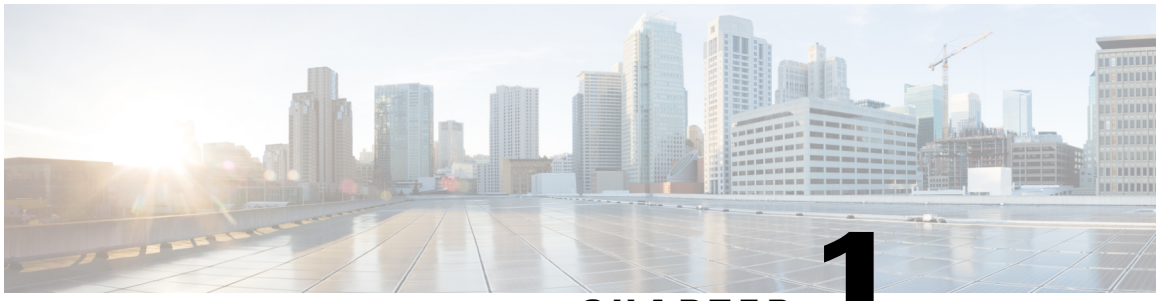
Cisco Nexus 1000V for KVM Interface Configuration Guide, Release 5.x

First Published: August 01, 2014

Last Modified: November 09, 2015

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Overview

This chapter contains the following sections:

Information About Interfaces

Ethernet Interfaces

All interfaces on the Cisco Nexus 1000V are Layer 2 Ethernet interfaces, which include access ports, trunk ports, private VLAN ports, and promiscuous ports.

Access Ports

An access port carries traffic for one VLAN. This type of port is a Layer 2 interface only.

Trunk Ports

A trunk port carries traffic for two or more VLANs. This port type is a Layer 2 interface only.

Virtual Ethernet Interfaces

Virtual Ethernet (vEthernet or vEth) interfaces are logical interfaces. Each vEthernet interface corresponds to a switch interface that is connected to a virtual port. The interface types are as follows:

- VM (interfaces connected to VM NICs)
- Linux Tap interface

vEthernet interfaces are created on the Cisco Nexus 1000V to represent virtual ports in use on the distributed virtual switch.

Management Interface

You can use the management interface to connect the device to a network for remote management using a Telnet client, the Simple Network Management Protocol (SNMP), or other management agents.

Port Channel Interfaces

A port channel is a logical interface that aggregates multiple physical interfaces. You can bundle up to eight individual links to physical ports into a port channel to improve bandwidth and redundancy. You can also use port channeling to load balance traffic across these channeled physical interfaces. For information about how to create port channels, see the *Cisco Nexus 1000V for KVM Port Profile Configuration Guide* .

VEM Management of LACP

The Cisco Nexus 1000V switch offloads operation of the Line Aggregation Control Protocol (LACP) from the VSM to the VEMs to prevent a situation where LACP cannot be negotiated with the upstream switch when the VEM is disconnected from the VSM (referred to as headless mode).

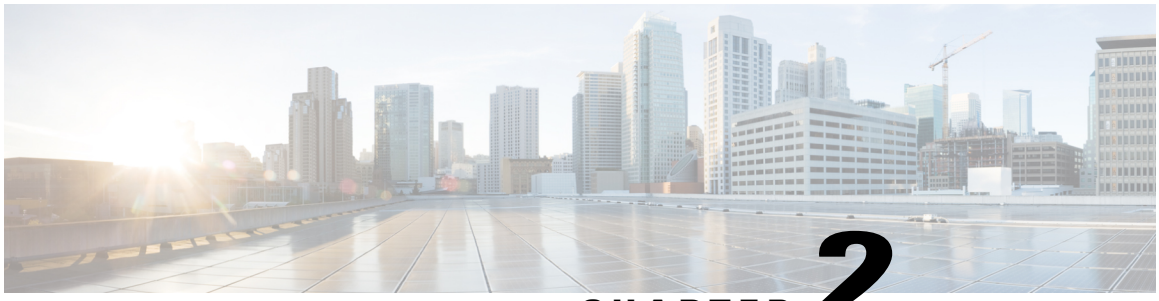
Simplifying the Interface Configuration with Port Profiles

You can use a port profile to simplify the interface configuration. You can configure a port profile and then assign it to multiple interfaces to give them all the same configuration. Changes to the port profile are propagated to the configuration of any interface that is assigned to it.

Note We do not recommend that you override port profile configurations by making changes to the assigned interface configurations. You should make configuration changes to interfaces only to quickly test a change or to disable a port.

High Availability for Interfaces

Interfaces support stateful and stateless restarts. A stateful restart occurs during a supervisor switchover. After the switchover, the Cisco Nexus 1000V applies the run-time configuration.



CHAPTER 2

Configuring Interface Parameters

This chapter contains the following sections:

Information About the Basic Interface Parameters

Description

For the vEthernet, and management interfaces, you can configure the description parameter to provide a name for the interface. Using a unique name for each interface allows you to quickly identify the interface when you are looking at a listing of multiple interfaces.

By default, the description for vEthernet interfaces is automatically formatted to contain information about the connected device. The description for a virtual Network Interface Card (vNIC), for example, contains the VM name and network adapter number. You keep this default description or you can override it with a description of your choosing.

Administrative Status

The administrative-status parameter determines whether an interface is up or down. When an interface is administratively down, it is disabled and unable to transmit data. When an interface is administratively up, it is enabled and able to transmit data.

Guidelines and Limitations

Interface parameters have the following guidelines and limitations:

- To specify an interface in the CLI, use the following guideline:
  - For a vEthernet port, use **vethernet** *number*, where *number* is a number from 1 to 256.

Specifying an Interface to Configure

You can use this procedure to specify an interface to configure.

Before You Begin

You are logged in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *interface*	Enters interface configuration mode for the specified interface.
Step 3	switch(config-if)# **show interface** *interface*	(Optional) Displays the current configuration of interfaces. The interface argument is defined as follows: • For the management interface, use **mgmt 0** or **mgmt0**. • For a vEthernet port, use **vethernet** *number*, where *number* is a number from 1 to 1048575.

```
switch# configure terminal
switch(config)# interface vethernet 5
switch(config-if)# show interface vethernet 5
switch(config-if)#
```

Configuring a Description

You can use this procedure to add a description to an interface.

Before You Begin

- You are logged in to the CLI in EXEC mode.
- A description is case-sensitive and can be up to 80 alphanumeric characters in length.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *interface*	Enters interface configuration mode for the specified interface.
Step 3	switch(config-if)# **description** *string*	Adds a description of up to 80 alphanumeric characters for the interface and saves it in the running configuration.
Step 4	switch(config-if)# **show interface** *interface*	(Optional) Displays the interface status, which includes the description.
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 interface description:

```
switch# configure terminal
switch(config)# interface vethernet 5
switch(config-if)# description vEthernet on module 5
switch(config-if)#
```

Shutting Down and Activating an Interface

You can use this procedure to shut down and restart interfaces.

Before You Begin

- You are logged in to the CLI in EXEC mode.
- When you shut down an interface, it becomes disabled and the output of monitoring commands show it as being down.
- To activate an interface that has been shut down, you must restart the device.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *interface*	Specifies an interface to configure, and enters interface configuration mode.

	Command or Action	Purpose
Step 3	switch(config-if)# **shutdown**	Disables the interface in the running configuration .
Step 4	switch(config-if)# **show interface** *interface*	(Optional) Displays the interface status, which includes the administrative status.
Step 5	switch(config-if)# **no shutdown**	Reenables the interface in the running configuration .
Step 6	switch(config-if)# **show interface** *interface*	(Optional) Displays the interface status, which includes the administrative status. • For the management interface, use **mgmt 0** or **mgmt0**.
Step 7	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 shut down vethernet interafce:

```
switch# configure terminal
switch(config)# interface vethernet 5
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

Clearing the Interface Counters

You can use this procedure to clear the interface counters.

Before You Begin

Log in to the CLI in EXEC mode, configuration mode, or interface configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **clear counters interface** *interface*	• **vethernet** *number***—**Virtual ethernet interface. The range is from 1 to 1048575. • **vethernet** *number***—**Virtual ethernet interface. The range is from 1 to 1048575. • **vethernet** *number***—**Virtual ethernet interface. The range is from 1 to 1048575. • **mgmt 0—**Management interface.

	Command or Action	Purpose
		• **vethernet** *number*—Virtual ethernet interface. The range is from 1 to 1048575. • **vethernet** *number*—Virtual ethernet interface. The range is from 1 to 1048575. Clears the counters for the specified interface:
Step 2	switch# **show interface** *interface*	(Optional) Displays the interface status, which includes the counters, for the specified interface: • **control 0**—Control interface. • **ethernet** *number*—Ethernet IEEE 802.3z. The range is from 1 to 514. • **mgmt 0**—Management interface. • **port-channel** *number*—Port Channel interface. The range is from 1 to 4096. • **vethernet** *number*—Virtual ethernet interface. The range is from 1 to 1048575.

The following example shows how to clear and reset the counters on vethernet 5:

```
switch# clear counters interface vethernet 5
switch#
```

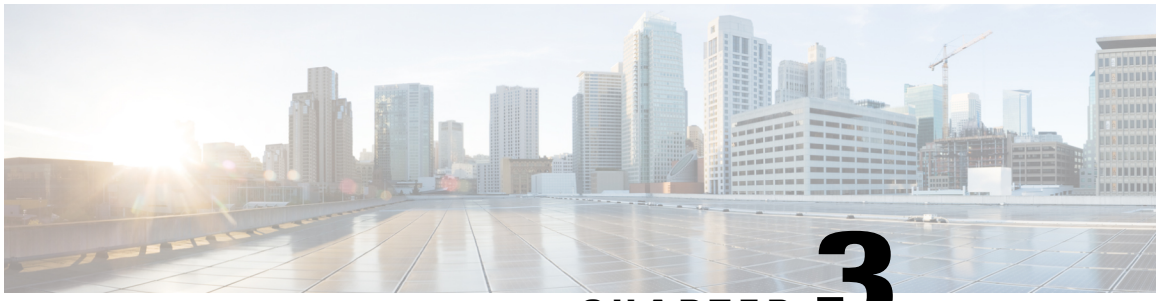
Verifying the Basic Interface Parameters

Use one of the following commands to verify the configuration:

Command	Purpose
show interface *interface*	Displays the configured states of one or all interfaces.
show interface brief	Displays a table of interface states.
show interface switchport	Displays the status of Layer 2 ports.

Feature History for Basic Interface Parameters

Feature Name	Releases	Feature Information
Basic interface parameters	Release 5.2(1)IC1(1.1)	This feature was introduced.



CHAPTER 3

Configuring Layer 2 Interfaces

This chapter contains the following sections:

Information About Configuring Switchport Mode Using Port Profiles

You can create port profiles that configure Layer 2 interfaces as access ports or trunk ports.

Access and Trunk Interfaces

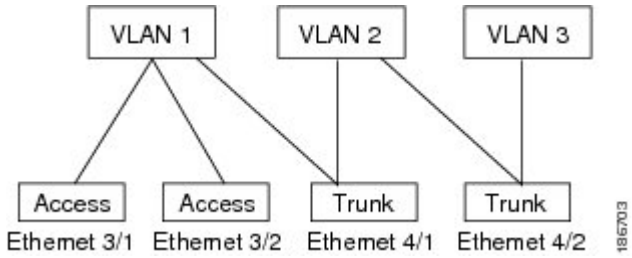
A Layer 2 port can be configured as an access or a trunk port as follows:

- 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. 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

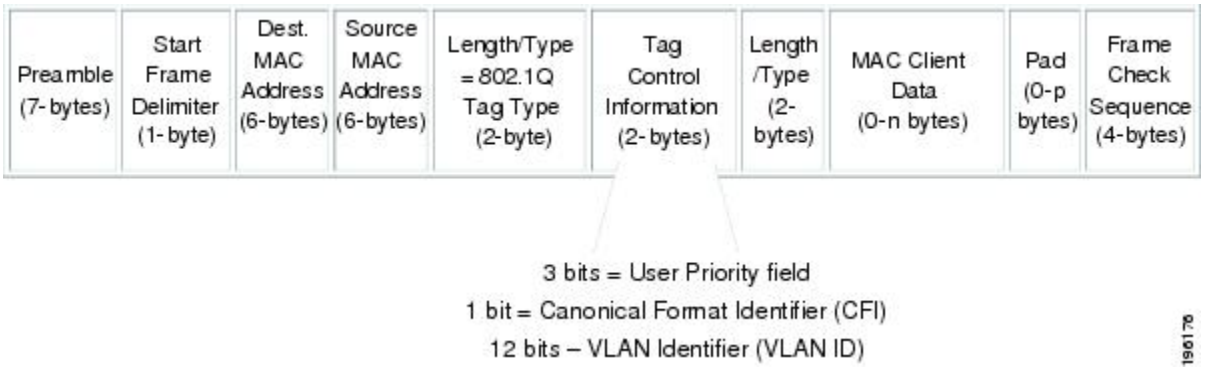
A trunk is a point-to-point link between the switch and another networking device. Trunks carry the traffic of multiple VLANs over a single link and allow you to extend VLANs across an entire network.

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

Figure 3: Header With 802.1Q Tag



High Availability

The software supports high availability for Layer 2 ports.

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.
- 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	VLAN 1
Native VLAN ID	VLAN 1
Native VLAN ID tagging	Disabled
Administrative state	Shutdown

Configuring a Port-Profile That Will Be Used to Configure an Interface as an Access Interface

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

Before You Begin

- The interface must be 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. The interface argument are defined as follows:

	Command or Action	Purpose
		• Use the **vethernet** *interface-number* command, 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 for 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.

This 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 vethernet 5
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 5
switch(config-if)#
```

Configuring Trunk Ports

You can 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.
- 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 IEEE 802.1Q Encapsulation, on page 10 for more information.
- 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 interface configuration mode. The interface argument is defined as follows: • For an Ethernet port, use the **ethernet** *slot/port* command, where *slot* is the module slot number and *port* is the port number. • For a vEthernet port, use the **vethernet** *interface-number* command, where *interface-number* is a number from 1 to 1048575.
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.

This 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 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. The interface argument is defined as follows: • For an Ethernet port, use the **ethernet** *slot/port* command, where *slot* is the module slot number and *port* is the port number. • For a vEthernet port, use the **vethernet** *interface-number* command, 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.

This 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. The interface argument is defined as follows: • For an Ethernet port, use the **ethernet** *slot/port* command, where *slot* is the module slot number and *port* is the port number. • For a vEthernet port, use the **vethernet** *interface-number* command, 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.

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:

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

Tagging 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.

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):

```
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.

Command	Purpose
show interface ethernet *slot/port* **counters** [**brief** | **detailed** | **errors** | **snmp** | **storm-control** | **trunk**]	Displays the counters for a specified Ethernet interface.
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 about the access and trunk interface for all Layer 2 interfaces.
show interface trunk [**module** *module-number* | **vlan** *vlan-id*]	Displays trunk configuration information.
show interface capabilities	Displays information about the capabilities of the interfaces.
show running-config interface ethernet *slot/port*	Displays configuration information about the specified interface.

Monitoring the Interface Counters

Use one of the following commands to monitor the interface counters:

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

This 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 3/30
switch(config-if)# switchport
switch(config-if)# switchport mode access
```

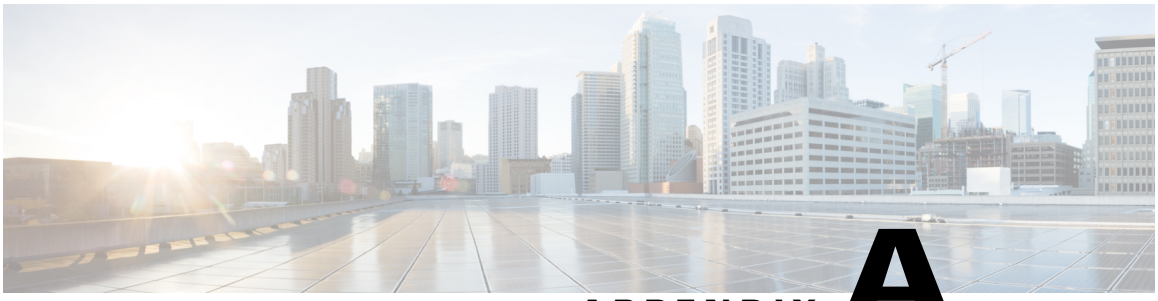
```
switch(config-if)# switchport access vlan 5
switch(config-if)#
```

This 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 3/32
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-if)# vlan dot1q tag native
switch(config-if)#
```

Feature History for Layer 2 Interface Parameters

Feature Name	Releases	Feature Information
Layer 2 interface parameters	Release 5.2(1)SK1(2.1)	This feature was introduced



APPENDIX A

Supported RFCs

This chapter contains the following sections:

Supported RFCs

The following tables lists the supported IETF RFCs for interfaces.

Table 2: IP Services RFCs

RFCs	Title
RFC 786	UDP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 1027	Proxy ARP
RFC 1591	DNS Client
RFC 1812	IPv4 routers

Supported RFCs