Cisco Nexus 1000V InterCloud Interface Configuration Guide, Release 5.2(1)IC1(1.1)

First Published: June 28, 2013

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-29146-01

CONTENTS

Preface

This preface contains the following sections:

Audience

This publication is for network administrators who configure and maintain Cisco Nexus devices.

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

- An understanding of virtualization
- Using VMM software to create a virtual machine and configure a VMware vSwitch
- Ability to create an account on provider cloud such as Amazon Web Services (AWS).
- Knowledge of VMware vNetwork Distributed Switch is not required.

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).

Convention	Description
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch 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:

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 for Cisco Nexus 1000V InterCloud

This section lists the documents used with the Cisco Nexus 1000V InterCloud and available on Cisco.com at the following URL:

http://www.cisco.com/en/US/partner/products/ps12904/tsd_products_support_series_home.html

General Information

Cisco Nexus 1000V InterCloud Release Notes

Install and Upgrade

Cisco Nexus 1000V InterCloud Installation Guide

Configuration Guides

Cisco Nexus 1000V InterCloud License Configuration Guide

Cisco Nexus 1000V InterCloud High Availability and Redundancy Configuration Guide

Cisco Nexus 1000V InterCloud Interface Configuration Guide

Cisco Nexus 1000V InterCloud Layer 2 Configuration Guide

Cisco Nexus 1000V InterCloud Port Profile Configuration Guide

Cisco Nexus 1000V InterCloud Security Configuration Guide

Cisco Nexus 1000V InterCloud System Management Configuration Guide

Reference Guides

Cisco Nexus 1000V InterCloud Command Reference

Cisco Nexus 1000V InterCloud Verified Scalability Reference

Cisco Nexus 1000V MIB Quick Reference

Troubleshooting and Alerts

Cisco Nexus 1000V Password Recovery Procedure

Cisco Nexus 1000V Documentation

Cisco Nexus 1000V for VMware vSphere Documentation

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

Cisco Prime Network Services Controller Documentation

http://www.cisco.com/en/US/products/ps13213/tsd_products_support_series_home.html

Documentation Feedback

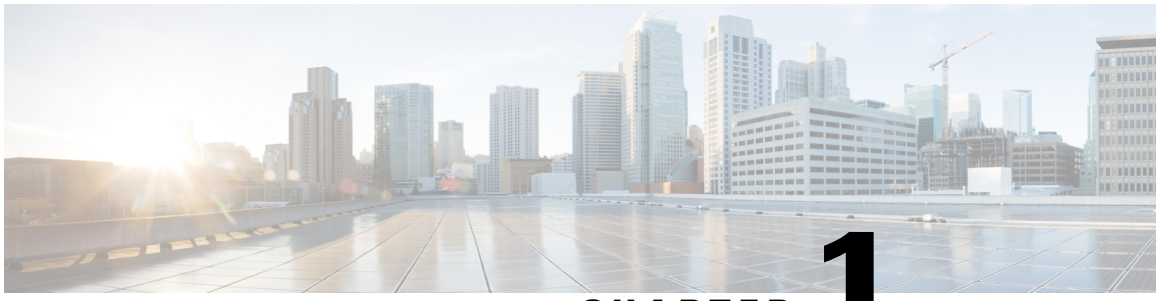
To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus1k-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

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

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

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



CHAPTER 1

Overview

This chapter contains the following sections:

Information About Interfaces

Virtual Ethernet Interfaces

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

- VM (interfaces connected to VM NICs)

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

Management Interface

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

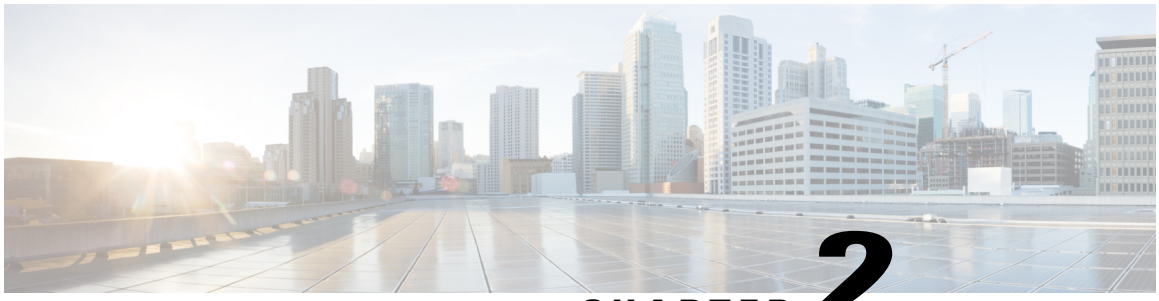
Simplifying the Interface Configuration with Port Profiles

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

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

High Availability for Interfaces

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



CHAPTER 2

Configuring Interface Parameters

This chapter contains the following sections:

Information About the Basic Interface Parameters

Description

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

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

Administrative Status

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

Guidelines and Limitations

Interface parameters have the following guidelines and limitations:

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

Specifying an Interface to Configure

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

Before You Begin

You are logged in to the CLI in EXEC mode.

Procedure

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

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

Configuring a Description

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

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *interface*	Enters interface configuration mode for the specified interface.
Step 3	switch(config-if)# **description** *string*	Adds a description of up to 80 alphanumeric characters for the interface and saves it in the running configuration.
Step 4	switch(config-if)# **show interface** *interface*	(Optional) Displays the interface status, which includes the description.
Step 5	switch(config-if)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to set the interface description:

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

Shutting Down and Activating an Interface

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

Before You Begin

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

Procedure

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

	Command or Action	Purpose
Step 3	switch(config-if)# **shutdown**	Disables the interface in the running configuration .
Step 4	switch(config-if)# **show interface** *interface*	(Optional) Displays the interface status, which includes the administrative status.
Step 5	switch(config-if)# **no shutdown**	Reenables the interface in the running configuration .
Step 6	switch(config-if)# **show interface** *interface*	(Optional) Displays the interface status, which includes the administrative status. • For the management interface, use **mgmt 0** or **mgmt0**.
Step 7	switch(config-if)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to shut down vethernet interafce:

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

Clearing the Interface Counters

You can use this procedure to clear the interface counters.

Before You Begin

You are logged in to the CLI in EXEC mode, configuration mode, or interface configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **clear counters** *interface*	Clears the counters for the specified interface: • **vethernet** *number* • **mgmt 0** or **mgmt0**
Step 2	switch# **show interface** *interface*	(Optional) Displays the interface status, which includes the counters, for the specified interface:

	Command or Action	Purpose
		• **vethernet** *number* • **mgmt 0** or **mgmt0**

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

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

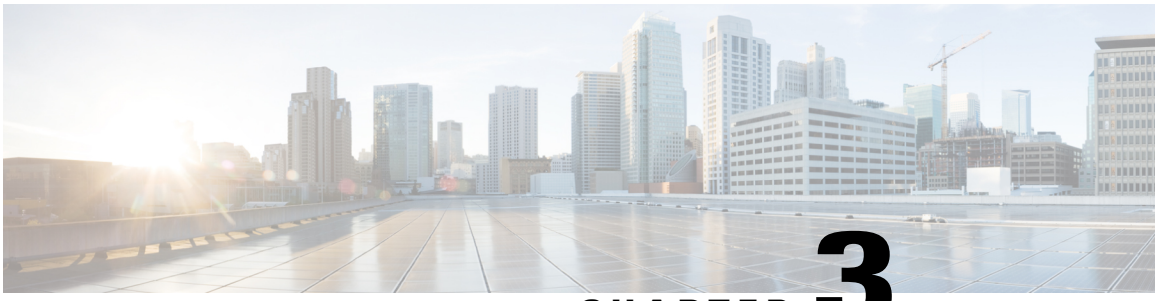
Verifying the Basic Interface Parameters

Use one of the following commands to verify the configuration:

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

Feature History for Basic Interface Parameters

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



CHAPTER 3

Configuring Layer 2 Interfaces

This chapter contains the following sections:

Information About Access and Trunk Interfaces

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

Note For information about configuring a Switched Port Analyzer (SPAN) destination interface, see the *Cisco Nexus 1000V InterCloud System Management Configuration Guide*.

Note For information about VLANs, MAC address tables, see the *Cisco Nexus 1000V InterCloud Layer 2 Configuration Guide*.

High Availability

The software supports high availability for Layer 2 ports.

Prerequisites for VLAN Trunking

VLAN trunking has the following prerequisite:

You are logged into the CLI.

Guidelines and Limitations

VLAN trunking has the following guidelines and limitations:

- Do not connect devices with access links because access links may partition a VLAN.
- When connecting Cisco switches through an 802.1Q trunk, make sure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning tree loops might result.
- If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled.
- If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.

Default Settings

Table 1: Default Settings for Access and Trunk Interfaces

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

Configuring a LAN Interface as a Layer 2 Access Port

An access port transmits packets on only one untagged VLAN. You can specify the VLAN, and it becomes the access VLAN. If you do not specify a VLAN for an access port, that interface carries traffic only on the default VLAN 1.

Procedure

Step 1 switch# **configure terminal**
Enters global configuration mode.

Step 2 switch(config)# [no] **vlan** *vlan-id*
Creates or deletes, and saves in the running configuration, a VLAN or a range or VLANs.

Step 3 switch(config)# **port-profile type vethernet** *name*
Enters port profile configuration mode for the named port profile. If the port profile does not already exist, it is created using the following characteristics:

- *name*—The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V.
- **type**—(Optional) The port profile type is vEthernet.

Step 4 switch(config-port-prof)# **switchport mode access**
Sets port mode access.

Step 5 switch(config-port-prof)# **switchport access vlan** [*vlan-id-access*]
Assigns an access VLAN ID to this port profile.

Note An access port transmits packets on only one untagged VLAN. You can specify the VLAN, and it becomes the access VLAN. If you do not specify a VLAN for an access port, that interface carries traffic only on the default VLAN 1. If you do not specify a VLAN ID, then VLAN 1 is used automatically.

Step 6 switch(config-port-prof)# **no shutdown**
Administratively enables all ports in the profile.

Step 7 switch(config-port-prof)# **state enabled**
Enables the port profile and applies its configuration to the assigned ports.

Step 8 switch(config-port-prof)# **system vlan** *vlan-id*
Adds system VLAN to this port profile. Specify the VLAN as configured in step 5.

Step 9 switch(config-port-prof)# **publish port-profile** <*name*>
Publishes port profile to Cisco Prime Network Services Controller.

Step 10 (Optional) switch(config-port-prof)# **copy running-config startup-config**
Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

```
switch# configure terminal
switch(config)# port-profile type vethernet mgmt-access
switch(config-port-prof)# switchport mode access
switch(config-port-prof)# switchport access vlan 72
switch(config-port-prof)# no shutdown
switch(config-port-prof)# state enabled
switch(config-port-prof)# system vlan 72
switch(config-port-prof)# publish port-profile mgmt-access
switch(config-port-prof)#
```

Configuring Trunk Ports

You can 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.
- A trunk port transmits untagged packets for one VLAN plus encapsulated, tagged, packets for multiple VLANs.
- The device supports 802.1Q encapsulation only.
- Be aware that the Cisco Nexus 1000V commands may differ from the Cisco IOS commands.

Procedure

Step 1 switch# **configure terminal**
Enters global configuration mode.

Step 2 switch(config)# [no] **vlan** *vlan-id*
Creates or deletes, and saves in the running configuration, a VLAN or a range or VLANs.

Step 3 switch(config)# **port-profile** [**type vethernet**] *name*
Enters port profile configuration mode for the named port profile. If the port profile does not already exist, it is created using the following characteristics:

- *name*—The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V.
- **type**—(Optional) The port profile type is vEthernet.

Step 4 switch(config-port-prof)# **switchport mode trunk**
Designates that the interfaces are to be used as a trunking ports.

A trunk port transmits untagged packets for the native VLAN and transmits encapsulated, tagged packets for all other VLANs.

Step 5 switch(config-port-prof)# **switchport trunk allowed vlan** {*allowed-vlans* | **add** *add-vlans* | **except** *except-vlans* | **remove** *remove-vlans* | **all** | **none**}
Designates the port profile as trunking and defines VLAN access to it as follows:

- *allowed-vlans*—Defines VLAN IDs that are allowed on the port.
- **add**—Lists VLAN IDs to add to the list of those allowed on the port.
- **except**—Lists VLAN IDs that are not allowed on the port.
- **remove**—Lists VLAN IDs whose access is to be removed from the port.
- **all**—Indicates that all VLAN IDs are allowed on the port, unless exceptions are also specified.
- **none**—Indicates that no VLAN IDs are allowed on the port.

Note If you do not configure allowed VLANs, then the default VLAN 1 is used as the allowed VLAN.

Step 6 switch(config-port-prof)# **no shutdown**
Administratively enables all ports in the profile.

Step 7 switch(config-port-prof)# **state enabled**
Enables the port profile and applies its configuration to the assigned ports.

Step 8 switch(config-port-prof)# **system vlan** *vlan-id*
Adds system VLAN to this port profile.

Step 9 switch(config-port-prof)# **publish port-profile** <*name*>
Publishes port profile to Cisco Prime Network Services Controller.

Step 10 (Optional) switch(config-port-prof)# **copy running-config startup-config**
Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

This example shows how to configure a trunk port profile.

```
switch# configure terminal
switch(config)# port-profile  port-profile type vethernet Trunk_To_Cloud
switch(config-port-prof)# switchport mode trunk
switch(config-port-prof)# switchport trunk allowed vlan 72,2315-2350
switch(config-port-prof)# no shutdown
switch(config-port-prof)# state enabled
switch(config-port-prof)# max ports 64
switch(config-port-prof)# system vlan 72
switch(config-port-prof)# publish port-profile
switch(config-port-prof)#
```

Verifying the Interface Configuration

Use one of the following commands to verify the access and trunk interface configuration information:

Command	Purpose
show interface vethernet [**brief** | **capabilities** | **counters** | **mac-address** | **status** | **switchport** | **trunk**]	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.
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 vethernet	Displays configuration information about the specified interface.

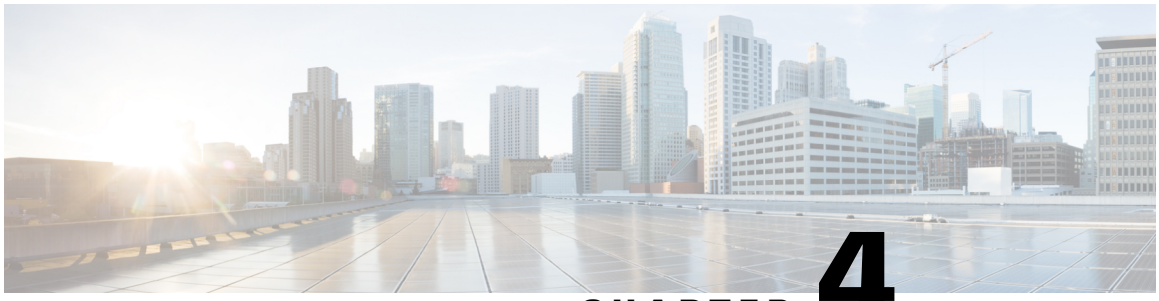
Monitoring the Interface Configuration

Use one of the following commands to display access and trunk interface configuration information:

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.

Feature History for Layer 2 Interface Parameters

Feature Name	Releases	Feature Information
Layer 2 interface parameters	Release 5.2(1)IC1(1.1)	This feature was introduced



CHAPTER 4

Configuring Virtual Ethernet Interfaces

This chapter contains the following sections:

Information About vEthernet Interfaces

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

- VM (interfaces connected to VM NICs)

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

vEthernet interfaces are mapped to connected ports by MAC address as well as DVPort number. When a server administrator changes the port profile assignment on a vNIC or hypervisor port, the same vEthernet interface is reused.

When bringing up a vEthernet interface where a change in the port profile assignment is detected, the Virtual Supervisor Module (VSM) automatically purges any manual configuration present on the interface. You can use the following command to prevent purging of the manual configuration:

no svs veth auto-config-purge

Guidelines and Limitations

vEthernet interface configuration has the following guideline and limitation:

MTU cannot be configured on a vEthernet interface.

Default Settings

Table 2: Default Settings for vEthernet Interface

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
Automatic deletion of vEthernet interfaces	Enabled
Automatic purge of manual configuration on vEthernet interfaces	Enabled
Automatic creation of vEthernet interfaces	Enabled

Configuring a vEthernet Access Interface

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

Before You Begin

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

Procedure

Step 1 switch# **configure terminal**
Enters global configuration mode.

Step 2 switch(config)# [no] **vlan** *vlan-id*
Creates or deletes, and saves in the running configuration, a VLAN or a range or VLANs.

Step 3 switch(config)# **port-profile type vethernet** *name*
Enters port profile configuration mode for the named port profile. If the port profile does not already exist, it is created using the following characteristics:

- *name*—The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V.
- **type**—(Optional) The port profile type is vEthernet.

Step 4 switch(config-port-prof)# **switchport mode access**
Sets port mode access.

Step 5 switch(config-port-prof)# **switchport access vlan** [*vlan-id-access*]
Assigns an access VLAN ID to this port profile.

Note An access port transmits packets on only one untagged VLAN. You can specify the VLAN, and it becomes the access VLAN. If you do not specify a VLAN for an access port, that interface carries traffic only on the default VLAN 1. If you do not specify a VLAN ID, then VLAN 1 is used automatically.

Step 6 switch(config-port-prof)# **no shutdown**
Administratively enables all ports in the profile.

Step 7 switch(config-port-prof)# **state enabled**
Enables the port profile and applies its configuration to the assigned ports.

Step 8 switch(config-port-prof)# **system vlan** *vlan-id*
Adds system VLAN to this port profile. Specify the VLAN as configured in step 5.

Step 9 switch(config-port-prof)# **publish port-profile** <*name*>
Publishes port profile to Cisco Prime Network Services Controller.

Step 10 (Optional) switch(config-port-prof)# **copy running-config startup-config**
Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

```
switch# configure terminal
switch(config)# port-profile type vethernet mgmt-access
switch(config-port-prof)# switchport mode access
switch(config-port-prof)# switchport access vlan 72
switch(config-port-prof)# no shutdown
switch(config-port-prof)# state enabled
switch(config-port-prof)# system vlan 72
switch(config-port-prof)# publish port-profile mgmt-access
switch(config-port-prof)#
```

Enabling or Disabling a vEthernet Interface

You can use this procedure to enable or disable a vEthernet interface.

Before You Begin

You are logged in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface vethernet** *interface-number*	Enters the interface configuration mode for the specified vEthernet interface (from 1 to 1048575).
Step 3	switch(config-if)# [**no**] **shutdown**	Enables or disables the vEthernet interface in the running configuration: • **shutdown**: Disables the vEthernet interface. • **no shutdown**: Enables the vEthernet interface.
Step 4	switch(config-if)# **show interface**	(Optional) Displays the interface status and information.
Step 5	switch(config-if)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to enable a vEthernet interface:

```
switch# configure terminal
switch(config)# interface vethernet 100
switch(config-if)# no shutdown
switch(config-if)# show interface veth100 status
```

Verifying the vEthernet Interface Configuration

Use one of the following commands to verify the configuration:

Command	Purpose
show interface vethernet *interface-number* [**brief** | **counters** [**detailed** [**all**] | **errors**] | **description** | **mac-address** | **status** [**down** | **err-disabled** | **inactive** | **module** *num* | **up**] | **switchport**]	Displays the vEthernet interface configuration.

Command	Purpose
show interface [**vethernet** *interface-number*]	Displays the complete interface configuration.
show interface [**vethernet** *interface-number*] **brief**	Displays abbreviated interface configuration.
show interface [**vethernet** *interface-number*] **description**	Displays the interface description.
show interface [**vethernet** *interface-number*] **mac-address**	Displays the interface MAC address. **Note** For vEth interfaces this shows the MAC address of the connected device.
show interface [**vethernet** *interface-number*] **status** [**down** | **err-disabled** | **inactive** | **module** *num* | **up**]	Displays interface line status.
show interface [**vethernet** *interface-number*] **switchport**	Displays interface switchport information.
show interface virtual [**vm** [*vm_name*]] [**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.
show interface virtual attach binding	Displays the hypervisor ports bound to the vEthernet.
show interface virtual attach binding detail	Displays the UUID of the Distributed Virtual Switch if available.
show interface virtual attach connectee device	Displays the name of the device connected to the vEthernet.
show interface virtual attach connectee *id*	Displays the ID of the port connected to the vEthernet.
show interface virtual attach connectee name	Displays the name of the entity (such as VM) connected to the vEthernet.
show interface virtual attach connectee status	Displays the attach status of the vEthernet and the port profile in use.
show interface virtual vem-info	Displays the VEM specific info for the vEthernet.

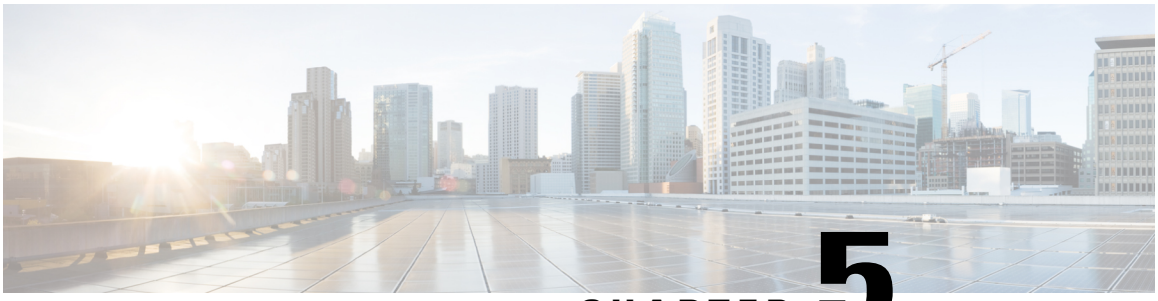
Monitoring the vEthernet Interface Configuration

Use one of the following commands to monitor the vEthernet interface configuration:

Command	Purpose
show interface [**vethernet** *interface-number*] **counters**	Displays the interface incoming and outgoing counters.
show interface [**vethernet** *interface-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** *interface-number*] **counters errors**	Displays the interface error counters.

Feature History for vEthernet Interfaces

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



CHAPTER 5

Configuring Top-N Reports

This chapter contains the following sections:

Top-N Reports Overview

Top-N reports allows you to collect and analyze data for each interface on a switch. The statistics for each port are sorted by one of the statistic types that are listed in the following table.

Table 3: Valid Top-N Statistic Types

Statistic Type	Definition
broadcast	Number of input/output broadcast packets
bytes	Number of input/output bytes
multicast	Number of input/output multicast packets
drops	Number of drops
packets	Number of input/output packets
utilization	Utilization

Top-N Reports Operation

When you enter the **collect top** command, processing begins and the system prompt reappears immediately. When processing completes, the reports are not displayed immediately on the screen; the reports are saved for later viewing. The Top-N reports notify you when the reports are complete by sending a syslog message to the screen.

To view the completed reports, enter the **show top counters interface report** command. Only completed reports are displayed. For reports that are not completed, there is a short description of the process information.

To terminate a Top-N reports process, enter the **clear top counters interface report** command. Pressing Ctrl-C does not terminate Top-N reports processes. The completed reports remain available for viewing until you remove them by entering the **clear top counters interface report**{ **all** *report_num* } command.

Collecting Interface Statistics for Top-N Reports

When enabling Top-N reports creation, note the following information:

- You can specify the number of busiest ports for which to create reports (the default is 20).
- You can specify the statistic type by which ports are determined to be the busiest (the default is utilization). The supported values for statistic_type are broadcast, bytes, multicast, drop, packets, and utilization.
- You can specify the interval over which statistics are collected (range: 0 through 999; the default is 30 seconds). For utilization report the interval range is 10-999.
- Except for a utilization report (configured with the sort-by utilization keywords), you can specify an interval of zero to create a report that displays the current counter values instead of a report that displays the difference between the start-of-interval counter values and the end-of-interval counter values.
- You can collect up to a max of five reports

Procedure

	Command or Action	Purpose
Step 1	switch(config)# **collect top** [*num*] **counters interface**{*all* | *vEthernet*}[**sort-by**{ **broadcast** | **bytes** | **drops** | **multicast** | **packets** | **utilization** }] [**interval** *seconds*]	Collects interface statistics for a Top-N report. **Note** You can get the interface statistics for a Top-N report sorted by broadcast, bytes, drops, multicast, packets, and utilization for vEthernet interfaces. In this release, the Cisco Nexus 1000V InterCloud supports only vEthernet interfaces.

This example shows how to collect interface statistics for Top-N reports for an interval of 76 seconds for the four ports with the highest utilization:

```
switch# collect top 4 counters interface all sort-by utilization interval 76
```

Displaying Top-N Reports

You can use this procedure to display Top-N reports. Top-N reports statistics are not displayed in the following situations:

- If a port is not present during the first poll.
- If a port is not present during the second poll.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# **show top counters interface report**	Displays Top-N reports. **Note** To display information about all the reports, do not enter the report number.
Step 2	switch(config)# **show top counters interface report** [*report_num*]	Displays Top-N reports for a specific report number.

This example shows how to display information about all the Top-N reports:

```
switch# show top counters interface report
```

This example shows how to display information about a specific Top-N report:

```
switch# show top counters interface report 1
```

Clearing Top-N Reports

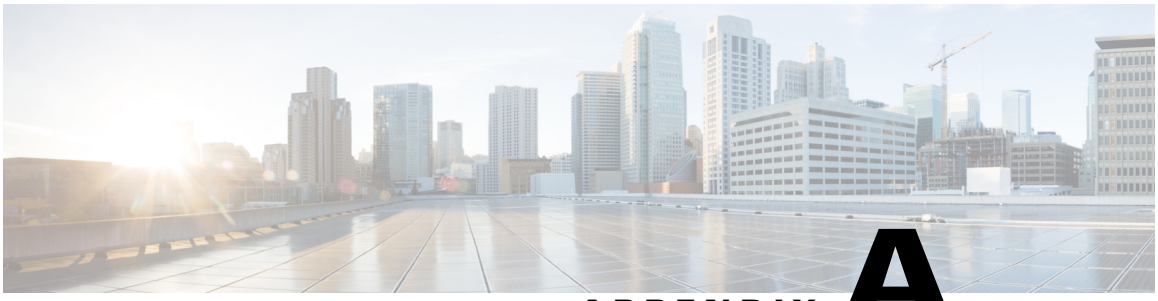
You can use this procedure to clear Top-N reports.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# **clear top counters interface report** {**all**|*rep_num* }	Clears all the Top-N reports. You can specify a particular report or you can use **all** to clear all reports. You can also use this command to cancel a report which is being collected.

This example shows how to remove Top-N reports:

```
switch# clear top counters interface report 4
```



APPENDIX A

Supported RFCs

This chapter contains the following sections:

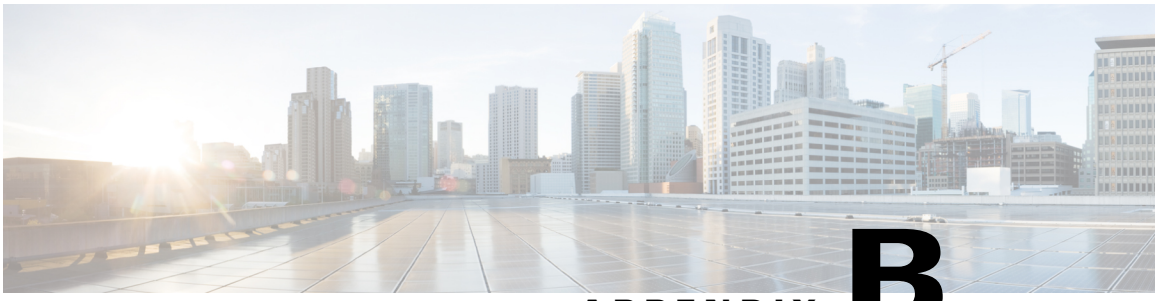
Supported RFCs

The following tables lists the supported IETF RFCs for interfaces.

Table 4: IP Services RFCs

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

Supported RFCs



APPENDIX B

Interface Configuration Limits

This chapter contains the following sections:

Interface Configuration Limits

The configuration limits are documented in the *Cisco Nexus 1000V InterCloud Verified Scalability Reference*.

Interface Configuration Limits