



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



Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(2)

October 21, 2011

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

Text Part Number: OL-20452-03

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(2)
© 2009 Cisco Systems, Inc. All rights reserved.



New and Changed Information

This chapter lists the content in this document that is either new or has been changed in Release 4.0(4)SV1(2), and where it is located.

Feature	Description	Changed in Release	Where Documented
Configuration limits	Configuration limits for vEthernet interfaces, vEthernet trunks, and port profiles were added.	4.0(4)SV1(2)	Chapter 7, “Interface Configuration Limits”
show interface vethernet command	<p>The show interface vethernet command now displays 5 minute input and output packet/bit rate statistics for the interfaces that you specify. The configuration example showing this command output was updated to reflect this change.</p> <p>Note The show interface ethernet command output also provides these new statistics.</p>	4.0(4)SV1(2)	Chapter 4, “Configuring Virtual Ethernet Interfaces”
vPC-Host Mode	Support for manual creation of subgroups.	4.0(4)SV1(2)	Chapter 5, “Configuring Port Channels”
Static Pinning	Support for attaching (or pinning) a vEthernet interface to a specific port channel subgroup.	4.0(4)SV1(2)	Chapter 5, “Configuring Port Channels”

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



C O N T E N T S

New and Changed Information iii

Preface ix

Audience ix

Document Organization ix

Document Conventions x

Recommended Reading xi

Related Documentation xi

Obtaining Documentation and Submitting a Service Request xii

Overview 1-1

Information About Interfaces 1-1

 Ethernet Interfaces 1-1

 Access Ports 1-1

 Trunk Ports 1-2

 Private VLAN Ports 1-2

 Promiscuous Ports 1-2

 Virtual Ethernet Interfaces 1-2

 Management Interface 1-2

 Port Channel Interfaces 1-2

Simplifying Interface Configuration with Port Profiles 1-3

High Availability for Interfaces 1-3

Configuring Interface Parameters 2-1

Information About the Basic Interface Parameters 2-1

 Description Parameter 2-2

 Speed and Duplex Modes 2-2

 Port MTU Size 2-3

 Administrative Status 2-3

 Cisco Discovery Protocol 2-3

 Port Channel Parameter 2-3

Guidelines and Limitations 2-4

Configuring the Basic Interface Parameters 2-4

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

Specifying an Interface to Configure	2-5
Configuring a Description	2-6
Dedicating Bandwidth to One Port	2-8
Configuring the Interface Speed and Duplex Modes	2-9
Configuring the System Jumbo MTU Size	2-12
Configuring the MTU Size	2-13
Configuring the Interface MTU Size	2-13
Configuring Bandwidth	2-14
Configuring the Throughput Delay	2-16
Shutting Down and Activating an Interface	2-17
Enabling or Disabling CDP	2-19
Clearing the Interface Counters	2-20
Verifying the Basic Interface Parameters	2-21
Feature History for Basic Interface Parameters	2-21
Configuring Layer 2 Interfaces	3-1
Information About Access and Trunk Interfaces	3-1
Access and Trunk Interfaces	3-1
IEEE 802.1Q Encapsulation	3-2
High Availability	3-3
Guidelines and Limitations	3-3
Default Settings	3-4
Configuring Access and Trunk Interfaces	3-4
Configuring a LAN Interface as a Layer 2 Access Port	3-4
Configuring Access Host Ports	3-6
Configuring Trunk Ports	3-7
Configuring the Native VLAN for 802.1Q Trunking Ports	3-9
Configuring the Allowed VLANs for Trunking Ports	3-11
Configuring the Device to Tag Native VLAN Traffic	3-12
Verifying the Interface Configuration	3-14
Monitoring the Interface Configuration	3-14
Configuration Examples for Access and Trunk Port Mode	3-14
Additional References	3-15
Related Documents	3-15
Standards	3-15
Feature History for Layer 2 Interface Parameters	3-15

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

Configuring Virtual Ethernet Interfaces	4-1
Information About vEthernet Interfaces	4-1
Guidelines and Limitations	4-1
Default Settings	4-2
Configuring vEthernet Interfaces	4-2
Configuring a vEthernet Access Interface	4-2
Configuring a Private VLAN on a vEthernet Interface	4-4
Enabling or Disabling a vEthernet Interface	4-6
Verifying the vEthernet Interface Configuration	4-7
Configuration Examples for vEthernet Interfaces	4-9
Additional References	4-10
Related Documents	4-10
Standards	4-10
Feature History for vEthernet Interface Parameters	4-10
Configuring Port Channels	5-1
Information About Port Channels	5-1
Port Channels	5-2
Compatibility Checks	5-2
Load Balancing Using Port Channels	5-4
LACP	5-5
Port Channel Modes	5-6
LACP ID Parameters	5-6
LACP Marker Responders	5-7
LACP-Enabled and Static Port Channels Differences	5-7
vPC Host Mode	5-8
Subgroup Creation Using CDP or Manual Method	5-9
Interface Assignment Using Static Pinning	5-9
High Availability	5-9
Prerequisites for Port Channels	5-9
Guidelines and Limitations	5-10
Default Settings	5-10
Configuring Port Channels	5-11
Configuring a Port Channel that Connects to a Single Upstream Switch	5-11
Configuring a Port Channel that Connects to Multiple Upstream Switches	5-12
Configuring Static Pinning	5-15
Removing the Port Channel and Group	5-17

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

Adding a Layer 2 Port to a Channel Group	5-17
Removing a Port from a Channel Group	5-19
Shutting Down and Restarting a Port Channel Interface	5-20
Configuring a Port Channel Description	5-21
Configuring LACP Port Channel Port Modes	5-22
Configuring the Speed and Duplex Settings for a Port Channel Interface	5-23
Configuring Port Channel Load Balancing	5-25
Restoring the Default Load-Balancing Method	5-26
Verifying the Port Channel Configuration	5-27
Monitoring the Port Channel Configuration	5-28
Configuration Example for Port Channels	5-28
Additional References	5-28
Related Documents	5-29
Standards	5-29
Feature History for Port Channels	5-29
Supported RFCs	6-1
IP Services RFCs	6-1
Interface Configuration Limits	7-1

INDEX



Preface

This document, *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(2)*, provides information for configuring Cisco Nexus 1000V interfaces.

This preface includes the following topics:

- [Audience, page ix](#)
- [Document Organization, page ix](#)
- [Document Conventions, page x](#)
- [Recommended Reading, page xi](#)
- [Related Documentation, page xi](#)
- [Obtaining Documentation and Submitting a Service Request, page xii](#)

Audience

This guide is for network administrators with the following experience and knowledge:

- An understanding of virtualization
- Using VMware tools to configure a vswitch



Note

Note: Knowledge of VMware vNetwork Distributed Switch is not a prerequisite.

Document Organization

This publication is organized as follows:

Chapter and Title	Description
Chapter 1, “Overview”	Provides an overview of Cisco Nexus 1000V interfaces.
Chapter 2, “Configuring Interface Parameters”	Describes the basic Cisco Nexus 1000V interface configuration.
Chapter 3, “Configuring Layer 2 Interfaces”	Describes how to configure Cisco Nexus 1000V access and trunk interfaces.

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

Chapter and Title	Description
Chapter 4, “Configuring Virtual Ethernet Interfaces”	Describes how to configure Cisco Nexus 1000V virtual Ethernet interfaces.
Chapter 5, “Configuring Port Channels”	Describes how to configure Cisco Nexus 1000V port channels.
Chapter 6, “Supported RFCs”	Lists the IETF RFCs supported in Cisco Nexus 1000V Beta 1 release.
Chapter 7, “Interface Configuration Limits”	Lists the maximum configuration limits for interface features.

Document Conventions

Command descriptions use these conventions:

boldface font	Commands and keywords are in boldface.
<i>italic font</i>	Arguments for which you supply values are in italics.
{ }	Elements in braces are required choices.
[]	Elements in square brackets are optional.
x y z	Alternative, mutually exclusive elements are separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use these conventions:

<code>screen font</code>	Terminal sessions and information the device displays are in screen font.
<code>boldface screen font</code>	Information you must enter is in boldface screen font.
<i><code>italic screen font</code></i>	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions for notes and cautions:



Note

Means reader *take note*. Notes contain helpful suggestions or references to material not covered in the manual.



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

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

Recommended Reading

Before configuring the Cisco Nexus 1000V, we recommend that you read and become familiar with the following documentation:

- *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(2)*
- *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)*
- *Cisco VN-Link: Virtualization-Aware Networking white paper*

Related Documentation

Cisco Nexus 1000V includes the following documents available on Cisco.com:

General Information

Cisco Nexus 1000V Release Notes, Release 4.0(4)SV1(2)

Cisco Nexus 1000V Compatibility Information, Release 4.0(4)SV1(2)

Install and Upgrade

Cisco Nexus 1000V Software Installation Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V Virtual Ethernet Module Software Installation Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V Software Upgrade Guide, Release 4.0(4)SV1(2)

Configuration Guides

Cisco Nexus 1000V License Configuration Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V XML API User Guide, Release 4.0(4)SV1(2)

Programming Guide

Cisco Nexus 1000V XML API User Guide, Release 4.0(4)SV1(2)

Reference Guides

Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(2)

Cisco Nexus 1000V MIB Quick Reference

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

Troubleshooting and Alerts

Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(2)

Cisco Nexus 1000V Password Recovery Guide

Cisco NX-OS System Messages Reference

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

Overview

This chapter provides an overview of the interface types supported in Cisco Nexus 1000V.

This chapter includes the following sections:

- [Information About Interfaces, page 1-1](#)
- [Simplifying Interface Configuration with Port Profiles, page 1-3](#)
- [High Availability for Interfaces, page 1-3](#)

Information About Interfaces

This section includes the following topics:

- [Ethernet Interfaces, page 1-1](#)
- [Virtual Ethernet Interfaces, page 1-2](#)
- [Management Interface, page 1-2](#)
- [Port Channel Interfaces, page 1-2](#)

Ethernet Interfaces

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

This section includes the following topics:

- [Access Ports, page 1-1](#)
- [Trunk Ports, page 1-2](#)
- [Private VLAN Ports, page 1-2](#)
- [Promiscuous Ports, page 1-2](#)

Access Ports

An access port carries traffic for one VLAN. This type of port is a Layer 2 interface only. For more information about access-port interfaces, see [Chapter 3, “Configuring Layer 2 Interfaces.”](#)

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

Trunk Ports

A trunk port carries traffic for two or more VLANs. This type of port is a Layer 2 interface only. For more information about trunk-port interfaces, see [Chapter 3, “Configuring Layer 2 Interfaces.”](#)

Private VLAN Ports

Private VLANs (PVLANS) are used to segregate Layer 2 ISP traffic and convey it to a single router interface. PVLANS achieve device isolation by applying Layer 2 forwarding constraints that allow end devices to share the same IP subnet while being Layer 2 isolated. In turn, the use of larger subnets reduces address management overhead. Three separate port designations are used. Each has its own unique set of rules that regulate the ability of each connected endpoint to communicate with other connected endpoints within the same private VLAN domain.

For more information about PVLANS, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(2)*.

Promiscuous Ports

A promiscuous port can talk to all other types of ports. A promiscuous port can talk to isolated ports as well as community ports, and those ports can also talk to promiscuous ports.

For more information about promiscuous ports, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(2)*

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)
- Service console
- vmkernel

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 Ethernet 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. For more information on the management interface, see the *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(2)*.

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 more information about port channel interfaces, see [Chapter 5, “Configuring Port Channels.”](#)

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

Simplifying Interface Configuration with Port Profiles

In Cisco Nexus 1000V, a port profile is a mechanism for simplifying the configuration of interfaces. 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. Only make configuration changes to interfaces to quickly test a change or to disabled a port.

For more information about port profiles, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)*.

High Availability for Interfaces

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

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



CHAPTER 2

Configuring Interface Parameters

This chapter describes how to configure the basic interface parameters or the parameters that are shared by multiple interfaces.

This chapter includes the following sections:

- [Information About the Basic Interface Parameters, page 2-1](#)
- [Guidelines and Limitations, page 2-4](#)
- [Configuring the Basic Interface Parameters, page 2-4](#)
- [Verifying the Basic Interface Parameters, page 2-21](#)
- [Feature History for Basic Interface Parameters, page 2-21](#)



Note

To configure Layer 2 access or trunking interfaces, see [Chapter 2, “Configuring Interface Parameters.”](#)

Information About the Basic Interface Parameters

This section includes the following topics:

- [Description Parameter, page 2-2](#)
- [Speed and Duplex Modes, page 2-2](#)
- [Port MTU Size, page 2-3](#)
- [Administrative Status, page 2-3](#)
- [Cisco Discovery Protocol, page 2-3](#)
- [Port Channel Parameter, page 2-3](#)

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

Description Parameter

For the vEthernet, Ethernet, and management interfaces, you can configure the description parameter to provide a recognizable 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.

For information about setting the description parameter for port channel interfaces, see the [“Configuring a Port Channel Description”](#) section on page 5-21.

For information about configuring this parameter for other interfaces, see the [“Configuring a Description”](#) section on page 2-6.

Speed and Duplex Modes

The speed and duplex modes are interrelated for each Ethernet and management interface. By default, each of these interfaces autonegotiates its speed and duplex modes with the other interface, but you can change these settings. If you change the settings, be sure to use the same speed and duplex mode settings on both interfaces, or use autonegotiation for at least one of the interfaces. [Table 2-1](#) shows the settings that work for each type of Ethernet and management interface.

Table 2-1 Speed and Duplex Mode Settings Used for Ethernet and Management Interfaces

Module Type	Speed Mode Setting	Duplex Mode Setting	Operational Speed (Mbps)	Operational Duplex Mode
32-port 10 GE Ethernet	Auto ¹	Auto ¹	10,000	Full
48-port 10/100/1000 Ethernet	Auto ¹	Auto ¹	1000	Full
			10 or 100	Half
	1000	Auto ¹ or full	1000	Full
	100	Auto ¹ or half	100	Half
		Full	100	Full
	10	Auto ¹ or half	10	Half
		Full	10	Full
Management	Auto ¹	Auto ¹	1000	Full
			10 or 100	Half
	1000	Auto ¹ or full	1000	Full
	100	Auto ¹ or half	100	Half
		Full	100	Full
	10	Auto ¹ or half	10	Half
		Full	10	Full

1. Default setting

For information about setting the speed and duplex modes for port channel interfaces, see the [“Configuring the Speed and Duplex Settings for a Port Channel Interface”](#) section on page 5-23.

For information about setting the speed and duplex modes for other interfaces, see the [“Configuring the Interface Speed and Duplex Modes”](#) section on page 2-9.

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

Port MTU Size

The maximum transmission unit (MTU) size specifies the maximum frame size that an Ethernet port can process. For transmissions to occur between two ports, you must configure the same MTU size for both ports. A port drops any frames that exceed its MTU size.

By default, The MTU size for each port is 1500 bytes, which is the IEEE 802.3 standard for Ethernet frames. Larger MTU sizes are possible for more efficient processing of data with less overhead. The larger frames, called jumbo frames, can be up to 9000 bytes in size, which is also the default system jumbo MTU size.

For a Layer 2 port, you can configure an MTU size as the system default of 1500 bytes or the system default jumbo MTU size of 9000 bytes.



Note

If you change the system jumbo MTU size, Layer 2 ports automatically use the system default MTU size of 1500 bytes unless you specify differently for some or all of those ports.

For information about setting the MTU size, see the [“Configuring the MTU Size” section on page 2-13](#).

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.

For more information, see the following sections:

- [Shutting Down and Restarting a Port Channel Interface, page 5-20](#).
- [Shutting Down and Activating an Interface, page 2-17](#).

Cisco Discovery Protocol

The Cisco Discovery Protocol (CDP) is a Layer 2 protocol that enables two devices that run CDP to learn about each other. You can use CDP to troubleshoot the network by displaying information about the neighboring devices that are linked through each interface. By default, CDP is enabled.

To configure CDP, see the [“Enabling or Disabling CDP” section on page 2-19](#).

Port Channel Parameter

A port channel is an aggregation of physical interfaces that comprise a logical interface. You can bundle up to eight individual interfaces into a port channel to provide increased bandwidth and redundancy. Port channeling also load balances traffic across these physical interfaces. The port channel stays operational if at least one physical interface within the port channel is operational.

Any configuration changes that you apply to the port channel are applied to each interface member of that port channel.

To configure port channels, see the [“Configuring Port Channels” section on page 5-1](#).

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

Guidelines and Limitations

Interface parameters have the following guidelines and limitations:

- Fiber-optic Ethernet ports must use Cisco-supported transceivers. To verify that the ports are using Cisco-supported transceivers, use the **show interface transceivers** command. Interfaces with Cisco-supported transceivers are listed as functional interfaces.
- Flow control, that is using IEEE 802.3x pause frames for controlling flow, is not supported.
- You usually configure Ethernet port speed and duplex mode parameters to auto to allow negotiation of the speed and duplex modes between ports. If you decide to configure the port speed and duplex modes manually for these ports, consider the following:
 - If you set the Ethernet port speed to auto, the device automatically sets the duplex mode to auto.
 - If you enter the **no speed** command, the device automatically sets both the speed and duplex parameters to auto (the **no speed** command produces the same results as the **speed auto** command).
 - If you configure an Ethernet port speed to a value other than auto (for example, 10, 100, or 1000 Mbps), you must configure the connecting port to match. Do not configure the connecting port to negotiate the speed.



Note

The device cannot automatically negotiate the Ethernet port speed and duplex modes if the connecting port is configured to a value other than auto.



Note

Changing the Ethernet port speed and duplex mode configuration might shut down and reenable the interface.

Configuring the Basic Interface Parameters

This section includes the following topics:

- [Specifying an Interface to Configure, page 2-5](#)
- [Configuring a Description, page 2-6](#)
- [Dedicating Bandwidth to One Port, page 2-8](#)
- [Configuring the Interface Speed and Duplex Modes, page 2-9](#)
- [Configuring the MTU Size, page 2-13](#)
- [Configuring Bandwidth, page 2-14](#)
- [Configuring the Throughput Delay, page 2-16](#)
- [Shutting Down and Activating an Interface, page 2-17](#)

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

- [Enabling or Disabling CDP, page 2-19](#)

Specifying an Interface to Configure

Use this procedure to specify an interface to configure.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **config t**
2. **interface** *interface*
3. **show interface** *interface*

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into the global configuration mode.

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

	Command	Purpose
Step 2	interface <i>interface</i> Example: <pre>n1000v(config)# interface ethernet 2/1 n1000v(config-if)#</pre>	<p>Specifies the interface that you are configuring.</p> <p>The <i>interface</i> argument is defined as follows:</p> <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 the management interface, use mgmt 0 or mgmt0. For a vEthernet port, use vethernet <i>number</i>, where <i>number</i> is a number from 1 to 1048575. <p>Note You do not need to add a space between the interface type and the slot/port or interface number. For example, for the Ethernet slot 4, port 5 interface, you can specify either “ethernet 4/5” or “ethernet4/5.”</p>
Step 3	show interface <i>interface</i> Example: <pre>n1000v(config-if)# show interface ethernet 2/1</pre>	<p>Displays the current configuration of interfaces.</p> <p>The <i>interface</i> argument is defined as follows:</p> <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 the management interface, use mgmt 0 or mgmt0. For a vEthernet port, use vethernet <i>number</i>, where <i>number</i> is a number from 1 to 1048575.

Configuring a Description

Use this procedure to add a description to a vEthernet or management interface.

BEFORE YOU BEGIN

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

- 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.

SUMMARY STEPS

- config t**
- interface** *interface*
- description** *string*
- show interface** *interface*
- exit**
- 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)#	Places you into the global configuration mode.
Step 2	interface interface Example: n1000v(config)# interface ethernet 2/1 n1000v(config-if)#	Specifies the interface that you are configuring. The <i>interface</i> argument is defined as follows: <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 the management interface, use mgmt 0 or mgmt0. For a vEthernet port, use vethernet number, where <i>number</i> is a number from 1 to 1048575.
Step 3	description string Example: n1000v(config-if)# description Ethernet port 3 on module 1. n1000v(config-if)#	Adds the description for the interface and saves it in the running configuration. For <i>string</i> , the description can be up to 80 alphanumeric characters. Note You do not need to use quotations around descriptions that include spaces.
Step 4	show interface interface Example: n1000v(config)# show interface ethernet 2/1	Displays the interface status, which includes the description.
Step 5	exit Example: n1000v(config-if)# exit n1000v(config)#	Exits the interface mode.
Step 6	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 interface description to Ethernet port 24 on module 3:

```
n1000v# config t
n1000v(config)# interface ethernet 3/24
n1000v(config-if)# description server1
n1000v(config-if)#
```

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

Dedicating Bandwidth to One Port

Use this procedure to dedicate bandwidth to one port by doing the following:

1. Administratively shutting down the four interfaces in the group.
2. Changing the rate mode to dedicated.
3. Administratively bringing the dedicated port up.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. `config t`
2. `interface ethernet slot/port, ethernet slot/port, ethernet slot/port, ethernet slot/port`
3. `shutdown`
4. `interface ethernet slot/port`
5. `rate-mode dedicated`
6. `no shutdown`
7. `show interface ethernet slot/port`
8. `exit`
9. `copy running-config startup-config`

DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code> Example: n1000v# <code>config t</code> n1000v(config)#	Places you into the global configuration mode.
Step 2	<code>interface ethernet slot/port, ethernet slot/port, ethernet slot/port, ethernet slot/port</code> Example: n1000v(config)# <code>interface ethernet 3/1, ethernet 3/3, ethernet 3/5, ethernet 3/7</code> n1000v(config-if)#	Specifies the Ethernet interfaces to configure, and enters interface configuration mode. The example shows how to specify one port for the dedicated mode.
Step 3	<code>shutdown</code> Example: n1000v(config)# <code>shutdown</code>	Administratively shuts down the ports in the running configuration.
Step 4	<code>interface ethernet slot/port</code> Example: n1000v(config)# <code>interface ethernet 3/1</code> n1000v(config)#	Specifies the first Ethernet interface in a group of interfaces.

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

	Command	Purpose
Step 5	rate-mode dedicated Example: n1000v(config-if)# rate-mode dedicated n1000v(config-if)#	Full bandwidth of 10 Gb is dedicated to one port in the running configuration. When you dedicate the bandwidth, all subsequent commands for the port are for dedicated mode.
Step 6	no shutdown Example: n1000v(config-if)# no shutdown	Brings the port administratively up in the running configuration.
Step 7	show interface ethernet slot/port Example: n1000v(config-if)# show interface ethernet 3/1	Displays the interface information including the current rate mode.
Step 8	exit Example: n1000v(config-if)# exit n1000v(config)#	Exits interface configuration mode.
Step 9	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 configure the dedicated mode for Ethernet port 4/17 in the group that includes ports 4/17, 4/19, 4/21, and 4/23:

```
n1000v# config t
n1000v(config)# interface ethernet 4/17, ethernet 4/19, ethernet 4/21, ethernet 4/23
n1000v(config-if)# shutdown
n1000v(config-if)# interface ethernet 4/17
n1000v(config-if)# rate-mode dedicated
n1000v(config-if)# no shutdown
n1000v(config-if)#
```

Configuring the Interface Speed and Duplex Modes

Use this procedure to configure the interface speed and duplex modes.

BEFORE YOU BEGIN

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

- The interface speed and duplex modes are interrelated, so you should configure both at the same time. To see the speeds and duplex modes that you can configure together for Ethernet and management interfaces, see the [“Speed and Duplex Modes” section on page 2-2](#).

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



Note

The interface speed that you specify can affect the duplex mode used for an interface, so you should set the speed before setting the duplex mode. If you set the speed for autonegotiation, the duplex mode is automatically set to be autonegotiated. If you specify a speed of 10 Mbps or 100 Mbps, the port is automatically configured to use half-duplex mode, but you can specify full-duplex mode instead. If you specify a speed of 1000 Mbps (1 Gbps) or faster, full duplex is automatically used.

- Make sure that the remote port has a speed setting that supports your changes for the local port. If you want to set the local port to use a specific speed, you must set the remote port for the same speed or set the local port to autonegotiate the speed.

SUMMARY STEPS

1. `conf t`
2. `interface interface`
3. `speed {{ 10 | 100 | 1000 | { auto [10 100 [1000]] } } | { 10000 | auto } }`
4. `duplex {full | half | auto}`
5. `show interface interface`
6. `exit`
7. `copy running-config startup-config`

DETAILED STEPS

	Command	Purpose
Step 1	<code>conf t</code> Example: n1000v# <code>conf t</code> n1000v(config)#	Enters the global configuration mode.
Step 2	<code>interface interface</code> Example: n1000v(config)# <code>interface ethernet 2/1</code> n1000v(config-if)#	Specifies the interface that you are configuring. The <i>interface</i> argument is defined as follows: <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 the management interface, use mgmt 0 or mgmt0.• For a vEthernet port, use vethernet number, where <i>number</i> is a number from 1 to 1048575.

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

	Command	Purpose
Step 3	speed {{10 100 1000 {auto [10 100 [1000]]}} {10000 auto}} Example: n1000v(config-if)# speed 1000 n1000v(config-if)#	<p>For Ethernet ports on the 48-port 10/100/1000 modules, sets the speed at 10 Mbps, 100 Mbps, or 1000 Mbps, or sets the port to auto negotiate its speed with the other 10/100/1000 port on the same link.</p> <p>For Ethernet ports on the 32-port 10-Gigabit Ethernet modules, sets the speed at 10,000 Mbps (10 Gbps) or sets the port to autonegotiate its speed with the other 10-Gigabit Ethernet port on the link.</p> <p>For management interfaces, sets the speed as 1000 Mbps or sets the port to autonegotiate its speed.</p>
Step 4	duplex {full half auto} Example: n1000v(config-if)# duplex full	Specifies the duplex mode as full, half, or autonegotiate.
Step 5	show interface <i>interface</i> Example: n1000v(config)# show interface <i>mgmt0</i>	<p>Displays the interface status, which includes the speed and duplex mode parameters.</p> <p>The <i>interface</i> argument is defined as follows:</p> <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 the management interface, use mgmt0 or mgmt0. For a vEthernet port, use vethernet <i>number</i>, where <i>number</i> is a number from 1 to 1048575.
Step 6	exit Example: n1000v(config-if)# exit n1000v(config)#	Exits interface configuration mode.
Step 7	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 speed of Ethernet port 1 on the 48-port 10/100/1000 module in slot 3 to 1000 Mbps and full-duplex mode:

```
n1000v# config t
n1000v(config)# interface ethernet 3/1
n1000v(config-if)# speed 1000
n1000v(config-if)# duplex full
n1000v(config-if)#
```

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

Configuring the System Jumbo MTU Size

Use this procedure to configure the system jumbo MTU size, which can be used to specify the MTU size for Layer 2 interfaces.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- You can specify an even number of bytes between 1500 and 9000. If you do not configure the system jumbo MTU size, it defaults to 1500 bytes.

SUMMARY STEPS

1. **config t**
2. **system jumbomtu *size***
3. **show running-config**
4. **interface ethernet *slot/port***
5. **mtu *size***
6. **exit**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into the global configuration mode.
Step 2	system jumbomtu <i>size</i> Example: n1000v(config)# system jumbomtu 8000	Specifies the system jumbo MTU size. Use an even number between 1500 and 9000.
Step 3	show running-config Example: n1000v(config)# show running-config	Displays the current operating configuration, including the system jumbo MTU size.
Step 4	interface ethernet <i>slot/port</i> Example: n1000v(config)# interface ethernet 2/2 n1000v(config-if)#	Specifies an interface to configure and enters interface configuration mode.
Step 5	mtu <i>size</i> Example: n1000v(config-if)# mtu 8000	Specifies either the default MTU size of 1500 or the system jumbo MTU size that you specified earlier.

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

	Command	Purpose
Step 6	exit Example: n1000v(config-if)# exit n1000v(config)#	Exits the interface mode.
Step 7	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 configure the system jumbo MTU as 8000 bytes and how to change the MTU specification for an interface that was configured with the previous jumbo MTU size:

```
n1000v# config t
n1000v(config)# system jumbomtu 8000
n1000v(config)# show running-config
n1000v(config)# interface ethernet 2/2
n1000v(config-if)# switchport
n1000v(config-if)# mtu 8000
n1000v(config-if)#
```

Configuring the MTU Size

Use this section to configure the size of the maximum transmission unit (MTU) for Layer 2 Ethernet interfaces.

This section includes the following topics:

- [Configuring the Interface MTU Size, page 2-13](#)
- [Configuring the System Jumbo MTU Size, page 2-12](#)

Configuring the Interface MTU Size

Use this procedure to configure the MTU for all interfaces.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- You can specify either of the following for MTU size:
 - The system default MTU size of 1500 bytes.
 - A system jumbo MTU size between 1500 and 9000 bytes.
- To configure the jumbo MTU size, see the “[Configuring the System Jumbo MTU Size](#)” section on [page 2-12](#).

SUMMARY STEPS

1. **config t**

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

2. **interface ethernet** *slot/port*
3. **mtu** *size*
4. **show interface ethernet** *slot/port*
5. **exit**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into the global configuration mode.
Step 2	interface ethernet <i>slot/port</i> Example: n1000v(config)# interface ethernet 3/1 n1000v(config-if)#	Specifies an Ethernet interface to configure, and enters interface configuration mode.
Step 3	mtu <i>size</i> Example: n1000v(config-if)# mtu 9216	Specifies either the default MTU size (1500) or the system jumbo MTU size (9000) unless you have changed the system jumbo MTU size.
Step 4	show interface ethernet <i>slot/port</i> Example: n1000v(config-if)# show interface type <i>slot/port</i>	Displays the interface status, which includes the MTU size.
Step 5	exit Example: n1000v(config-if)# exit n1000v(config)#	Exits interface configuration mode.
Step 6	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 configure the Ethernet interface 3/1 with the default MTU size of 1500 bytes:

```
n1000v# config t
n1000v(config)# interface ethernet 3/1
n1000v(config-if)# mtu 1500
n1000v(config-if)#
```

Configuring Bandwidth

Use this procedure to configure bandwidth for Ethernet interfaces.

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

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- The physical level uses an unchangeable bandwidth of 1 GB, but you can configure a value from 1 to 10,000,000 Kb for Level 3 protocols.

SUMMARY STEPS

1. **config t**
2. **interface ethernet *slot/port***
3. **bandwidth *value***
4. **show interface ethernet *slot/port***
5. **exit**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into the global configuration mode.
Step 2	interface ethernet <i>slot/port</i> Example: n1000v(config)# interface ethernet 3/1 n1000v(config-if)#	Specifies an Ethernet interface to configure, and enters interface configuration mode.
Step 3	bandwidth <i>value</i> Example: n1000v(config-if)# bandwidth 1000000	Assigns the specified bandwidth to the interface in the running configuration. The bandwidth is an information-only value from 1 to 10,000,000.
Step 4	show interface ethernet <i>slot/port</i> Example: n1000v(config-if)# show interface ethernet <i>slot/port</i>	Displays the interface status, which includes the bandwidth value.
Step 5	exit Example: n1000v(config-if)# exit n1000v(config)#	Exits interface configuration mode.
Step 6	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.

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

EXAMPLES

The following example shows how to configure an informational value of 1,000,000 Kb for the Ethernet slot 3, port 1 interface bandwidth parameter:

```
n1000v# config t
n1000v(config)# interface ethernet 3/1
n1000v(config-if)# bandwidth 1000000
n1000v(config-if)#
```

Configuring the Throughput Delay

Use this procedure to configure throughput delay for the Ethernet interface informational display.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **config t**
2. **interface ethernet *slot/port***
3. **delay *value***
4. **show interface ethernet *slot/port***
5. **exit**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into the global configuration mode.
Step 2	interface ethernet <i>slot/port</i> Example: n1000v(config)# interface ethernet 3/1 n1000v(config-if)#	Specifies an interface to configure, and enters interface configuration mode.
Step 3	delay <i>value</i> Example: n1000v(config-if)# delay 10000	Assigns the delay time to the interface in the running configuration. The delay time is specified in tens of microseconds.
Step 4	show interface ethernet <i>slot/port</i> Example: n1000v(config)# show interface ethernet 3/1	Displays the interface status, which includes the throughput-delay time.

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

	Command	Purpose
Step 5	exit Example: n1000v(config-if)# exit n1000v(config)#	Exits the interface configuration mode.
Step 6	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 configure the throughput-delay time to 100,000 microseconds for the Ethernet port 3/1:

```
n1000v# config t
n1000v(config)# interface ethernet 3/1
n1000v(config-if)# delay 10000
n1000v(config-if)#
```

Shutting Down and Activating an Interface

Use this procedure to shut down and restart Ethernet or management interfaces.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- When you shut down an interface, it becomes disabled. As a result, the following occurs:
 - The output of monitoring commands show it as being down.
 - Dynamic routing protocols relay this information to other network servers.
 - The interface is not included in routing updates.
 - When the interfaces are shut down.
- To activate an interface that has been shut down, you must restart the device.

SUMMARY STEPS

1. **config t**
2. **interface** *interface*
3. **shutdown**
4. **show interface** *interface*
5. **no shutdown**
6. **show interface** *interface*
7. **exit**
8. **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)#	Places you into the global configuration mode.
Step 2	interface interface Example 1: n1000v(config)# interface ethernet 2/1 n1000v(config-if)#	Specifies the interface that you are configuring. The <i>interface</i> argument is defined as follows: <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 the management interface, use mgmt 0 or mgmt0.
Step 3	shutdown Example: n1000v(config-if)# shutdown	Disables the interface in the running configuration.
Step 4	show interface interface Example: n1000v(config-if)# show interface ethernet 2/1	Displays the interface status, which includes the administrative status.
Step 5	no shutdown Example: n1000v(config-if)# no shutdown	Reenables the interface in the running configuration.
Step 6	show interface interface Example: n1000v(config-if)# show interface ethernet 2/1	Displays the interface status, which includes the administrative status. The <i>interface</i> argument is defined as follows: <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 the management interface, use mgmt 0 or mgmt0.
Step 7	exit Example: n1000v(config-if)# exit n1000v(config)#	Exits the interface configuration mode.
Step 8	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 change the administrative status for Ethernet port 3/1 from disabled to enabled:

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

```
n1000v# config t
n1000v(config)# interface ethernet 3/1
n1000v(config-if)# shutdown
n1000v(config-if)# no shutdown
n1000v(config-if)#
```

Enabling or Disabling CDP

Use this procedure to enable or disable the Cisco Discovery Protocol (CDP) for Ethernet and management interfaces.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- Make sure that CDP is enabled at both ends of the link.

SUMMARY STEPS

1. **config t**
2. **interface** *interface*
3. **cdp enable**
no cdp enable
4. **show cdp interface** *interface*
5. **exit**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into the global configuration mode.
Step 2	interface <i>interface</i> Example 1: n1000v(config)# interface ethernet 3/1 n1000v(config-if)#	Specifies the interface that you are configuring. The <i>interface</i> argument is defined as follows: <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 the management interface, use mgmt 0 or mgmt0.

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

	Command	Purpose
Step 3	cdp enable Example: n1000v(config-if)# cdp enable	Enables CDP for the interface in the running configuration. To work, this parameter must be enabled for both interfaces on the same link.
	no cdp enable Example: n1000v(config-if)# no cdp enable	Disables CDP for the interface in the running configuration. As soon as you disable CDP for one of two interfaces, CDP is disabled for the link.
Step 4	show cdp interface <i>interface</i> Example: n1000v(config-if)# show cdp interface <i>interface</i>	Displays the CDP status for the interface in the running configuration. The <i>interface</i> argument is defined as follows: <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 the management interface, use mgmt 0 or mgmt0.
Step 5	exit Example: n1000v(config-if)# exit n1000v(config)#	Exits the interface configuration mode.
Step 6	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 enable CDP for Ethernet port 3/1:

```
n1000v# config t
n1000v(config)# interface ethernet 3/1
n1000v(config-if)# cdp enable
n1000v(config-if)#
```

The following example shows how to disable CDP for Ethernet port 3/1:

```
n1000v# config t
n1000v(config)# interface ethernet 3/1
n1000v(config-if)# no cdp enable
n1000v(config-if)#
```

Clearing the Interface Counters

Use this procedure to clear the Ethernet and management interface counters. You can perform this task from the EXEC mode, configuration mode, or interface configuration mode.

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

SUMMARY STEPS

1. `clear counters interface`
2. `show interface interface`

DETAILED STEPS

	Command	Purpose
Step 1	clear counters <i>interface</i> Example: n1000v# <code>clear counters ethernet 2/1</code> n1000v#	Clears the Ethernet or management counters for the specified interface: The <i>interface</i> argument is defined as follows: <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 the management interface, use mgmt 0 or mgmt0.
Step 2	show interface <i>interface</i>	Displays the interface status, which includes the counters. The <i>interface</i> argument is defined as follows: <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 the management interface, use mgmt 0 or mgmt0.

EXAMPLES

The following example shows how to clear and reset the counters on Ethernet port 5/5:

```
n1000v# clear counters ethernet 5/5
n1000v#
```

Verifying the Basic Interface Parameters

Use the commands listed here to verify the basic interface parameters

To display port configuration information, use one of the following commands:

Command	Purpose
show cdp	Displays the CDP status.
show interface <i>interface</i>	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

This section provides the feature history for basic interface parameters.

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

Feature Name	Releases	Feature Information
Basic interface parameters	4.0	This feature was introduced.



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](#)
- [Guidelines and Limitations, page 3-3](#)
- [Configuring Access and Trunk Interfaces, page 3-4](#)
- [Verifying the Interface Configuration, page 3-14](#)
- [Monitoring the Interface Configuration, page 3-14](#)
- [Configuration Examples for Access and Trunk Port Mode, page 3-14](#)
- [Default Settings, page 3-4](#)
- [Additional References, page 3-15](#)
- [Feature History for Layer 2 Interface Parameters, page 3-15](#)



Note

For information about configuring a Switched Port Analyzer (SPAN) destination interface, see the *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(2)*.



Note

for information about VLANs, MAC address tables, and private VLANs, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(2)*.

Information About Access and Trunk Interfaces

This section includes the following topics:

- [Access and Trunk Interfaces, page 3-1](#)
- [IEEE 802.1Q Encapsulation, page 3-2](#)
- [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:

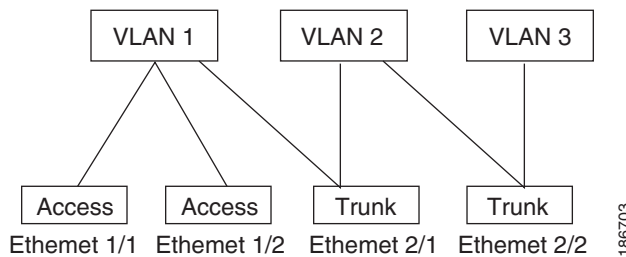
Send document comments to nexus1k-docfeedback@cisco.com.

- 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 4.0(4)SV1(2)* 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

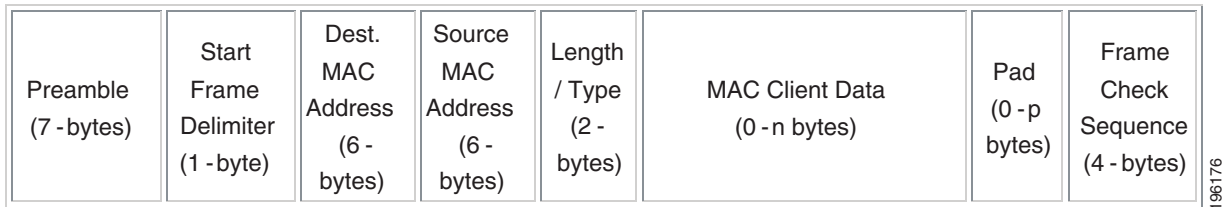
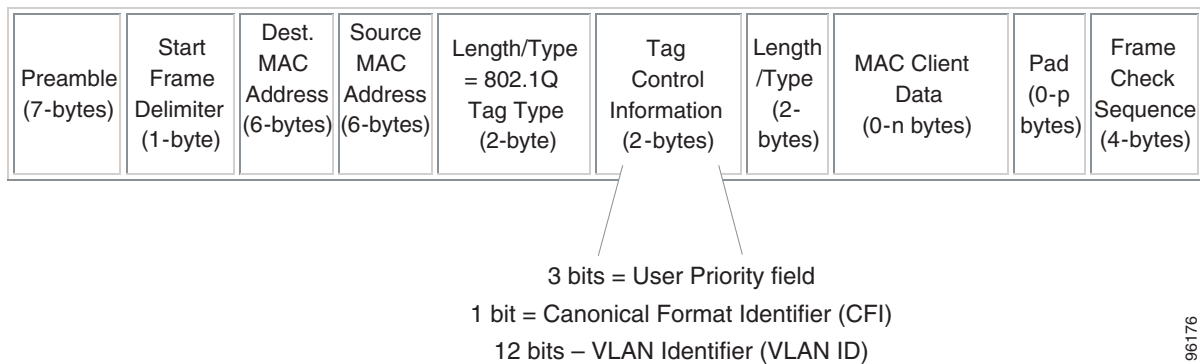


Figure 3-3 Header With 802.1Q Tag



High Availability

High availability is supported 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.
- 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.

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

Default Settings

The following table lists the default settings for Layer 2 interfaces.

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

Configuring Access and Trunk Interfaces

This section includes the following topics:

- [Configuring a LAN Interface as a Layer 2 Access Port, page 3-4](#)
- [Configuring Access Host Ports, page 3-6](#)
- [Configuring Trunk Ports, page 3-7](#)
- [Configuring the Native VLAN for 802.1Q Trunking Ports, page 3-9](#)
- [Configuring the Allowed VLANs for Trunking Ports, page 3-11](#)
- [Configuring the Device to Tag Native VLAN Traffic, page 3-12](#)



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

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:

- You are logged in to the CLI in EXEC mode.
- 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. **exit**
6. **show interface**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	interface <i>interface</i> 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	switchport mode access 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	switchport access vlan <i>vlan-id</i> 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	exit Example: n1000v(config-if)# exit n1000v(config)#	Exits the interface configuration mode and returns you to global configuration mode.

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

	Command	Purpose
Step 6	show interface Example: n1000v(config)# show interface	(Optional) Displays the interface status and information.
Step 7	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 access port that carries traffic for VLAN 5 only:

```
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 Access Host Ports

Use this procedure to configure a port as an access port in order to optimize the performance of ports connected to end stations.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- Ensure that you are configuring the correct interface to an interface that is an end station.
- You should apply the **switchport host** command only to interfaces that are connected to an end station.
- An access host port handles the Spanning Tree Protocol (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 about port channel interfaces.

- The interface can be either Ethernet or vEthernet.

SUMMARY STEPS

1. **config t**
2. **interface** *interface*
3. **switchport host**
4. **exit**
5. **show interface**

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

6. copy running-config startup-config

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into 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 host Example: n1000v(config-if)# switchport host	Designates the interface as an access host port in the running configuration, which immediately moves it 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: n1000v(config-if)# exit n1000v(config)#	Exits the interface configuration mode and returns you to global configuration mode.
Step 5	show interface Example: n1000v(config)# show interface	(Optional) Displays the interface status and information.
Step 6	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 access port with PortFast enabled and port channel disabled:

```
n1000v# config t
n1000v(config)# interface ethernet 3/1
n1000v(config-if)# switchport host
n1000v(config-if)#
```

Configuring Trunk Ports

Use this procedure to configure a Layer 2 port as a trunk port.

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

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- 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. **exit**
5. **show interface**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into 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.
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.

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

	Command	Purpose
Step 4	exit Example: n1000v(config-if)# exit n1000v(config)#	Exits the interface configuration mode and returns you to global configuration mode.
Step 5	show interface Example: n1000v(config)# show interface	(Optional) Displays the interface status and information.
Step 6	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

Use this procedure to configure the native VLAN for 802.1Q trunk ports.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- If you do not configure a native VLAN, 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. **exit**
5. **show vlan**
6. **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)#	Places you into 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	exit Example: n1000v(config-if)# exit n1000v(config)#	Exits the interface configuration mode and returns you to global configuration mode.
Step 5	show vlan Example: n1000v(config)# show vlan	(Optional) Displays the status and information of VLANs.
Step 6	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)#
```


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

Configuring the Allowed VLANs for Trunking Ports

Use this procedure to specify the VLAN IDs that are allowed on a trunk port.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- Make sure that you are configuring the correct interface and that the interface is a trunk.

SUMMARY STEPS

1. **config t**
2. **interface** *interface*
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: n1000v# config t n1000v(config)#	Places you into 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.
Step 3	switchport trunk allowed vlan { <i>vlan-list</i> all none [add except none remove { <i>vlan-list</i> }]}	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>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>

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

	Command	Purpose
Step 4	exit Example: n1000v(config-if)# exit n1000v(config)#	Exits the interface configuration mode and returns you to global configuration mode.
Step 5	show vlan Example: n1000v# show vlan	(Optional) Displays the status and information for VLANs.
Step 6	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 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

Use this procedure to maintain tagging on a packet that enters an 802.1Q trunked interface with a tag matching the native VLAN ID. Untagged traffic is dropped although control traffic is still carried on the interface.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- 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. **exit**
4. **show vlan**

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

5. copy running-config startup-config

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into 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.
Step 3	exit Example: n1000v(config)# exit n1000v#	Exits global configuration mode and returns you to EXEC mode.
Step 4	show vlan Example: n1000v# show vlan	(Optional) Displays the status and information for VLANs.
Step 5	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#
```

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

Verifying the Interface Configuration

Use the following commands to display and verify access and trunk interface information.

Command	Purpose
show interface ethernet <i>slot/port</i> [brief counters debounce description mac-address status transceiver]	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.

Monitoring the Interface Configuration

Use the following commands to display and monitor access and trunk interface information.

Command	Purpose
clear counters [<i>interface</i>]	Clears the counters.
show interface counters [module <i>module</i>]	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 <i>module</i>]	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
```

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

```
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 3-15](#)
- [Standards, page 3-15](#)

Related Documents

Related Topic	Document Title
Port channels	Chapter 5, “Configuring Port Channels”
VLANs, private VLANs, and STP	<i>Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(2)</i>
System management	<i>Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(2)</i>
Release Notes	<i>Cisco Nexus 1000V Release Notes, Release 4.0(4)SV1(2)</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.

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

Feature Name	Releases	Feature Information
Layer 2 interface parameters	4.0	This feature was introduced.



CHAPTER 4

Configuring Virtual Ethernet Interfaces

This chapter describes how to configure virtual Ethernet (vEthernet or vEth) interfaces.

This chapter includes the following sections:

- [Information About vEthernet Interfaces, page 4-1](#)
- [Guidelines and Limitations, page 4-1](#)
- [Default Settings, page 4-2](#)
- [Configuring vEthernet Interfaces, page 4-2](#)
- [Verifying the vEthernet Interface Configuration, page 4-7](#)
- [Configuration Examples for vEthernet Interfaces, page 4-9](#)
- [Additional References, page 4-10](#)
- [Feature History for vEthernet Interface Parameters, page 4-10](#)

Information About vEthernet 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)
- Service console
- vmkernel

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

Guidelines and Limitations

vEthernet interface configuration has the following guideline and limitation:

- MTU cannot be configured on a vEthernet interface.

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

Default Settings

The following are default settings for virtual Ethernet interfaces.

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

Configuring vEthernet Interfaces

This section includes the following topics:

- [Configuring a vEthernet Access Interface, page 4-2](#)
- [Configuring a Private VLAN on a vEthernet Interface, page 4-4](#)
- [Enabling or Disabling a vEthernet Interface, page 4-6](#)

Configuring a vEthernet Access Interface

Use this procedure to configure a vEthernet interface for use as an access interface.

BEFORE YOU BEGIN

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

- You are logged into the CLI in EXEC mode.
- If you do not add a description to the vEthernet interface, then one of the following descriptions is added at attach time. If you add a description and then remove it using the **no description** command, then one of the following descriptions is added to the interface:
 - For a VM—*VM-Name, Network Adapter number*
 - For a VMK—*VMware VMkernel, vmk number*
 - For a VSWIF—*VMware Service Console, vswif number*

SUMMARY STEPS

1. **config t**
2. **interface vethernet** *interface-number*
3. **description** *string*
4. **switchport access vlan** *vlan-id*
5. **switchport mode access**

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

6. `show interface interface-number`
7. `copy running-config startup-config`

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	interface vethernet interface-number Example: n1000v(config)# interface vethernet 100 n1000v(config-if)#	Places you into interface configuration mode for the specified vEthernet interface. For <i>interface-number</i> , the range is from 1 to 1048575.
Step 3	description string Example: n1000v(config-if)# description accessvlan	Adds a description to the interface in the running configuration. For <i>string</i> , the description can be up to 80 alphanumeric characters. Note You do not need to use quotations around descriptions that include spaces.
Step 4	switchport access vlan vlanid Example: n1000v(config-if)# switchport access vlan 5	Configures the vEthernet interface as an access interface and specifies the VLAN ID in the running configuration. For <i>vlanid</i> , the range is from 1 to 4094.
Step 5	switchport mode access Example: n1000v(config-if)# switchport mode access n1000v(config-if)#	Configures the vEthernet interface for use as an access interface in the running configuration.
Step 6	show interface interface-number Example: n1000v(config-if)# show interface vethernet1	(Optional) Displays the interface status and information. For <i>interface-number</i> , the range is from 1 to 1048575.
Step 7	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.

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

Configuring a Private VLAN on a vEthernet Interface

Use this procedure to configure a private VLAN (PVLAN) on a vEthernet interface.

BEFORE YOU BEGIN

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

- You are logged into the CLI in EXEC mode.

SUMMARY STEPS

- config t**
- interface vethernet** *interface-number*
- description** *string*
- switchport access vlan** *vlan-id*
- switchport mode private-vlan host**
- switchport private-vlan host-association** *primary-vlan-id*
- show interface**
- copy running-config startup-config**

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	interface vethernet <i>interface-number</i> Example: n1000v(config)# interface vethernet 1 n1000v(config-if)#	Places you into interface configuration mode for the specified vEthernet interface. For <i>interface-number</i> , the range is from 1 to 1048575.
Step 3	description <i>string</i> Example: n1000v(config-if)# description isp_pvlan1	Adds a description to the interface in the running configuration. For <i>string</i> , the description can be up to 80 alphanumeric characters. Note You do not need to use quotations around descriptions that include spaces.
Step 4	switchport access vlan <i>vlan-id</i> Example: n1000v(config-if)# switchport access vlan 5	Configures the vEthernet interface as an access interface and specifies the VLAN ID in the running configuration. For <i>vlan-id</i> , the range is from 1 to 4094.
Step 5	switchport mode private-vlan host Example: n1000v(config-if)# switchport mode private-vlan host	Configures the vEthernet interface for a PVLAN host in the running configuration.

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

	Command	Purpose
Step 6	switchport private-vlan host-association <i>primary-vlanid</i> Example: n1000v(config-if)# switchport private-vlan host-association 5	Configures the vEthernet interface for a host association with a specific primary VLAN ID in the running configuration. For <i>primary-vlanid</i> , the range is from 1 to 4094.
Step 7	show interface Example: n1000v# show interface	(Optional) Displays the interface status and information.
Step 8	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 configure a vEthernet interface to use in a private vlan:

```
n1000v# config t
n1000v(config)# interface vethernet 1
n1000v(config-if)# description isp_pvlan1
n1000v(config-if)# switchport access vlan 5
n1000v(config-if)# switchport mode private-vlan host
n1000v(config-if)# switchport private-vlan host-association 5
n1000v(config-if)# show interface vethernet 1
Vethernet1 is up
  Port description is gentoo, Network Adapter 1
  Hardware is Virtual, address is 0050.5687.3bac
  Owner is VM "gentoo", adapter is Network Adapter 1
  Active on module 4
  VMware DVS port 1
  Port-Profile is vm
  Port mode is access
  5 minute input rate 1 bytes/second, 0 packets/second
  5 minute output rate 94 bytes/second, 1 packets/second
  Rx
  655 Input Packets 594 Unicast Packets
  0 Multicast Packets 61 Broadcast Packets
  114988 Bytes
  Tx
  98875 Output Packets 1759 Unicast Packets
  80410 Multicast Packets 16706 Broadcast Packets 0 Flood Packets
  6368452 Bytes
  0 Input Packet Drops 0 Output Packet Drops
```

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

Enabling or Disabling a vEthernet Interface

Use this procedure to enable or disable a vEthernet interface.

SUMMARY STEPS

1. **config t**
2. **interface vethernet** *interface-number*
3. **[no] shutdown**
4. **show interface**
5. **copy running-config startup-config**

BEFORE YOU BEGIN

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

- You are logged into the CLI in EXEC mode.

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	interface vethernet <i>interface-number</i> Example: n1000v(config)# interface vethernet 100 n1000v(config-if)#	Places you into interface configuration mode for the specified vEthernet interface. For <i>interface-number</i> , the range is from 1 to 1048575.
Step 3	[no] shutdown Example: n1000v(config-if)# no shutdown n1000v(config-if)#	Enables or disables the vEthernet interface in the running configuration: <ul style="list-style-type: none">• shutdown—Disables the vEthernet interface.• no shutdown—Enables the vEthernet interface.
Step 4	show interface Example: n1000v# 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 enable a vEthernet interface:

```
n1000v# config t
n1000v(config)# interface vethernet 100
```

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

```
n1000v(config)# no shutdown
n1000v(config-if)# show interface veth100 status
```

```
-----
Port          Name          Status  Vlan    Duplex  Speed  Type
-----
Veth100      --              up      1       auto    auto   auto
n1000v(config-if)#
```

Verifying the vEthernet Interface Configuration

Use the following commands to display and verify the vEthernet interface information.

Command	Purpose
show interface vethernet <i>interface-number</i> [brief counters detailed [all] errors] description mac-address status down err-disabled inactive module <i>num</i> up] switchport]	Displays the vEthernet interface configuration.
show interface [vethernet <i>interface-number</i>]	Displays the complete interface configuration.
show interface [vethernet <i>interface-number</i>] brief	Displays abbreviated interface configuration.
show interface [vethernet <i>interface-number</i>] counters	Displays the interface incoming and outgoing counters.
show interface [vethernet <i>interface-number</i>] counters detailed [all]	Displays detailed information for all counters. Note If 'all' is not specified then only non-zero counters are shown.
show interface [vethernet <i>interface-number</i>] counters errors	Displays the interface error counters.
show interface [vethernet <i>interface-number</i>] description	Displays the interface description.
show interface [vethernet <i>interface-number</i>] mac-address	Displays the interface MAC address. Note For vEth interfaces this shows the MAC address of the connected device.
show interface [vethernet <i>interface-number</i>] status down err-disabled inactive module <i>num</i> up]	Displays interface line status.
show interface [vethernet <i>interface-number</i>] switchport	Displays interface switchport information.
show interface virtual [vm [<i>vm_name</i>] vmk vswif] [module <i>mod_no</i>]	Displays virtual interfaces only.
show interface virtual port-mapping [vm [<i>name</i>] vmk vswif description] [<i>module num</i>]	Displays mappings between vEth and VMware DVPort.

The following example shows how to display vEthernet 1:

```
n1000v# show interface veth1
Vethernet1 is up
  Port description is gentool1, Network Adapter 1
  Hardware is Virtual, address is 0050.56bd.42f6
  Owner is VM "gentool1", adapter is Network Adapter 1
  Active on module 33
  VMware DVS port 100
  Port-Profile is vlan48
```

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

```

Port mode is access
Rx
491242 Input Packets 491180 Unicast Packets
7 Multicast Packets 55 Broadcast Packets
29488527 Bytes
Tx
504958 Output Packets 491181 Unicast Packets
1 Multicast Packets 13776 Broadcast Packets 941 Flood Packets
714925076 Bytes
11 Input Packet Drops 0 Output Packet Drops
n1000v#

```

The following example shows how to display information for all vEthernet interfaces:

```
n1000v# show interface virtual
```

```

-----
Port          Adapter      Owner          Mod Host
-----
Veth1                  Vm1-kl61       2
Veth2                  VM1-kl65       5
Veth3                  VM2-kl61       2
Veth1      Net Adapter 1  austen-gentool 33  austen-strider.austen.
Veth2      Net Adapter 2  austen-gentool 33  austen-strider.austen.
n1000v#

```

The following example shows how to display the descriptions for all vEthernet interfaces:

```
n1000v# show interface virtual description
```

```

-----
Interface      Description
-----
Veth1          gentool, Network Adapter 1
Veth2          gentool, Network Adapter 2
Veth3          VMware VMkernel, vmk1
Veth4          VMware Service Console, vswif1

```

The following example shows how to display the counters for all vEthernet interfaces:

```
n1000v# show interface counters
```

```

-----
Port          InOctets  InUcastPkts  InMcastPkts  InBcastPkts
-----
mgmt0          42754      --           0             --
Eth2/2        41423421  112708      125997       180167
Eth5/2        39686276  119152      93284        180100
Eth5/6        4216279   9530        31268        40
Veth1           0           0           0             0
Veth2           0           0           0             0
Veth3           0           0           0             0
Veth4           0           0           0             0
Veth5           0           0           0             0
Veth6           0           0           0             0
Veth7           0           0           0             0
Veth100        0           0           0             0
-----
Port          OutOctets  OutUcastPkts  OutMcastPkts  OutBcastPkts
-----
mgmt0          3358      --           --            --

```

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

```

Eth2/2          23964739      116150      516          52768
Eth5/2          26419473      111598      571          52420
Eth5/6          1042930       9548        536          14
Veth1           393589         0           6150         0
Veth2           393600         0           6150         0
Veth3           393600         0           6150         0
Veth4           0             0           0            0
Veth5           0             0           0            0
Veth6           0             0           0            0
Veth7           0             0           0            0
Veth100         0             0           0            0

n1000v#

```

The following example shows how to display the virtual port mapping for all vEthernet interfaces:

```
n1000v# show interface virtual port-mapping
```

```

-----
Port          Hypervisor Port  Status  Reason
-----
Veth1         DVPort100        up      none
Veth2         DVPort160        up      none

```

The following example shows how to display the running configuration information for all vEthernet interfaces:

```

n1000v# show running-config interface veth1
version 4.0(4)SV1(1)

interface Vethernet1
  inherit port-profile vlan48
  description gentool, Network Adapter 1

```

Configuration Examples for vEthernet Interfaces

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

```

n1000v# configure terminal
n1000v(config)# interface vethernet 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 vethernet 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)#

```

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

Additional References

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

- [Related Documents, page 4-10](#)
- [Standards, page 4-10](#)

Related Documents

Related Topic	Document Title
Port Profiles	<i>Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)</i>
VLANs and private VLANs	<i>Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(2)</i>
System management	<i>Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(2)</i>
Release Notes	<i>Cisco Nexus 1000V Release Notes, Release 4.0(4)SV1(2)</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 vEthernet Interface Parameters

This section provides the feature history for vEthernet interface parameters.

Feature Name	Releases	Feature Information
vEthernet interface parameters	4.0	This feature was introduced.



CHAPTER 5

Configuring Port Channels

This chapter describes how to configure port channels and includes the following topics:

- [Information About Port Channels, page 5-1](#)
- [High Availability, page 5-9](#)
- [Prerequisites for Port Channels, page 5-9](#)
- [Guidelines and Limitations, page 5-10](#)
- [Configuring Port Channels, page 5-11](#)
- [Verifying the Port Channel Configuration, page 5-27](#)
- [Monitoring the Port Channel Configuration, page 5-28](#)
- [Configuration Example for Port Channels, page 5-28](#)
- [Additional References, page 5-28](#)
- [Additional References, page 5-28](#)
- [Feature History for Port Channels, page 5-29](#)

Information About Port Channels

A port channel is an aggregation of multiple physical interfaces that creates a logical interface. You can bundle up to eight individual active links into a port channel to provide increased bandwidth and redundancy. Port channeling also load balances traffic across these physical interfaces. The port channel stays operational as long as at least one physical interface within the port channel is operational.

You can use static port channels, with no associated aggregation protocol, for a simplified configuration.

This section includes the following topics:

- [Port Channels, page 5-2](#)
- [Compatibility Checks, page 5-2](#)
- [Load Balancing Using Port Channels, page 5-4](#)
- [LACP, page 5-5](#)
- [vPC Host Mode, page 5-8](#)

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

Port Channels

A port channel bundles physical links into a channel group to create a single logical link that provides the aggregate bandwidth of up to eight physical links. If a member port within a port channel fails, the traffic previously carried over the failed link switches to the remaining member ports within the port channel.

You can bundle up to eight ports into a static port channel without using any aggregation protocol.

**Note**

The device does not support Port Aggregation Protocol (PAgP) for port channels.

Each port can be in only one port channel. All the ports in a port channel must be compatible; they must use the same speed and duplex mode (see the [“Compatibility Checks” section on page 5-2](#)). When you run static port channels with no aggregation protocol, the physical links are all in the **on** channel mode.

You can create port channels directly by creating the port channel interface, or you can create a channel group that acts to aggregate individual ports into a bundle. When you associate an interface with a channel group, the software creates a matching port channel automatically if the port channel does not already exist. In this instance, the port channel assumes the Layer 2 configuration of the first interface. You can also create the port channel first. In this instance, the Cisco Nexus 1000V creates an empty channel group with the same channel number as the port channel and takes the default Layer 2 configuration, as well as the compatibility configuration (see the [“Compatibility Checks” section on page 5-2](#)).

**Note**

The port channel is operationally up when at least one of the member ports is up and is in the channeling state. The port channel is operationally down when all member ports are operationally down.

Compatibility Checks

When you add an interface to a port channel group, the following compatibility checks are made before allowing the interface to participate in the port channel:

- Network layer
- (Link) speed capability
- Speed configuration
- Duplex capability
- Duplex configuration
- Port mode
- Access VLAN
- Trunk native VLAN
- Tagged or untagged
- Allowed VLAN list
- MTU size
- SPAN—cannot be a SPAN source or a destination port
- Storm control

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

To view the full list of compatibility checks performed by the Cisco Nexus 1000V, use the **show port-channel compatibility-parameters**.

You can only add interfaces configured with the channel mode set to **on** to static port channels. You can configure these attributes on an individual member port. If you configure a member port with an incompatible attribute, the Cisco Nexus 1000V suspends that port in the port channel.

Alternatively, you can force ports with incompatible parameters to join the port channel if the following parameters are the same:

- (Link) speed capability
- Speed configuration
- Duplex capability
- Duplex configuration

When the interface joins a port channel, some of its individual parameters are removed and replaced with the values on the port channel as follows:

- Bandwidth
- Delay
- Extended Authentication Protocol over UDP
- VRF
- IP address (v4 and v6)
- MAC address
- Spanning Tree Protocol
- NAC
- Service policy
- Quality of Service (QoS)
- Access control lists (ACLs)

The following interface parameters remain unaffected when the interface joins or leaves a port channel:

- Description
- CDP
- MDIX
- Rate mode
- Shutdown
- SNMP trap

**Note**

When you delete the port channel, the software sets all member interfaces as if they were removed from the port channel.

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

Load Balancing Using Port Channels

The Cisco Nexus 1000V load balances traffic across all operational interfaces in a port channel by hashing the addresses in the frame to a numerical value that selects one of the links in the channel. Port channels provide load balancing by default. Port channel load balancing uses MAC addresses, IP addresses, or Layer 4 port numbers to select the link. Port channel load balancing uses either source or destination addresses or ports, or both source and destination addresses or ports.

You can configure the load balancing mode to apply to all port channels that are configured on the entire device or on specified modules. The per-module configuration takes precedence over the load-balancing configuration for the entire device. You can configure one load balancing mode for the entire device, a different mode for specified modules, and another mode for the other specified modules. You cannot configure the load balancing method per port channel.

You can configure the type of load balancing algorithm used. You can choose the load balancing algorithm that determines which member port to select for egress traffic by looking at the fields in the frame.

**Note**

The default load balancing method uses source MAC addresses.

You can configure one of the following methods to load balance across the port channel:

- Destination MAC address
- Source MAC address
- Source and Destination MAC address
- Destination IP address and VLAN
- Source IP address and VLAN
- Source and destination IP address and VLAN
- Destination TCP/UDP port number
- Source TCP/UDP port number
- Source and destination TCP/UDP port number
- Destination IP address and TCP/UDP port number
- Source IP address and TCP/UDP port number
- Source and destination IP address and TCP/UDP port number
- Destination IP address, TCP/UDP port number, and VLAN
- Source IP address, TCP/UDP port number, and VLAN
- Source and destination IP address, TCP/UDP port number, and VLAN
- Destination IP address
- Source IP address
- Source and Destination IP address
- VLAN only
- Source Virtual Port ID

When you configure source IP address load balancing, the source MAC address is used to balance the traffic load. When you configure the destination MAC address load balancing method, the traffic load is balanced using the destination MAC address.

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

The load balancing methods that use port channels do not apply to multicast traffic. Regardless of the method configured, multicast traffic uses the following methods for load balancing with port channels:

- Multicast traffic with Layer 4 information—Source IP address, source port, destination IP address, and destination port
- Multicast traffic without Layer 4 information—Source IP address and destination IP address
- Non-IP multicast traffic—Source MAC address and destination MAC address

To configure port channel load balancing, see the [“Configuring Port Channel Load Balancing” procedure on page 5-25](#).

LACP

Link Aggregation Control Protocol (LACP) lets you configure up to 16 interfaces into a port channel. A maximum of eight interfaces can be active, and a maximum of eight interfaces can be placed in a standby state. [Figure 5-1](#) shows how individual links can be combined into LACP port channels and channel groups as well as function as individual links.

On the Cisco Nexus 1000V, LACP is enabled globally by default.



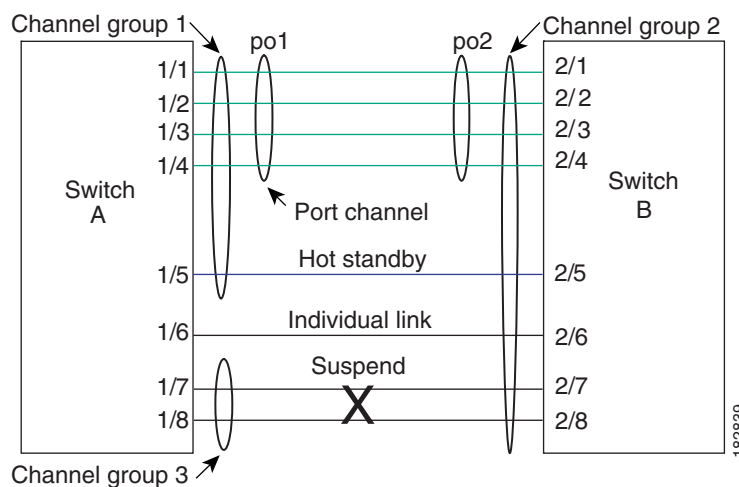
Note

When you delete the port channel, the associated channel group is automatically deleted. All member interfaces revert to their original configuration.

This section includes the following topics:

- [Port Channel Modes, page 5-6](#)
- [LACP ID Parameters, page 5-6](#)
- [LACP Marker Responders, page 5-7](#)
- [LACP-Enabled and Static Port Channels Differences, page 5-7](#)

Figure 5-1 Individual Links Combined into a Port Channel



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

Port Channel Modes

Individual interfaces in port channels are configured with channel modes. When you run static port channels with no aggregation protocol, the channel mode is always set to **on**.

You enable LACP for each channel by setting the channel mode for each interface to **active** or **passive**. You can configure either channel mode for individual links in the LACP channel group when you are adding the links to the channel group.

Table 5-1 describes the channel modes.

Table 5-1 Channel Modes for Individual Links in a Port Channel

Channel Mode	Description
passive	LACP mode that places a port into a passive negotiating state in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.
active	LACP mode that places a port into an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets.
on	<p>All static port channels (that are not running LACP) remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device displays an error message.</p> <p>You enable LACP on each channel by configuring the interface in that channel for the channel mode as either active or passive. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group.</p> <p>The default port channel mode is on.</p>

Both the passive and active modes allow LACP to negotiate between ports to determine if they can form a port channel based on criteria such as the port speed and the trunking state. The passive mode is useful when you do not know whether the remote system, or partner, supports LACP.

Ports can form an LACP port channel when they are in different LACP modes if the modes are compatible as in the following examples:

- A port in **active** mode can form a port channel successfully with another port that is in **active** mode.
- A port in **active** mode can form a port channel with another port in **passive** mode.
- A port in **passive** mode cannot form a port channel with another port that is also in **passive** mode, because neither port will initiate negotiation.
- A port in **on** mode is not running LACP and cannot form a port channel with another port that is in **active** or **passive** mode.

LACP ID Parameters

This section describes the LACP parameters in the following topics:

- [LACP System Priority, page 5-7](#)
- [LACP Port Priority, page 5-7](#)
- [LACP Administrative Key, page 5-7](#)

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

LACP System Priority

Each system that runs LACP has an LACP system priority value. You can accept the default value of 32768 for this parameter, or you can configure a value between 1 and 65535. LACP uses the system priority with the MAC address to form the system ID and also uses the system priority during negotiation with other devices. A higher system priority value means a lower priority.



Note

The LACP system ID is the combination of the LACP system priority value and the MAC address.

LACP Port Priority

Each port that is configured to use LACP has an LACP port priority. You can accept the default value of 32768 for the LACP port priority, or you can configure a value between 1 and 65535. LACP uses the port priority with the port number to form the port identifier.

LACP uses the port priority to decide which ports should be put in standby mode when there is a limitation that prevents all compatible ports from aggregating and which ports should be put into active mode. A higher port priority value means a lower priority for LACP. You can configure the port priority so that specified ports have a lower priority for LACP and are most likely to be chosen as active links, rather than hot-standby links.

LACP Administrative Key

LACP automatically configures an administrative key value that is equal to the channel-group number on each port configured to use LACP. The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by these factors:

- Port physical characteristics, such as the data rate and the duplex capability
- Configuration restrictions that you establish

LACP Marker Responders

You can dynamically redistribute the data traffic by using port channels. This redistribution may result from a removed or added link or a change in the load-balancing scheme. Traffic redistribution that occurs in the middle of a traffic flow can cause misordered frames.

LACP uses the Marker Protocol to ensure that frames are not duplicated or reordered due to this redistribution. The Marker Protocol detects when all the frames of a given traffic flow are successfully received at the remote end. LACP sends Marker PDUs on each of the port-channel links. The remote system responds to the Marker PDU once it receives all the frames received on this link prior to the Marker PDU. The remote system then sends a Marker Responder. Once the Marker Responders are received by the local system on all member links of the port channel, the local system can redistribute the frames in the traffic flow with no chance of misordering. The software supports only Marker Responders.

LACP-Enabled and Static Port Channels Differences

[Table 5-2](#) summarizes the major differences between port channels with LACP enabled and static port channels.

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

Table 5-2 Port Channels with LACP Enabled and Static Port Channels

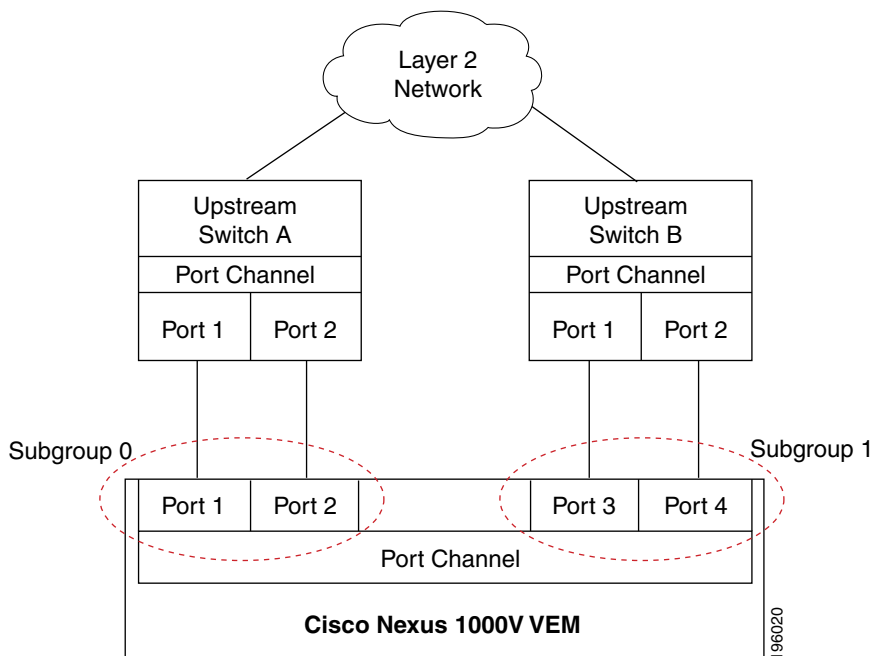
Configurations	Port Channels with LACP Enabled	Static Port Channels
Protocol applied	Enable globally	Not applicable
Channel mode of links	Can be either: <ul style="list-style-type: none"> Active Passive 	Can only be On
Maximum number of links in channel	16	8

vPC Host Mode

Virtual port channel in host mode (vPC-HM) allows member ports in a port channel to connect to multiple upstream switches. With vPC-HM, ports are grouped into subgroups (0–31) for traffic separation.

As shown in [Figure 5-2](#), for traffic separation using vPC-HM, member ports 1 and 2 are assigned to subgroup ID 0 and member ports 3 and 4 are assigned to subgroup ID 1.

Figure 5-2 Using vPC-HM to Connect a Port Channel to Multiple Upstream Switches



To configure an interface in vPC-HM, see the [“Configuring a Port Channel that Connects to Multiple Upstream Switches”](#) section on page 5-12.

vPC-HM can also be configured on a port profile. For more information, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)*.

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

See the “[Subgroup Creation Using CDP or Manual Method](#)” section on page 5-9 and the “[Interface Assignment Using Static Pinning](#)” section on page 5-9 to learn how subgroups are created and how interfaces are assigned.

Subgroup Creation Using CDP or Manual Method

If Cisco Discovery Protocol (CDP) is enabled on the upstream switches, then the subgroups can be automatically created using CDP information. If CDP is not enabled on the upstream switches, then you must manually create subgroups by assigning subgroup IDs to the Ethernet interfaces.

You configure this setting as part of the port channel configuration. For more information, see the “[Configuring a Port Channel that Connects to Multiple Upstream Switches](#)” section on page 5-12.

Interface Assignment Using Static Pinning

Static pinning allows you to assign (or pin) a vEthernet interface to a particular subgroup of a vPC-HM. This assignment allows traffic from the vEthernet interface to be forwarded only through the member ports in the subgroup. This feature assumes that you have manually configured subgroup IDs for the port members of the port channel.

To pin a vEthernet interface to a specific port channel subgroup, see the “[Configuring Static Pinning](#)” section on page 5-15.

You can also pin vEthernet interfaces to subgroups in port profile configuration mode. For more information, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)*.

High Availability

Port channels provide high availability by load balancing traffic across multiple ports. If a physical port fails, the port channel is still operational if there is an active member in the port channel.

Port channels support stateful and stateless restarts. A stateful restart occurs on a supervisor switchover. After the switchover, the Cisco Nexus 1000V applies the runtime configuration after the switchover.

Prerequisites for Port Channels

Port channeling has the following prerequisites:

- You are logged into the Cisco Nexus 1000V in EXEC mode.
- All ports for a single port channel must meet the compatibility requirements. See the “[Compatibility Checks](#)” section on page 5-2 for more information about the compatibility requirements.
- You can use virtual vPC-HM to configure a port channel even when the physical ports are connected to two different switches.

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

Guidelines and Limitations

Port channeling has the following guidelines and restrictions:

- Port channels across modules are not supported.
- Port channels can be formed with multiple upstream links only when they satisfy the compatibility requirements and under the following conditions:
 - The uplinks from the host are going to the same upstream switch.
 - The uplinks from the host going to multiple upstream switches are configured with vPC-HM.
- You can configure port channels using a port profile. For more information, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)*.
- You can configure up to 256 port channels,
- You can configure multiple port channels on a device.
- After you configure a port channel, the configuration that you apply to the port channel interface affects the port channel member ports. The configuration that you apply to the member ports affects only the member port where you apply the configuration.
- You must remove the port security information from a port before you can add that port to a port channel. Similarly, you cannot apply the port security configuration to a port that is a member of a channel group.
- You can configure ports that belong to a port channel group as PVLAN ports.
- All ports in the port channel must be in the same Cisco Nexus 1000V module; you cannot configure port channels across Cisco Nexus 1000V modules.
- Any configuration changes that you apply to the port channel is applied to every member interface of that port channel.
- Channel member ports cannot be a source or destination SPAN port.
- In order to support LACP when inband/AIPC are also carried over the link, you must configure the following commands on the ports connected to the ESX host:
 - **spanning-tree portfast trunk**
 - **spanning-tree bpdupfilter enable**



Note If you have a separate dedicated NIC for control traffic, these settings are not required.

- There should be at least two links that connect two switches when inband/AIPC are also carried over the LACP channel.

Default Settings

The following table lists the default settings for port channels.

Parameters	Default
Port channel	Admin up
LACP	Enabled

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

Parameters	Default
Load balancing method for Layer 2 interfaces	Source and destination MAC address
Load balancing per module	Disabled
Channel mode	on

Configuring Port Channels

This section includes the following topics:

- [Configuring a Port Channel that Connects to a Single Upstream Switch, page 5-11](#)
- [Configuring a Port Channel that Connects to Multiple Upstream Switches, page 5-12](#)
- [Configuring Static Pinning, page 5-15](#)
- [Removing the Port Channel and Group, page 5-17](#)
- [Adding a Layer 2 Port to a Channel Group, page 5-17](#)
- [Removing a Port from a Channel Group, page 5-19](#)
- [Shutting Down and Restarting a Port Channel Interface, page 5-20](#)
- [Configuring a Port Channel Description, page 5-21](#)
- [Configuring LACP Port Channel Port Modes, page 5-22](#)
- [Configuring the Speed and Duplex Settings for a Port Channel Interface, page 5-23](#)
- [Configuring Port Channel Load Balancing, page 5-25](#)
- [Configuring Port Channel Load Balancing, page 5-25](#)
- [Restoring the Default Load-Balancing Method, page 5-26](#)



Note

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

Configuring a Port Channel that Connects to a Single Upstream Switch

Use this procedure to configure a port channel whose member ports connect to a single upstream switch. If the member ports connect to multiple upstream switches, see the [“Configuring a Port Channel that Connects to Multiple Upstream Switches”](#) section on page 5-12.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- When you create a port channel, an associated channel group is automatically created.

SUMMARY STEPS

1. `config t`
2. `interface port-channel channel-number`

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

- 3. `show port-channel summary`
- 4. `copy running-config startup-config`

DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code> Example: <code>n1000v# config t</code> <code>n1000v(config)#</code>	Places you into the global configuration mode.
Step 2	<code>interface port-channel channel-number</code> Example: <code>n1000v(config)# interface port-channel 1</code> <code>n1000v(config-if)#</code>	Places you into the interface configuration mode for the specified port channel. For <i>channel-number</i> , the range is from 1 to 4096. If the channel group does not already exist, it is automatically created as a port channel group whose member ports all connect to the same upstream switch.
Step 3	<code>show port-channel summary</code> Example: <code>n1000v(config-if)# show port-channel summary</code>	(Optional) Displays the port channel configuration.
Step 4	<code>copy running-config startup-config</code> Example: <code>n1000v(config-if)# copy running-config startup-config</code>	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

EXAMPLES

The following example shows how to create a port channel:

```
n1000v# config t
n1000v(config)# interface port-channel 1
```

Configuring a Port Channel that Connects to Multiple Upstream Switches

Use this procedure to configure a port channel in virtual port channel host mode (vPC-HM).
If the member ports connect to a single upstream switch, see the [“Configuring a Port Channel that Connects to a Single Upstream Switch”](#) section on page 5-11.

BEFORE YOU BEGIN

- Before beginning this procedure, you must know or do the following:
- You are logged in to the CLI in EXEC mode.
 - In vPC-HM, the port channel member ports connect to multiple upstream switches, and the traffic must be managed in separate subgroups.
 - When you create a port channel, an associated channel group is automatically created.

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

- vPC-HM is only supported in port channels configured in the **on** mode. vPC-HM is not supported for LACP channels that use the **active** and **passive** modes.
- You need to know whether CDP is configured in the upstream switches. If configured, then CDP creates a subgroup for each upstream switch to manage its traffic separately. If not configured, then you must manually configure subgroups to manage the traffic flow on the separate switches.
- If you are using CDP with the default CDP timer (60 seconds), links that advertise that they are in service and then out of service in quick succession can take up to 60 seconds to be returned to service.
- If any subgroup has more than one member port, you must configure a port channel for the member ports of each subgroup on the upstream switch.
- If vPC-HM is not configured when port channels connect to multiple upstream switches, then the VMs behind the Cisco Nexus 1000V receive duplicate packets from the network for unknown unicast floods, multicast floods, and broadcasts.
- The **sub-group** command used in this procedure overrides any subgroup configuration specified in the port profile inherited by the port channel interface.
- You can also configure vPC-HM on the port profile. For more information, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)*.

SUMMARY STEPS

1. **config t**
2. **interface port-channel** *channel-number*
3. Do one of the following:
 - Enter **sub-group cdp** and proceed to step 8.
 - Enter **sub-group manual** and proceed to the next step.
4. **exit**
5. **interface ethernet** *range*
6. **sub-group-id** *number*
7. Repeat steps 5. and 6. for each port member connected to an upstream switch that is not configured for CDP.
8. **show port-channel summary**
9. **show running-config interface ethernet** *range*
10. **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)#	Places you into the global configuration Mode.
Step 2	interface port-channel <i>channel-number</i> Example: n1000v(config)# interface port-channel 12 n1000v(config-if)#	Places you into the interface configuration mode for the specified port channel. <ul style="list-style-type: none"> • <i>channel-number</i>: The range is from 1 to 4096. If the channel group does not already exist, it is automatically created as a port channel group whose member ports all connect to the same upstream switch.
Step 3	Do one of the following: <ul style="list-style-type: none"> • sub-group cdp • sub-group manual Example: n1000v(config-if)# sub-group cdp Example: n1000v(config-if)# sub-group manual	The sub-group cdp command identifies the port channel as being in vPC-HM and configures CDP as the information used to automatically create subgroups for managing the traffic flow. Proceed to Step 8 . The sub-group manual command identifies the port channel as being in vPC-HM and sets the configuration method to manual. This method is used if CDP is not configured on the upstream switch(es). Proceed to the next step. Note These commands overrides any subgroup configuration specified in the port-profile inherited by the port channel interface.
Step 4	exit Example: n1000v(config-if)# exit n1000v(config)# e	Exits Interface Configuration mode and returns you to Configuration mode.
Step 5	interface ethernet <i>range</i> Example: n1000v(config)# interface ethernet 3/2-3 n1000v(config-if)#	Places you into interface configuration mode for the specified interface range.
Step 6	sub-group-id <i>number</i> Example: n1000v(config-if)# sub-group-id 0	Configures the specified port channel members as vPC-HM so that the specified subgroup can manage traffic for one of the two upstream switches. For <i>number</i> , the range is from 0 to 31. Tip Assign the same subgroup ID for Ethernet ports connected to the same upstream switch.
Step 7	Repeat Step 5 and Step 6 for each port member connected to an upstream switch that is not configured for CDP.	

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

	Command	Purpose
Step 8	show port-channel summary Example: n1000v(config-if)# show port-channel summary	(Optional) Displays the port channel configuration.
Step 9	show running-config interface ethernet range Example: n1000v(config-if)# show running-config interface ethernet 3/2-3	(Optional) Displays the subgroup ID configuration.
Step 10	copy running-config startup-config Example: n1000v(config-if)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Configuring Static Pinning

Use this procedure to configure static pinning on a vEthernet interface.



Note

You can also configure static pinning on a port profile. For information, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)*.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **config t**
2. **interface vethernet** *interface-number*
3. **pinning id** *sub-group_id*
4. **show running-config interface vethernet** *interface-number*
5. **module vem** *module_number* **execute vemcmd show pinning**
6. **copy running-config startup-config**

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

DETAILED STEPS

	Command	Description
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you in the global configuration mode.
Step 2	interface vethernet <i>interface-number</i> Example: n1000v(config)# interface vethernet 1 n1000v(config-if)#	Places you into the interface configuration mode for the specified interface. For <i>interface-number</i> , the range is from 1 to 1048575.
Step 3	pinning id <i>sub-group_id</i> Example: n1000v(config-if)# pinning id 0	Assigns (or pins) a vEthernet interface to a specific port channel subgroup. For <i>sub_group_id</i> , the range is from 0 to 31.
Step 4	show running-config interface vethernet <i>interface-number</i> Example: n1000v(config-if)# show running-config interface vethernet 1	(Optional) Displays the pinning configuration of the specified interface. For <i>interface-number</i> , the range is from 1 to 1048575.
Step 5	module vem <i>module_number</i> execute vemcmd show pinning Example: n1000v(config-if)# module vem 3 execute vemcmd show pinning	(Optional) Displays the pinning configuration on the specified VEM.
Step 6	copy running-config startup-config Example: n1000v(config-if)# 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 pin subgroup ID 0 to vEthernet interface 1:

```
n1000v(config)# config t
n1000v(config)# interface vethernet 1
n1000v(config-if)# pinning id 0
n1000v(config-if)# show running-config interface vethernet 1
version 4.0(4)SV1(2)

interface Vethernet3
 service-policy type qos input policy1
 pinning id 0

n1000v(config-if)# exit
n1000v(config)# exit
n1000v# module vem 3 execute vemcmd show pinning
LTL      IfIndex  PC_LTL  VSM_SGID  VEM_SGID  Eff_SGID
  48      1b040000    304        0         0         0

n1000v(config-if)# copy running-config startup-config
```


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

Removing the Port Channel and Group

Use this procedure to remove a port channel and delete the associated channel group.

BEFORE YOU BEGIN

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

-
- You are logged in to the CLI in EXEC mode.
- For details about how the interface configuration changes when you delete a port channel, see the [“Compatibility Checks” section on page 5-2](#).

SUMMARY STEPS

1. **config t**
2. **no channel-group** *channel-number*
3. **no interface port-channel** *channel-number*

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into the global configuration mode.
Step 2	no channel-group <i>channel-number</i> Example: n1000v(config)# no channel-group port-channel 1	Removes the channel group configuration from an interface.
Step 3	no interface port-channel <i>channel-number</i> Example: n1000v(config)# no interface port-channel 1	Removes the port channel and deletes the associated channel group.

Adding a Layer 2 Port to a Channel Group

Use this procedure to add a Layer 2 port to a channel group.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.

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

- All Layer 2 member ports must run in full-duplex mode and at the same speed.
- If the port channel does not yet exist, it is automatically created when you create the channel group.


Note

If you cannot add a particular interface to a particular port channel, an error message signals a compatibility problem.

SUMMARY STEPS

1. **config t**
2. **interface ethernet** *slot/port*
3. **switchport mode trunk**
4. **switchport trunk** {**allowed vlan** *vlan-id* | **native** *vlan-id*}
5. **channel-group** *channel-number* [**mode** {**on** | **active** | **passive**}]
6. **show interface type** *slot/port*
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into the global configuration mode.
Step 2	interface ethernet <i>slot/port</i> Example: n1000v(config)# interface ethernet 1/4 n1000v(config-if)	Places you into the interface configuration mode for the specified interface.
Step 3	switchport mode trunk Example: n1000v(config-if)# switchport mode trunk	(Optional) Configures the interface as a trunk port.
Step 4	switchport trunk { allowed vlan <i>vlan-id</i> native <i>vlan-id</i> } Example: n1000v(config-if)# switchport trunk native 3	(Optional) Configures necessary parameters for a trunk port.
Step 5	channel-group <i>channel-number</i> [mode { on active passive }] Example: n1000v(config-if)# channel-group 5	Configures the port in a channel group and sets the mode. <ul style="list-style-type: none"> • <i>channel number</i>—The <i>channel-number</i> range is from 1 to 4096. The port channel associated with this channel group is automatically created if the port channel does not already exist. • mode—All static port channel interfaces are set to mode on.

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

	Command	Purpose
Step 6	show interface <i>type slot/port</i> Example: n1000v(config-if)# show interface port channel 5	(Optional) Displays interface information.
Step 7	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 add the Ethernet interface 1/4 to channel group 5:

```
n1000v# config t
n1000v(config)# interface ethernet 1/4
n1000v(config-if)# switchport
n1000v(config-if)# channel-group 5
```

Removing a Port from a Channel Group

Use this procedure to remove a port from a channel group and return the port to its original configuration.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **config t**
2. **no channel-group**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into the global configuration mode.
Step 2	no channel-group Example: n1000v(config)# no channel-group	Removes the port from the channel group and returns it to its original configuration.

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

Shutting Down and Restarting a Port Channel Interface

Use this procedure to shut down and restart a port channel interface.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- When you shut down a port channel interface, no traffic passes, and the interface is administratively down.

SUMMARY STEPS

1. **config t**
2. **interface port-channel** *channel-number*
3. **shutdown** | **no shutdown**
4. **show interface port-channel** *channel-number*
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into the global configuration mode.
Step 2	interface port-channel <i>channel-number</i> Example: n1000v(config)# interface port-channel 2 n1000v(config-if)	Places you into the interface configuration mode for the specified port channel interface.
Step 3	shutdown Example: n1000v(config-if)# shutdown no shutdown Example: n1000v(config-if)# no shutdown	Shuts down the interface. No traffic passes and the interface displays as administratively down. The default is no shutdown . Brings the interface back up. The interface displays as administratively up. If there are no operational problems, traffic passes. The default is no shutdown .
Step 4	show interface port-channel <i>channel-number</i> Example: n1000v(config-if)# show interface port-channel 2	(Optional) Displays interface information for the specified port channel.
Step 5	copy running-config startup-config Example: n1000v(config-if)# copy running-config startup-config	(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 bring up the interface for port channel 2:

```
n1000v# config t
n1000v(config)# interface port-channel 2
n1000v(config-if)# no shutdown
```

Configuring a Port Channel Description

Use this procedure to configure a description for a port channel.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

- config t**
- interface port-channel** *channel-number*
- description** *string*
- show interface port-channel** *channel-number*
- copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into the global configuration mode.
Step 2	interface port-channel <i>channel-number</i> Example: n1000v(config)# interface port-channel 2 n1000v(config-if)	Places you into interface configuration mode for the specified port channel interface. For <i>channel number</i> , the range is from 1 to 4096. The port channel associated with this channel group is automatically created if the port channel does not already exist.
Step 3	description <i>string</i> Example: n1000v(config-if)# description engineering	Adds a description to the port channel interface. For <i>string</i> , the description can be up to 80 alphanumeric characters. Note You do not need to use quotations around descriptions that include spaces.

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

	Command	Purpose
Step 4	show interface port-channel <i>channel-number</i> Example: n1000v(config-if)# show interface port-channel 2	(Optional) Displays interface information for the specified port channel.
Step 5	copy running-config startup-config Example: n1000v(config-if)# 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 add a description to port channel 2:

```
n1000v# config t
n1000v(config)# interface port-channel 2
n1000v(config-if)# description engineering
```

Configuring LACP Port Channel Port Modes

Use this procedure to configure the LACP mode for individual links in an LACP port channel. This setting indicates whether the link is allowed to operate with LACP.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- The default port channel mode is **on**.
- When you configure port channels with no associated aggregation protocol, all interfaces on both sides of the link remain in the **on** channel mode.

SUMMARY STEPS

1. **config t**
2. **interface** *interface*
3. **channel-group** *number* **mode** {**active** | **on** | **passive**}
4. **show port-channel summary**
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)#	Places you in the global configuration mode.
Step 2	interface interface Example 1: n1000v(config)# interface ethernet 1/4 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	channel-group number mode {active on passive} Example: n1000v(config-if)# channel-group 5 mode active	Specifies the port mode as active or passive for the specified link. When you run port channels with no associated aggregation protocol, the port-channel mode is always on. The default port channel mode is on.
Step 4	show port-channel summary Example: n1000v(config-if)# show port-channel summary	(Optional) Displays summary information about the port channels.
Step 5	copy running-config startup-config Example: n1000v(config-if)# 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 LACP-enabled interface to the active port channel mode for Ethernet interface 1/4 in channel group 5:

```
n1000v# config t
n1000v (config)# interface ethernet 1/4
n1000v(config-if)# channel-group 5 mode active
```

Configuring the Speed and Duplex Settings for a Port Channel Interface

Use this procedure to configure the speed and duplex settings for a port channel interface.

BEFORE YOU BEGIN

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

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

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

- config t**
- interface port-channel** *channel-number*
- speed** {10 | 100 | 1000 | auto}
- duplex** {auto | full | half}
- show interface port-channel** *channel-number*
- copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into the global configuration mode.
Step 2	interface port-channel <i>channel-number</i> Example: n1000v(config)# interface port-channel 2 n1000v(config-if)	Specifies the port channel interface that you want to configure and enters the interface mode.
Step 3	speed {10 100 1000 auto} Example: n1000v(config-if)# speed auto	Sets the speed for the port channel interface. The default is auto for autonegotiation.
Step 4	duplex {auto full half} Example: n1000v(config-if)# speed auto	Sets the duplex mode for the port channel interface. The default is auto for autonegotiation.
Step 5	show interface port-channel <i>channel-number</i> Example: n1000v(config-if)# show interface port-channel 2	(Optional) Displays interface information for the specified port channel.
Step 6	copy running-config startup-config Example: n1000v(config-if)# 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 port channel 2 to 100 Mbps:

```
n1000v# config t
n1000v(config)# interface port channel 2
n1000v(config-if)# speed 100
```


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

Configuring Port Channel Load Balancing

Use this procedure to configure port channel load balancing.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- You can configure port channel load balancing for the entire device or for a single module.
- Module-based load balancing takes precedence over device-based load balancing.
- The default load balancing method is the source MAC address.
- For more information about port channel load balance, see the [“Load Balancing Using Port Channels”](#) section on page 5-4.

SUMMARY STEPS

1. **config t**
2. **port-channel load-balance ethernet {dest-ip-port | dest-ip-port-vlan | destination-ip-vlan | destination-mac | destination-port | source-dest-ip-port | source-dest-ip-port-vlan | source-dest-ip-vlan | source-dest-mac | source-dest-port | source-ip-port | source-ip-port-vlan | source-ip-vlan | source-mac | source-port | source-virtual-port-id | vlan-only}**
3. **show port-channel load-balance**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into the global configuration mode.
Step 2	port-channel load-balance ethernet {dest-ip-port dest-ip-port-vlan destination-ip-vlan destination-mac destination-port source-dest-ip-port source-dest-ip-port-vlan source-dest-ip-vlan source-dest-mac source-dest-port source-ip-port source-ip-port-vlan source-ip-vlan source-mac source-port source-virtual-port-id vlan-only} Example: n1000v(config)# port-channel load-balance ethernet source-destination-mac	Configures the load balance method for the device or module. The range depends on the device. The default load balancing method uses the source MAC address.

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

	Command	Purpose
Step 3	show port-channel load-balance Example: n1000v(config)# show port-channel load-balance	(Optional) Displays the port channel load-balancing method.
Step 4	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 configure the source IP load-balancing method for port channels on module 5:

```
n1000v# config t
n1000v(config)# port-channel load-balance ethernet source-ip module 5
```

Restoring the Default Load-Balancing Method

Use this procedure to restore the default load-balancing method.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **config t**
2. **no port-channel load-balance ethernet**
3. **show port-channel load-balance**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into the global configuration mode.
Step 2	no port-channel load-balance ethernet Example: n1000v(config)# no port-channel load-balance ethernet	Restores the default load-balancing method, which is the source MAC address.

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

	Command	Purpose
Step 3	show port-channel load-balance Example: n1000v(config)# show port-channel load-balance	(Optional) Displays the port channel load-balancing method.
Step 4	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.

Verifying the Port Channel Configuration

To display the port channel configuration, perform the following tasks

Command	Purpose
show interface port-channel <i>channel-number</i>	Displays the status of a port channel interface.
show port-channel compatibility-parameters	Displays the parameters that must be the same among the member ports in order to join a port channel.
show port-channel database [interface port-channel <i>channel-number</i>]	Displays the aggregation state for one or more port channel interfaces.
show port-channel load-balance	Displays the type of load balancing in use for port channels.
show port-channel summary	Displays a summary for the port channel interfaces.
show port-channel traffic	Displays the traffic statistics for port channels.
show port-channel usage	Displays the range of used and unused channel numbers.
show running-config interface ethernet <i>port/slot</i>	Displays information about the running configuration of the specified Ethernet interface.
show running-config interface port-channel <i>channel-number</i>	Displays information on the running configuration of the port channel.
show running-config interface vethernet <i>interface-number</i>	Displays information about the running configuration of the specified vEthernet interface.

For more information about the command output, see the *Cisco Nexus 1000V Command Reference, Release 4.0(4)SVI(2)*.

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

Monitoring the Port Channel Configuration

You can display port channel interface configuration information.

Command	Purpose
<code>clear counters interface port-channel channel-number</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 and output packets and bytes.
<code>show interface counters errors [module module]</code>	Displays information on the number of error packets.

Configuration Example for Port Channels

The following example shows how to create a port channel and add two Layer 2 interfaces to that port channel:

```
n1000v# config t
n1000v(config)# interface port-channel 5
n1000v(config-if)# interface ethernet 1/4
n1000v(config-if)# switchport
n1000v(config-if)# channel-group 5 mode active
n1000v(config-if)# interface ethernet 1/7
n1000v(config-if)# switchport
n1000v(config-if)# channel-group 5 mode
```

Additional References

For additional information related to implementing port channels, see the following sections:

- [Related Documents, page 5-29](#)
- [Standards, page 5-29](#)

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

Related Documents

Related Topic	Document Title
Configuring Layer 2 interface	Chapter 3, “Configuring Layer 2 Interfaces”
System management	<i>Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(2)</i>
Release Notes	<i>Cisco Nexus 1000V Release Notes, Release 4.0(4)SV1(2)</i>

Standards

Standards	Title
IEEE 802.3ad	—

Feature History for Port Channels

This section provides the feature history for port channels.

Feature Name	Releases	Feature Information
Port Profiles	4.0	This feature was introduced.
vPC-Host Mode	4.0(4)SV1(2)	Support for manual creation of subgroups.
Static Pinning	4.0(4)SV1(2)	Support for attaching (or pinning) a vEthernet interface to a specific port channel subgroup.

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



CHAPTER 6

Supported RFCs

This section lists the supported IETF RFCs for interfaces.

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

Beta Release 4.0(4)SV1(2) Draft -- Cisco Confidential



CHAPTER 7

Interface Configuration Limits

Table 7-1 lists the configuration limits for interfaces.

Table 7-1 *Interface Configuration Limits*

Interface	Maximum per DVS	Maximum per Host
vEthernet interfaces	2000	216
vEthernet trunks	256	8
Port channels	256	8

Beta Release 4.0(4)SV1(2) Draft -- Cisco Confidential



INDEX

A

access ports

- configuration example [3-14, 4-9](#)
- configuring [3-4](#)
- default setting [3-4, 4-2](#)
- host ports [3-2, 3-6](#)
- VLANs [3-2](#)

administrative state

- configuring [2-17](#)

administrative status

- defined [2-3](#)

asymmetric port channel [5-8](#)

B

bandwidth

- configuring [2-14](#)
- dedicated [2-8](#)

C

CDP

- configuring [2-19](#)
- defined [2-3](#)

channel modes

- active [5-6, 5-22](#)
- configuring [5-22](#)
- default setting [5-6](#)
- LACP [5-6](#)
- passive [5-6, 5-22](#)
- port channels [5-6](#)

Cisco Discovery Protocol

See CDP.

class-map limits [7-1](#)

clear counters command [2-21](#)

configuration limits [7-1](#)

D

default settings

- access ports [3-4, 4-2](#)
- port channels [5-6, 5-10](#)
- trunk ports [3-4, 4-2](#)

description

- configuring [2-6](#)
- defined [2-2](#)

documentation

- additional publications [iv-xi](#)

duplex mode

- configuring [2-9, 5-23](#)
- defined [2-2](#)

E

examples

- access ports [3-14, 4-9](#)
- trunk ports [3-14, 4-9](#)

G

guidelines

- port channels [5-10](#)

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

I

IEEE 802.1Q

trunk ports [3-2](#)

interface

access port [3-4](#)

administrative state

configuring [2-17](#)

administrative status

defined [2-3](#)

bandwidth

configuring [2-14](#)

dedicated [2-8](#)

CDP

configuring [2-19](#)

defined [2-3](#)

description

configuring [2-6](#)

defined [2-2](#)

duplex mode

configuring [2-9](#)

defined [2-2](#)

host ports [3-6](#)

jumbo MTU, configuring [2-12](#)

LACP [5-5](#)

Layer 2 [3-1](#)

MTU

defined [2-3](#)

restarting [2-17](#)

shutting down [2-17](#)

specifying [2-5](#)

speed

configuring [2-9](#)

defined [2-2](#)

statistics [3-14](#)

throughput delay

configuring [2-16](#)

trunk ports [3-7](#)

tagged native VLAN traffic [3-12](#)

types, specifying [2-5](#)

verifying [3-14](#)

verifying vEth [4-7](#)

J

jumbo MTU, configuring [2-12](#)

L

LACP

admin key [5-7](#)

channel groups [5-5](#)

channel modes [5-6](#)

description [5-5 to 5-7](#)

MAC address [5-7](#)

Marker Protocol [5-7](#)

number of members per channel [5-5](#)

port channels [5-5](#)

system ID [5-7](#)

system priority [5-7](#)

Layer 2, interface [3-1](#)

limitations

configuration [7-1](#)

port channels [5-10](#)

Link Aggregation Control Protocol. See LACP

load balancing

algorithms [5-4](#)

multicast traffic [5-5](#)

port channels [5-4, 5-25](#)

M

match criteria limit [7-1](#)

maximum transmission unit. See MTU.

MTU

defined [2-3](#)

multicast traffic

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

load balancing using port channels [5-5](#)

P

PAgP, unsupported [5-2](#)

policy map limits [7-1](#)

Port Aggregation Protocol. See PAgP.

port channel, host mode [5-8](#)

port channels

compatibility checks [5-2](#)

compatibility requirements [5-17](#)

configuring [5-2](#)

creating [5-11](#)

default settings [5-10](#)

description [5-21](#)

duplex mode [5-23](#)

guidelines [5-10](#)

interoperation with other features [5-10](#)

LACP [5-5](#)

Layer 2 port, adding [5-17](#)

limitations [5-10](#)

load balancing [5-4, 5-25](#)

modes [5-22](#)

purpose [5-2](#)

speed [5-23](#)

statistics [5-28](#)

trunk ports [3-3](#)

verifying [5-27](#)

ports

access [3-1](#)

multiple VLANs [3-1](#)

trunks [3-1](#)

R

related documents [iv-xi](#)

S

service policy limits [7-1](#)

speed

configuring [2-9](#)

defined [2-2](#)

port channel [5-23](#)

statistics

interface [3-14](#)

port channels [5-28](#)

T

throughput delay

configuring [2-16](#)

transceivers

using Cisco supported transceivers [2-4](#)

trunk ports

802.1X [3-3](#)

allowed VLANs [3-11](#)

configuration example [3-14, 4-9](#)

configuring [3-7](#)

default settings [3-4, 4-2](#)

native VLAN ID [3-9](#)

port channels [3-3](#)

tagging VLANs [3-2](#)

VLANs [3-2](#)

V

verifying

interface [3-14](#)

Layer 2 interfaces [3-14](#)

port channels [5-27](#)

vEth interface [4-7](#)

vEthernet Interface

verifying [4-7](#)

vethernet interface

pvlan command example [4-5](#)

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

vPC-HM

about [5-8](#)