Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV2(2.1)

First Published: June 21, 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-28789-01

CONTENTS

Preface

Preface vii

Audience vii

Document Conventions vii

Related Documentation for Nexus 1000V Series NX-OS Software for VMware vSphere ix

Documentation Feedback x

Obtaining Documentation and Submitting a Service Request x

CHAPTER 1

New and Changed Information 1

New and Changed Information 1

CHAPTER 2

Overview 5

Information About Port Profiles and Port Groups 5

Information About Live Policy Changes 6

Information About Uplink Profiles 6

Information About Port Profile Inheritance 6

Consistent Port Profile Configuration 7

Information About Atomic Inheritance 7

Information About Rollback to a Consistent Configuration 7

Information About Interface Quarantine 7

CHAPTER 3

Creating Port Profiles 9

Information About Port Profiles 9

Information About Port Profile States 9

Information About vEthernet Port Binding 10

Guidelines and Limitations for Creating Port Profiles 10

Default Settings 11

Configuring Port Profiles 12

Creating a Port Profile 12
Configuring VMware Attributes 13
Port Mode Configuration 15
VLAN Ranges 15
Configuring a Trunking Profile 15
Configuring an Access Profile 18
Clearing a Port Management Policy 19
Port Binding for vEthernet Port Profiles Configuration 21
Configuring a Default Port Binding Type 21
Configuring Port Binding for a vEthernet Port Profile 22
Configuring a Port Profile with Dynamic or Static Port Binding 24
Verifying Port Binding on vCenter Server 26
Enabling a Port Profile 27
Removing a Port Profile 28
Standards for Creating Port Profiles 30
Feature History for Port Profiles 30

CHAPTER 4 Configuring Port Profile Inheritance 31
Information About Port Profile Inheritance 31
Guidelines and Limitations for Configuring Port Profile Inheritance 32
Inheriting a Configuration from a Port Profile 33
Removing Inherited Policies from a Port Profile 34

CHAPTER 5 Configuring System Port Profiles 37
Information About System Port Profiles 37
Guidelines and Limitations for System Port Profiles 37
Creating a System Port Profile 38
Deleting System VLANs from a Port 41
Modifying the System VLANs in a Trunk Mode Port Profile 41
Converting a Port Profile to an Access Profile with a System VLAN 42
Converting an Access Port Profile to a Trunk Port Profile 44
Modifying System VLANs in an Access Mode Port Profile 45
Feature History for System Port Profiles 47

CHAPTER 6 Configuring a Private VLAN in a Port Profile 49

Information About Private VLANs 49
Configuring a Port Profile as a Private VLAN 49
Feature History for Private VLAN Port Profiles 52

CHAPTER 7 Restricting Port Profile Visibility 53
Information About Restricting Port Profile Visibility 53
Information About Port Profile Visibility 53
Information About Allow Groups or Users 53
Guidelines and Limitations for Restricting Port Profile Visibility 54
Defining DVS Access in vSphere Client 55
Enabling the Port Profile Role Feature 58
Restricting Port Profile Visibility on the VSM 59
Removing a Port Profile Role 62
Feature History for Restricting Port Profile Visibility 63

CHAPTER 8 Verifying the Port Profile Configuration 65
Verifying the Port Profile Configuration 65
Feature History for Port Profile Verification 68

APPENDIX A Port Profile Configuration Limits 71
Port Profile Configuration Limits 71

Preface

This preface contains the following sections:

- Audience, page vii
- Document Conventions, page vii
- Related Documentation for Nexus 1000V Series NX-OS Software for VMware vSphere, page ix
- Documentation Feedback , page x
- Obtaining Documentation and Submitting a Service Request, page x

Audience

This publication is for experienced 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 VMware software to create a virtual machine and configure a VMware vSwitch

Note 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.

Convention	Description
[x]	Square brackets enclose an optional element (keyword or argument).
[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 Nexus 1000V Series NX-OS Software for VMware vSphere

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

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

General Information

Cisco Nexus 1000V Documentation Roadmap

Cisco Nexus 1000V Release Notes

Cisco Nexus 1000V and VMware Compatibility Information

Install and Upgrade

Cisco Nexus 1000V Installation and Upgrade Guide

Configuration Guides

Cisco Nexus 1000V High Availability and Redundancy Configuration Guide

Cisco Nexus 1000V Interface Configuration Guide

Cisco Nexus 1000V Layer 2 Switching Configuration Guide

Cisco Nexus 1000V License Configuration Guide

Cisco Nexus 1000V Network Segmentation Manager Configuration Guide

Cisco Nexus 1000V Port Profile Configuration Guide

Cisco Nexus 1000V Quality of Service Configuration Guide

Cisco Nexus 1000V REST API Plug-in Configuration Guide

Cisco Nexus 1000V Security Configuration Guide

Cisco Nexus 1000V System Management Configuration Guide

Cisco Nexus 1000V vCenter Plugin Configuration Guide

Cisco Nexus 1000V VXLAN Configuration Guide

Programming Guide

Cisco Nexus 1000V XML API Configuration Guide

Reference Guides

Cisco Nexus 1000V Command Reference

Cisco Nexus 1000V Resource Availability Reference

Troubleshooting and Alerts

Cisco Nexus 1000V Troubleshooting Guide

Cisco Nexus 1000V Password Recovery Procedure

Cisco NX-OS System Messages Reference

Cloud Services Platform Documentation

The *Cisco Cloud Services Platform* documentation is available at http://www.cisco.com/en/US/partner/products/ps12752/tsd_products_support_series_home.html.

Virtual Security Gateway Documentation

The *Cisco Virtual Security Gateway for Nexus 1000V Series Switch* documentation is available at http://www.cisco.com/en/US/products/ps11208/tsd_products_support_model_home.html.

Virtual Wide Area Application Services (vWAAS) Documentation

The *Virtual Wide Area Application Services* documentation is available at http://www.cisco.com/en/US/products/ps6870/tsd_products_support_series_home.html.

ASA 1000V Cloud Firewall Documentation

The *ASA 1000V Cloud Firewall* documentation is available at http://www.cisco.com/en/US/products/ps12233/tsd_products_support_series_home.html.

Documentation Feedback

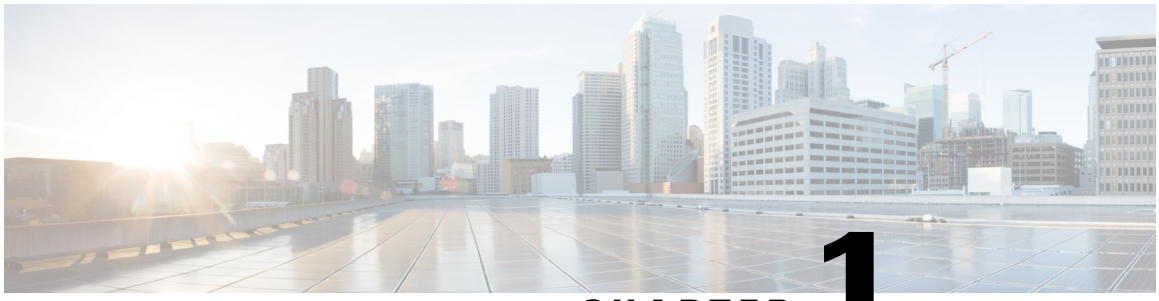
To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus1k-docfeedback@cisco.com . We appreciate your feedback.

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

New and Changed Information

This chapter contains the following sections:

- New and Changed Information, page 1

New and Changed Information

This section lists new and changed content in this document by software release.

To find additional information about new features or command changes, see the following:

- *Cisco Nexus 1000V Release Notes*
- *Cisco Nexus 1000V Command Reference*

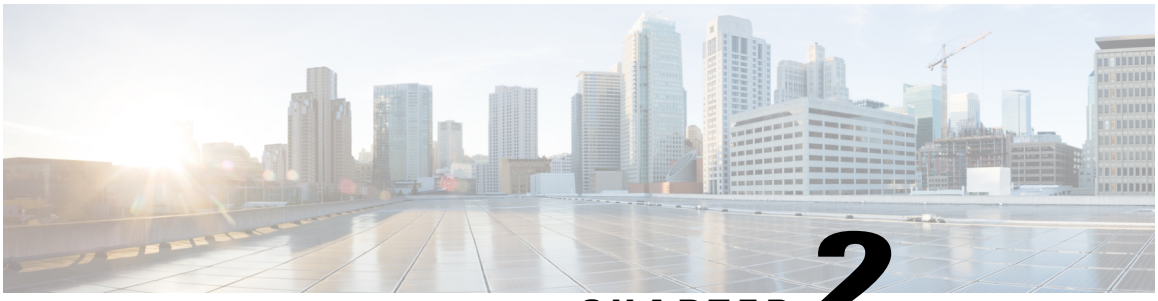
Table 1: New and Changed Information

Feature	Description	Changed in release	Where Documented
Port binding	You can configure a static port binding with the **auto** option.	4.2(1)SV1(4a)	Configuring Port Binding for a vEthernet Port Profile, on page 22
Port binding	You can configure a port binding with the dynamic [auto] option.	4.2(1)SV1(4a)	Configuring Port Binding for a vEthernet Port Profile, on page 22
Port channel	The "Creating a Port Profile for a Port Channel" chapter was moved into the *Cisco Nexus 1000V Interface Configuration Guide*.	4.2(1)SV1(4)	Configuring Port Channels

Feature	Description	Changed in release	Where Documented
Port binding	You can configure port binding for vEthernet port profiles that affects how VMware port IDs are assigned.	4.2(1)SV1(4)	Configuring Port Binding for a vEthernet Port Profile, on page 22
Restrict the visibility of Port Profiles	Restricts port profile visibility by user or user group.	4.2(1)SV1(4)	Restricting Port Profile Visibility on the VSM, on page 59
mtu command added	The **mtu** command replaces the **system mtu** command for uplink, Ethernet type port profiles.	4.2(1)SV1(4)	Creating a System Port Profile, on page 38
system mtu command removed	The **system mtu** command is removed and replaced by the **mtu** command for port profiles.	4.2(1)SV1(4)	Creating a System Port Profile, on page 38
show port-profile sync-status command added	Displays interfaces that are out of sync with the port profile.	4.2(1)SV1(4)	Verifying the Port Profile Configuration, on page 65
show port-profile virtual usage command added	Displays the port profile usage by interface.	4.2(1)SV1(4)	Verifying the Port Profile Configuration, on page 65
Atomic Inheritance	Port profile configuration applied to member interfaces.	4.2(1)SV1(4)	Information About Atomic Inheritance, on page 7
Port Profile Rollback	After configuration failure, a port profile and its member interfaces are rolled back to the last good configuration.	4.2(1)SV1(4)	Information About Rollback to a Consistent Configuration, on page 7
Interface Quarantine	After a configuration failure, interfaces are shut down to maintain accurate configuration.	4.2(1)SV1(4)	Information About Interface Quarantine, on page 7

Feature	Description	Changed in release	Where Documented
system mtu command	This command allows you to preserve a non-default MTU setting on the PNIC attached to the Cisco Nexus 1000V across reboots of the ESX server.	4.0(4)SV1(3)	Creating a System Port Profile, on page 38
show running-config port-profile	New command for displaying the port profile configuration.	4.0(4)SV1(2)	Verifying the Port Profile Configuration, on page 65
Uplink port profile	Port profiles are not classified as uplink, but are, instead, configured as Ethernet or vEthernet.	4.0(4)SV1(2)	Cisco Nexus 1000V Interface Configuration Guide
Configuration limits	Added configuration limits for vEthernet interfaces, vEthernet trunks, port profiles, system profiles, and PVLANs.	4.0(4)SV1(2)	Port Profile Configuration Limits, on page 71
vPC-Host Mode	Support for the following: • Manual creation of subgroups. • Connecting to upstream switches that do not support port channels using MAC Pinning.	4.0(4)SV1(2)	Cisco Nexus 1000V Interface Configuration Guide
MAC Pinning	Connecting to upstream switches that do not support port channels using the MAC-pinning command.	4.0(4)SV1(2)	Cisco Nexus 1000V Interface Configuration Guide
Static Pinning	Support for pinning or directing traffic for a vEthernet interface, control VLAN, or packet VLAN to a specific port channel subgroup.	4.0(4)SV1(2)	Cisco Nexus 1000V Interface Configuration Guide

Feature	Description	Changed in release	Where Documented
Port Profile Type	Creation of port-profiles includes the optional type field, which specifies the port profile as either Ethernet or vEthernet. By default, a port profiles is created as a vEthernet type.	4.0(4)SV1(2)	Creating a Port Profile, on page 12
[**no**] **capability uplink** command	The capability uplink command has been superseded by the port-profile [type {ethernet | vethernet}] name command. To configure a port profile with uplink capability, configure the port profile as an Ethernet type.	4.0(4)SV1(2)	Creating a Port Profile, on page 12
show running-config command	This command now shows the port profile type (Ethernet or vEthernet). Also, you can optionally specify to show only the port profile configurations.	4.0(4)SV1(2)	Verifying the Port Profile Configuration, on page 65
show port-profile *name* command	This command shows the port profile type and does not show the capability uplink. This command also shows the pinning and channel-group configuration.	4.0(4)SV1(2)	Verifying the Port Profile Configuration, on page 65



CHAPTER 2

Overview

This chapter contains the following sections:

- Information About Port Profiles and Port Groups, page 5
- Information About Live Policy Changes, page 6
- Information About Uplink Profiles, page 6
- Information About Port Profile Inheritance , page 6
- Consistent Port Profile Configuration, page 7

Information About Port Profiles and Port Groups

A port profile is a collection of interface-level configuration commands that are combined to create a complete network policy.

A port group is a representation of a port profile on the VMware vCenter server. Every port group on the VMware vCenter server is associated with a port profile on the Cisco Nexus 1000V. Network administrators configure port profiles, and then server administrators can use the corresponding port groups on the VMware vCenter server to assign ports to port profiles.

In the VMware vCenter Server, a port profile is represented as a port group. You assign the vEthernet or Ethernet interfaces to a port group in VMware vCenter to do the following:

- Define port configuration by policy.
- Apply a single policy across a large number of ports.

Port profiles are created on the VSM and propagated to VMware vCenter Server as VMware port groups using the VMware VIM API. After propagation, a port profile appears within VMware vSphere Client and is available to apply to the vNICs on a virtual machine.

Information About Live Policy Changes

Port profiles are not static entities but dynamic policies that can change as network needs change. Changes to active port profiles are applied to each switch port that is using the profile. This simplifies the process of applying new network policies or changing an existing policy.

Information About Uplink Profiles

Port profiles also manage the physical NICs within a VMware ESX host. When a port profile is defined, the network administrator determines whether the profile will be used to manage vEthernet interfaces or physical NICs. By default, the port profile is assumed to be used for vEthernet management.

To define a port profile for use on physical NICs, the network administrator must create the profile as an Ethernet type. When this option is used, the port profile will be available only to the server administrator to apply to physical NICs within an VMware ESX server.

Note In an installation where multiple Ethernet port profiles are active on the same VEM, it is recommended that they do not carry the same VLAN(s). The allowed VLAN list should be mutually exclusive.

Overlapping VLANs can be configured but may cause duplicate packets to be received by virtual machines in the network.

Uplink port profiles are applied to a physical NIC when a VMware ESX host is first added to the Cisco Nexus 1000V. The server administrator is presented with a dialog box in which they can select the following:

- physical NICs to associate with the VEM
- uplink port profiles to associate with the physical NICs

In addition, the server administrator can apply uplink port profiles to interfaces that are added to the VEM after the host has been added to the switch.

Information About Port Profile Inheritance

You can apply the configuration from an existing port profile as the default configuration for another port profile. This is called inheritance. The configuration of the parent is copied to and stored in the child port profile. You can also override the inheritance by configuring the attributes explicitly in the child port profile.

You can also explicitly remove port profile inheritance, so that a port profile returns to the default settings, except where there has been a direct configuration.

Consistent Port Profile Configuration

Information About Atomic Inheritance

To maintain a consistent configuration among the interfaces in a port profile, the entire port profile configuration is applied to its member interfaces (sometimes referred to as inheritance).

This is new in Release 4.2(1)SV1(4), and the concept is called Atomic Inheritance. In previous Cisco Nexus 1000V releases, whatever configuration could be applied from the port profile was applied to its interfaces, and whatever was not applicable was ignored.

Information About Rollback to a Consistent Configuration

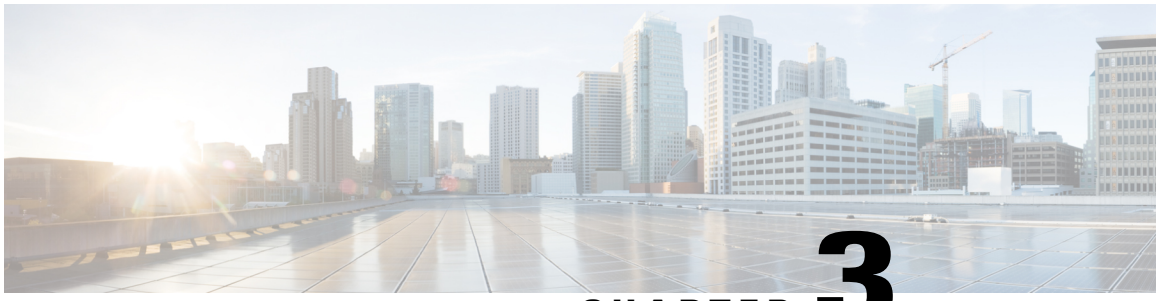
When you update the configuration in a port profile, its member interfaces are also updated. If the configuration fails, the port profile and its member interfaces are rolled back to the last known good configuration for the port profile.

Information About Interface Quarantine

Interfaces are sectioned off and shut down when a port profile configuration is in error. This is a new feature in Release 4.2(1)SV1(5.1), and is called Interface Quarantine.

When an interface is quarantined, it maintains its mapping to the port profile, but is administratively shut down until you explicitly bring it up using the no shutdown command. If the port profile configuration is still in error, then the interface is again shut.

If you create a port profile with a command error, for example a private VLAN mapping error or service policy map error, then an attempt to apply this port profile to an interface shuts down the interface. The error is not copied to the interface and a system message is generated with details of the error. In this case, you must correct the error in the port profile, return the interface to service, and apply the corrected port profile to the interface.



CHAPTER 3

Creating Port Profiles

This chapter contains the following sections:

- Information About Port Profiles, page 9
- Guidelines and Limitations for Creating Port Profiles, page 10
- Default Settings, page 11
- Configuring Port Profiles, page 12
- Port Mode Configuration, page 15
- Port Binding for vEthernet Port Profiles Configuration, page 21
- Enabling a Port Profile, page 27
- Removing a Port Profile, page 28
- Standards for Creating Port Profiles, page 30
- Feature History for Port Profiles, page 30

Information About Port Profiles

Information About Port Profile States

The following table describes port profile behavior.

State	Behavior
Disabled (the default)	When disabled, a port profile behaves as follows: • Its configuration is not applied to assigned ports. • If exporting policies to a VMware port group, the port group is not created on the vCenter Server.

State	Behavior
Enabled	When enabled, a port profile behaves as follows: • Its configuration is applied to assigned ports. • If configured with the VMware port-group attribute, the port group is created on the vCenter Server.

Information About vEthernet Port Binding

You can configure either static, dynamic, or ephemeral port binding for vEthernet port profiles. The following table shows how this setting controls how ports are assigned in the VMware port group.

Type	Behavior
Static (the default)	A DVPortID is assigned from the port group pool when you first assign the port group to the port. The DVPortID persists for the life of the network adapter. The port group has a fixed number of ports.
Dynamic	A DVPortID is assigned to a virtual machine only when the virtual machine is powered on and its NIC is in a connected state. The DVPortID is freed when the virtual machine is powered off or the virtual machine's NIC is disconnected. Virtual machines connected to a port group configured with dynamic binding must be powered on and off through the VMware vCenter Server. Dynamic binding can be used in environments where you have more virtual machines than available ports, but do not plan to have a greater number of virtual machines active than you have available ports. For example, if you have 300 virtual machines and 100 ports, but will never have more than 90 virtual machines active at one time, then dynamic binding would be appropriate for your port group.
Ephemeral	A new DVPortID is assigned to the port every time the VM is powered on. The port keeps this same DVPortID while the VM is up. All available DVS ports are shared. Ports are not allocated from the port group pool. **Note** If a system administrator changes the port profile assignment for an interface, any manual configuration on the interface is purged if either port profile is configured with ephemeral port binding. This purging of manual configurations occurs regardless of your auto purge setting.

Guidelines and Limitations for Creating Port Profiles

- Once a port profile is created as either an Ethernet or vEthernet type, you cannot change the type.
- In an installation where multiple Ethernet port profiles are active on the same VEM, it is recommended that they do not carry the same VLAN(s). The allowed VLAN list should be mutually exclusive.

Overlapping VLANs can be configured but may cause duplicate packets to be received by virtual machines in the network.

- To maintain consistency between the port profile definition and what is applied to an interface, if a port profile modification is rejected by any port, the modification is rejected by the port profile too.
- If you create a port profile with a command error, for example a private VLAN mapping error or service policy map error, then an attempt to apply this port profile to an interface shuts down the interface. The error is not copied to the interface and a system message is generated with details of the error. In this case, you must correct the error in the port profile. Then return the interface to service and apply the corrected port profile using the following command sequence:

1 **no shutdown**

2 **default shutdown**

For more information, see the *Cisco Nexus 1000V Troubleshooting Guide*.

- MTU can only be configured for uplink, Ethernet type port profiles.
- If you configure MTU for an Ethernet port profile, your ESX host may generate the following error:

```
2010 Nov 15 04:35:27 my-n1k %VEM_MGR-SLOT3-1-VEM_SYSLOG_ALERT: vssnet :
sf_platform_set_mtu: Failed setting MTU for VMW port with portID 33554475.
```

  In this case, the MTU value you have set is not supported by the VEM physical NIC. See your VMware documentation for more information about supported MTU for PNIC.
- Before configuring a port profile, the Cisco Nexus 1000V software must be initially configured. For information, see the *Cisco Nexus 1000V Installation and Upgrade Guide*.
- The Cisco Nexus 1000V must be connected to the VMware vCenter Server.

Default Settings

The following table lists the default settings in the port profile configuration.

Parameter	Default
capability l3control	No
description	-
administrative state	all ports disabled
switchport mode (**access** or **trunk**)	**access**
system vlan *vlan_list*	-
type	**vethernet**
access port vlan	VLAN 1
max-ports	32

Parameter	Default
min-ports	32
vmware port-group *name*	Port profile name
vEthernet port-bindings	Static

Configuring Port Profiles

Creating a Port Profile

Before You Begin

- You are logged in to the CLI in EXEC mode.
- You know whether the ports need to be initialized with system settings.
- You have identified the characteristics needed for this port profile.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **port-profile** [**type** {**ethernet** | **vethernet**}] *name*
3. (Optional) switch(config-port-prof)# **description** *profile_description*
4. (Optional) switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [*name profile-name*]
5. (Optional) switch(config-port-prof)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** [**type** {**ethernet** | **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 can be Ethernet or vEthernet. Once configured, the type cannot be changed. The default is the vEthernet type. Defining a port profile type as Ethernet allows the port profile to be used for physical (Ethernet) ports. In the vCenter Server, the

	Command or Action	Purpose
		corresponding port group can be selected and assigned to physical ports (PNICs). **Note** If a port profile is configured as an Ethernet type, then it cannot be used to configure VMware virtual ports.
Step 3	switch(config-port-prof)# **description** *profile_description*	(Optional) Adds a description of up to 80 ASCII characters in length to the port profile. This description is automatically pushed to vCenter Server.
Step 4	switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [*name profile-name*]	(Optional) Displays the configuration for verification.
Step 5	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to create a new port profile:

```
switch(config)# port-profile type ethernet AllAccess1
switch(config-port-prof)# description all_access
switch(config-port-prof)# show port-profile name AllAccess1
port-profile AllAccess1
  description: all_access
  type: ethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: -
  inherit:
  config attributes:
  evaluated config attributes:
  assigned interfaces:
switch(config-port-prof)#
```

Configuring VMware Attributes

Before You Begin

- You are logged in to the CLI in EXEC mode.
- You know if you will configure the VMware port group with the same name as the port profile or if you will specify an alternate name for the VMware port group.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **port-profile** [**type** {**ethernet** | **vethernet**}] *name*
3. switch(config-port-prof)# **vmware port-group** [*pg_name*]
4. switch(config-port-prof)# **max-ports** *num*
5. (Optional) switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
6. (Optional) switch(config-port-prof)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** [**type** {**ethernet** | **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 can be Ethernet or vEthernet. Once configured, the type cannot be changed. The default is the vEthernet type. Defining a port profile type as Ethernet allows the port profile to be used for physical (Ethernet) ports. In the vCenter Server, the corresponding port group can be selected and assigned to physical ports (PNICs). **Note** If a port profile is configured as an Ethernet type, then it cannot be used to configure VMware virtual ports.
Step 3	switch(config-port-prof)# **vmware port-group** [*pg_name*]	Designates the port profile as a VMware port group. The port profile is mapped to a VMware port group of the same name unless you specify a name here. When you connect the VSM to vCenter Server, the port group is distributed to the virtual switch on the vCenter Server.
Step 4	switch(config-port-prof)# **max-ports** *num*	Designates the maximum number of ports that can be assigned to this non-uplink port profile. The default is 32 ports. When the specified maximum number of ports is reached, no more ports can be assigned.
Step 5	switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]	(Optional) Displays the configuration for verification.
Step 6	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Port Mode Configuration

VLAN Ranges

In accordance with the IEEE 802.1Q standard, up to 4094 VLANs are supported. The following table describes the available VLAN ranges and their use.

Table 2: VLAN Ranges

VLAN Numbers	Range	Usage
1	Normal	Cisco default. You can use this VLAN, but you cannot modify or delete it.
2-1005	Normal	You can create, use, modify, and delete these VLANs.
1006-4094	Extended	You can create, name, and use these VLANs. You cannot change the following parameters: • State is always active. • VLAN is always enabled. You cannot shut down these VLANs.
3968-4047 and 4094	Internally allocated	These 80 VLANs, plus VLAN 4094, are allocated for internal device use. You cannot create, delete, or modify any VLANs within the block reserved for internal use.

Configuring a Trunking Profile

Before You Begin

- You are logged in to the CLI in EXEC mode.
- You have already created the port profile using the Creating a Port Profile, on page 12 procedure.
- You know the needed VLAN configuration for this port profile and that it is to be used in trunk mode.
- A VLAN must already be created on the switch before you can assign it to a port profile.
- You know the supported VLAN ranges described in Configuring Port Mode.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **port-profile** [**type** {**ethernet** | **vethernet**}] *name*
3. switch(config-port-prof)# **switchport mode trunk**
4. switch(config-port-prof)# **no shutdown**
5. (Optional) switch(config-port-prof)# **switchport trunk allowed vlan** {*allowed-vlans* | **add** *add-vlans* | **except** *except-vlans* | **remove** *remove-vlans* | **all** | **none**}
6. (Optional) switch(config-port-prof)# **switchport trunk native vlan** *vlan-id*
7. (Optional) switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
8. (Optional) switch(config-port-prof)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** [**type** {**ethernet** | **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 can be Ethernet or vEthernet. Once configured, the type cannot be changed. The default is the vEthernet type. Defining a port profile type as Ethernet allows the port profile to be used for physical (Ethernet) ports. In the vCenter Server, the corresponding port group can be selected and assigned to physical ports (PNICs). **Note** If a port profile is configured as an Ethernet type, then it cannot be used to configure VMware virtual ports.
Step 3	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 4	switch(config-port-prof)# **no shutdown**	Administratively enables all ports in the profile.
Step 5	switch(config-port-prof)# **switchport trunk allowed vlan** {*allowed-vlans* | **add** *add-vlans* | **except** *except-vlans* | **remove** *remove-vlans* | **all** | **none**}	(Optional) 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.

	Command or Action	Purpose
		• **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)# **switchport trunk native vlan** *vlan-id*	(Optional) Sets the trunking native characteristics when the interface is in trunking mode. If you do not configure a native VLAN, then the default VLAN 1 is used as the native VLAN.
Step 7	switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]	(Optional) Displays the configuration for verification.
Step 8	switch(config-port-prof)# **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 trunking port profile, allowing all VLANs, and setting VLAN 3 as its native VLAN.

```
switch# configure terminal
switch(config)# port-profile TrunkProf
switch(config-port-prof)# switchport mode trunk
switch(config-port-prof)# no shutdown
switch(config-port-prof)# switchport trunk allowed vlan all
switch(config-port-prof)# switchport trunk native vlan 3
switch(config-port-prof)# show port-profile name TrunkProf
port-profile TrunkProf
  description:
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    switchport mode trunk
    switchport trunk native vlan 3
    switchport trunk allowed vlan all
    no shutdown
  evaluated config attributes:
    switchport mode trunk
    switchport trunk native vlan 3
    switchport trunk allowed vlan all
    no shutdown
  assigned interfaces:
switch(config-port-prof)#
```

Configuring an Access Profile

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.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **port-profile** [**type** {**ethernet** | **vethernet**}] *name*
3. switch(config-port-prof)# **switchport mode access**
4. switch(config-port-prof)# **no shutdown**
5. (Optional) switch(config-port-prof)# **switchport access vlan** [*vlan-id-access*]
6. (Optional) switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
7. (Optional) switch(config-port-prof)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** [**type** {**ethernet** | **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 can be Ethernet or vEthernet. Once configured, the type cannot be changed. The default is the vEthernet type. Defining a port profile type as Ethernet allows the port profile to be used for physical (Ethernet) ports. In the vCenter Server, the corresponding port group can be selected and assigned to physical ports (PNICs). **Note** If a port profile is configured as an Ethernet type, then it cannot be used to configure VMware virtual ports.
Step 3	switch(config-port-prof)# **switchport mode access**	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 4	switch(config-port-prof)# **no shutdown**	Administratively enables all ports in the profile.
Step 5	switch(config-port-prof)# **switchport access vlan** [*vlan-id-access*]	(Optional) Assigns an access VLAN ID to this port profile.

	Command or Action	Purpose
		Note If you do not specify a VLAN ID, then VLAN 1 is used automatically.
Step 6	switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]	(Optional) Displays the configuration for verification.
Step 7	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to configure a port profile with switch access ports, enabling the ports, and then adding an access VLAN:

```
switch# configure terminal
switch(config)# port-profile AccessProf
switch(config-port-prof)# switchport mode access
switch(config-port-prof)# no shutdown
switch(config-port-prof)# switchport access vlan 300
switch(config-port-prof)# show port-profile name AccessProf
port-profile AccessProf
  description: allaccess4
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group: AccessProf
  max ports: 5
  inherit:
  config attributes:
    switchport mode access
    switchport access vlan 300
    no shutdown
  evaluated config attributes:
    switchport mode access
    switchport access vlan 300
    no shutdown
  assigned interfaces:
switch(config-port-prof)#
```

Clearing a Port Management Policy

You can use this procedure to remove either of the following port management policies from an existing port profile configuration:

- **shutdown**
- **switchport mode**

Note After removing the configuration for an attribute, the attribute does not appear in **show** command output.

Before You Begin

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

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **port-profile** *name*
3. **default** {**shutdown** | **switchport mode**}
4. (Optional) switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
5. (Optional) switch(config-port-prof)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** *name*	Enters port profile configuration mode for the named port profile.
Step 3	**default** {**shutdown**	**switchport mode**}	Removes either the shutdown or the switchport mode configuration from the port profile. • **shutdown—**Reverts port profile ports to the shutdown state. • **switchport mode—**Reverts port profile ports to switch access ports.
Step 4	switch(config-port-prof)# **show port-profile** [**brief**	**expand-interface**	**usage**] [**name** *profile-name*]	(Optional) Displays the configuration for verification.
Step 5	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to change the administrative state of a port profile back to its default setting (all ports disabled):

```
switch# configure treminal
switch(config)# port-profile AccessProf
switch(config-port-prof)# default shutdown
switch(config-port-prof)# show port-profile name AccessProf
port-profile AccessProf
  description: allaccess4
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: 8
  pinning packet-vlan: 8
  system vlans: none
  port-group: AccessProf
```

```
  max ports: 5
  inherit:
  config attributes:
    switchport mode access
  evaluated config attributes:
    switchport mode access
  assigned interfaces:
switch(config-port-prof)#
```

Port Binding for vEthernet Port Profiles Configuration

Configuring a Default Port Binding Type

You can use this procedure to configure the type of port binding (static, dynamic, or ephemeral) to apply by default to all new vEthernet port profiles.

Before You Begin

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

- You are logged in to the CLI in EXEC mode.
- You know the type of port binding (static, dynamic, or ephemeral) you want to use as a default for all new vEthernet port profiles.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **port-profile default port-binding** {**static** [**auto**] **dynamic** [**auto**] | **ephemeral**}
3. (Optional) switch(config-port-prof)# **show running-config**
4. (Optional) switch(config-port-prof)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile default port-binding** {**static** [**auto**] **dynamic** [**auto**] | **ephemeral**}	Configures a default port binding type to be applied automatically to all new vEthernet port profiles unless explicitly configured otherwise: • **Static**: A DVPortID is assigned from the port group pool when you first assign the port group to the port. The DVPortID persists for the life of the network adapter. The port group has a fixed number of ports. If you include the **auto** option, Cisco Nexus 1000V creates port profiles with both min-ports and max-ports, which are initially inherited from the global defaults and can be redefined by the user at a later time. By configuring the binding type with the **auto** option, Cisco Nexus 1000V adjusts the number of

	Command or Action	Purpose
		ports per profile created at the vCenter server based on the usage of the port groups. • **Dynamic**: A DVPortID is assigned to a virtual machine only when the virtual machine is powered on and its NIC is in a connected state. The DVPortID is freed when the virtual machine is powered off or the virtual machine's NIC is disconnected. The **auto** option for dynamic binding works as described for static binding. • **Ephemeral**: A new DVPortID is assigned to the port every time the VM is powered on. The port keeps this same DVPortID while the VM is up. All available DVS ports are shared. Ports are not allocated from the port group pool.
Step 3	switch(config-port-prof)# **show running-config**	(Optional) Displays the configuration for verification.
Step 4	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to configure the dynamic port binding type as the default for all new vEthernet port profiles created:

```
switch# configure terminal
switch(config)# port-profile default port-binding dynamic
switch(config-port-prof)#
```

Configuring Port Binding for a vEthernet Port Profile

You can use this procedure to configure the type of port binding (static, dynamic, or ephemeral) for an existing vEthernet port profile.

Before You Begin

- You are logged in to the CLI in EXEC mode.
- You have already created the vEthernet port profile using Creating a Port Profile, on page 12.
- You know the type of port binding (static, dynamic, or ephemeral) you want to apply to this vEthernet port profile.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **port-profile** [**type** {**vethernet**}] *profile-name*
3. switch(config-port-prof)# **port-binding** {**static** [**auto**] **dynamic** [**auto**] | **ephemeral**}
4. (Optional) switch(config-port-prof)# **show port-profile** [**name** *profile-name*]
5. (Optional) switch(config-port-prof)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** [**type** {**vethernet**}] *profile-name*	Enters port profile configuration mode for the named vEthernet port profile.
Step 3	switch(config-port-prof)# **port-binding** {**static** [**auto**] **dynamic** [**auto**] | **ephemeral**}	Configures a default port binding type to be applied automatically to all new vEthernet port profiles unless explicitly configured otherwise: • **Static**: A DVPortID is assigned from the port group pool when you first assign the port group to the port. The DVPortID persists for the life of the network adapter. The port group has a fixed number of ports. ◦ **auto**: Port profiles are created with both min-ports and max-ports, which are initially inherited from the global defaults and can be redefined by the user at a later time. By configuring the binding type with the **auto** option, the Cisco Nexus 1000V will adjust the number of ports per profile created at the vCenter server based on the usage of the port groups. • **Dynamic**: A DVPortID is assigned to a virtual machine only when the virtual machine is powered on and its NIC is in a connected state. The DVPortID is freed when the virtual machine is powered off or the virtual machine's NIC is disconnected. ◦ See **auto** option above. • **Ephemeral**: A new DVPortID is assigned to the port every time the VM is powered on. The port keeps this same DVPortID while the VM is up. All available DVS ports are shared. Ports are not allocated from the port group pool.
Step 4	switch(config-port-prof)# **show port-profile** [**name** *profile-name*]	(Optional) Displays the configuration for verification.

	Command or Action	Purpose
Step 5	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to configure the dynamic port binding type for the existing port profile named target-pp.

```
switch# configure terminal
switch(config)# port-profile target-pp
switch(config-port-prof)# port-binding dynamic
switch(config-port-prof)#
```

Configuring a Port Profile with Dynamic or Static Port Binding

You can use this procedure to configure a port profile (static or dynamic) with or without the auto option.

Before You Begin

You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **port-profile** [**type** {**vethernet**}] *profile-name*
3. switch(config-port-prof)# **vmware port-group** [*pg_name*]
4. switch(config-port-prof)# **port-binding** {**static** [**auto**] **dynamic** [**auto**] | **ephemeral**}
5. switch(config-port-prof)# **max-ports** *number*
6. switch(config-port-prof)# **min-ports** *number*
7. switch(config-port-prof)# **state enabled**
8. (Optional) switch(config-port-prof)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** [**type** {**vethernet**}] *profile-name*	Enters port profile configuration mode for the named vEthernet port profile.
Step 3	switch(config-port-prof)# **vmware port-group** [*pg_name*]	Designates the port profile as a VMware port group. The port profile is mapped to a VMware port group of the same name unless you specify a name here. When you connect the VSM to vCenter Server, the port group is distributed to the virtual switch on the vCenter Server.

	Command or Action	Purpose
Step 4	switch(config-port-prof)# **port-binding** {**static** [**auto**] **dynamic** [**auto**] | **ephemeral**}	Configures a default port binding type to be applied automatically to all new vEthernet port profiles unless explicitly configured otherwise: • **Static**: A DVPortID is assigned from the port group pool when you first assign the port group to the port. The DVPortID persists for the life of the network adapter. The port group has a fixed number of ports. ◦ **auto**: Port profiles are created with both min-ports and max-ports, which are initially inherited from the global defaults and can be redefined by the user at a later time. By configuring the binding type with the **auto** option, the Cisco Nexus 1000V will adjust the number of ports per profile created at the vCenter server based on the usage of the port groups. • **Dynamic**: A DVPortID is assigned to a virtual machine only when the virtual machine is powered on and its NIC is in a connected state. The DVPortID is freed when the virtual machine is powered off or the virtual machine's NIC is disconnected. ◦ See **auto** option above. • **Ephemeral**: A new DVPortID is assigned to the port every time the VM is powered on. The port keeps this same DVPortID while the VM is up. All available DVS ports are shared. Ports are not allocated from the port group pool.
Step 5	switch(config-port-prof)# **max-ports** *number*	Designates the maximum number of ports that can be assigned to this non-uplink port profile. The default value is the global default at the time of port profile creation. When the specified maximum number of ports is reached, no more ports can be assigned. The valid range is 1 to 1024. **Note** Do not configure a value less than min-ports.
Step 6	switch(config-port-prof)# **min-ports** *number*	Designates the minimum number of ports that can be assigned to this non-uplink port profile. The default value is the global default at the time of port profile creation. The valid range is 1 to 1024. **Note** Do not configure a value greater than max-ports.
Step 7	switch(config-port-prof)# **state enabled**	Enables the port profile and applies its configuration to the assigned ports. If the port profile is a VMware port group, the port group will be created in the vswitch on vCenter Server.

	Command or Action	Purpose
Step 8	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to configure the dynamic auto port binding type:

```
switch# configure terminal
switch(config)# port-profile type vethernet dynamic_auto_pp
switch(config-port-prof)# vmware port-group
switch(config-port-prof)# port-binding dynamic auto
switch(config-port-prof)# max-ports 128
switch(config-port-prof)# min-ports 64
switch(config-port-prof)# state enabled
switch(config-port-prof)# copy running-config startup-config
```

Verifying Port Binding on vCenter Server

Before You Begin

You are logged in to vCenter Server on the host.

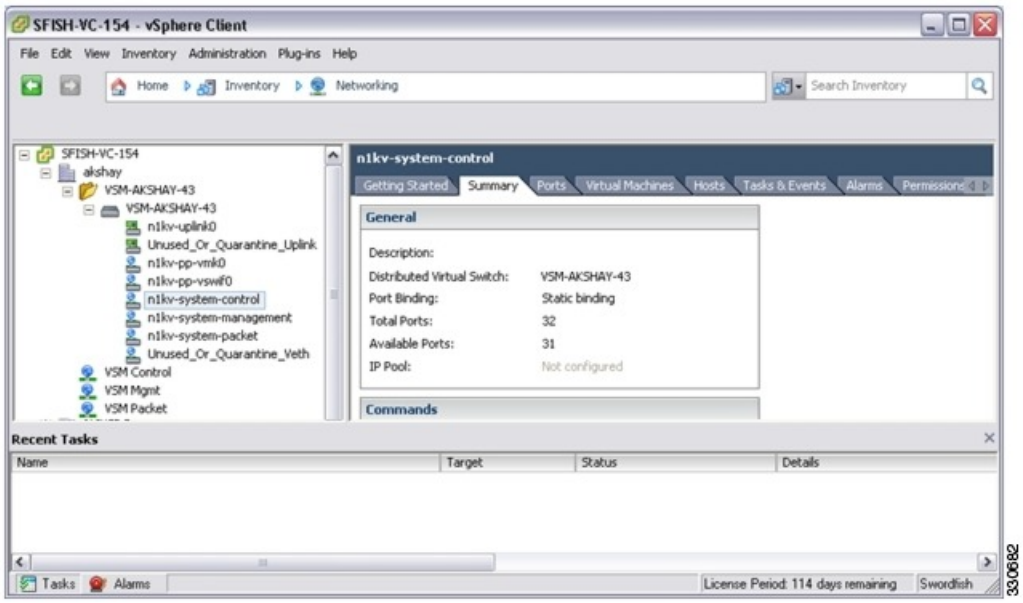
SUMMARY STEPS

1. From your DVS in the **Networking** tab, choose the port group, and then click the **Summary** tab.

DETAILED STEPS

From your DVS in the **Networking** tab, choose the port group, and then click the **Summary** tab.

Figure 1: vSphere Client Summary Tab Window



The **General** section of the **Summary** tab displays the type of port binding for this port group.

Enabling a Port Profile

Before You Begin

- You are logged in to the CLI in EXEC mode.
- You have already created the port profile using Creating a Port Profile, on page 12.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **port-profile** [**type** {**vethernet**}] *profile-name*
3. switch(config-port-prof)# **state enabled**
4. switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
5. (Optional) switch(config-port-prof)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** [**type** {**vethernet**}] *profile-name*	Enters port profile configuration mode for the named vEthernet port profile.
Step 3	switch(config-port-prof)# **state enabled**	Enables the port profile and applies its configuration to the assigned ports. If the port profile is a VMware port group, the port group will be created in the vswitch on vCenter Server.
Step 4	switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]	Displays the configuration for verification.
Step 5	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to enable a port profile.

```
switch# configure terminal
switch(config)# port-profile AccessProf
switch(config-port-prof)# state enabled
switch(config-port-prof)# show port-profile name AccessProf
port-profile AccessProf
  description: allaccess4
  status: enabled
capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    channel-group auto mode on
  evaluated config attributes:
    channel-group auto mode on
  assigned interfaces:
switch(config-port-prof)#
```

Removing a Port Profile

Before You Begin

- You are logged in to the CLI in EXEC mode.
- If the port profile is inherited by another port profile, you need to remove the inheritance from the other port profile before removing this port profile. If you do not remove the inheritance first, the procedure fails. See Removing Inherited Policies from a Port Profile, on page 34.

SUMMARY STEPS

1. switch# **configure terminal**
2. (Optional) switch(config)# **show port-profile virtual usage name** *profile_name*
3. switch(config)# **no port-profile** *profile_name*
4. (Optional) switch(config)# **show port-profile** [**name** *profile-name*]
5. (Optional) switch(config)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **show port-profile virtual usage name** *profile_name*	(Optional) Verifies if active interfaces use this port profile. **Note** You cannot remove a port profile if there are active interfaces associated with it.
Step 3	switch(config)# **no port-profile** *profile_name*	Removes the port profile configuration and operational settings. When you remove a port profile that is mapped to a VMware port group, the associated port group and settings within the vCenter Server are also removed.
Step 4	switch(config)# **show port-profile** [**name** *profile-name*]	(Optional) Displays the configuration for verification.
Step 5	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to remove a port profile:

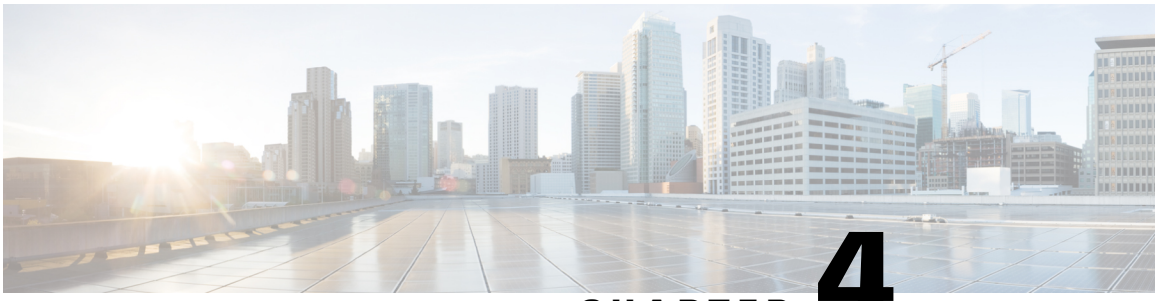
```
switch# configure terminal
switch(config)# show port-profile virtual usage name AccessProf
--------------------------------------------------------------------------------
Port Profile               Port        Adapter        Owner
--------------------------------------------------------------------------------
n1kv-uplink0               Po1
                           Eth3/2      vmnic1         localhost.
                           Eth3/3      vmnic2         localhost.
vlan1767                   Veth7       Net Adapter 1  all-tool-7
AccessProf                 vEth12      vmnic1         localhost.
switch(config)# no port-profile AccessProf
switch(config)# show port-profile name AccessProf
ERROR: port-profile AccessProf does not exist
switch(config)# copy running-config startup-config
switch(config)#
```

Standards for Creating Port Profiles

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

Feature History for Port Profiles

Feature Name	Releases	Feature Information
Port Binding	4.2(1)SV1(4a)	You can configure a static port binding with the **auto** option.
Port Binding	4.2(1)SV1(4a)	You can configure a port binding with the **dynamic** [**auto**] option.
Atomic Inheritance	4.2(1)SV1(4)	Port Profile configuration applied to member interfaces.
Port Profile Rollback	4.2(1)SV1(4)	After configuration failure, a port profile and its member interfaces are rolled back to the last good configuration.
Interface Quarantine	4.2(1)SV1(4)	After a configuration failure, interfaces are shut down to maintain accurate configuration.
Port Profile Type	4.0(4)SV1(2)	Port profiles are configured as either Ethernet or vEthernet type. By default, a port profile is created as vEthernet type.
[**no**] **capability uplink** command	4.0(4)SV1(2)	The **capability uplink** command has been replaced with the **port-profile** [**type** {**ethernet** | **vethernet**}] *name* command. To configure a port profile with uplink capability, configure the port profile as an Ethernet type. The **no capability uplink** command has been removed.
Port Profiles	4.0(4)SV1(1)	This feature was introduced.



CHAPTER 4

Configuring Port Profile Inheritance

This chapter contains the following sections:

- Information About Port Profile Inheritance, page 31
- Guidelines and Limitations for Configuring Port Profile Inheritance, page 32
- Inheriting a Configuration from a Port Profile, page 33
- Removing Inherited Policies from a Port Profile, page 34

Information About Port Profile Inheritance

You can apply the configuration from an existing port profile as the default configuration for another port profile. This is called inheritance. The configuration of the parent port profile is copied to and stored in the child port profile. You can also override the inheritance by configuring the attributes explicitly in the child port profile.

Table 3: Port Profile Inheritance Settings

	Can it be inherited?	
Port Profile Setting	**Yes**	**No**
acl	X	
capability iscsi-multipath	X	
capability l3 control		X
channel group	X	
default (resets characteristic to its default)	X	
description		X

	Can it be inherited?	
Port Profile Setting	**Yes**	**No**
inherit	X	
interface state (shut/no shut)	X	
mtu		X
name	X	
netflow	X	
pinning	X	
port security	X	
private vlan configuration	X	
service-port	X	
state (enabled or disabled)		X
switchport mode (access or trunk)	X	
system vlan vlan list		X
virtual-service-domain	X	
vlan configuration	X	
VMware max-ports		X
VMware port-group name		X

Guidelines and Limitations for Configuring Port Profile Inheritance

- Inherited port profiles cannot be changed or removed from an interface using the Cisco Nexus 1000V CLI. This can only be done through the VMware vCenter Server.
- 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.
- You can change a setting directly on a port profile to override the inherited settings.

- You can also explicitly remove port profile inheritance, so that a port profile returns to the default settings, except where there has been a direct configuration. For more information, see Removing Inherited Policies from a Port Profile, on page 34.
- The Cisco Nexus 1000V software must be initially configured. For information, see the *Cisco Nexus 1000V Installation and Upgrade Guide*.
- The Cisco Nexus 1000V must be connected to the VMware vCenter Server.
- Once a port profile is created, you cannot change its type (Ethernet or vEthernet).

Inheriting a Configuration from a Port Profile

You can use this procedure to apply the configuration from an existing port profile as the default configuration for another port profile.

You are familiar with the port profile characteristics shown in Table 3: Port Profile Inheritance Settings, on page 31 and whether they can be inherited.

Tip The port profile type cannot be inherited from another port profile.

Before You Begin

- You are logged in to the CLI in EXEC mode.
- To identify the port profile with a configuration you want to use, use the **show port profiles** command to view your existing port profiles.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **port-profile** [**type** {**ethernet** | **vethernet**}] *name*
3. switch(config-port-prof)# **inherit port-profile** *name*
4. (Optional) switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [*name profile-name*]
5. (Optional) switch(config-port-prof)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** [**type** {**ethernet** | **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.

	Command or Action	Purpose
		• **type—**(Optional) The port profile type can be Ethernet or vEthernet. Once configured, the type cannot be changed. The default is the vEthernet type. Defining a port profile type as Ethernet allows the port profile to be used for physical (Ethernet) ports. In the vCenter Server, the corresponding port group can be selected and assigned to physical ports (PNICs). **Note** If a port profile is configured as an Ethernet type, then it cannot be used to configure VMware virtual ports.
Step 3	switch(config-port-prof)# **inherit port-profile** *name*	Adds the inherited configuration of the named profile as a default configuration.
Step 4	switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [*name profile-name*]	(Optional) Displays the configuration for verification.
Step 5	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to inherit the port profile configuration of another port profile:

```
switch# configure terminal
switch(config)# port-profile AllAccess2
switch(config-port-prof)# inherit port-profile AllAccess1
switch(config-port-prof)# show port-profile name AllAccess2
port-profile AllAccess2
  description:
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit: port-profile AllAccess1
  config attributes:
  evaluated config attributes:
  assigned interfaces:
switch(config-port-prof)#
```

Removing Inherited Policies from a Port Profile

If you have configured policies independently of inheritance, then they will not be removed when you remove the inheritance. Only the policies that are configured solely through the inheritance are removed.

Before You Begin

You are logged in to the CLI in configuration mode.

SUMMARY STEPS

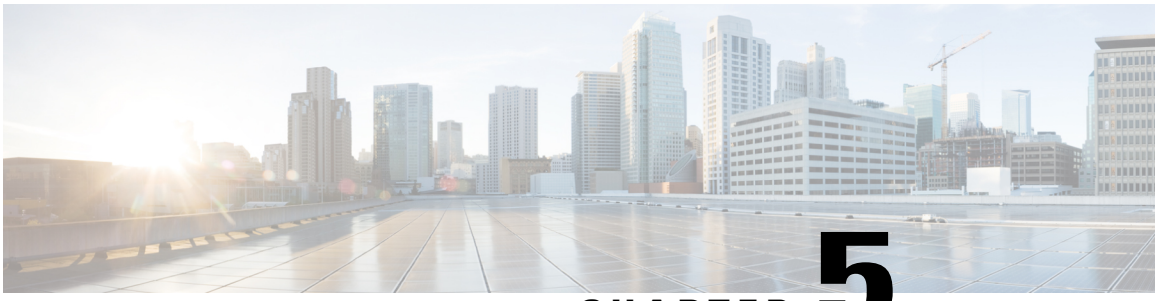
1. switch# **configure terminal**
2. (Optional) switch(config)# **show port-profile virtual usage name** *profile_name*
3. switch(config)# **port-profile** *name*
4. switch(config-port-prof)# **no inherit port-profile** *profile_name*
5. (Optional) switch(config-port-prof)# **show port-profile virtual usage name** *profile_name*
6. (Optional) switch(config-port-prof)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **show port-profile virtual usage name** *profile_name*	(Optional) Displays the policies inherited in the named port profile.
Step 3	switch(config)# **port-profile** *name*	Enters port profile configuration mode for the named port profile.
Step 4	switch(config-port-prof)# **no inherit port-profile** *profile_name*	Removes the inherited policies from the named port-profile. The port profile settings are returned to the defaults, except for the port profile type and any settings that were explicitly configured independent of those inherited.
Step 5	switch(config-port-prof)# **show port-profile virtual usage name** *profile_name*	(Optional) Displays the policies inherited for verification of the removal.
Step 6	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to remove inherited policies from a port profile:

```
switch# configure terminal
switch(config)# show port-profile virtual usage name AccessProf
switch(config)# port-profile Access4
switch(config-port-prof)# no inherit port-profile AccessProf
switch(config-port-prof)# show port-profile virtual usage name AccessProf
switch(config-port-prof)# copy running-config startup-config
```



CHAPTER 5

Configuring System Port Profiles

This chapter contains the following sections:

- Information About System Port Profiles, page 37
- Guidelines and Limitations for System Port Profiles, page 37
- Creating a System Port Profile, page 38
- Deleting System VLANs from a Port, page 41
- Modifying the System VLANs in a Trunk Mode Port Profile, page 41
- Modifying System VLANs in an Access Mode Port Profile, page 45
- Feature History for System Port Profiles, page 47

Information About System Port Profiles

System port profiles are designed to establish and protect those ports and VLANs which need to be configured before the VEM contacts the VSM.

For this reason, the following ports must use system VLANs:

- Control and packet VLANs in the uplinks that communicate with the VSM.
- Management VLAN in the uplinks and VMware kernel NICs used for VMware vCenter server connectivity or SSH or Telnet connections.
- Storage VLAN used by the VSM for VM file system access in the uplinks and VMware kernel NICs used for iSCSI or network file systems. This is needed only in the host that runs the VSM on the VEM.
- VSM ports on the VEM must be system ports.

Guidelines and Limitations for System Port Profiles

- System VLANs must be used sparingly and only as described in the Information About System Port Profiles, on page 37.

- For maximum system port profiles per host and DVS, see the Port Profile Configuration Limits, on page 71.
- In a single ESX host, one VLAN can be a system VLAN on one port but a regular VLAN on another.
- You cannot delete a system VLAN when the port profile is in use.
- You can add or delete VLANs that are not system VLANs when the port profile is in use because one or more distributed virtual switch (DVS) ports are carrying that profile.
- System VLANs can be added to a port profile, even when the port profile is in use.
- You can only delete a system VLAN from a port profile after removing the port profile from service. This is to prevent accidentally deleting a critical VLAN, such as the management VLAN for a host, or the storage VLAN for the VSM.
- A system port profile cannot be converted to a port profile that is not a system port profile.
- The native VLAN on a system port profile can be a system VLAN but it does not have to be.
- When a system port profile is in use, you can change the native VLAN as follows:
  - From one VLAN that is not a system VLAN to another VLAN that is not a system VLAN.
  - From a VLAN that is not a system VLAN to a system VLAN
  - From one system VLAN to another system VLAN
- When a system port profile is in use, you cannot change the native VLAN from a system VLAN to a VLAN that is not a system VLAN.
- Reboots of the ESX can result in an MTU mismatch and failure of the VSM and VEM. If you use an MTU other than 1500 (the default), for example in networks with jumbo frames, then you must configure the MTU in the system port profile so that it is preserved across reboots of the ESX.

Creating a System Port Profile

A system port profile must be of the Ethernet type because it is used for physical ports. This procedure configures the Ethernet type.

Before You Begin

- You are logged in to the CLI in EXEC mode.
- The VSM is connected to vCenter Server.
- You have configured the following:
  - Port admin status is active (no shutdown).
  - Port mode is access or trunk.
  - VLANs that are to be used as system VLANs already exist.
  - VLANs are configured as access VLANs or trunk-allowed VLANs.
- In an installation where multiple Ethernet port profiles are active on the same VEM, it is recommended that they do not carry the same VLAN(s). The allowed VLAN list should be mutually exclusive.

Overlapping VLANs can be configured but may cause duplicate packets to be received by virtual machines in the network.

- For more information, see the *Cisco Nexus 1000V Interface Configuration Guide*.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **port-profile** [**type** {**ethernet** | **vethernet**}] *name*
3. (Optional) switch(config-port-prof)# **description** *profile-description*
4. switch(config-port-prof)# **switchport mode trunk**
5. switch(config-port-prof)# **switchport trunk allowed vlan** {*vlan-id-list* | **all** | **none** | [**add** | **except** | **remove** {*vlan-list*}]}
6. switch(config-port-prof)# **no shutdown**
7. switch(config-port-prof)# **system vlan** *vlan-id-list*
8. (Optional) switch(config-port-prof)# **mtu** *mtu-size*
9. (Optional) switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [*name profile-name*]
10. (Optional) switch(config-port-prof)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** [**type** {**ethernet** | **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 can be Ethernet or vEthernet. Once configured, the type cannot be changed. The default is the vEthernet type. Defining a port profile type as Ethernet allows the port profile to be used for physical (Ethernet) ports. In the vCenter Server, the corresponding port group can be selected and assigned to physical ports (PNICs). **Note** If a port profile is configured as an Ethernet type, then it cannot be used to configure VMware virtual ports. Once a port profile is created, you cannot change its type (Ethernet or vEthernet).
Step 3	switch(config-port-prof)# **description** *profile-description*	(Optional) Adds a description of up to 80 ASCII characters in length to the port profile. This description is automatically pushed to vCenter Server.
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.

	Command or Action	Purpose
Step 5	switch(config-port-prof)# **switchport trunk allowed vlan** {*vlan-id-list* | **all** | **none** | [**add** | **except** | **remove** {*vlan-list*}]}	Designates the port profile as trunking and defines VLAN access to it as follows: • **allowed vlan—**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. 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**	Changes the port to administrative status so that system VLAN can be configured. **Note** If you do not change the port state, then you will see the following error when you try to configure system VLAN: ERROR: Cannot set system vlans. Change port admin status to 'no shutdown' and retry.
Step 7	switch(config-port-prof)# **system vlan** *vlan-id-list*	Adds system VLANs to this port profile.
Step 8	switch(config-port-prof)# **mtu** *mtu-size*	(Optional) Designates the MTU size. • If you do not set the MTU size here, the default of 1500 is used. • Must be an even number between 1500 and 9000. The MTU size you set must be less than or equal to the fixed system jumbomtu size of 9000. The MTU configured on an interface takes precedence over the MTU configured on a port profile. For more information, see the *Cisco Nexus 1000V Interface Configuration Guide*.
Step 9	switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [*name profile-name*]	(Optional) Displays the configuration for verification.
Step 10	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to create a system port profile:

```
switch# configure terminal
switch(config)# port-profile AccessProf
```

```
switch(config-port-prof)# description "System profile for critical ports"
switch(config-port-prof)# system vlan 1
switch(config-port-prof)# show port-profile name AccessProf
port-profile AccessProf
  description:
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: 1
  port-group:
  max ports: 32
  inherit: port-profile xyz
  config attributes:
    switchport mode access
    switchport access vlan 1
    switchport trunk allowed vlan 1-10
    channel-group auto mode on sub-group cdp
    no shutdown
  evaluated config attributes:
    switchport mode access
    switchport access vlan 1
    switchport trunk allowed vlan 1-10
    mtu 1500
    channel-group auto mode on sub-group cdp
    no shutdown
  assigned interfaces:
switch(config-port-prof)#
```

Deleting System VLANs from a Port

Before You Begin

- You are logged in to vCenter Server.
- The VSM is connected to vCenter Server.

SUMMARY STEPS

1. From the vCenter Server, delete the port from the DVS.
2. Add the port to the vCenter Server with a different or modified port profile.

DETAILED STEPS

Step 1 From the vCenter Server, delete the port from the DVS.

Step 2 Add the port to the vCenter Server with a different or modified port profile.

Modifying the System VLANs in a Trunk Mode Port Profile

You can use the following procedures to change the set of system VLANs in a trunk mode port profile without removing all system VLANs.

Before You Begin

- You are logged in to the vCenter server.
- You are logged in to the Cisco Nexus 1000V CLI in EXEC mode.
- The VSM is connected to the vCenter Server.
- You know the VLAN ID of a system VLAN in your network. It does not matter which system VLAN it is.
- You know the VLAN IDs of the system VLANs required for the port profile you are modifying.

SUMMARY STEPS

1. From the upstream switch for each VEM that carries this profile, shut off the switch port that carries the control VLAN.
2. Convert the port profile to an access profile with a system VLAN.
3. Convert the access port profile back to a trunk profile.
4. From the upstream switch for each VEM that carries this profile, unshut the switchport that carries the control VLAN.

DETAILED STEPS

Step 1 From the upstream switch for each VEM that carries this profile, shut off the switch port that carries the control VLAN.

Step 2 Convert the port profile to an access profile with a system VLAN.
See Converting a Port Profile to an Access Profile with a System VLAN, on page 42

Step 3 Convert the access port profile back to a trunk profile.
See Converting an Access Port Profile to a Trunk Port Profile, on page 44

Step 4 From the upstream switch for each VEM that carries this profile, unshut the switchport that carries the control VLAN. The VEMS are reconnected to the VSM.

Converting a Port Profile to an Access Profile with a System VLAN

You can use this procedure to change the set of system VLANs in a trunk mode port profile without removing all system VLANs.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **port-profile** [**type** {**ethernet** | **vethernet**}] *name*
3. switch(config-port-prof)# **no system vlan**
4. switch(config-port-prof)# **switchport mode access**
5. switch(config-port-prof)# **switchport access vlan** *vlan-id*
6. switch(config-port-prof)# **no shutdown**
7. switch(config-port-prof)# **system vlan** *vlan-id-list*

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** [**type** {**ethernet** | **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 can be Ethernet or vEthernet. Once configured, the type cannot be changed. The default is the vEthernet type. Defining a port profile type as Ethernet allows the port profile to be used for physical (Ethernet) ports. In the vCenter Server, the corresponding port group can be selected and assigned to physical ports (PNICs). **Note** If a port profile is configured as an Ethernet type, then it cannot be used to configure VMware virtual ports.
Step 3	switch(config-port-prof)# **no system vlan**	Remove the system VLAN from a port profile.
Step 4	switch(config-port-prof)# **switchport mode access**	Sets port mode access.
Step 5	switch(config-port-prof)# **switchport access vlan** *vlan-id*	Set the access mode of an interface.
Step 6	switch(config-port-prof)# **no shutdown**	Changes the port to administrative status so that system VLAN can be configured. **Note** If you do not change the port state, then you will see the following error when you try to configure system VLAN:ERROR: Cannot set system vlans. Change port admin status to 'no shutdown' and retry.
Step 7	switch(config-port-prof)# **system vlan** *vlan-id-list*	Adds system VLANs to this port profile.

The trunk port profile is converted to an access port profile with a system VLAN.

This example shows how to convert a trunk port profile to an access port profile.

```
switch# configure terminal
switch(config)# port-profile Trunk_System_Prof
switch(config-port-prof)# no system vlan
switch(config-port-prof)# switchport mode access
switch(config-port-prof)# switchport access vlan 1
switch(config-port-prof)# system vlan 300
switch(config-port-prof)#
```

Converting an Access Port Profile to a Trunk Port Profile

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **port-profile** [**type** {**ethernet** | **vethernet**}] *name*
3. switch(config-port-prof)# **switchport mode trunk**
4. **system vlan** *vlan-id-list*
5. (Optional) switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [*name profile-name*]
6. (Optional) switch(config-port-prof)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** [**type** {**ethernet** | **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 can be Ethernet or vEthernet. Once configured, the type cannot be changed. The default is the vEthernet type. Defining a port profile type as Ethernet allows the port profile to be used for physical (Ethernet) ports. In the vCenter Server, the corresponding port group can be selected and assigned to physical ports (PNICs). **Note** If a port profile is configured as an Ethernet type, then it cannot be used to configure VMware virtual ports.

	Command or Action	Purpose
Step 3	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 4	**system vlan** *vlan-id-list*	Adds system VLANs to this port profile.
Step 5	switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [*name profile-name*]	(Optional) Displays the configuration for verification.
Step 6	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to convert an access port profile to a trunk port profile.

```
switch# config terminal
switch(config)# port-profile Trunk_System_Prof
switch(config-port-prof)# switchport mode trunk
switch(config-port-prof)# system vlan 114,115
switch(config-port-prof)# show port-profile name Trunk_System_Prof
port-profile Trunk_System_Prof
  description:
  type: vethernet
  status: enabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: 114,115
  port-group:
  max ports: 32
  inherit:
  config attributes:
    switchport mode trunk
    switchport trunk allowed vlan all
    no shutdown
  evaluated config attributes:
    switchport mode trunk
    switchport trunk allowed vlan all
    mtu 1500
    no shutdown
  assigned interfaces:
switch(config-port-prof)# copy running-config startup-config
```

Modifying System VLANs in an Access Mode Port Profile

You can use this procedure to change the set of system VLANs in an access port profile without removing all system VLANs.

Before You Begin

- You are logged in to vCenter Server.
- You are logged in to the Cisco Nexus 1000V CLI in EXEC mode.

- The VSM is connected to vCenter server.
- You know the VLAN IDs of the system VLANs required for the port profile you are modifying.
- From the upstream switch for each VEM that carries this profile, shut off the switch port that carries the control VLAN.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **port-profile** [**type** {**ethernet** | **vethernet**}] *name*
3. switch(config-port-prof)# **system vlan** *vlan-id-list*
4. (Optional) switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [*name profile-name*]
5. (Optional) switch(config-port-prof)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** [**type** {**ethernet** | **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 can be Ethernet or vEthernet. Once configured, the type cannot be changed. The default is the vEthernet type. Defining a port profile type as Ethernet allows the port profile to be used for physical (Ethernet) ports. In the vCenter Server, the corresponding port group can be selected and assigned to physical ports (PNICs). **Note** If a port profile is configured as an Ethernet type, then it cannot be used to configure VMware virtual ports.
Step 3	switch(config-port-prof)# **system vlan** *vlan-id-list*	Adds system VLANs to this port profile.
Step 4	switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [*name profile-name*]	(Optional) Displays the configuration for verification.
Step 5	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to change the set of system VLANs in an access port profile without removing all system VLANs.

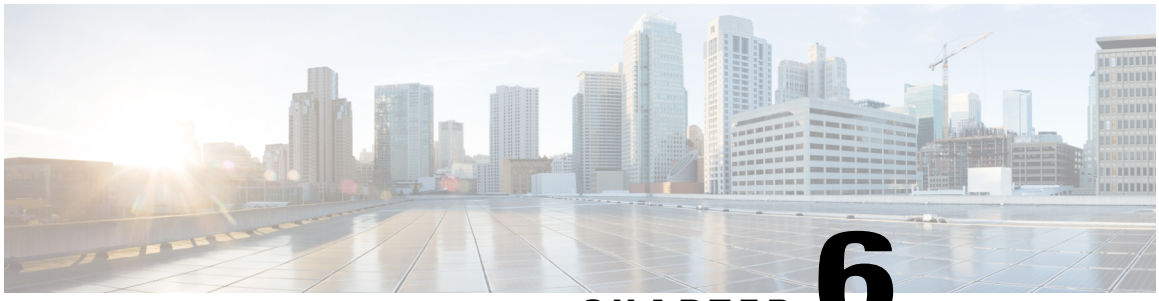
```
switch# configure terminal
switch(config)# port-profile Access_System_Prof
switch(config-port-prof)# system vlan 114,115
switch(config-port-prof)# show port-profile name Access_System_prof
port-profile Access_System_Prof
  description:
  type: vethernet
  status: enabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: 114,115
  port-group:
  max ports: 32
  inherit:
  config attributes:
    switchport mode access
    switchport trunk allowed vlan all
    no shutdown
  evaluated config attributes:
    switchport mode access
    switchport trunk allowed vlan all
    mtu 1500
    no shutdown
  assigned interfaces:
switch(config-port-prof)# copy running-config startup-config
```

What to Do Next

From the upstream switch for each VEM that carries this profile, unshut the switchport that carries the control VLAN.

Feature History for System Port Profiles

Feature Name	Release	Feature Information
MTU	4.2(1)SV1(4)	The **system mtu** command is removed and replaced with the **mtu** command.
system mtu	4.0(4)SV1(3)	The **system mtu** command allows you to preserve a non-default MTU setting on the PNIC attached to the Cisco Nexus 1000V across reboots of the ESX server.
System Port Profiles	4.0(4)SV1(1)	This feature was introduced.



CHAPTER 6

Configuring a Private VLAN in a Port Profile

This chapter contains the following sections:

- Information About Private VLANs , page 49
- Configuring a Port Profile as a Private VLAN, page 49
- Feature History for Private VLAN Port Profiles, page 52

Information About Private VLANs

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.

For more information about PVLANs, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide*.

Configuring a Port Profile as a Private VLAN

Before You Begin

- You are logged in to the CLI in EXEC mode.
- You know the VLAN IDs for both the primary and secondary VLAN in the private VLAN pair.
- You know whether this private VLAN inherits its configuration.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **port-profile** [**type** {**ethernet** | **vethernet**}] *name*
3. switch(config-port-prof)# **switchport mode private-vlan** {**host**| **promiscuous**|**trunk promiscuous**}
4. switch(config-port-prof)# **switchport private-vlan host-association** *primary-vlan secondary-vlan*
5. switch(config-port-prof)# **switchport private-vlan trunk allowed vlan** *vlan-range*
6. switch(config-port-prof)# **switchport private-vlan mapping** *primary_vlan* [**add** | **remove**] *secondary_vlan*
7. switch(config-port-prof)# **switchport private-vlan mapping trunk** *primary_vlan* [**add** | **remove**] *secondary_vlan*
8. (Optional) switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [*name profile-name*]
9. (Optional) switch(config-port-prof)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** [**type** {**ethernet** | **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 can be Ethernet or vEthernet. Once configured, the type cannot be changed. The default is the vEthernet type. Defining a port profile type as Ethernet allows the port profile to be used for physical (Ethernet) ports. In the vCenter Server, the corresponding port group can be selected and assigned to physical ports (PNICs). **Note** If a port profile is configured as an Ethernet type, then it cannot be used to configure VMware virtual ports.
Step 3	switch(config-port-prof)# **switchport mode private-vlan** {**host**| **promiscuous**|**trunk promiscuous**}	Designates the port profile for use as a private VLAN and defines the ports as follows: • **promiscuous**—vEthernet ports that belong to the primary VLAN and communicate with the Layer 3 gateway. Promiscuous ports can communicate with any interface in the PVLAN domain, including those associated with secondary VLANs. • **host**—vEthernet ports that belong to the secondary VLAN as one of the following: ◦ Community PVLAN host port

	Command or Action	Purpose
		◦ Isolated PVLAN host port • **trunk promiscuous—**A physical Ethernet trunk port which carries both regular non-PVLAN traffic and PVLAN traffic. When traffic comes from a PVLAN host port, the packet is translated to the primary VLAN packet.
Step 4	switch(config-port-prof)# **switchport private-vlan host-association** *primary-vlan secondary-vlan*	Assigns the primary and secondary VLAN IDs to the port profile and saves this association in the running configuration. • *primary-vlan***—**Specifies a primary VLAN ID. You can specify only one primary VLAN ID. • *secondary-vlan***—**Specifies the secondary VLAN ID. You can specify only one secondary VLAN ID.
Step 5	switch(config-port-prof)# **switchport private-vlan trunk allowed vlan** *vlan-range*	Sets the allowed VLANs and VLAN IDs when interface is in private-vlan trunking mode.
Step 6	switch(config-port-prof)# **switchport private-vlan mapping** *primary_vlan* [**add** | **remove**] *secondary_vlan*	Maps the primary VLAN ID to the secondary VLAN ID for the port profile.
Step 7	switch(config-port-prof)# **switchport private-vlan mapping trunk** *primary_vlan* [**add** | **remove**] *secondary_vlan*	Designates the primary private VLAN. The range of valid values is 1 to 3967.
Step 8	switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [*name profile-name*]	(Optional) Displays the configuration for verification.
Step 9	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

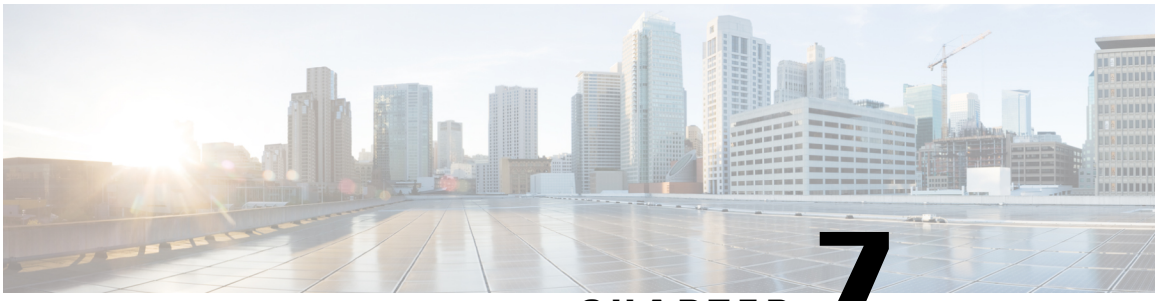
The following examples show different ways that port profiles can be configured as private VLANs.

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# port-profile type vethernet pvcomm
switch(config-port-prof)# vmware port-group
switch(config-port-prof)# switchport mode private-vlan host
switch(config-port-prof)# switchport private-vlan host-association 153 154
switch(config-port-prof)# no shutdown
switch(config-port-prof)# state enabled
switch(config-port-prof)# show run port-profile pv154

!Command: show running-config port-profile pv154
!Time: Fri Jan  7 15:10:43 2011

version 4.2(1)SV1(4)
port-profile type vethernet pv154
  vmware port-group
```

```
  switchport mode private-vlan host
  switchport private-vlan host-association 153 154
  no shutdown
  max-ports 1024
  state enabled


switch(config-port-prof)# port-profile type vethernet pvprom
switch(config-port-prof)# vmware port-group
switch(config-port-prof)# switchport mode private-vlan promiscuous
switch(config-port-prof)# switchport private-vlan mapping 153 154-155
switch(config-port-prof)# no shutdown
switch(config-port-prof)# state enabled
switch(config-port-prof)# show run port-profile pvprom

!Command: show running-config port-profile pvprom
!Time: Fri Jan  7 15:11:43 2011

version 4.2(1)SV1(4)
port-profile type vethernet pv153
  vmware port-group
  switchport mode private-vlan promiscuous
  switchport private-vlan mapping 153 154-155
  no shutdown
  max-ports 1024
  state enabled

switch(config-port-prof)# port-profile type ethernet pvpromtrunk
switch(config-port-prof)# vmware port-group
switch(config-port-prof)# switchport mode private-vlan trunk promiscuous
switch(config-port-prof)# switchport private-vlan mapping trunk 153 154-155
switch(config-port-prof)# switchport private-vlan mapping trunk 156 157
switch(config-port-prof)# switchport private-vlan trunk allowed vlan all
switch(config-port-prof)# no shutdown
switch(config-port-prof)# state enabled
switch(config-port-prof)# show run port-profile pvpromtrunk

!Command: show running-config port-profile pvpromtrunk
!Time: Fri Jan  7 15:12:24 2011

version 4.2(1)SV1(4)
port-profile type ethernet pvpromtrunk
  vmware port-group
  switchport mode private-vlan trunk promiscuous
  switchport private-vlan mapping trunk 153 154-155
  switchport private-vlan mapping trunk 156 157
  switchport private-vlan trunk allowed vlan 1-3967,4048-4093
  no shutdown
  state enabled
```

Feature History for Private VLAN Port Profiles

Feature Name	Release	Feature Information
Private VLAN Port Profiles	4.0(4)SV1(1)	This feature was introduced.



CHAPTER 7

Restricting Port Profile Visibility

This chapter contains the following sections:

- Information About Restricting Port Profile Visibility, page 53
- Guidelines and Limitations for Restricting Port Profile Visibility, page 54
- Defining DVS Access in vSphere Client, page 55
- Enabling the Port Profile Role Feature, page 58
- Restricting Port Profile Visibility on the VSM, page 59
- Removing a Port Profile Role, page 62
- Feature History for Restricting Port Profile Visibility, page 63

Information About Restricting Port Profile Visibility

Information About Port Profile Visibility

You can restrict which VMware vCenter users or user groups have visibility into specific port groups on the Cisco Nexus 1000V.

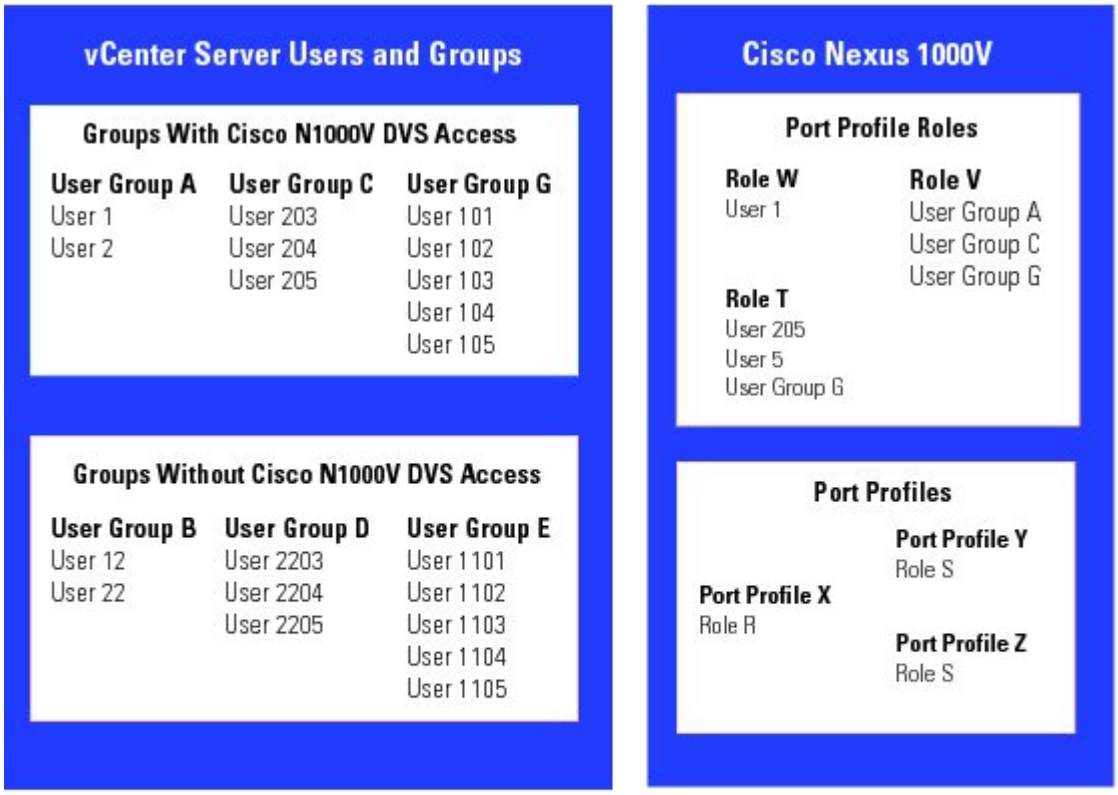
Before you can restrict the visibility of a port group, the server administrator must define which VMware vCenter users and user groups have access to the Cisco Nexus 1000V DVS top level folder in VMware vCenter Server. Once this is done, the network administrator can further define the visibility of specific port groups on the VSM. This configuration on the VSM is then published to the VMware vCenter Server so that access to specific port groups is restricted.

Information About Allow Groups or Users

You can save the time of defining access on the VSM per user by, instead, adding new users to groups in VMware vCenter where access is already defined. Group members defined in VMware vCenter automatically gain access to the port groups defined for the group.

You can see in the following figure the relationship between users and groups in vCenter Server and port profiles and port profile roles in Cisco Nexus 1000V.

Figure 2: Port Profile Visibility: User, Groups, Roles, and Port Profiles



- **Multiple users and groups can be assigned to a role.**
- **Only one role can be assigned to a port profile at a time.**
- **A role can be assigned to multiple port profiles.**
- **Up to 256 port profile roles are allowed per VSM.**
- **A total of 16 users and groups are allowed per role.**

33282

Guidelines and Limitations for Restricting Port Profile Visibility

- The server administrator does not propagate access from the DVS down to lower folders. Instead, port group access is defined by the network administrator on the VSM and then published to the VMware vCenter Server.
- The Cisco Nexus 1000V VSM must be connected to the VMware vCenter Server before port profile roles are created or assigned. If this connection is not in place when port profile visibility is updated on the VSM, it is not published to VMware vCenter Server and is not affected.
- The following are guidelines for port profile roles on the VSM:
  - You cannot remove a port profile role if a port profile is assigned to it. You must first remove the role from the port profile.

- Multiple users and groups can be assigned to a role.
- Only one role can be assigned to a port profile.
- A role can be assigned to multiple port profiles.

- You can define up to 256 port-profile-roles per VSM.
- You can define a total of 16 users and groups per role.

Defining DVS Access in vSphere Client

The server administrator can use this procedure to allow access to the top level Cisco Nexus 1000V DVS folder in vSphere client.

Before You Begin

- You are logged in to the vSphere Client.
- You know which users or groups need access to the DVS.
- This procedure defines who can access the Cisco Nexus 1000V DVS. Access to individual port groups is done on the VSM, using the Restricting Port Profile Visibility on the VSM, on page 59.

SUMMARY STEPS

1. In the **vSphere Client** window, do the following:
2. In the **Select Users and Groups** window, do the following:
3. In the **Assign Permission** window, do the following:

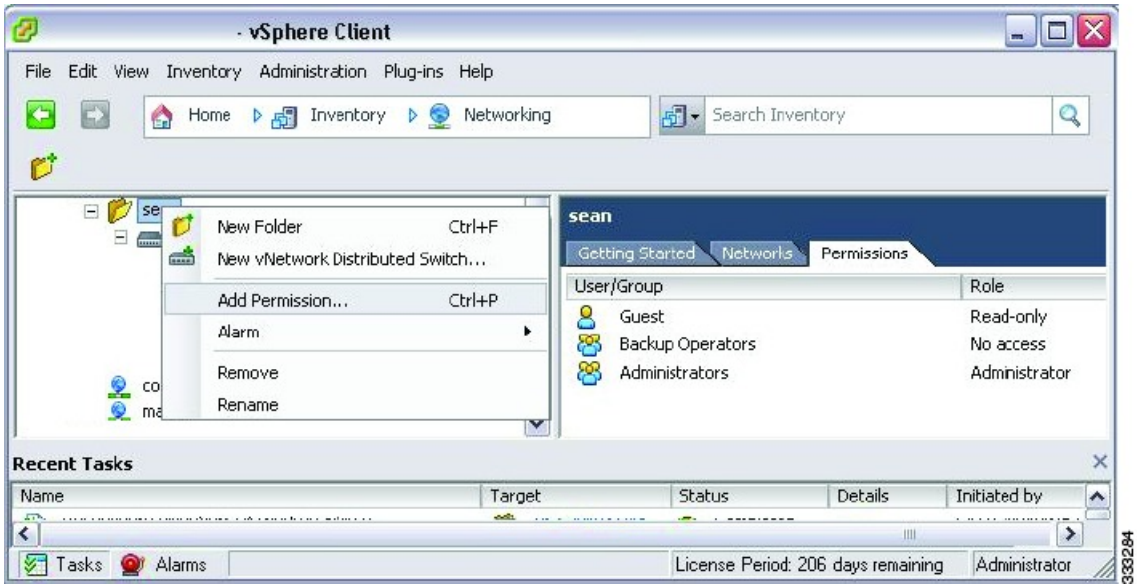
DETAILED STEPS

Step 1 In the **vSphere Client** window, do the following:

a) Choose **Inventory > Networking**.

b) Choose **Add Permission**.

Figure 3: vSphere Client Window



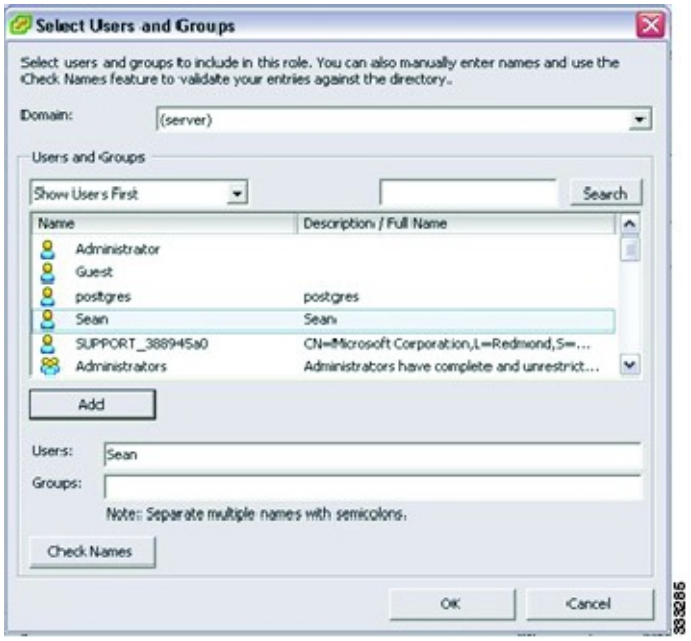
Step 2 In the **Select Users and Groups** window, do the following:

a) Choose the name from the list of users and groups.

b) Click **Add**.

c) Click **OK**.

Figure 4: Select Users and Groups Window



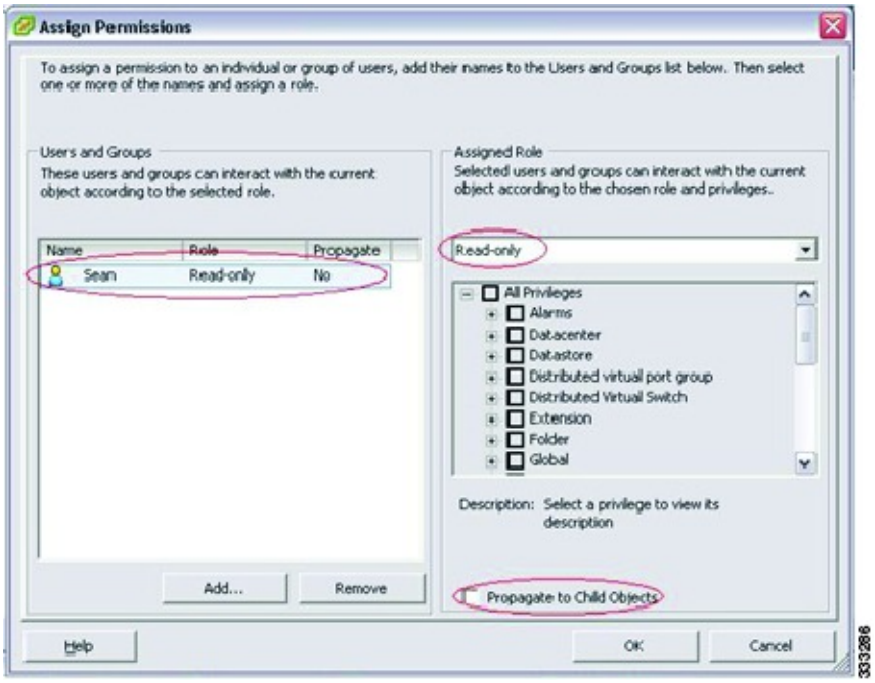
Step 3 In the **Assign Permission** window, do the following:

a) From the **Assigned Role** selection list, choose a role for this user or group.

b) Make sure that the **Propagate to Child Objects** check box is unchecked.

c) Click **OK.**

Figure 5: Assign Permissions Window



The user is granted the same access to the DVS object. In the example shown, user Sean is granted read-only access to the DVS folder object and eventually the DVS object.

Note Do not propagate the role definition here. Specific port group access is configured on the VSM which is then pushed to vSphere Client.

The user may now access the top level Cisco Nexus 1000V DVS folder according to the assigned role.

Note To restrict access to specific port groups, go to the Restricting Port Profile Visibility on the VSM, on page 59.

Enabling the Port Profile Role Feature

Before You Begin

You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **feature port-profile-role**
3. (Optional) switch(config)# **show feature**
4. (Optional) switch(config)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **feature port-profile-role**	Enables the port profile roles feature to restrict user and group access.
Step 3	switch(config)# **show feature**	(Optional) Displays the configuration for verification.
Step 4	switch(config)# **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 the port profile role feature.

```
switch# configure terminal
switch(config)# feature port-profile-role adminUser
switch(config)# show feature
Feature Name          Instance  State
--------------------  --------  --------
dhcp-snooping         1         enabled
http-server           1         enabled
ippool                1         enabled
lacp                  1         enabled
lisp                  1         enabled
lisphelper            1         enabled
netflow               1         disabled
port-profile-roles    1         enabled
private-vlan          1         disabled
sshServer             1         enabled
tacacs                1         enabled
telnetServer          1         enabled
switch(config)# copy running-config startup-config
```

Restricting Port Profile Visibility on the VSM

The network administrator can use this procedure to create a role for restricting port profile visibility on the VSM which is then pushed to vCenter Server.

Before You Begin

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

- You know which users or groups should have access to the role you are creating.
- You have already created the users and groups to be assigned to this role in vCenter and have access to the Cisco Nexus 1000V DVS folder where the VSM resides. See the Defining DVS Access in vSphere Client, on page 55.
- You have enabled the port profile role feature using the Enabling the Port Profile Role Feature, on page 58.
- You have identified the characteristics needed for this role:
  - role name
  - role description
  - users to assign
  - groups to assign
  - port profile to assign

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **port-profile-role** *role-name*
3. (Optional) switch(config-port-prof-role)# **description** *role-description*
4. (Optional) switch(config-port-prof-role)# **show port-profile-role users**
5. (Optional) Enter one or more **user** or **group** roles.
6. switch(config-port-prof-role)# **exit**
7. switch(config)# **port-profile** *profile-name*
8. switch(config-port-prof)# **assign port-profile-role** *role-name*
9. (Optional) switch(config-port-prof)# **show port-profile-role** [**name** *role-name*]
10. (Optional) switch(config-port-prof)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile-role** *role-name*	Enters port profile role configuration mode for the named role. If the role does not already exist, it is created with the following characteristic: • *role-name*—The role name can be up to 32 characters and must be unique for each role on the Cisco Nexus 1000V.
Step 3	switch(config-port-prof-role)# **description** *role-description*	(Optional) Adds a description of up to 32 characters to the role. This description is automatically pushed to vCenter Server.

	Command or Action	Purpose
Step 4	switch(config-port-prof-role)# **show port-profile-role users**	(Optional) Displays all the users on vCenter Server who have access to the DVS parent folder and who can be assigned to the role.
Step 5	Enter one or more **user** or **group** roles.	(Optional) Assigns a user or a group to the role. The user or group gains the ability to use all port profiles assigned to the role. • switch(config-port-prof-role)# **user** *user-name* • switch(config-port-prof-role)# **group** *group-name* **Note** Multiple users and groups can be assigned to a role. The users and groups must exist on vCenter server and must have access to the top level Cisco Nexus 1000V DVS folder in vSphere client. For more information, see the Defining DVS Access in vSphere Client, on page 55.
Step 6	switch(config-port-prof-role)# **exit**	Exits port-profile-role configuration mode and returns you to global configuration mode.
Step 7	switch(config)# **port-profile** *profile-name*	Enters port profile configuration mode for the named port profile.
Step 8	switch(config-port-prof)# **assign port-profile-role** *role-name*	Assigns the role to a port profile. The port group is updated in vCenter Server and the user or group assigned to this role is granted access. The user or group can assign the port group to a vNIC in a virtual machine or vSWIF or vMKNIC on a host. **Note** Only one role can be assigned to a port profile. A role can be assigned to multiple port profiles.
Step 9	switch(config-port-prof)# **show port-profile-role** [**name** *role-name*]	(Optional) Displays the configuration for verification.
Step 10	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to define access for the allaccess2 port profile by creating and assigning the adminUser port profile role.

```
switch# configure terminal
switch(config)# port-profile-role adminUser
switch(config-port-prof-role)# description adminOnly
switch(config-port-prof-role)# user hdbaar
switch(config-port-prof-role)# exit
switch(config)# port-profile allaccess2
switch(config-port-prof)# assign port-profile-role adminUser
switch(config-port-prof)# show port-profile-role name adminUser
```

```
Name: adminUser
Description: adminOnly
Users:
    hdbaar (user)
Assigned port-profiles:
    allaccess2
switch(config-port-prof)# copy running-config startup-config
```

Removing a Port Profile Role

You can use this procedure to remove a role that was used for restricting port profile visibility on vCenter Server.

Before You Begin

- You are logged in to the CLI in EXEC mode.
- You cannot remove a port profile role if a port profile is assigned to it. You must first remove the role from the port profile. This procedure includes a step for doing this.

SUMMARY STEPS

1. (Optional) switch# **show port-profile-role** [*name role-name*]
2. switch# **configure terminal**
3. switch(config)# **port-profile** [**type** {**ethernet** | **vethernet**}] *name*
4. switch(config-port-prof)# **no assign port-profile-role** *role-name*
5. switch(config-port-prof)# **exit**
6. switch(config)# **no port-profile-role** *role-name*
7. (Optional) switch# **show port-profile-role** [*name role-name*]
8. (Optional) switch(config)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **show port-profile-role** [*name role-name*]	(Optional) Displays the port profile role including any port profiles assigned to it. If there are port profiles assigned to the role, they must be removed before you can remove the role.
Step 2	switch# **configure terminal**	Enters global configuration mode.
Step 3	switch(config)# **port-profile** [**type** {**ethernet** | **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 can be Ethernet or vEthernet. Once configured, the type cannot be changed. The default is the vEthernet type.

	Command or Action	Purpose
		Defining a port profile type as Ethernet allows the port profile to be used for physical (Ethernet) ports. In the vCenter Server, the corresponding port group can be selected and assigned to physical ports (PNICs). **Note** If a port profile is configured as an Ethernet type, then it cannot be used to configure VMware virtual ports.
Step 4	switch(config-port-prof)# **no assign port-profile-role** *role-name*	Removes the role from the port profile. The port group is updated in vCenter Server.
Step 5	switch(config-port-prof)# **exit**	Exits port-profile configuration mode and returns you to global configuration mode.
Step 6	switch(config)# **no port-profile-role** *role-name*	Removes the role from the VSM.
Step 7	switch# **show port-profile-role** [*name role-name*]	(Optional) Displays the port profile role including any port profiles assigned to it. If there are port profiles assigned to the role, they must be removed before you can remove the role.
Step 8	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

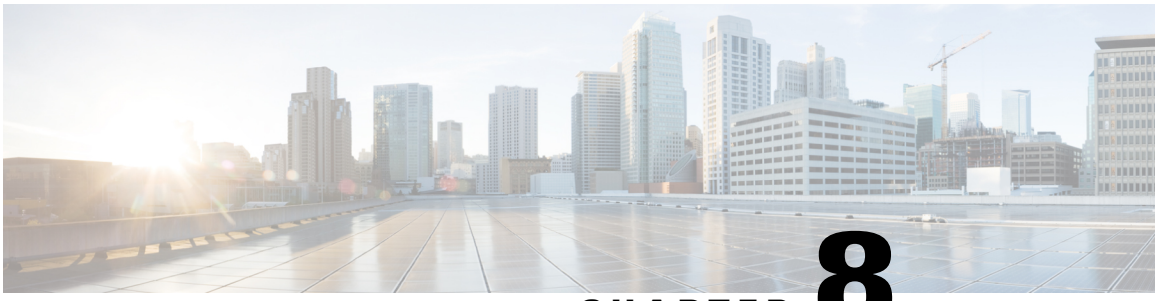
This example shows how to remove a port profile role.

```
switch# show port-profile-role name adminUser
Name: adminUser
Description: adminOnly
Users:
    hdbaar (user)
Assigned port-profiles:
    allaccess2
switch# configure terminal
switch(config)# port-profile allaccess2
switch(config-port-prof)# no assign port-profile-role adminUser
switch(config-port-prof)# exit
switch(config)# no port-profile-role adminUser
switch(config)# show port-profile-role name adminUser
switch(config)# copy running-config startup-config
switch(config)#
```

Feature History for Restricting Port Profile Visibility

This section provides the feature history for restricting port profile visibility.

Feature Name	Releases	Feature Information
Restricting Port Profile Visibility	4.2(1)SV1(4)	This feature was introduced.



CHAPTER 8

Verifying the Port Profile Configuration

This chapter contains the following sections:

- Verifying the Port Profile Configuration, page 65
- Feature History for Port Profile Verification, page 68

Verifying the Port Profile Configuration

Use one of the following commands to verify the configuration:

- **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
- **show port-profile-role** [**name** *port-profile-role-name*]
- **show running-config port-profile** [*profile-name*]
- **show port-profile-role users**
- **show port-profile sync-status** [**interface** *if-name*]
- **show port-profile virtual usage** [**name** *profile-name*]
- **show running-config port-profile** [*prof-name*]

For detailed information about the command output, see the *Cisco Nexus 1000V Command Reference*.

show port profile

```
switch# show port-profile
port-profile UpLinkProfile1
  description:
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    channel-group auto mode on mac-pinning
  evaluated config attributes:
```

```
    channel-group auto mode on mac-pinning
  assigned interfaces:
port-profile UpLinkProfile2
  description:
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    channel-group auto mode on sub-group cdp
  evaluated config attributes:
    channel-group auto mode on sub-group cdp
  assigned interfaces:
port-profile UpLinkProfile3
  description:
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    channel-group auto mode on sub-group manual
  evaluated config attributes:
    channel-group auto mode on sub-group manual
  assigned interfaces:
switch#
```

show port-profile name UpLinkProfile

```
switch# show port-profile name UpLinkProfile3
port-profile UpLinkProfile3
  description:
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    channel-group auto mode on sub-group manual
  evaluated config attributes:
    channel-group auto mode on sub-group manual
  assigned interfaces:
switch#
```

show port-profile brief

```
switch# show port-profile brief
--------------------------------------------------------------------------------
Port                                  Profile  Remote Conf  Eval  Child Child
Profile                               State    Mgmt   Items Items Intfs Profs
--------------------------------------------------------------------------------
UplinkProfile1                        enabled  vmware     3     3     1     0
UplinkProfile2                        enabled  vmware     3     3     2     0
Ubuntu-Profile                        enabled  vmware     3     3     1     0
switch#
```

show port-profile virtual usage

```
switch# show port-profile virtual usage
--------------------------------------------------------------------------------
Port Profile                Port        Adapter        Owner
--------------------------------------------------------------------------------
n1kv-uplink0                Po1
                            Eth3/2      vmnic1         localhost.
                            Eth3/3      vmnic2         localhost.
vlan1767                    Veth7       Net Adapter 1  all-tool-7
                            Veth8       Net Adapter 1  all-tool-8
aipc1765                    Veth4       Net Adapter 1  bl-h-s
inband1766                  Veth6       Net Adapter 3  bl-h-s
mgmt1764                    Veth5       Net Adapter 2  bl-h-s
vpc-mac-uplink              Po7
                            Eth5/2      vmnic1         localhost.
                            Eth5/3      vmnic2         localhost.
ch-vpc-mac-uplink           Po2
                            Po3
                            Eth4/2      vmnic1         VDANIKLNCOS
                            Eth4/3      vmnic2         VDANIKLNCOS
ch-aipc1765                 Veth1       Net Adapter 1  bl-h-p
ch-mgmt1764                 Veth2       Net Adapter 2  bl-h-p
ch-inband1766               Veth3       Net Adapter 3  bl-h-p
switch#
```

show port-profile expand-interface name UplinkProfile1

```
switch# show port-profile expand-interface name UplinkProfile1
port-profile UplinkProfile1
Ethernet2/2
    switchport mode trunk
    switchport trunk allowed vlan 110-119
    no shutdown
switch#
```

show port-profile expand-interface

```
switch# show port-profile expand-interface
port-profile UplinkProfile1
Ethernet2/2
    switchport mode trunk
    switchport trunk allowed vlan 110-119
    no shutdown

port-profile UplinkProfile2
Ethernet2/3
    switchport mode trunk
    switchport trunk allowed vlan 117
    no shutdown
Ethernet2/4
    switchport mode trunk
    switchport trunk allowed vlan 117
    no shutdown

port-profile Ubuntu-Profile
Vethernet439
    switchport mode access
    switchport access vlan 118
    no shutdown
switch#
```

show port-profile sync-status

```
switch# show port-profile sync-status interface ethernet 3/2
Ethernet3/2
 port-profile: uplink
 interface status: quarantine
 sync status: out of sync
 cached commands:
```

```
 errors:
    command cache overrun
 recovery steps:
    bring interface online
switch#
```

show running-config port-profile

```
switch# show running-config port-profile
port-profile type ethernet UplinkProfile1
  description "Profile for critical system ports"
  vmware port-group
  switchport mode access
  switchport access vlan 113
  switchport trunk native vlan 113
  channel-group auto mode on
  no shutdown
port-profile type vethernet UplinkProfile2
  vmware port-group
  vmware max-ports 5
  switchport mode trunk
  switchport trunk native vlan 112
  channel-group auto mode on sub-group cdp
  no shutdown
switch#
```

show port-profile-role

```
switch# show port-profile-role name adminUser

Name: adminUser
Description: adminOnly
Users:
    hdbaar (user)
Assigned port-profiles:
    allaccess2
switch#
```

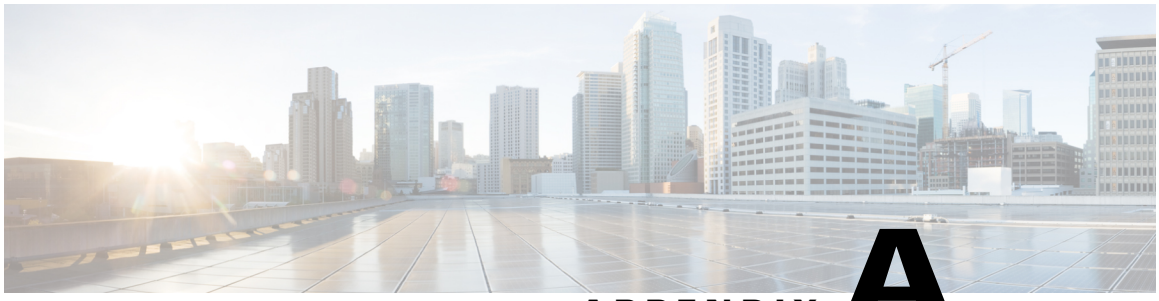
show port-profile-role users

```
switch# show port-profile-role users
Groups:
  Administrators
  TestGroupB
Users:
  dbaar
  fgreen
  suchen
  mariofr
switch#
```

Feature History for Port Profile Verification

Feature Name	Releases	Feature Information
show port-profile-role users	4.2(1)SV1(4)	This command output shows the available users and groups.
show port-profile-role	4.2(1)SV1(4)	This command output shows the configuration for port profile roles.
show running-config port-profile	4.0(4)SV1(2)	This command output shows the configuration for port profiles.

Feature Name	Releases	Feature Information
show running-config	4.0(4)SV1(2)	This command output has the following changes: • Shows the port profile type (Ethernet or vEthernet). • Optionally, you can display running configurations for all port profiles or a specific port profile.
show port-profile *name*	4.0(4)SV1(2)	This command output shows the port profile type, pinning, and channel-group configuration. The uplink capability is removed from the output of this command since port profiles used as uplinks are now configured as Ethernet type instead.
Port Profile verification	4.0(4)SV1(1)	This feature was introduced.



APPENDIX A

Port Profile Configuration Limits

This chapter contains the following sections:

- Port Profile Configuration Limits, page 71

Port Profile Configuration Limits

The configuration limits are documented in the *Cisco Nexus 1000V Resource Availability Reference*.

Port Profile Configuration Limits

INDEX

A

access profile 18
  configuring 18

C

clearing 19
  port management policy 19
configuration limits 71
  port profile 71
configuring 13, 15, 18, 21, 22, 24, 49
  access profile 18
  default port binding type 21
  port binding for vEthernet port profile 22
  port profile 24
  port profile as a private VLAN 49
  trunking profile 15
  VMware attributes 13
configuring port profile inheritance 32
  guidelines and limitations 32
converting 44
  access port profiles to trunk port profiles 44
creating 12, 38
  port profiles 12
  system port profile 38

D

default settings 11
  port profiles 11
defining DVS access 55
  in vSphere Client 55
deleting 41
  system VLANs from a port 41

E

enabling 27, 58
  port profile role feature 58
  port profiles 27

F

feature history 30, 47, 52, 63
  port profiles 30
  private VLAN port profiles 52
  restricting port profile visibility 63
  system port profiles 47

G

guidelines and limitations 10, 32, 37, 54
  configuring port profile inheritance 32
  creating port profiles 10
  restricting port profile visibility 54
  system port profiles 37

I

information about 5, 6, 7, 9, 31, 37, 49, 53
  allow groups and users 53
  atomic inheritance 7
  interface quarantine 7
  live policy changes 6
  port groups 5
  port profile inheritance 6, 31
  port profile states 9
  port profile visibility 53
  port profiles 5
  private VLANs 49
  rollback to a consistent configuration 7
  system port profiles 37
  uplink profiles 6

inheriting 33
configuration from a port profile 33

M

modifying 45
system VLANs in an access mode port profile 45
modifying system VLANs 41, 42
in a trunk mode port profile 41, 42

N

new and changed information 1

P

port profile 28, 71
configuration limits 71
removing 28
port profile role 62
removing 62
port profile role feature 58
enabling 58
port profile states 9
information about 9
port profiles 11, 12
creating 12
default settings 11

R

removing 28, 34, 62
inherited policies from a port profile 34
port profile role 62
port-profile 28
restricting 59
port profile visibility on the VSM 59

S

standards 30
creating port profiles 30
system port profile 38
creating 38

V

verifying 26, 65
port profile configuration 65
port-binding on vCenter Server 26
vEthernet port binding 10
VLAN ranges 15
VMware attributes 13
configuring 13