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

Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(1)

June 7, 2010

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-19414-02

Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(1)

CONTENTS

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

Preface

This document, *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(1)*, provides information for configuring Cisco Nexus 1000V interfaces.

This preface includes the following topics:

Audience

This guide is for experienced network system users.

Document Organization

This document is organized into the following chapters:

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

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

Document Conventions

Command descriptions use these conventions:

boldface font	Commands and keywords are in boldface.
italic font	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:

`screen font`	Terminal sessions and information the device displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
`italic screen font`	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.

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(1)

Cisco Nexus 1000V and VMware Compatibility Information, Release 4.0(4)SV1(1)

Install and Upgrade

Cisco Nexus 1000V Software Installation Guide, Release 4.0(4)SV1(1)

Cisco Nexus 1000V Virtual Ethernet Module Software Installation Guide, Release 4.0(4)SV1(1)

Configuration Guides

Cisco Nexus 1000V License Configuration Guide, Release 4.0(4)SV1(1)

Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(1)

Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(1)

Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(1)

Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(1)

Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.0(4)SV1(1)

Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(1)

Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(1)

Cisco Nexus 1000V High Availability and Redundancy Reference, Release 4.0(4)SV1(1)

Reference Guides

Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(1)

Cisco Nexus 1000V MIB Quick Reference

Troubleshooting and Alerts

Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(1)

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.

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

CHAPTER 1

Overview

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

This chapter includes the following sections:

Simplifying Interface Configuration with Port Profiles

In Cisco Nexus 1000V, port profiles are used to configure interfaces. A port profile can be assigned to multiple interfaces giving them all the same configuration. Changes to the port profile can be propagated automatically to the configuration of any interface assigned to it.

In VMware VirtualCenter (VC) a port profile is represented as a port group. The vEthernet or Ethernet interfaces are assigned in VC to a port profile for:

- Defining port configuration by policy.
- Applying a single policy across a large number of ports.
- Supporting both vEthernet and Ethernet ports.

Port profiles that are configured as uplinks, can be assigned by the server administrator to physical ports (a vmnic or a pnic). Port profiles that are not configured as uplinks can be assigned to a VM virtual port.

Note While manual interface configuration overrides that of the port profile, it is not the recommended process. Manual interface configuration is only used, for example, to quickly test a change or allow a port to be disabled without having to change the inherited port profile.

For more information about port profiles, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(1)*.

For more information about assigning port profiles, see your VMware documentation.

To verify that the profiles are assigned as expected, use the following show commands:

show port-profile usage

show running-config interface *interface-id*

Note: The output of the command **show running-config interface** *interface-id* shows a config line such as, `inherit port-profile MyProfile,` indicating the inherited port profile.

Note Inherited port profiles cannot be changed or removed from an interface using the Cisco Nexus 1000V CLI. This can only be done through the VC.

Note Inherited port profiles are automatically configured by the Cisco Nexus 1000V when the ports are attached on the hosts. This is done by matching up the VMware port group assigned by the system administrator with the port profile that created it.

Information About Interfaces

This section includes the following topics:

Ethernet Interfaces

Ethernet interfaces include access ports, trunk ports, private VLAN hosts and promiscuous ports, and routed ports.

This section includes the following topics:

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.”

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 having its own unique set of rules regulating the ability of each connected endpoint to communicate with other connected endpoints within the same private VLAN domain.

For more information about PVLAN, see the document, *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(1)*.

Virtual Ethernet Interfaces

Virtual Ethernet (vEthernet or vEth) interfaces are logical interfaces. Each vEth interface corresponds to a switch interface connected to a virtual port. These include the following interface types:

- VM (interfaces connected to VM NICs)
- service console
- vmkernel

The vEth 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(1)*.

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."

Configuration Limits

Table 1-1 lists the Cisco Nexus 1000V Release 4.0(4)SV1(1) configuration limits for port channels.

Table 1-1 Cisco NX-OS Release 4.1 Configuration Limits

Feature	Maximum Limit
Active VLANs	512
Port channels	256

High Availability for Interfaces

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

CHAPTER 2

Configuring Interface Parameters

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

This chapter includes the following sections:

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

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 5-18.

For information about configuring this parameter for other interfaces, see the "Configuring the Description" section on page 2-7.

Speed Mode and Duplex Mode

The speed mode and duplex mode are interrelated for each Ethernet and management interface. By default, each of these interfaces autonegotiates its speed and duplex mode 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 setting 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 mode and duplex mode for port channel interfaces, see the "Configuring the Speed and Duplex Settings for a Port Channel Interface" section on page 5-21.

For information about setting the speed and duplex speed for other interfaces, see the "Configuring the Interface Speed and Duplex Mode" section on page 2-10.

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, each port has an MTU of 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 9216 bytes in size, which is also the default system jumbo MTU size.

On a Layer 3 interface, you can configure an MTU size between 576 and 9216 bytes. You can configure up to 64 MTU settings for each I/O module.

Note The global LAN port MTU size applies to the traffic through a Layer 3 Ethernet LAN port that is configured with a non-default MTU size.

For a Layer 2 port, you can configure an MTU size that is either the system default (1500 bytes) or the system jumbo MTU size (initially 9216 bytes).

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

For information about setting the MTU size, see the "Configuring the MTU Size" section on page 2-12.

Bandwidth

Ethernet ports have a fixed bandwidth of 1,000,000 Kb at the physical level. Layer 3 protocols use a bandwidth value that you can set for calculating their internal metrics. The value that you set is used for informational purposes only by the Layer 3 protocols—it does not change the fixed bandwidth at the physical level. For example, the Interior Gateway Routing Protocol (IGRP) uses the minimum path bandwidth to determine a routing metric, but the bandwidth at the physical level remains 1,000,000 Kb.

For information see the "Configuring Bandwidth" section on page 2-15.

Throughput Delay

Specifying a value for the throughput-delay parameter provides a value used by Layer 3 protocols; it does not change the actual throughput delay of an interface. The Layer 3 protocols can use this value to make operating decisions. For example, the IGRP can use the delay setting to differentiate between a satellite link and a land link. The delay value that you set is in the tens of microseconds.

For information see the "Configuring the Throughput Delay" section on page 2-16.

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 information see the following:

- "Shutting Down and Restarting a Port Channel Interface" section on page 5-17.
- "Shutting Down and Activating the Interface" section on 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.

For information see the following:

- "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.

You can create a Layer 2 port channel by bundling compatible Layer 2 interfaces, or you can create Layer 3 port channels by bundling compatible Layer 3 interfaces. You cannot combine Layer 2 and Layer 3 interfaces in the same port channel.

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.

Guidelines and Limitations

Follow these guidelines and limitations for configuring the basic interface parameters:

- 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.
- A port can be either a Layer 2 or a Layer 3 interface; it cannot be both simultaneously.

  By default, each port is a Layer 3 interface. You can change a Layer 3 interface into a Layer 2 interface by using the **switchport** command. Conversely, you can change a Layer 2 interface into a Layer 3 interface by using the **no switchport** command.
- 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 allownegotiation of the speed and duplex mode 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 mode if the connecting port is configured to a value other than auto.

Caution 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 the Interfaces to Configure

Before you can configure the parameters for one or more interfaces of the same type, you must specify the type and the identities of the interfaces. The following table shows the interface types and identities that you should use for specifying the Ethernet and management interfaces.

Interface Type	Identity
Ethernet	I/O module slot numbers and port numbers on the module.
Management	0 (for port 0)

To verify the current configuration of interfaces, you can display their properties. Use the **show interface** command along with a specification of the interface type and identities.

SUMMARY STEPS

1. **config t**
2. **interface** *interface*

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into the CLI Global Configuration mode.
Step 2	**interface** *type number*	Specifies the interface that you are configuring. For an Ethernet port, use "ethernet *slot*/*port*." For the management interface, use "mgmt0." **Note** You do not need to add a space between the interface type and the port or slot/port number. For example, for the Ethernet slot 4, port 5 interface, you can specify either "ethernet 4/5" or "ethernet4/5." The management interface is either "mgmt0" or "mgmt 0."
	Example 1: n1000v(config)# interface ethernet 2/1 n1000v(config-if)#	This example shows how to specify the slot 2, port 1 Ethernet interface.
	Example 2: n1000v(config)# interface mgmt0 n1000v(config-if)#	This example shows how to specify the management interface.

Configuring the Description

You can provide textual interface descriptions for the Ethernet and management interfaces. Descriptions can be a maximum of 80 case-sensitive alphanumeric characters.

SUMMARY STEPS

1. **config t**
2. **interface** *interface*
3. **description** *text*
4. **show 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 CLI Global Configuration mode.
Step 2	**interface** *interface* **Example:** n1000v(config)# interface ethernet 2/1 n1000v(config-if)# n1000v(config)# interface mgmt0 n1000v(config-if)#	Specifies an Ethernet or vEthernet interface to configure, and places you into the Interface Configuration mode for that interface. Example 1 shows how to specify the slot 2 port, 1 Ethernet interface. Example 2 shows how to specify the management interface.
Step 3	**description** *text* **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.
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.

This 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)#
```

Dedicating Bandwidth to One Port

When you dedicate the bandwidth to one port, you must first administratively shut down the four ports in the group, change the rate mode to dedicated, and then bring the dedicated port administratively up.

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	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into the CLI Global Configuration Mode.

Step 2	**interface ethernet** *slot/port*, **ethernet** *slot/port*, **ethernet** *slot/port*, **ethernet** *slot/port*
	
	Example:
	`n1000v(config)# interface ethernet 3/1, ethernet 3/3, ethernet 3/5, ethernet 3/7`
	`n1000v(config-if)#`
		Specifies an Ethernet interface to configure, and enters interface configuration mode.
		
		The example shows how to specify one port for the dedicated mode.

Step 3	**shutdown** **Example:** `n1000v(config)#` **shutdown**	Administratively shuts down the ports in the running configuration.

Step 4	**interface ethernet** *slot/port*
	
	Example:
	`n1000v(config)# interface ethernet 3/1`
	`n1000v(config)#`
		Specifies the first Ethernet interface in a group of interfaces.

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 configuraiton. When you dedicate the bandwidth, all subsequent commands for the port are for dedicated mode.

	Command	Purpose
Step 6	**no shutdown** **Example:** `n1000v(config-if)# no shutdown`	Brings the port administratively up in the running coniguration.
Step 7	**show interface ethernet** *slot/port* **Example:** `n1000v(config)# 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 the interface 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.

This 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 Mode

The interface speed and duplex mode are interrelated, so you should configure both of their parameters at the same time. To see which speeds and duplex modes you can configure together for Ethernet and management interfaces, see .

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 10- or 100-Mbps speed, 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.

BEFORE YOU BEGIN

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. **config 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	**config t** **Example:** svs# config t svs(config)#	Enters the global configuration mode.
Step 2	**interface** *interface* **Example 1:** svs(config)# interface ethernet 2/1 svs(config-if)# **Example 2:** svs(config)# interface mgmt0 svs(config-if)#	Specifies the interface that you are configuring. You can specify the interface type and identity. For an Ethernet port, use "ethernet *slot/port*." For the management interface, use "mgmt0." Example 1 shows how to specify the slot 2 port 1 Ethernet interface. Example 2 shows how to specify the management interface.
Step 3	**speed** {{**10** | **100** | **1000** | {**auto** [**10 100** [**1000**]]}} | {**10000** | **auto**}} **Example:** svs(config-if)# speed 1000 svs(config-if)#	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. For Ethernet ports on the 32-port 10 GE modules, sets the speed at 10,000 Mbps (10 Gbps) or sets the port to autonegotiate its speed with the other 10 GE port on the link. For management interfaces, sets the speed as 1000 Mbps or sets the port to autonegotiate its speed.

	Command	Purpose
Step 4	**duplex** {**full** | **half** | **auto**} **Example:** svs(config-if)# duplex full	Specifies the duplex mode as full, half, or autonegotiate.
Step 5	**show interface** *interface* **Example:** svs(config)# show interface *mgmt0*	Displays the interface status, which includes the speed and duplex mode parameters.
Step 6	**exit** **Example:** svs(config-if)# exit svs(config)#	Exits the interface mode.
Step 7	**copy running-config startup-config** **Example:** svs(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

This 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:

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

Configuring the MTU Size

You can configure the maximum transmission unit (MTU) size for Layer 2 and Layer 3 Ethernet interfaces. For Layer 3 interfaces, you can configure the MTU to be between 576 and 9216 bytes (even values are required). For Layer 2 interfaces, you can configure the MTU to be either the system default MTU (1500 bytes) or the system jumbo MTU size (which has the default size of 9216 bytes).

Note You can change the system jumbo MTU size, but if you change that value, you should also update the Layer 2 interfaces that use that value so that they use the new system jumbo MTU value. If you do not update the MTU value for Layer 2 interfaces, those interfaces will use the system default MTU (1500 bytes).

This section includes the following topics:

Configuring the Interface MTU Size

For Layer 3 interfaces, you can configure an MTU size that is between 576 and 9216 bytes.

For Layer 2 interfaces, you can configure all Layer 2 interfaces to use either the default MTU size (1500 bytes) or the system jumbo MTU size (default size of 9216 bytes). If you need to use a different system jumbo MTU size for Layer 2 interfaces, see the "Configuring the System Jumbo MTU Size" section on page 2-14.

SUMMARY STEPS

1. **config t**
2. **interface ethernet** *slot/port*
3. **switchport** | {**no switchport**}
4. **mtu** *size*
5. **show interface ethernet** *slot/port*
6. **exit**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** svs# config t svs(config)#	Places you into the CLI Global Configuration Mode.
Step 2	**interface ethernet** *slot/port* **Example:** svs(config)# interface ethernet 3/1 svs(config-if)#	Specifies an Ethernet interface to configure, and enters interface configuration mode.
Step 3	**switchport** | {**no switchport**}	Specifies to use Layer 2 or Layer 3.
Step 4	**mtu** ***size*** **Example:** svs(config-if)# mtu 9216 svs(config-if)#	For a Layer 2 interface, specifies either the default MTU size (1500) or the system jumbo MTU size (9216 unless you have changed the system jumbo MTU size). For a Layer 3 interface, specifies any even number between 576 and 9216.
Step 5	**show interface ethernet** *slot/port* **Example:** svs(config)# show interface *type slot/port*	Displays the interface status, which includes the MTU size.
Step 6	**exit** **Example:** svs(config-if)# exit svs(config)#	Exits the interface mode.
Step 7	**copy running-config startup-config** **Example:** svs(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

This example shows how to configure the Layer 2 Ethernet port 3/1 with the default MTU size (1500).

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

Configuring the System Jumbo MTU Size

You can configure the system jumbo MTU size, which can be used to specify the MTU size for Layer 2 interfaces. You can specify an even number between 1500 and 9216. 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** *type slot/port*
5. **mtu** *size*
6. **exit**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** svs# config t svs(config)#	Places you into the CLI Global Configuration Mode.
Step 2	**system jumbomtu** *size* **Example:** svs(config)# system jumbomtu 8000 svs(config-if)#	Specifies the system jumbo MTU size. Use an even number between 1500 and 9216.
Step 3	**show running-config** **Example:** svs(config)# show running-config	Displays the current operating configuration, which includes the system jumbo MTU size.
Step 4	**interface** *type slot/port*	Specifies an interface to configure and enters the interface configuration mode.
Step 5	**mtu** *size*	For a Layer 2 interface, specifies either the default MTU size (1500) or the system jumbo MTU size that you specified earlier. For a Layer 3 interface, specifies any even size between 576 and 9216.
Step 6	**exit** **Example:** svs(config-if)# exit svs(config)#	Exits the interface mode.
Step 7	**copy running-config startup-config** **Example:** svs(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

This 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:

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

Configuring Bandwidth

You can configure the bandwidth for Ethernet interfaces. The physical level uses an unchangeable bandwidth of 1 GB, but you can configure a value of 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 CLI Global Configuration Mode.
Step 2	**interface ethernet** *slot/port* **Example:** n1000v(config)# interface ethernet 3/1 n1000v(config-if)#	Specifies an Ethernet interface to configure, and enters interface configuration mode.
Step 3	**bandwidth** *value* **Example:** n1000v(config-if)# bandwidth 1000000 n1000v(config-if)#	Assigns the specified bandwidth to the interface in the running configuration. The bandwide is an information-only value between 1 and 10,000,000.
Step 4	**show interface ethernet** *slot/port* **Example:** n1000v(config)# show interface ethernet *slot/port*	Displays the interface status, which includes the bandwidth value.

	Command	Purpose
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.

This 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

You can configure the interface throughput delay for Ethernet interfaces. The actual delay time does not change, but you can set an informational value between 1 and 16777215, where the value represents the number of tens of microseconds.

SUMMARY STEPS

1. **config t**
2. **interface ethernet** *slot/port*
3. **delay** *tens_of_microseconds*
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 CLI Global Configuration Mode.
Step 2	**interface ethernet** *slot/port* **Example:** n1000v(config)# interface ethernet 3/1 n1000v(config-if)#	Specifies an interface to configure, and enters Interface Configuration mode.

	Command	Purpose

Step 3	**delay** *value*
	
	Example:
	`n1000v(config-if)# delay 10000`
	`n1000v(config-if)#`
		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** *slot/port*
	
	Example:
	`n1000v(config)# show interface ethernet 3/1`
	`n1000v(config-if)#`
		Displays the interface status, which includes the throughput-delay time.

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.

This example shows how to configure the throughput-delay time to 100,000 microseconds for the slot 3 port 1 Ethernet interface:

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

Shutting Down and Activating the Interface

You can shut down and restart Ethernet or management interfaces. When you shut down interfaces, they become disabled and all monitoring displays show them as being down. This information is communicated to other network servers through all dynamic routing protocols. When the interfaces are shut down, the interface is not included in any routing updates. To activate the interface, 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**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into the CLI Global Configuration mode.
Step 2	**interface** *interface* **Example:** n1000v(config)# interface ethernet 2/1 n1000v(config-if)# n1000v(config)# interface mgmt0 n1000v(config-if)#	Specifies the interface that you are configuring. You can specify the interface type and identity. For an Ethernet port, use "ethernet *slot*/*port*." For the management interface, use "mgmt0." Example 1 shows how to specify the slot 2, port 1 Ethernet interface. Example 2 shows how to specify the management interface.
Step 3	**shutdown** **Example:** n1000v(config-if)# shutdown n1000v(config-if)#	Disables the interface in the running configuration.
Step 4	**show interface** *interface* **Example:** n1000v(config-if)# show interface ethernet 2/1 n1000v(config-if)#	Displays the interface status, which includes the administrative status.
Step 5	**no shutdown** **Example:** n1000v(config-if)# no shutdown n1000v(config-if)#	Reenables the interface in the running configuration.
Step 6	**show interface** *interface* **Example:** n1000v(config-if)# show interface ethernet 2/1 n1000v(config-if)#	Displays the interface status, which includes the administrative status.
Step 7	**exit** **Example:** n1000v(config-if)# exit n1000v(config)#	Exits the interface 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.

This example shows how to change the administrative status for Ethernet port 3/1 from disabled to enabled:

```
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

You can enable or disable the Cisco Discovery Protocol (CDP) for Ethernet and management interfaces. This protocol works only when you have it enabled on both interfaces on the same link.

BEFORE YOU BEGIN

Make sure that the remote port also has CDP enabled.

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 CLI Global Configuration mode.
Step 2	**interface** *interface* **Example 1:** n1000v(config)# interface ethernet 2/1 n1000v(config-if)# **Example 2:** n1000v(config)# interface mgmt0 n1000v(config-if)#	Specifies an Ethernet or vEthernet interface to configure, and places you into the Interface Configuration mode for that interface. Example 1 shows how to specify the slot 2 port 1 Ethernet interface. Example 2 shows how to specify the management interface.
Step 3	**cdp enable** **Example:** n1000v(config-if)# cdp enable n1000v(config-if)#	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 n1000v(config-if)#	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.

	Command	Purpose
Step 4	**show cdp interface** *interface* **Example:** n1000v(config-if)# show cdp interface *interface*	Displays the CDP status for the interface in the running configuration.
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.

This example shows how to enable CDP for the Ethernet slot 3, port 1 interface:

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

This example shows how to disable CDP for the Ethernet slot 3, port 1 interface:

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

Verifying the Basic Interface Parameters

You can verify the basic interface parameters by displaying their values. You can also clear the counters listed when you display the parameter values.

DETAILED STEPS

To display Layer 2 port configuration information, use the appropriate **show** command for the parameters you need to display.

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

Clearing the Interface Counters

You can clear the Ethernet and management interface counters shown with the **show interfaces** command. You can perform this task from the EXEC mode, configuration mode, or interface configuration mode.

SUMMARY STEPS

1. **clear counters** *interface*
2. **show interface** *interface*

DETAILED STEPS

	Command	Purpose
Step 1	**clear counters** *interface* **Example:** n1000v# clear counters ethernet 2/1 n1000v#	Clears the Ethernet or management interface counters.
Step 2	**show interface** ***interface***	Displays the interface status, which includes the counters.

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

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

CHAPTER 3

Configuring Layer 2 Interfaces

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

This chapter includes the following topics:

Note For information about configuring a SPAN destination interface, see the document, *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(1).*

Note for information about VLANs, MAC address tables, and private VLANs, see the document, *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(1).*

Access and Trunk Interfaces

This section includes the following topics:

Information About Access and Trunk Interfaces

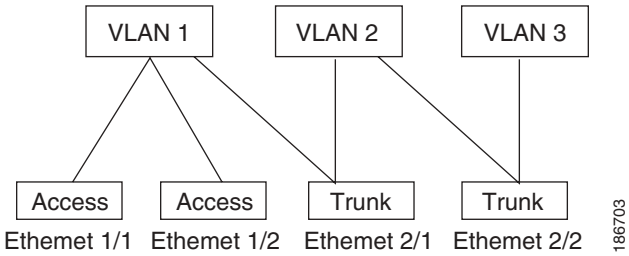
A Layer 2 port can be configured as an access or a trunk port as follows:

- An access port can have only one VLAN configured on that port; it can carry traffic for only one VLAN.
- A trunk port can have two or more VLANs configured on that port; it can carry traffic for several VLANs simultaneously.

By default, all ports on the Cisco Nexus 1000V are Layer 2 ports. You can change the default port mode. See the *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(1)* for information about setting the default port mode.

Figure 3-1 show 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.

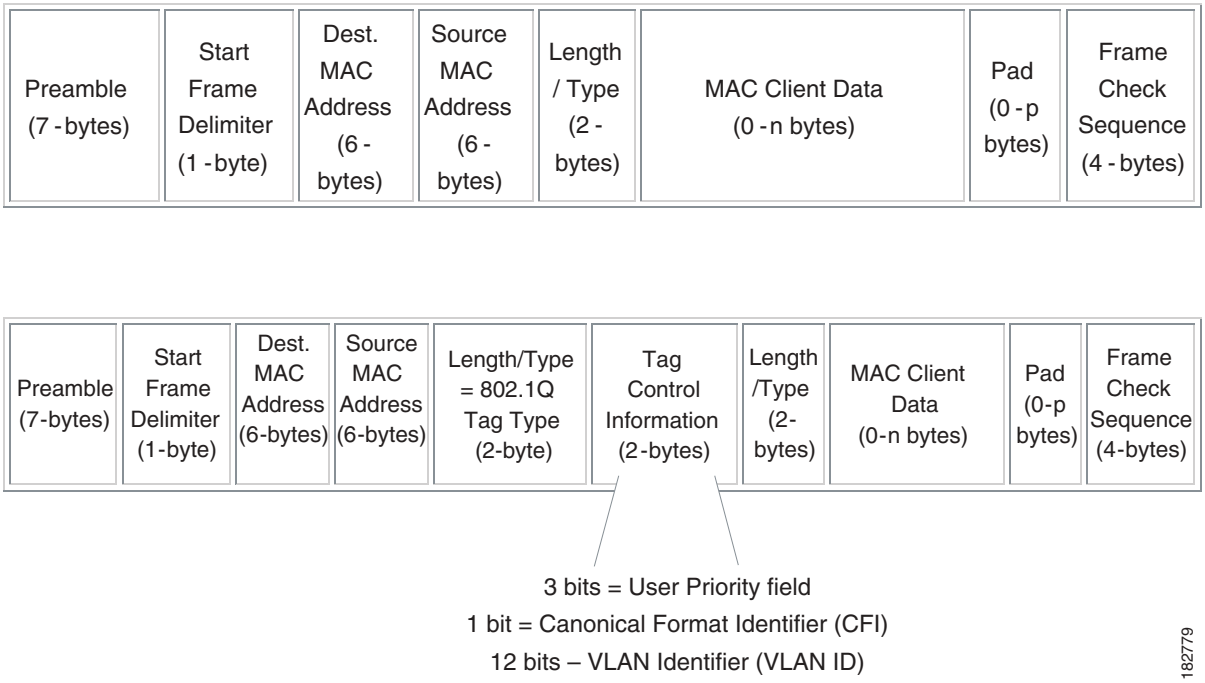
A Layer 2 interface can function as either an access port or a trunk port; it cannot function as both port types simultaneously.

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). This tag carries information about the specific VLAN to which the frame and packet belong. This method allows packets that are encapsulated for several different VLANs to traverse the same port and maintain traffic separation between the VLANs. Also, the encapsulated VLAN tag allows the trunk to move traffic end-to-end through the network on the same VLAN.

Figure 3-2 Header Without and With 802.1Q Tag



High Availability

The software supports high availability for Layer 2 ports.

Prerequisites for VLAN Trunking

- You are logged inn to the CLI.

Guidelines and Limitations

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

- 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.

Configuring Access and Trunk Interfaces

This section includes the following topics:

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

- Ensure that you are configuring a Layer 2 interface.
- 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.

SUMMARY STEPS

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

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Paces you into CLI Global Configuration mode.
Step 2	**interface** {{*type slot/port*} | {**port-channel** *number*}} **Example:** n1000v(config)# interface ethernet 3/1 n1000v(config-if)#	Specifies an Ethernet or vEthernet interface to configure, and places you into the Interface Configuration mode for that interface.
Step 3	**switchport mode** {**access** | **trunk**} **Example:** n1000v(config-if)# switchport mode access	Sets the interface as a nontrunking nontagged, single-VLAN Layer 2 interface in the running configuration. An access port can carry traffic in one VLAN only. By default, an access port carries traffic for VLAN1; to set the access port to carry traffic for a different VLAN, use the **switchport access vlan** command.
Step 4	**switchport access vlan** *vlan-id* **Example:** n1000v(config-if)# switchport access vlan 5	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.
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.

This 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 optimize the performance of access ports that are connected to end stations by simultaneously setting that port as an access port.

BEFORE YOU BEGIN

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

- 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 connected to an end station.
- An access host port handles the STP like an edge port and immediately moves to the forwarding state without passing through the blocking and learning states.
- Configuring an interface as an access host port also disables port channeling on that interface.

Note See Chapter 5, "Configuring Port Channels" for information about port channel interfaces.

- The interface can be either Ethernet or vEthernet.

SUMMARY STEPS

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

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Paces you into CLI Global Configuration mode.

Step 2	**interface** *type slot/port*
	
	Example:
	`n1000v(config)# interface ethernet 3/1`
	`n1000v(config-if)#`
		Specifies an Ethernet or vEthernet interface to configure, and places you into the Interface Configuration mode for that interface.

Step 3	**switchport host** **Example:** `n1000v(config-if)# switchport host`	Designates the interface as an access host port in the running configuration, This immediately moves it to the spanning tree forwarding state and disables port channeling on this interface. **Note** Apply this command only to end stations.

	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.

This 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.

BEFORE YOU BEGIN

- Before you configure a trunk port, ensure that you are configuring a Layer 2 interface.
- The interface can be either Ethernet or vEthernet.
- A trunk port transmits untagged packets for one VLAN plus encapsulated, tagged, packets for multiple VLANs. (See 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** {*type slot/port* | **port-channel** *number*}
3. **switchport mode** {**access** | **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)#	Paces you into CLI Global Configuration mode.
Step 2	**interface** {*type slot/port* | **port-channel** *number*} **Example:** n1000v(config)# interface ethernet 3/1 n1000v(config-if)#	Specifies an Ethernet or vEthernet interface to configure, and places you into Interface Configuration mode for that interface.
Step 3	**switchport mode** {**access** | **trunk**} **Example:** n1000v(config-if)# switchport mode trunk	Sets the interface as a Layer 2 trunk port in the running configuration. A trunk port can carry traffic in one or more VLANs on the same physical link (VLANs are based on the trunk-allowed VLANs list). By default, a trunk interface can carry traffic for all VLANs. To specify that only certain VLANs are allowed on the specified trunk, use the **switchport trunk allowed vlan** command.
Step 4	**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.

This 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. If you do not configure this parameter, the trunk port uses the default VLAN as the native VLAN ID.

SUMMARY STEPS

1. **config t**
2. **interface** {*type slot/port* | **port-channel** *number*}

3. **switchport trunk native vlan** *vlan-id*
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)#	Paces you into CLI Global Configuration mode.
Step 2	**interface** {*type slot/port* | **port-channel** *number*} **Example:** n1000v(config)# interface ethernet 3/1 n1000v(config-if)#	Specifies an Ethernet or vEthernet interface to configure, and places you into Interface Configuration mode for that interface.
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 returnx 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.

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

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

Configuring the Allowed VLANs for Trunking Ports

Use this procedure to specify the IDs for the VLANs that are allowed on the specific trunk port.

BEFORE YOU BEGIN

- Before you configure the allowed VLANs for the specified trunk ports, ensure that you are configuring the correct interfaces and that the interfaces are trunks.

SUMMARY STEPS

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

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Paces you into CLI Global Configuration mode.

Step 2	**interface** {**ethernet** *slot/port* | **port-channel** *number*} **Example:** `n1000v(config)# interface ethernet 3/1`	Specifies an Ethernet or vEthernet interface to configure, and places you into Interface Configuration mode for that interface.
Step 3	**switchport trunk allowed vlan** {*vlan-list* **all** | **none** [**add** |**except** | **none** | **remove** {*vlan-list*}]} **Example:** `n1000v(config-if)# switchport trunk allowed vlan add 15-20#`	Sets the allowed VLANs for the trunk interface in the running configuration. The default is to allow all VLANs on the trunk interface: 1 to 3967 and 4048 to 4094. VLANs 3968 to 4047 are the default VLANs reserved for internal use by default; this group of VLANs is configurable. By default, all VLANs are allowed on all trunk interfaces. **Note** You cannot add internally allocated VLANs as allowed VLANs on trunk ports. The system returns a message if you attempt to list an internally allocated VLAn as an allowed VLAN.

Step 4	**exit**
	
	Example:
	`n1000v(config-if)# exit`
	`n1000v(config)#`
		Exits the Interface Configuration mode and returns you to CLI Global Configuration mode.

	Command	Purpose
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.

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

```
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, when working with 802.1Q trunked interfaces, to maintain the tagging for all packets that enter with a tag that matches the native VLAN ID. Untagged traffic is dropped (you will still carry control traffic on that interface).

BEFORE YOU BEGIN

- The **vlan dot1q tag native** global command changes the behavior of all native VLAN ID interfaces on all trunks on the device.
- This feature applies to the entire device; you cannot apply it to selected VLANs on a device.

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**
5. **copy running-config startup-config**

DETAILED STEPS

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

This example shows how to change the behavior of the native VLAN on an 802.1Q trunked interface to maintain the tagged packets and drop all untagged traffic (except control traffic):

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

Verifying Interface Configuration

To display access and trunk interface configuration information, use one of the following commands:

Command	Purpose
show interface ethernet *slot/port* [**brief** | | **counters** | **debounce** | **description** | **mac-address** | **status** | **transceiver**]	Displays the interface configuration
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.

Command	Purpose
show interface trunk [**module** *module-number* | **vlan** *vlan-id*]	Displays trunk configuration information.
show interface capabilities	Displays information on the capabilities of the interfaces.
show running-config interface ethernet *slot/port*	Displays configuration information about the specified interface.

Displaying and Clearing Statistics

To display access and trunk interface configuration information, use one of the following commands:

Command	Purpose
clear counters [*interface*]	Clears the counters.
show interface counters [**module** *module*]	Displays input and output octets unicast packets, multicast packets, and broadcast packets.
show interface counters detailed [**all**]	Displays input packets, bytes, and multicast as well as output packets and bytes.
show interface counters errors [**module** *module*]	Displays information on the number of error packets.

Access and Trunk Port Mode Example Configurations

The following example shows how to configure a Layer 2 access interface and assign the access VLAN for that interface:

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

The following example shows how to configure a Layer 2 trunk interface, assign the native VLAN and the allowed VLANs, and configure the device to tag the native VLAN traffic on the trunk interface:

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

Default Settings

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

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

Additional References

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

- Related Documents, page 3-14
- Standards, page 3-14

Related Documents

Related Topic	Document Title
Port channels	Chapter 5, "Configuring Port Channels"
VLANs, private VLANs, and STP	*Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(1)*
System management	*Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(1)*
Release Notes	*Cisco Nexus 1000V Release Notes, Release 4.0(4)SV1(1)*

Standards

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

MIBs

MIBs	MIBs Link
• BRIDGE-MIB • IF-MIB • CISCO-IF-EXTENSION-MIB • ETHERLIKE-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

CHAPTER 4

Configuring Virtual Ethernet Interfaces

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

This chapter includes the following topics:

Guidelines and Limitations

The following are guidelines and limitations to consider when configuring vEthernet interfaces:

- MTU cannot be configured on a vEthernet interface.

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 autoformatted 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 autoformatted 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
6. `show interface vethid`
7. `copy run start`

DETAILED STEPS

	Command	Purpose

Step 1	**`config t`**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into CLI Global Configuration mode.

Step 2	**`interface vethernet`** *`interface-number`*
	
	Example:
	`n1000v(config)# interface vethernet 100`
	`n1000v(config-if)#`
		Places you into CLI Interface Configuration mode for the specified vEth interface.
		
		Interface-number: 1-1048575 allowable range

Step 3	**`description`** *`string`*
	
	Example:
	`n1000v(config-if)# description accessvlan`
	`n1000v(config-if)#`
		Adds a description to the interface in the running configuration.
		
		string: Can be up to 80 alphanumeric characters.

Step 4	**`switchport access vlan`** *`vlanid`*
	
	Example:
	`n1000v(config-if)# switchport access vlan 5`
	`n1000v(config-if)#`
		Configures the vEth interface as an access interface and specifies the VLAN ID in the running configuration.
		
		VLAN ID: Allowable range = 1-4094

Step 5	**`switchport mode`** `{access | private-vlan {host | promiscuous} | trunk}`
	
	Example:
	`n1000v(config-if)# switchport mode access`
	`n1000v(config-if)#`
		Configures the vEth interface switchport mode in the running configuration.
		• access
		• private-vlan: host or promiscuous
		• trunk

	Command	Purpose

Step 6	**show interface**
	
	Example:
	`n1000v(config-if)# show interface vethernet1`
	`n1000v(config-if)#`
		(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.

Configuring a vEthernet Private VLAN Interface

Use this procedure to configure a vEthernet interface for PVLAN.

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

1. **config t**
2. **interface vethernet** *interface-number*
3. **description** *string*
4. **switchport access vlan** *vlan-id*
5. **switchport mode private-vlan host**
6. **switchport private-vlan host-association** *primary vlan-id*
7. **show interface**
8. **copy running-config startup-config**

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into CLI Global Configuration mode.

Step 2	**interface vethernet** *interface-number*
	
	Example:
	`n1000v(config)# interface vethernet 1`
	`n1000v(config-if)#`
		Places you into CLI Interface Configuration mode for the specified vEth interface.
		
		Interface-number: 1-1048575 allowable range

Step 3	**description** *string* **Example:** `n1000v(config-if)# description isp_pvlan1`	Adds a description to the interface in the running configuration. **string**: Can be up to 80 alphanumeric characters.

	Command	Purpose
Step 4	**switchport access vlan** *vlanid* **Example:** `n1000v(config-if)# switchport access vlan 5`	Configures the vEth interface as an access interface and specifies the VLAN ID in the running configuration. VLAN: Allowable range = 1-4094

Step 5	`switchport mode {access | private-vlan {host | promiscuous} | trunk}`
	
	Example:
	`n1000v(config-if)# switchport mode private-vlan host`
		Configures the vEth interface for private vlan host in the running configuration.
		• access
		• private-vlan: host or promiscuous
		• trunk

Step 6	**switchport private-vlan host-association** *primary vlanid* **Example:** `n1000v(config-if)# switchport private-vlan host-association 5`	Configures the vEth interface for a host association with a specific primary VLAN ID in the running configuration. host-association: primary VLAN ID primary private -VLAN ID: allowable range 1-4094
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.

This 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 vethernet1
Vethernet1 is up
    Hardware is Virtual, address is 0050.5681.4af0
    Owner is VM "R-1"
    Active on module 14
    Port-Profile is vlan1160
    Port mode is access
    Rx
    32219 Input Packets 31263 Unicast Packets
    0 Multicast Packets 956 Broadcast Packets
    2527232 Bytes
    Tx
    15626 Output Packets 0 Unicast Packets
    0 Multicast Packets 15626 Broadcast Packets 15626 Flood Packets
    937560 Bytes
    0 Input Packet Drops 0 Output Packet Drops
n1000v(config-if)#
```

Enabling or Disabling a vEthernet Interface

Use this procedure to enable or disable a vEtherenet interface.

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 CLI Global Configuration mode.

Step 2	**interface vethernet** *interface-number*
	
	Example:
	`n1000v(config)# interface vethernet 100`
	`n1000v(config-if)#`
		Places you into CLI Interface Configuration mode for the specified vEth interface.
		Interface-number: 1-1048575 allowable range

Step 3	**[no] shutdown**
	
	Example:
	`n1000v(config-if)# no shutdown`
	`n1000v(config-if)#`
		Enables or disables the vEthernet interface in the running configuration.
		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.

This example shows how to enable a vEthernet interface:

```
n1000v# config t
n1000v(config)# interface vethernet 100
n1000v(config)# no shutdown
n1000v(config-if)# show interface veth100 status

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

Verifying vEthernet Interface Configuration

Use the following commands to display vEthernet interface configurations:

Command	Purpose
show interface vethernet *vif-number* [**brief** | | **counters [detailed [all]** | **errors]** | **description** | **mac-address** | **status** [down | err-disabled | inactive | module *num* | up] | **switchport**	Displays the vEthernet interface configuration.
show interface [vethernet *vif-number*]	Displays the complete interface configuration.
show interface [vethernet *vif-number*] brief	Displays abbreviated interface configuration.
show interface [vethernet *vif-number*] counters	Displays the interface incoming and outgoing counters.
show interface [vethernet *vif-number*] 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 *vif-number*] counters errors	Displays the interface error counters .
show interface [vethernet *vif-number*] description	Displays the interface description.
show interface [vethernet *vif-number*] mac-address	Displays the interface MAC address. **Note** For vEth interfaces this shows the MAC address of the connected device.
show interface [vethernet *vif-number*] status [down | err-disabled | inactive | module *num* | up]	Displays interface line status.
show interface [vethernet *vif-number*] switchport	Displays interface switchport information.
show interface virtual [vm [vm_name] | vmk | vswif] [module mod_no]	Displays virtual interfaces only.
show interface virtual port-mapping [vm [name] | vmk | vswif | description] [module num]	Displays mappings between veth and VMware DVPort.

vEthernet Show Command Examples

```
n1000v# show interface veth1
Vethernet1 is up
    Port description is gentoo1, Network Adapter 1
    Hardware is Virtual, address is 0050.56bd.42f6
    Owner is VM "gentoo1", adapter is Network Adapter 1
    Active on module 33
    VMware DVS port 100
    Port-Profile is vlan48
    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#
```

```
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-gentoo1            33  austen-strider.austen.
Veth2       Net Adapter 2  austen-gentoo1            33  austen-strider.austen.
n1000v#


n1000v# show interface virtual description

--------------------------------------------------------------------------------
Interface   Description
--------------------------------------------------------------------------------
Veth1       gentoo1, Network Adapter 1
Veth2       gentoo1, Network Adapter 2
Veth3       VMware VMkernel, vmk1
Veth4       VMware Service Console, vswif1


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            --            --            --
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#


n1000v# show interface virtual port-mapping
```

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


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

interface Vethernet1
  inherit port-profile vlan48
  description gentoo1, Network Adapter 1
```

vEthernet Interface Example Configurations

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)#
```

Default Settings

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

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

Additional References

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

- Related Documents, page 4-9
- Standards, page 4-9

Related Documents

Related Topic	Document Title
Port Profiles	*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(1)*
VLANs and private VLANs	*Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(1)*
System management	*Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(1)*
Release Notes	*Cisco Nexus 1000V Release Notes, Release 4.0(4)SV1(1)*

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.	—

CHAPTER 5

Configuring Port Channels

This chapter describes how to configure port channels in the Cisco Nexus 1000V.

This chapter includes the following sections:

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

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

Viewing the Compatability Checks

To view the full list of compatability checks performed by the Cisco Nexus 1000V, use the following command:

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.

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 is source MAC address.

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 Destinaiton 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 traffic load. When you configure the destination MAC address load balancing method, traffic load is balanced using the destination MAC address.

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

To configure port channel load balance, see the "Configuring Port Channel Load Balance" procedure on page 5-22.

LACP

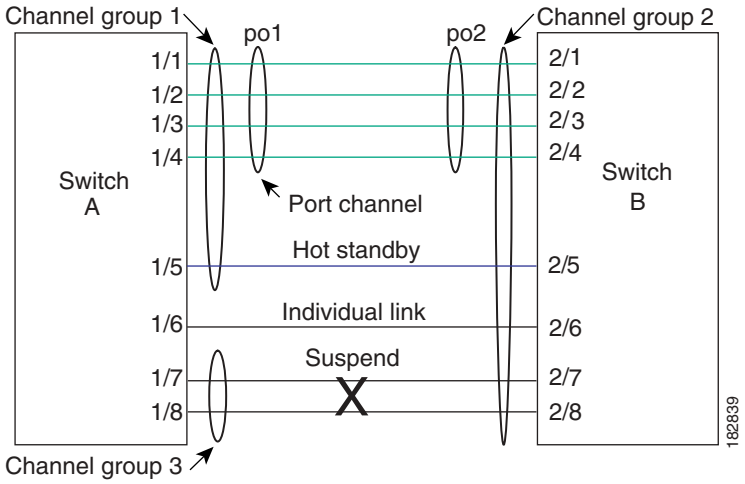
Link Aggregation Control Protocol (LACP) lets you configure up to 16 interfaces into a port channel. A maximum of eight interfaces can be active, and a maximum of eight interfaces can be placed in a standby state. Figure 5-1 shows how individual links can be combined into LACP port channels and channel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

For the Cisco Nexus 1000V, LACP is enabled globally by deafult.

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:

Figure 5-1 Individual Links Combined into a Port Channel



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	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. 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. The default port-channel mode is **on**.

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:

- High Availability, page 5-9
- LACP Port Priority, page 5-7
- LACP Administrative Key, page 5-7

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 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.

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

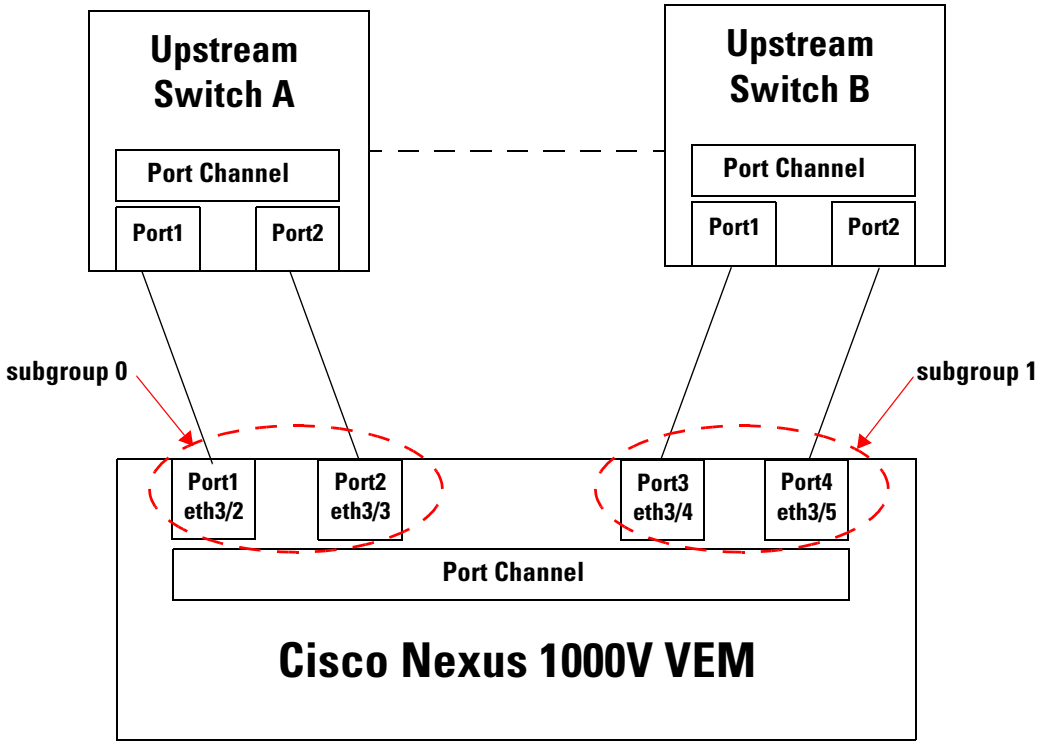
Configurations	Port Channels with LACP Enabled	Static Port Channels
Protocol applied	Enable globally	Not applicable
Channel mode of links	Can be either: • Active • Passive	Can only be On
Maximum number of links in channel	16	8

vPC Host Mode

Virtual port channel host mode (vPC-HM) allows member ports in a port channel to connect to two different upstream switches. With vPC-HM, ports are grouped into two subgroups for traffic separation. If CDP is enabled on the upstream switch, then the subgroups are automatically created using CDP information. If CDP is not enabled on the upstream switch, then you must manually create the subgroup on the interface.

As shown in Figure 5-2, in vPC-HM, member ports are assigned a subgroup ID (0 or 1)for traffic separation.

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



To configure an interface in vPC-HM, see the "Configuring a Port Channel that Connects to Two Upstream Switches" procedure on page 5-12.

vPC-HM can also be configured on the port profile. For more information, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(1)*.

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 on the compatibility requirements.

- You can use asymmetric port channel in host mode (vPC-HM) to configure a port channel even when the physical ports are connected to two different switches.

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 same upstream switch.
  - the uplinks from the host are going to two upstream switches and are configured with vPC-HM.
- Port channels can be configured using a port-profile. For more information, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(1)*.
- 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.
- Ports that belong to a port channel group can also be configured as private VLAN 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 on the ports going towards the ESX host:
  - spanning-tree portfast trunk
  - spanning-tree bpdufilter enable

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

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

Configuring Port Channels

This section includes the following topics:

Note Be aware that the Cisco Nexus 1000V commands for this feature 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 all connect to the same upstream switch.

If the member ports connect to two upstream switches, use the "Configuring a Port Channel that Connects to Two Upstream Switches" procedure on page 5-12.

BEFORE YOU BEGIN

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

- When you create a port channel, an associated channel group is automatically created.

SUMMARY STEPS

1. **config t**
2. **interface port-channel** *channel-number*
3. **show port-channel summary**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into the CLI Global Configuration Mode.
Step 2	**interface port-channel** *channel-number* **Example:** n1000v(config)# interface port-channel 1 n1000v(config-if)#	Places you into the Interface Configuration mode for the specified port channel. 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. To create a port channel group whose member ports connect to two different switches, use the
Step 3	**show port-channel summary** **Example:** n1000v(config-router)# show port-channel summary	(Optional) Displays the port channel configuration.
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.

This example shows how to create a port channel:

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

Configuring a Port Channel that Connects to Two Upstream Switches

Use this procedure to add virtual port channel host mode (vPC-HM) to a port channel. In vPC-HM, the port channel member ports connect to two upstream switches, and the traffic must be managed in separate subgroups.

If the member ports connect to a single upstream switch, use the "Configuring a Port Channel that Connects to a Single Upstream Switch" procedure on page 5-11.

BEFORE YOU BEGIN

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

- When you create a port channel, an associated channel group is automatically created.
- 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 know whether CDP is configured in the upstream switches. If so, then CDP creates a subgroup in each upstream switch to manage its traffic separately.
- If CDP is not configured in the upstream switch, 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 a subgroup has more than one member port, a port channel must be configured for the member ports of each sub group on the upstream switch.
- If vPC-HM is not configured when port channels connect to two different upstream switches, then the VMs behind the Cisco Nexus 1000V receive duplicate packets from the network for broadcast/unknown floods/multicast.
- vPC-HM can also be configured on the port profile. For more information, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(1)*.

SUMMARY STEPS

1. **config t**
2. **interface port-channel** *channel-number*
3. **sub-group cdp**
4. **Do one of the following**
   - If CDP is not configured for the upstream switch(es), then continue with the next step.
   - If CDP is configured for the upstream switch(es), then go to Step 9.
5. **exit**
6. **interface ethernet** *range*
7. **sub-group-id** *number*
8. Repeat steps 6 and 7 for each port member connected to an upstream switch that is not configured for CDP.
9. **show port-channel summary**
10. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into the CLI Global Configuration Mode.
Step 2	**interface port-channel** *channel-number* **Example:** n1000v(config)# interface port-channel 12 n1000v(config-if)#	Places you into the Interface Configuration mode for the specified port channel. The allowable range is from 1 to 4096. If the channel group does not already exist, it is automatically created.

	Command	Purpose

Step 3	**sub-group cdp**
	
	Example:
	`n1000v(config-if)# sub-group cdp`
	`n1000v(config-if)#`
		Identifies the port channel as being in vPC-HM which requires that the traffic must be managed separately for each of the two upstream switches connected to the member ports.
		
		If it is configured in the upstream switches, CDP information is collected for this purpose. If CDP is not configured in the upstream switches, then you must configure subgroups manually.

Step 4	Do one of the following: – If CDP is not configured for both upstream switch(es), then continue with the next step. – If CDP is configured for both upstream switch(es), then go to Step 9.	

Step 5	**exit**
	
	Example:
	`n1000v(config-if)# exit`
	`n1000v(config)#`
		Exits the Interface Configuration mode for the port channel and returns you to Global Configuration mode.

Step 6	**interface ethernet** *range*
	
	Example:
	`n1000v(config)# interface ethernet3/2-3`
	`n1000v(config-if)#`
		Places you into Interface Configuration mode for the specified interface range.

Step 7	**sub-group id** *number*
	
	Example:
	`n1000v(config-if)# sub-group-id 0`
	`n1000v(config-if)#`
		Configures the specified port channel members as vPC-HM so that the specified subgoup can manage traffic for one of the two upstream switches.
		
		Allowable subgroup numbers = 0 or 1

Step 8	Repeat Step 6 and Step 7 for each port member connected to an upstream switch that is not configured for CDP.	
Step 9	**show port-channel summary** **Example:** `n1000v(config-if)# show port-channel summary`	(Optional) Displays the port channel configuration.
Step 10	**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.

Removing the Port Channel and Group

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

BEFORE YOU BEGIN

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

- For details about how the interface configuration changes when you delete a port channel, see the "Compatibility Checks" section on page 5-2 .

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into the CLI Global Configuration Mode.

Step 2	**no channel-group** *channel-number* **Example:** `n1000v(config)# no channel-group port-channel 1`	
Step 3	**no interface port-channel** *channel-number* **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:

- 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** *type slot/port*
3. **switchport**

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

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into the CLI Global Configuration Mode

Step 2	**interface** *type slot/port*
	
	Example:
	n1000v(config)# interface ethernet 1/4
	n1000v(config-if)
		Places you into the Interface Configuration mode for the specified interface.

Step 3	**switchport** **Example:** n1000v(config-if)# switchport	Configures the interface as a Layer 2 access port.
Step 4	**switchport mode trunk** **Example:** n1000v(config-if)# switchport mode trunk	(Optional) Configures the interface as a Layer 2 trunk port.
Step 5	**switchport trunk** {**allowed vlan** *vlan-id* | **native** *vlan-id*} **Example:** n1000v(config-if)# switchport trunk native 3	(Optional) Configures necessary parameters for a Layer 2 trunk port.
Step 6	**channel-group** *channel-number* [**mode** {**on** | **active** | **passive**}] **Example:** n1000v(config-if)# channel-group 5	Configures the port in a channel group and sets the mode. The channel-number 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. All static port channel interfaces are set to mode **on**.
Step 7	**show interface** *type slot/port* **Example:** n1000v(config-router)# show interface port channel 5	(Optional) Displays interface 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.

This example shows how to add the Layer 2 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.

DETAILED STEPS

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

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. **exit**
5. **show interface port-channel** *channel-number*
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into the CLI Global Configuration mode.

Step 2	**interface port-channel** *channel-number*
	
	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 n1000v(config-if)#	Shuts down the interface. No traffic passes and the interface displays as administratively down. The default is no shutdown.
	no shutdown **Example:** n1000v(config-if)# no shutdown n1000v(config-if)#	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	**exit** **Example:** n1000v(config-if)# exit n1000v(config)#	Returns you to the CLI Global Configuration mode.
Step 5	**show interface port-channel** *channel-number* **Example:** n1000v(config-router)# show interface port-channel 2	(Optional) Displays interface information for the specified port channel.
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.

This 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

1. **config t**
2. **interface port-channel** *channel-number*
3. **description**
4. **exit**
5. **show interface port-channel** *channel-number*
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into the CLI Global Configuration Mode

Step 2	**interface port-channel** *channel-number*
	
	Example:
	`n1000v(config)# interface port-channel 2`
	`n1000v(config-if)`
		Places you into Interface Configuration mode for the specified port channel interface.

Step 3	**description**
	
	Example:
	`n1000v(config-if)# description engineering`
	`n1000v(config-if)#`
		Adds a description to the port channel interface.
		• Up to 80 characters
		• Default: no description

Step 4	**exit**
	
	Example:
	`n1000v(config-if)# exit`
	`n1000v(config)#`
		Returns you to Global Configuration mode.

Step 5	**show interface port-channel** *channel-number* **Example**: `n1000v(config-router)# show interface port-channel 2`	(Optional) Displays interface information for the specified port channel.
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.

This 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 the 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** *type slot/port*
3. **channel-group** *number* **mode** {**active** | **on** | **passive**}
4. **show port-channel summary**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Places you in the CLI Global Configuration mode.

Step 2	**interface** *type slot/port*
	
	Example:
	switch(config)# interface ethernet 1/4
	switch(config-if)
		Specifies an Ethernet or vEthernet interface to configure, and places you into the Interface Configuration mode for that interface.

Step 3	**channel-group** *number* **mode** {**active** | **on** | **passive**} **Example:** switch(config-if)# channel-group 5 mode active	Specifies the port mode as active or passive for the 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.

	Command	Purpose
Step 4	**show port-channel summary** **Example:** `switch(config-if)# show port-channel summary`	(Optional) Displays summary information about the port channels.
Step 5	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

This example shows how to set the LACP-enabled interface to the active port-channel mode for Ethernet interface 1/4 in channel group 5:

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

Configuring the Speed and Duplex Settings for a Port Channel Interface

You can 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:

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

SUMMARY STEPS

1. **config t**
2. **interface port-channel** *channel-number*
3. **speed** {**10** | **100** | **1000** | **auto**}
4. **duplex** {**auto** | **full** | **half**}
5. **exit**
6. **show interface port-channel** *channel-number*
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into the CLI Global Configuration Mode.

Step 2	**interface port-channel** *channel-number*
	
	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 n1000v(config-if)#	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 n1000v(config-if)#	Sets the duplex for the port channel interface. The default is auto for autonegotiation.
Step 5	**exit** **Example:** n1000v(config-if)# exit n1000v(config)#	Exits the interface mode and returns to the configuration mode.
Step 6	**show interface port-channel** *channel-number* **Example**: n1000v(config-router)# show interface port-channel 2	(Optional) Displays interface information for the specified port channel.
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.

This 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
```

Configuring Port Channel Load Balance

Use this procedure to configure port channel load balance for the entire device or one module.

BEFORE YOU BEGIN

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

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

- 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 CLI 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 n1000v(config)#	Configures the load balance method for the device or module. The range depends on the device. The default load balancing method is source MAC address.
Step 3	**show port-channel load-balance** **Example**: n1000v(config-router)# show port-channel load-balance	(Optional) Displays the port channel load balance 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.

This example shows how to configure source IP load balance for port channels on module 5:

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

Restoring Load Balance Default Method

Use this procedure to restore the default load balance method.

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into the CLI Global Configuration mode.

Step 2	**no port-channel load-balance ethernet** **Example:** `n1000v(config)# no port-channel load-balance ethernet`	Restores the default load balance method, source MAC address.
Step 3	**show port-channel load-balance** **Example:** `n1000v(config-router)# show port-channel load-balance`	(Optional) Displays the port channel load balance 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

Use the following commands to display port channel configuration information.

Command	Purpose
show interface port-channel *channel-number*	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** *channel-number*]	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 port-channel *channel-number*	Displays information on the running configuration of the port channel.

For more information about command output, see the *Cisco Nexus 1000V Command Reference, Beta 2 Release*.

```
n1000v# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
1     Po1(SU)     Eth      NONE      Eth3/2(P)    Eth3/3(P)    Eth3/4(P)
                                     Eth3/5(P)    Eth3/6(P)
0      2           2  VIRT     UP    UP    1  Trunk
```

Displaying Statistics

Use the following commands to display port channel interface configuration information,

Command	Purpose
clear counters interface port-channel *channel-number*	Clears the counters.
show interface counters [**module** *module*]	Displays input and output octets unicast packets, multicast packets, and broadcast packets.
show interface counters detailed [**all**]	Displays input packets, bytes, and multicast and output packets and bytes.
show interface counters errors [**module** *module*]	Displays information on the number of error packets.

Port Channel Example Configuration

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
```

Default Settings

The following table lists the default settings for port channels.

Parameters	Default
Port channel	Admin up
Load balancing method for Layer 3 interfaces	Source and destination IP address
Load balancing method for Layer 2 interfaces	Source and destination MAC address
Load balancing per module	Disabled
Channel mode	on

Additional References

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

- Related Documents, page 5-27
- Standards, page 5-27

Related Documents

Related Topic	Document Title
Configuring Layer 2 interface	Chapter 3, "Configuring Layer 2 Interfaces"
System management	*Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(1)*
Release Notes	*Cisco Nexus 1000V Release Notes, Release 4.0(4)SV1(1)*

Standards

Standards	Title
IEEE 802.3ad	—

CHAPTER 6

Supported RFCs

This appendix lists the IETF RFCs for interfaces supported in Cisco Nexus 1000V Beta 1 release.

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*

INDEX

I

J

L

V