



CHAPTER 3

Configuring Layer 2 Interfaces

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



Note

A Layer 2 port can function as either a trunk port, an access port, or a private VLAN port. See the *Cisco DCNM Layer 2 Switching Configuration Guide* 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](#)
- [Displaying and Clearing Statistics, page 3-11](#)
- [Additional References, page 3-11](#)



Note

See the *Cisco NX-OS System Management Configuration Guide* for information on configuring a SPAN destination interface.

For more information about the Data Center Network Manager features, see the *Cisco Data Center Network Manager Fundamentals Guide*.

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 DCNM Layer 2 Switching Configuration Guide* for information on VLANs, 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 DCNM Layer 2 Switching Configuration Guide* 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 NX-OS High Availability and Redundancy Configuration Guide* 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.

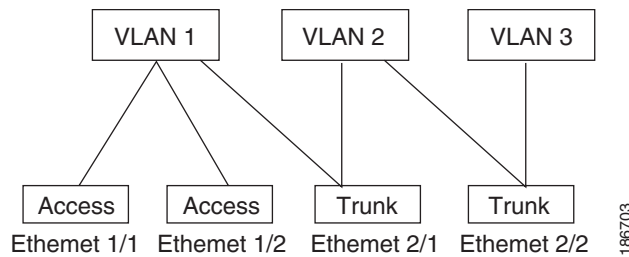
You change the default port setting to Layer 2 using the command-line interface (CLI). See the *Cisco NX-OS Interfaces Command Reference* for information on changing the default port setting to Layer 2 for the system.

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

[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 DCNM Layer 2 Switching Configuration Guide* 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 DCNM Unicast Routing Configuration Guide* 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

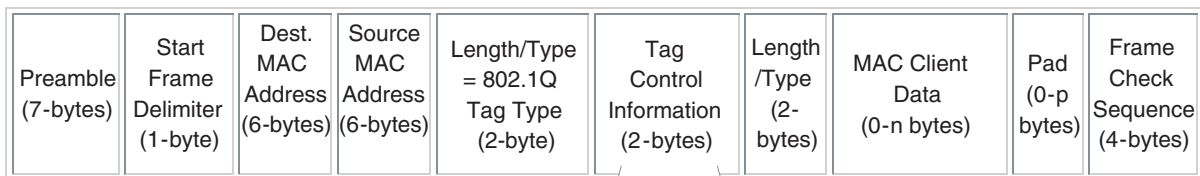
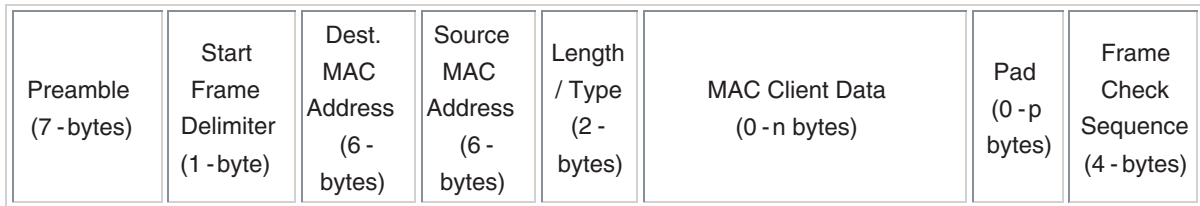
For information about VLANs, see the *Cisco DCNM Layer 2 Switching Configuration Guide*.

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 DCNM Layer 2 Switching Configuration Guide* 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 DCNM Layer 2 Switching Configuration Guide* 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 NX-OS High Availability and Redundancy Configuration Guide* 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 device, and trunk ports cannot carry VLANs from different devices.



Note

See the *Cisco DCNM Virtual Device Context Configuration Guide* 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
DCNM	Layer 2 port modes require no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For a complete explanation of the DCNM licensing scheme, see the <i>Cisco DCNM Licensing Guide</i> .
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 NX-OS Licensing Guide</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.

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:

- [Configuring a LAN Interface as a Layer 2 Access Port, page 3-8](#)
- [Configuring a Trunk Port, page 3-9](#)
- [Configuring the Device to Tag Native VLAN Traffic, page 3-10](#)

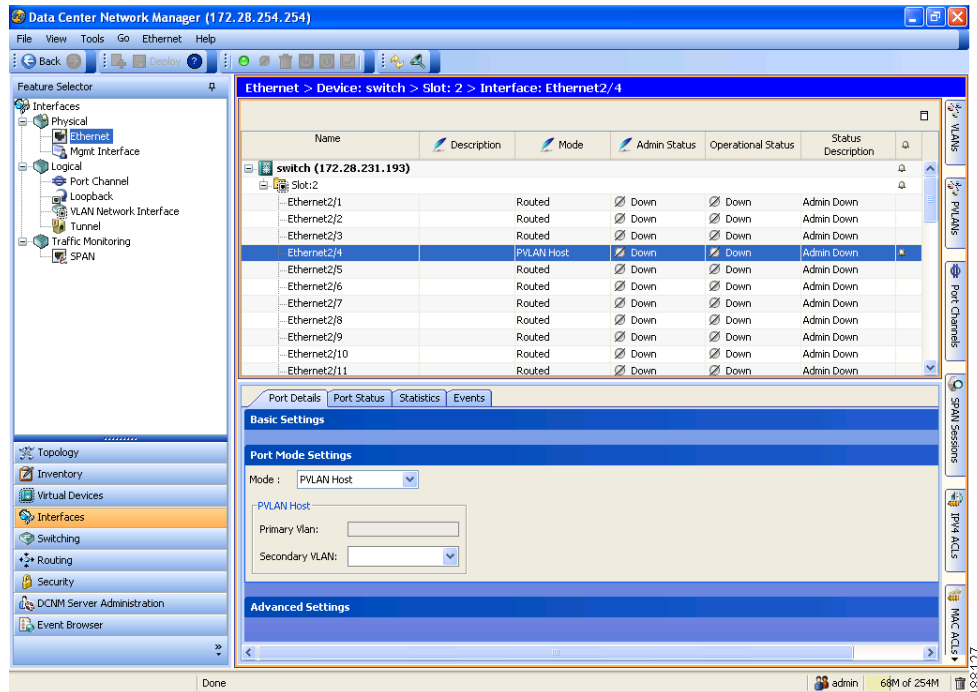
Send document comments to nexus7k-docfeedback@cisco.com

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.

You use the Ethernet pane to configure a Layer 2 access port (see [Figure 3-3](#)).

Figure 3-3 Ethernet Pane, Port Mode Settings



DETAILED STEPS

To configure a Layer 2 access port, follow these steps:

- Step 1** From the Feature Selector pane, choose **Interfaces > Physical > Ethernet** to open the Ethernet pane.
- Step 2** From the Contents pane, in the Summary pane, double-click the device to display the interfaces.
- Step 3** Click the slot to display the list of interfaces.
- Step 4** Click the interface.
The system highlights the interface in the Summary pane, and tabs appear in the Details pane.
- Step 5** In the Details pane, click the **Port Details** tab.
- Step 6** Click the **Port Mode Settings** section.
- Step 7** From the Mode drop-down list, choose **Access** to configure the port as an access port.
Routed is the default port mode.
- Step 8** In the Access VLAN field, specify the access VLAN by using a known VLAN, assigning a VLAN from among the VLANs on this device, or creating a new VLAN.

Send document comments to nexus7k-docfeedback@cisco.com

The default access VLAN is VLAN1. The range is VLAN 1 to 4094, excluding the internally assigned VLANs 3968 to 4047 and 4094.

Step 9 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Configuring a Trunk Port

**Note**

You can pre-provision a trunk port while the actual port is still in access mode. From the main menu, choose **Tools > Global Preferences > Pre Provisioning** to access or hide the screen that allows and displays this functionality. See the *Cisco DCNM Fundamentals Configuration Guide* for information on pre-provisioning.

You can configure a Layer 2 port as a trunk port, which transmits untagged packets for one VLAN plus transmits encapsulated, tagged, packets for multiple VLANs.

**Note**

The device supports 802.1Q encapsulation only.

You use the Ethernet pane to configure a Layer 2 trunk port (see [Figure 3-3](#)).

DETAILED STEPS

To configure a Layer 2 trunk port, follow these steps:

Step 1 From the Feature Selector pane, choose **Interfaces > Physical > Ethernet** to open the Ethernet pane.

Step 2 From the Contents pane, in the Summary pane, double-click the device to display the interfaces.

Step 3 Click the slot to display the list of interfaces.

Step 4 Click the interface.

The system highlights the interface in the Summary pane, and tabs appear in the Details pane.

Step 5 In the Details pane, click the **Port Details** tab.

Step 6 Click the **Port Mode Settings** section.

Step 7 From the Mode drop-down list, choose **Trunk** to configure the port as a trunk port.

**Note**

Do not change the dimmed value in the Encapsulation row from dot1q. The IEEE 802.1Q encapsulation method is the only supported encapsulation method.

Step 8 In the Allowed VLAN field, enter the numbers of the VLANs or select the VLANs that are allowed to run on this trunk port.

VLANs 1 to 4094 are the default. VLANs 3968 to 4047 and 4094 are internally allocated for device use.

Step 9 In the Native VLAN field, specify, choose, or create the native VLAN for this trunk port.

The default native VLAN is VLAN1. The range is from VLAN 1 to 4094, excluding the internally assigned VLANs 3968 to 4047 and 4094.

Send document comments to nexus7k-docfeedback@cisco.com

Step 10 From the menu bar, choose **File > Deploy** to apply your changes to the device.

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.

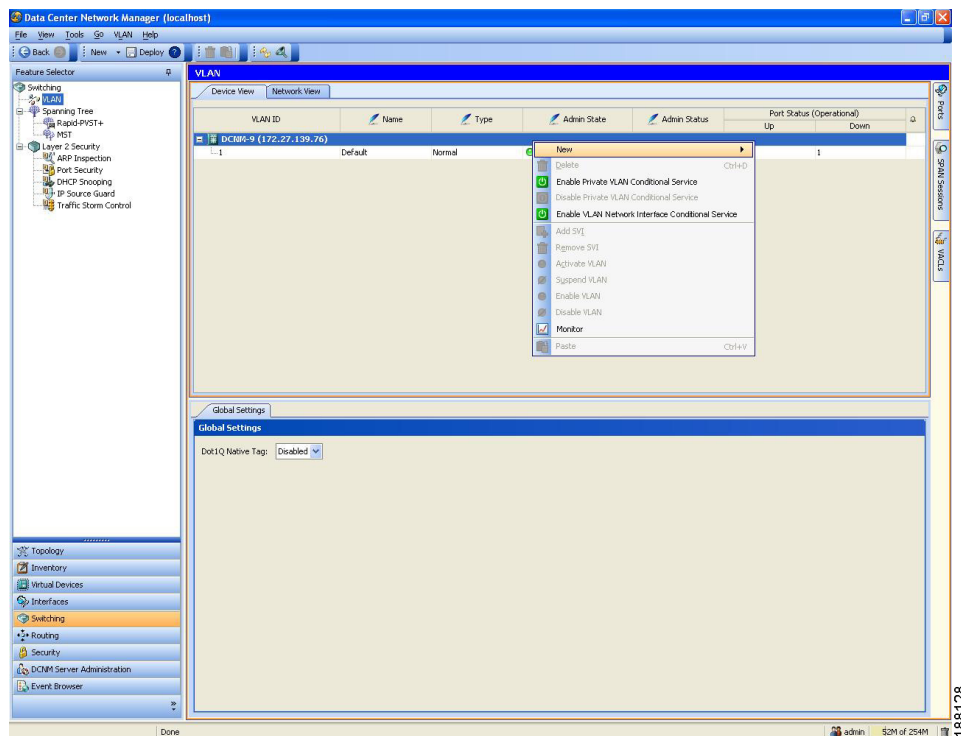


Note

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.

You use the VLAN pane to configure the device to maintain the tagging for all native VLANs for all trunking ports (see [Figure 3-4](#)).

Figure 3-4 VLAN Pane, Global Settings



DETAILED STEPS

To configure the device to maintain tagging on the native VLAN for trunk ports, follow these steps:

- Step 1** From the Feature Selector pane, choose **Switching > VLAN** to open the VLAN pane.
- Step 2** In the Summary pane, click the **Device View** tab.
- Step 3** Click the device that you want to configure.

Send document comments to nexus7k-docfeedback@cisco.com

The system highlights the device in the Summary pane, and tabs appear in the Details pane.

- Step 4** In the Details pane, click the **Global Settings** tab.
- Step 5** From the Dot1Q Native Tag drop-down list, choose **Enabled** to configure the device to maintain the 802.1q tag on the native VLAN for all trunking ports.
The default is disabled.
- Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Displaying and Clearing Statistics

The following window appears in the Statistics tab:

- Port Traffic Statistics—Displays information on ports, including unicast, multicast, discards, and so forth.
- Trunk Statistics—Displays information on the trunk when you select a trunk port, including unicast, multicast, and so forth.
- Port Error Counters—Displays errors on the access or trunk interface, including alignments, collisions, runts, giants, and so forth.

Field Descriptions

The field descriptions for the fields discussed in this chapter are in [Chapter 2, “Configuring Basic Interface Parameters.”](#)

Additional References

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

- [Related Documents, page 3-12](#)
- [Standards, page 3-12](#)
- [MIBs, page 3-12](#)

Send document comments to 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, STP	<i>Cisco DCNM Layer 2 Switching Configuration Guide</i>
Interfaces	<i>Cisco NX-OS Interfaces Configuration Guide</i>
System management	<i>Cisco NX-OS System Management Configuration Guide</i>
High availability	<i>Cisco NX-OS High Availability and Redundancy Guide</i>
VDCs	<i>Cisco DCNM Virtual Device Context Configuration Guide</i>
Licensing	<i>Cisco DCNM Licensing Guide</i>
Release Notes	<i>Cisco DCNM 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 	<p>To locate and download MIBs, go to the following URL:</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>