5	copy running-config startup-config Example: switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

This 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):

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

Changing the System Default Port Mode to Layer 2

You can set the system default port mode to Layer 2 access ports.

SUMMARY STEPS

1. **config t**
2. **system default switchport [shutdown]**
3. **exit**
4. **show interface brief**
5. **copy running-config startup-config**

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: switch# config t switch(config)#	Enters configuration mode.
Step 2	system default switchport [shutdown] Example: switch(config-if)# switchport trunk allowed vlan add 15-20#	Sets the default port mode for all interfaces on the system to Layer 2 access port mode. By default, all the interfaces are Layer 3.
Step 3	exit Example: switch(config-if)# exit switch(config)#	Exits the interface mode.
Step 4	show interface brief Example: switch# show interface brief	(Optional) Displays the status and information for interfaces.
Step 5	copy running-config startup-config Example: switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

This example shows how to set the system ports to be Layer 2 access ports by default:

```
switch# config t
switch(config-if)# system default switchport
switch(config-if)#
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Verifying Interface Configuration

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

Command	Purpose
<code>show interface ethernet slot/port [brief counters debounce description flowcontrol mac-address status transceiver]</code>	Displays the interface configuration
<code>show interface brief</code>	Displays interface configuration information, including the mode.
<code>show interface switchport</code>	Displays information, including access and trunk interface, information for all Layer 2 interfaces.
<code>show interface trunk [module module-number vlan vlan-id]</code>	Displays trunk configuration information.
<code>show interface capabilities</code>	Displays information on the capabilities of the interfaces.
<code>show running-config interface ethernet slot/port</code>	Displays configuration information about the specified interface.

For detailed information about these commands, see the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.0*.

Displaying and Clearing Statistics

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

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.

Access and Trunk Port Mode Example Configurations

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
```

Send document comments to nexus7k-docfeedback@cisco.com

```
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)# switchport trunk allowed vlan 5, 10
switch(config-if)# exit
switch(config)# vlan dot1q tag native
switch(config)#
```

Default Settings

Table 3-1 lists the default settings for device access and trunk port mode parameters.

Table 3-1 *Default 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

Additional References

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

- [Related Documents, page 3-20](#)
- [Standards, page 3-20](#)
- [MIBs, page 3-20](#)

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Related Documents

Related Topic	Document Title
Configuring Layer 3 interfaces	Chapter 4, “Configuring Layer 3 Interfaces”
Port channels	Chapter 5, “Configuring Port Channels”
VLANs, private VLANs, and STP	<i>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.0</i>
Command reference	<i>Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 4.0</i>
Interfaces	<i>Cisco DCNM Interfaces Configuration Guide</i>
System management	<i>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.0</i>
High availability	<i>Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 4.0</i>
VDCs	<i>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.0</i>
Licensing	<i>Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0</i>
Release Notes	<i>Cisco Nexus 7000 Series NX-OS Release Notes, Release 4.0</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.	—

MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"> • BRIDGE-MIB • IF-MIB • CISCO-IF-EXTENSION-MIB • ETHERLIKE-MIB 	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml