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

Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1) SV1(4)

October 4, 2012

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-22820-01

Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1) SV1(4)

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:

- Release Notes.
- Command Reference.

Feature	Description	Changed in release	Where Documented
Port channel	The Creating a Port Profile for a Port Channel chapter was moved into the *Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4)*.	4.2(1)SV1(4)	"Configuring Port Channels"
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 vEthernet Port Profiles"
Restrict the visibility of Port Profiles	Restricts port profile visibility by user or user group.	4.2(1)SV1(4)	"Restricting Port Profile Visibility"
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"
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"
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"
show port-profile virtual usage command added	Displays the port profile usage by interface.	4.2(1)SV1(4)	"Verifying the Port Profile Configuration"
Atomic Inheritance	Port profile configuration applied to member interfaces.	4.2(1)SV1(4)	"Overview"
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)	"Overview"

Feature	Description	Changed in release	Where Documented
Interface Quarantine	After a configuration failure, interfaces are shut down to maintain accurate configuration.	4.2(1)SV1(4)	"Overview"
show running-config port-profile	New command for displaying the port profile configuration.	4.0(4)SV1(2)	"Verifying the Port Profile Configuration"
Uplink port profile	Port profiles are not classified as uplink, but are, instead, configured as Ethernet or vEthernet.	4.0(4)SV1(2)	Removed from this document.
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"
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)	"Configuring Port Channels in Port Profiles"
MAC Pinning	Connecting to upstream switches that do not support port channels using the MAC-pinning command.	4.0(4)SV1(2)	"Configuring Port Channels in Port Profiles"
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)	"Configuring Port Channels in Port Profiles"
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 Port Profiles"
[**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. The **no capability uplink** command has been removed.	4.0(4)SV1(2)	"Creating Port Profiles"
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"

Feature	Description	Changed in release	Where Documented
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"
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)	"Configuring System Port Profiles"

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

CONTENTS

New and Changed Information iii

Preface xi

- Audience xi
- Document Organization xi
- Document Conventions xii
- Recommended Reading xiii
- Available Documents xiii
- Obtaining Documentation and Submitting a Service Request xv

Overview 1-1

- Port Profiles and Port Groups 1-1
- Live Policy Changes 1-2
- Uplink Profiles 1-2
- Port Profile Inheritance 1-2
- Consistent Port Profile Configuration 1-3
  - Atomic Inheritance 1-3
  - Rollback to a Consistent Configuration 1-3
  - Interface Quarantine 1-3

Creating Port Profiles 2-1

- Information About Port Profiles 2-1
  - Port Profile States 2-1
  - vEthernet Port Binding 2-2
- Guidelines and Limitations 2-2
- Default Settings 2-3
- Configuring Port Profiles 2-3
  - Creating a Port Profile 2-4
  - Configuring VMware Attributes 2-5
  - Configuring Port Mode 2-7
    - Configuring a Trunking Profile 2-8
    - Configuring an Access Profile 2-11
    - Clearing a Port Management Policy 2-13

Configuring Port Binding for vEthernet Port Profiles 2-14
Configuring a Default Port Binding Type 2-15
Configuring Port Binding for a vEthernet Port Profile 2-16
Verifying Port Binding on vCenter Server 2-18
Enabling a Port Profile 2-18
Removing a Port Profile 2-20
Additional References 2-21
Related Documents 2-21
Standards 2-22
Feature History for Port Profiles 2-22

Configuring Port Profile Inheritance 3-1
Information About Port Profile Inheritance 3-1
Guidelines and Limitations 3-2
Inheriting a Configuration from a Port Profile 3-2
Removing Inherited Policies from a Port Profile 3-4

Configuring System Port Profiles 4-1
Information About System Port Profiles 4-1
Guidelines and Limitations for System Port Profiles 4-2
Creating a System Port Profile 4-2
Deleting System VLANs from a Port 4-6
Modifying the System VLANs in a Port Profile 4-6
Modifying the System VLANs in a Trunk Mode Port Profile 4-7
Modifying System VLANs in an Access Mode Port Profile 4-8
Feature History for System Port Profiles 4-10

Configuring a Private VLAN in a Port Profile 5-1
Information About Private VLANs 5-1
Configuring a Port Profile as a Private VLAN 5-1
Feature History for Private VLAN Port Profiles 5-4

Restricting Port Profile Visibility 6-1
Information About Port Profile Visibility 6-1
Allow Groups or Users 6-1
Guidelines and Limitations 6-2
Defining DVS Access in vSphere Client 6-3
Enabling the Port Profile Role Feature 6-5

Restricting Port Profile Visibility on the VSM 6-6
Removing a Port Profile Role 6-9
Feature History for Restricting Port Profile Visibility 6-11

Verifying the Port Profile Configuration 7-1
Verifying the Port Profile Configuration 7-1
Feature History for Port Profile Verification 7-5

Port Profile Configuration Limits A-1

INDEX

Preface

The Port Profile Configuration document describes how to create and configure port profiles, the primary mechanism for defining and applying network policy to switch interfaces.

This preface describes the following aspects of this document:

- Audience, page xi
- Document Organization, page xi
- Document Conventions, page xii
- Recommended Reading, page xiii
- Available Documents, page xiii
- Obtaining Documentation and Submitting a Service Request, page xv

Audience

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

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

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

Document Organization

This publication is organized as follows:

Chapter and Title	Description
Chapter 1, “Overview”	Describes port profiles and their use.
Chapter 2, “Creating Port Profiles”	Describes how to create, enable, and configure port profiles.
Chapter 3, “Configuring Port Profile Inheritance”	Describes port profile inheritance, how to configure it, and how to remove inheritance from a port profile.

Chapter and Title	Description
Chapter 4, "Configuring System Port Profiles"	Describes system port profiles and how to configure them.
Chapter 5, "Configuring a Private VLAN in a Port Profile"	Describes how to configure a port profile to be used as a private VLAN (PVLAN).
Chapter 6, "Restricting Port Profile Visibility"	Describes how to restrict visibility of port profiles to a user or a group of users.
Chapter 7, "Verifying the Port Profile Configuration"	Lists and shows examples of commands used to verify port profile configurations
Appendix A, "Port Profile Configuration Limits"	Lists the maximum configuration limits for port profile features.

Document Conventions

Command descriptions use these conventions:

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

Screen examples use these conventions:

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

This document uses the following conventions for notes and cautions:

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

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

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

Recommended Reading

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

- *Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(4)*
- *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4)*
- *Cisco VN-Link: Virtualization-Aware Networking* white paper

Available Documents

This section lists the documents used with the Cisco Nexus 1000 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, Release 4.2(1)SV1(4)

Cisco Nexus 1000V Release Notes, Release 4.2(1)SV1(4)

Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(4)

Cisco Nexus 1010 Management Software Release Notes, Release 4.2(1)SP1(2)

Install and Upgrade

Cisco Nexus 1000V Virtual Supervisor Module Software Installation Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V Software Upgrade Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V VEM Software Installation and Upgrade Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1010 Virtual Services Appliance Hardware Installation Guide

Cisco Nexus 1010 Software Installation and Upgrade Guide, Release 4.2(1)SP1(2)

Configuration Guides

Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1010 Software Configuration Guide, Release 4.2(1)SP1(2)

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

Programming Guide

Cisco Nexus 1000V XML API User Guide, Release 4.2(1)SV1(4)

Reference Guides

Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)

Cisco Nexus 1000V MIB Quick Reference

Cisco Nexus 1010 Command Reference, Release 4.2(1)SP1(2)

Troubleshooting and Alerts

Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V Password Recovery Guide

Cisco NX-OS System Messages Reference

Virtual Security Gateway Documentation

Cisco Virtual Security Gateway for Nexus 1000V Series Switch Release Notes, Release 4.2(1)VSG(1)

Cisco Virtual Security Gateway, Release 4.2(1)VSG1(1) and Cisco Virtual Network Management Center, Release 1.0.1 Installation Guide

Cisco Virtual Security Gateway for Nexus 1000V Series Switch License Configuration Guide, Release 4.2(1)VSG1(1)

Cisco Virtual Security Gateway for Nexus 1000V Series Switch Configuration Guide, Release 4.2(1)VSG1(1)

Cisco Virtual Security Gateway for Nexus 1000V Series Switch Command Reference, Release 4.2(1)VSG1(1)

Virtual Network Management Center

Release Notes for Cisco Virtual Network Management Center, Release 1.0.1

Cisco Virtual Security Gateway, Release 4.2(1)VSG1(1) and Cisco Virtual Network Management Center, Release 1.0.1 Installation Guide

Cisco Virtual Network Management Center CLI Configuration Guide, Release 1.0.1

Cisco Virtual Network Management Center GUI Configuration Guide, Release 1.0.1

Cisco Virtual Network Management Center XML API Reference Guide, Release 1.0.1

Network Analysis Module Documentation

Cisco Network Analysis Module Software Documentation Guide, 4.2

Cisco Nexus 1000V NAM Virtual Service Blade Installation and Configuration Guide

Network Analysis Module Command Reference Guide, 4.2

User Guide for the Cisco Network Analysis Module Virtual Service Blades, 4.2

Cisco Network Analysis Module Software Release Notes, 4.2

Obtaining Documentation and Submitting a Service Request

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

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

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

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

CHAPTER 1

Overview

This chapter provides an overview of port profiles, the primary mechanism by which network policy is defined and applied to switch interfaces.

This chapter includes the following sections:

- Port Profiles and Port Groups, page 1-1
- Live Policy Changes, page 1-2
- Uplink Profiles, page 1-2
- Port Profile Inheritance, page 1-2
- Consistent Port Profile Configuration, page 1-3

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 vCenter server. Every port group on the 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 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 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.

When a newly-provisioned virtual machine is powered on, a vEthernet interface is created on the Cisco Nexus 1000V for each of the virtual machine vNICs. The vEthernet inherits the definitions in the selected port profile.

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.

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.

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.

For more information, see the "Configuring Port Profile Inheritance" section on page 3-1.

Consistent Port Profile Configuration

This section includes the following topics:

- Atomic Inheritance, page 1-3
- Rollback to a Consistent Configuration, page 1-3
- Interface Quarantine, page 1-3

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.

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. This is new in Release 4.2(1)SV1(4).

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(4), 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. For more information, see the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(4)*.

CHAPTER 2

Creating Port Profiles

This chapter describes how to create, enable, or remove a port profile or add VMware attributes, access or trunk ports, ACLs, and NetFlow.

This chapter includes the following sections:

- Information About Port Profiles, page 2-1
- Guidelines and Limitations, page 2-2
- Default Settings, page 2-3
- Configuring Port Profiles, page 2-3
- Additional References, page 2-21
- Feature History for Port Profiles, page 2-22

Information About Port Profiles

Port profiles simplify interface configuration by defining policies that can be reused for multiple interfaces. For more information about port profiles, see Chapter 1, "Overview."

Port Profile States

A port profile can be in one of two states: enabled or disabled. Port profiles are disabled by default. Table 2-1 describes port profile behavior in these two states.

To enable a port profile, see the "Enabling a Port Profile" procedure on page 2-18.

Table 2-1 Port Profile States

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.

Table 2-1 Port Profile States (continued)

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.

vEthernet Port Binding

You can configure either static or ephemeral port binding for vEthernet port profiles. Table 2-2 shows how this setting controls how ports are assigned in the VMware port group.

Table 2-2 vEthernet Port Binding

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.
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. For more information about configuring **svs veth auto-config-purge**, see the *Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4).*

Guidelines and Limitations

Use the following guidelines and limitations when configuring 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, Release 4.2(1)SV1(4)*.

- MTU can only be configured for uplink, Ethernet type port profiles.
- If you configure MTU for any 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 Getting Started Guide, Release 4.2(1)SV1(4)*.
- The Cisco Nexus 1000V must be connected to the vCenter Server.

Default Settings

Table 2-3 lists the default settings in the port profile configuration.

Table 2-3 Port Profile Defaults

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
vmware port-group name	Port profile name
vEthernet port-binding	Static

Configuring Port Profiles

This section includes the following topics:

- Creating a Port Profile, page 2-4
- Configuring VMware Attributes, page 2-5
- Configuring Port Mode, page 2-7
- Configuring Port Binding for vEthernet Port Profiles, page 2-14
- Enabling a Port Profile, page 2-18
- Removing a Port Profile, page 2-20

Creating a Port Profile

You can use this procedure to create a new port profile.

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 whether the ports need to be initialized with system settings.
- You have identified the characteristics needed for this port profile.

SUMMARY STEPS

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

DETAILED STEPS

	Command	Description

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Enters global configuration mode.

Step 2	**port-profile** [**type** {**ethernet** | **vethernet**}] *name*
	
	Example:
	`n1000v(config)# port-profile type ethernet AllAccess1`
	`n1000v(config-port-prof)#`
		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	Description
Step 3	**description** *profiledescription* **Example:** n1000v(config-port-prof)# description all_access n1000v(config-port-prof)#	(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	**show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*] **Example:** n1000v(config-port-prof)# show port-profile name AllAccess1	(Optional) Displays the configuration for verification.
Step 5	**copy running-config startup-config** **Example:** n1000v(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.

EXAMPLES

This example shows how to create a new port profile:

```
n1000v(config)# port-profile type ethernet AllAccess1
n1000v(config-port-prof)# description all_access
n1000v(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:
n1000v(config-port-prof)#
```

Configuring VMware Attributes

You can use this procedure to designate a port profile as a VMware port profile.

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 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.
- The **max-ports** command is available only for non-uplink profiles.

- You know if you want to restrict the maximum number of ports that can be assigned to the port profile. If so, you know what the maximum number is.

SUMMARY STEPS

1. **config t**
2. **port-profile** [**type** {**ethernet** | **vethernet**}] *name*
3. **vmware port-group** [*pg_name*]
4. **max-ports** *number*
5. **show port-profile** [**brief** | **expand-interface** | **usage**] [name *profile-name*]
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Description/Result

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Enters global configuration mode.

Step 2	**port-profile** [**type** {**ethernet** | **vethernet**}] *name*
	
	Example:
	`n1000v(config)# port-profile AccessProf`
	`n1000v(config-port-prof)#`
		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	**vmware port-group** [*pg_name*]
	
	Example:
	`n1000v(config-port-prof)# vmware port-group`
	`n1000v(config-port-prof)#`
		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	**max-ports** *num*
	
	Example:
	`n1000v(config-port-prof)# max-ports 5`
	`n1000v(config-port-prof)#`
		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.

	Command	Description/Result
Step 5	**show port-profile** [**brief** | **expand-interface** | **usage**] [name *profile-name*] **Example:** n1000v(config-port-prof)# show port-profile name AccessProf	(Optional) Displays the configuration for verification.
Step 6	**copy running-config startup-config** **Example:** n1000v(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.

EXAMPLES

This example shows how to designate a port profile as a VMware port profile and set the maximum allowed ports to five:

```
Example:
n1000v# config t
n1000v(config)# port-profile AccessProf
n1000v(config-port-prof)# vmware port-group
n1000v(config-port-prof)# max-ports 5
n1000v(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:
  evaluated config attributes:
  assigned interfaces:n1000v(config-port-prof)#
```

Configuring Port Mode

You can use the following procedures to designate trunking or access ports and configure VLANs for an existing port profile.

- Configuring a Trunking Profile, page 2-8
- Configuring an Access Profile, page 2-11
- Clearing a Port Management Policy, page 2-13

BEFORE YOU BEGIN

Before beginning the procedures in this section, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You know whether you are configuring the port profile as an access port or trunk port.

  - An access port transmits packets on only one untagged VLAN. You can specify the VLAN, and it becomes the access VLAN. If you do not specify a VLAN for an access port, that interface carries traffic only on the default VLAN 1.
  - A trunk port transmits untagged packets for the native VLAN and transmits encapsulated, tagged packets for all other VLANs.
- You know the needed VLAN configuration for this port profile.
- A VLAN must already be created on the switch before you can assign it to a port profile.
- You know the VLAN ID for the VLAN that you are assigning.
- VLAN 1 is the default VLAN. You cannot create, modify, or delete this VLAN.
- In accordance with the IEEE 802.1Q standard, up to 4094 VLANs are supported. Table 2-4 describes the available VLAN ranges and their use.

Table 2-4 VLAN Ranges

VLANs 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

You can use this procedure to define a trunking port profile including the VLANs that are allowed on the interfaces.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- You have already created the port profile using the "Creating a Port Profile" procedure on page 2-4.
- 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 Table 2-4 on page 2-8.
- If you do not configure allowed VLANs in this procedure, then the default VLAN 1 is used.
- If you do not configure a native VLAN in this procedure, then the default VLAN 1 is used.

SUMMARY STEPS

1. **config t**
2. **port-profile** *name*
3. **switchport mode** {**access** | **trunk**}
4. **no shutdown**
5. **switchport trunk allowed vlan** {*allowed-vlans* | add *add-vlans* | except *except-vlans* | remove *remove-vlans* | all | none}
6. **switchport trunk native vlan** *vlan-id*
7. **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
8. **copy running-config startup-config**

DETAILED STEPS

	Command	Description

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Enters global configuration mode.

Step 2	**port-profile** *name*
	
	Example:
	`n1000v(config)# port-profile TrunkProf`
	`n1000v(config-port-prof)#`
		Enters port profile configuration mode for the named port profile.

Step 3	**switchport mode trunk**
	
	Example:
	`n1000v(config-port-prof)# switchport mode trunk`
	`n1000v(config-port-prof)#`
		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	**no shutdown**
	
	Example:
	`n1000v(config-port-prof)# no shutdown`
	`n1000v(config-port-prof)#`
		Administratively enables all ports in the profile.

	Command	Description
Step 5	**switchport trunk allowed vlan** {*allowed-vlans* | **add** *add-vlans* | **except** *except-vlans* | **remove** *remove-vlans* | **all** | **none**} **Example:** n1000v(config-port-prof)# switchport trunk allowed vlan all	(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. • **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	**switchport trunk native vlan** *vlan-id* **Example:** n1000v(config-port-prof)# switchport trunk native vlan 3	(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	**show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*] **Example:** n1000v(config-port-prof)# show port-profile TrunkProf	(Optional) Displays the configuration for verification.
Step 8	**copy running-config startup-config** **Example:** n1000v(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.

EXAMPLES

This example shows how to configure a trunking port profile, allowing all VLANs, and setting VLAN 3 as its native VLAN.

```
Example:
n1000v# config t
n1000v(config)# port-profile TrunkProf
n1000v(config-port-prof)# switchport mode trunk
n1000v(config-port-prof)# no shutdown
n1000v(config-port-prof)# switchport trunk allowed vlan all
n1000v(config-port-prof)# switchport trunk native vlan 3
n1000v(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:
n1000v(config-port-prof)#
```

Configuring an Access Profile

Use this procedure to add an access VLAN to the access port in an existing port profile.

BEFORE YOU BEGIN

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

- 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. **config t**
2. **port-profile** *name*
3. **switchport mode** {**access** | **trunk**}
4. **no shutdown**
5. **switchport access vlan** *vlan-id-access*
6. **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Description

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Enters global configuration mode.

Step 2	**port-profile** *name*
	
	Example:
	`n1000v(config)# port-profile AccessProf`
	`n1000v(config-port-prof)#`
		Enters port profile configuration mode for the named port profile.

	Command	Description
Step 3	**switchport mode** {**access** | **trunk**} **Example:** n1000v(config-port-prof)# switchport mode access n1000v(config-port-prof)#	Designates the interfaces as either switch access ports (the default) or trunks.
Step 4	**no shutdown** **Example:** n1000v(config-port-prof)# no shutdown n1000v(config-port-prof)#	Administratively enables all ports in the profile.
Step 5	**switchport access vlan** *vlan-id-access.* **Example:** n1000v(config-port-prof)# switchport access vlan 300	(Optional) Assigns an access VLAN ID to this port profile. **Note** If you do not specify a VLAN ID, then VLAN 1 is used automatically.
Step 6	**show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*] **Example:** n1000v(config-port-prof)# show port-profile AccessProf	(Optional) Displays the configuration for verification.
Step 7	**copy running-config startup-config** **Example:** n1000v(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.

EXAMPLES

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

```
Example:
n1000v# config t
n1000v(config)# port-profile AccessProf
n1000v(config-port-prof)# switchport mode access
n1000v(config-port-prof)# no shutdown
n1000v(config-port-prof)# switchport access vlan 300
n1000v(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:
```

```
n1000v(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

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- Removing the shutdown configuration changes the state of the port profile ports to shutdown.
- Removing the switchport mode converts the port profile ports to switch access ports.
- After removing the configuration for an attribute, the attribute does not appear in show command output.

SUMMARY STEPS

1. **config t**
2. **port-profile** *name*
3. **default** {**shutdown** | **switchport mode**}
4. **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Description

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Enters global configuration mode.

Step 2	**port-profile** *name*
	
	Example:
	`n1000v(config)# port-profile AccessProf`
	`n1000v(config-port-prof)#`
		Enters port profile configuration mode for the named port profile.

	Command	Description
Step 3	**default** {**shutdown** | **switchport mode**} **Example:** n1000v(config-port-prof)# default switchport mode n1000v(config-port-prof)#	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	**show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*] **Example:** n1000v(config-port-prof)# show port-profile name AccessProf	(Optional) Displays the configuration for verification.

EXAMPLES

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

```
n1000v# config t
n1000v(config)# port-profile AccessProf
n1000v(config-port-prof)# default shutdown
n1000v(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:
n1000v(config-port-prof)#
```

Configuring Port Binding for vEthernet Port Profiles

You can use the following procedures in this section to configure port binding for vEthernet port profiles:

- Configuring a Default Port Binding Type, page 2-15
- Configuring Port Binding for a vEthernet Port Profile, page 2-16
- Verifying Port Binding on vCenter Server, page 2-18

BEFORE YOU BEGIN

Before beginning the procedures in this section, you must know or do the following:

- You have read the "vEthernet Port Binding" section on page 2-2.

- Once a vEthernet port profile has been created as a port group on the vCenter Server, you are not allowed to change its port binding type.
- You are not allowed to configure max ports for vEthernet port profiles with ephemeral port binding.
- You are not allowed to configure port binding for Ethernet type port profiles. Port binding is only available for vEthernet port profiles.
- Manual configurations on an interface are purged when the system administrator changes its port profile if either port profile is configured with ephemeral port binding. This occurs regardless of your auto purge setting**.**

  For more information about the **svs auto-config-purge** command, see the *Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4).*

Configuring a Default Port Binding Type

You can use this procedure to configure the type of port binding (static 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 or ephemeral) you want to use as a default for all new vEthernet port profiles.

SUMMARY STEPS

1. **config t**
2. **port-profile default port-binding** {**static** | **ephemeral**}
3. **show running-config**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Description
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.

	Command	Description
Step 2	**port-profile default port-binding** {**static** | **ephemeral**} **Example:** n1000v(config)# port-profile default port-binding ephemeral n1000v(config)#	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. • **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	**show running-config** **Example:** n1000v(config)# show running-config	(Optional) Displays the configuration for verification.
Step 4	**copy running-config startup-config** **Example:** n1000v(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.

EXAMPLES

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

```
n1000v# config t
n1000v(config)# port-profile default port-binding ephemeral
n1000v(config)#
```

Configuring Port Binding for a vEthernet Port Profile

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

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 have already created the vEthernet port profile using the "Creating a Port Profile" procedure on page 2-4.
- You know the type of port binding (static or ephemeral) you want to apply to this vEthernet port profile.

SUMMARY STEPS

1. **config t**

2. **port-profile** [**type** {**vethernet**}] *profile-name*
3. **port-binding** {**static** | **ephemeral**}
4. **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Description
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	**port-profile** [**type** {**vethernet**}] *profile-name* **Example:** n1000v(config)# port-profile AccessProf n1000v(config-port-prof)#	Enters port profile configuration mode for the named vEthernet port profile.
Step 3	**port-binding** {**static** | **ephemeral**} **Example:** n1000v(config-port-prof)# port-binding ephemeral n1000v(config-port-prof)#	Configures the type of port binding for this vEthernet port profile. • **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. • **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	**show port-profile** [**name** *profile-name*] **Example:** n1000v(config-port-prof)# show port-profile name AccessProf	(Optional) Displays the configuration for verification.
Step 5	**copy running-config startup-config** **Example:** n1000v(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.

EXAMPLES

This example shows how to configure the ephemeral port binding type for the existing port profile named ephemeral-pp:

```
n1000v# config t
n1000v(config)# port-profile ephemeral-pp
n1000v(config-port-prof)# port-binding ephemeral
n1000v(config-port-prof)#
```

Verifying Port Binding on vCenter Server

You can use this procedure to verify the port binding configuration for a port group in vCenter Server.

BEFORE YOU BEGIN

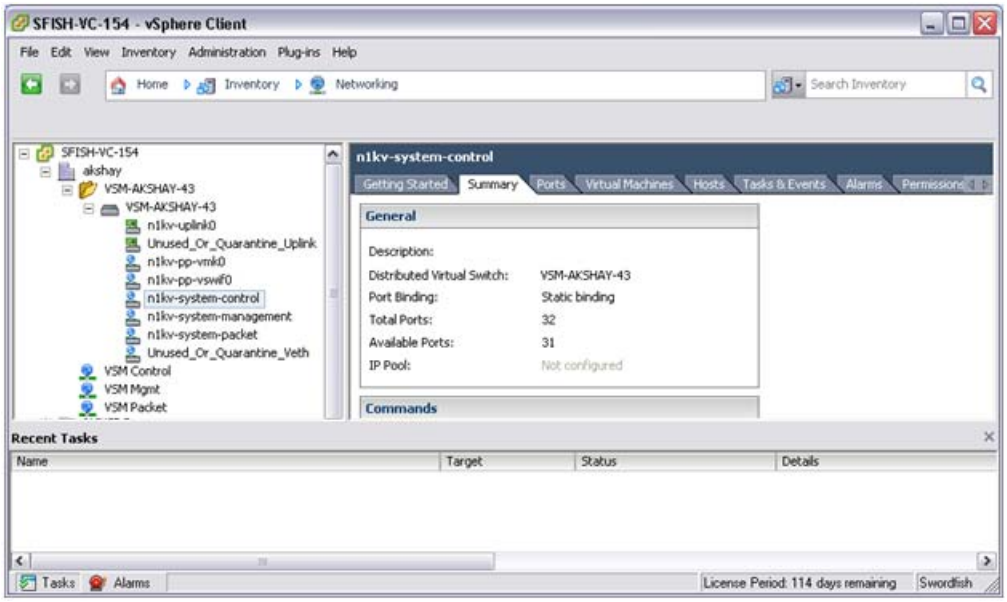
Before beginning this procedure, you must know or do the following:

- You are logged in to vCenter Server on the host.

DETAILED STEPS

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

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



Enabling a Port Profile

You can use this procedure to enable an existing port profile.

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 have already created the port profile using the "Creating a Port Profile" procedure on page 2-4.

SUMMARY STEPS

1. **config t**

2. **port-profile** [**type** {**ethernet** | **vethernet**}] *name*
3. **state enabled**
4. **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Description
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	**port-profile** [**type** {**ethernet** | **vethernet**}] *name* **Example:** n1000v(config)# port-profile AccessProf n1000v(config-port-prof)#	Enters port profile configuration mode for the named port profile.
Step 3	**state enabled** **Example:** n1000v(config-port-prof)# state enabled n1000v(config-port-prof)#	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	**show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*] **Example:** n1000v(config-port-prof)# show port-profile name AccessProf	(Optional) Displays the configuration for verification.
Step 5	**copy running-config startup-config** **Example:** n1000v(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.

EXAMPLES

This example shows how to enable a port profile:

```
n1000v# config t
n1000v(config)# port-profile AccessProf
n1000v(config-port-prof)# state enabled
n1000v(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:
n1000v(config-port-prof)#
```

Removing a Port Profile

You can use this procedure to remove a port profile.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- If 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, page 3-4.
- 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.

SUMMARY STEPS

1. **config t**
2. (Optional) **show port-profile virtual usage name** *profile_name*
3. **no port-profile** *profile_name*
4. **show port-profile name** *profile_name*
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Description

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Enters global configuration mode.

Step 2	**show port-profile virtual usage name** *profile_name* **Example:** `n1000v(config)# show port-profile virtual usage name AccessProf`	(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	**no port-profile** *profile_name*
	
	Example:
	`n1000v(config)# no port-profile AccessProf`
	`n1000v(config)#`
		Removes the port profile configuration and operational settings.

	Command	Description
Step 4	**show port-profile name** *profile_name* **Example:** n1000v(config)# show port-profile name AccessProf ERROR: port-profile AccessProf does not exist n1000v(config)#	(Optional) Verifies that the port profile does not exist.
Step 5	**copy running-config startup-config** **Example:** n1000v(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.

EXAMPLES

This example shows how to remove a port profile:

```
n1000v# config t
n1000v(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.
n1000v(config)# no port-profile AccessProf
n1000v(config)# show port-profile name AccessProf
ERROR: port-profile AccessProf does not exist
n1000v(config)# copy running-config startup-config
```

Additional References

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

- Related Documents, page 2-21
- Standards, page 2-22

Related Documents

Related Topic	Document Title
Complete command syntax, command modes, command history, defaults, usage guidelines, and examples for all Cisco Nexus 1000V commands.	*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)*
Port Profile Inheritance	"Configuring Port Profile Inheritance" section on page 3-1
System Port Profiles	"Configuring System Port Profiles" section on page 4-1
Port Channels	"Configuring Port Channels in Port Profiles" section on page 5-1
Private VLANs	"Configuring a Private VLAN in a Port Profile" section on page 5-1

Related Topic	Document Title
Port profile roles	"Restricting Port Profile Visibility" section on page 6-1
Verifying port profiles	"Verifying the Port Profile Configuration" section on page 7-1
Configuration limits	"Port Profile Configuration Limits" section on page A-1
Configuring interfaces including port channels	*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4)*
Adding an IP or MAC access control list (ACL) to a port profile.	*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(4)*
Adding a NetFlow flow monitor to a port profile.	*Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(4)*

Standards

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

Feature History for Port Profiles

This section provides the feature history for port profiles.

Feature Name	Releases	Feature Information
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 Profiles	4.0(4)SV1(1)	This feature was introduced.
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.

CHAPTER 3

Configuring Port Profile Inheritance

This chapter describes how to configure port profile inheritance, including the following:

- Information About Port Profile Inheritance, page 3-1
- Inheriting a Configuration from a Port Profile, page 3-2
- Removing Inherited Policies from a Port Profile, page 3-4

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 3-1 lists the port profile settings and shows whether they can be inherited.

Table 3-1 Port Profile Settings Inheritance

	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
inherit	X	
interface state (shut/no shut)	X	
mtu		X
name	X	
netflow	X	
pinning	X	
port security	X	

Table 3-1 Port Profile Settings Inheritance (continued)

Port Profile Setting	Can it be inherited?	
	Yes	No
private vlan configuration	X	
qos policy	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

Follow these guidelines and limitations when 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 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 the "Removing Inherited Policies from a Port Profile" procedure on page 3-4.
- The Cisco Nexus 1000V software must be initially configured. For information, see the *Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(4)*.
- The Cisco Nexus 1000V must be connected to the 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.

Before You Begin

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

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

- To identify the port profile with a configuration you want to use, use the following command to view your existing port profiles:
  - **show port profiles**
- You are familiar with the port profile characteristics shown in Table 3-1 on page 3-1, and whether they can be inherited.
- The port profile type cannot be inherited from another port profile.

SUMMARY STEPS

1. **config t**
2. **port-profile** [**type** {**ethernet** | **vethernet**}] *name*
3. **inherit port-profile** *name*
4. **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Description

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Enters global configuration mode.

Step 2	**port-profile** [**type** {**ethernet** | **vethernet**}] name
	
	Example:
	`n1000v(config)# port-profile type vethernet AllAccess2`
	`n1000v(config-port-prof)#`
		Enters port profile configuration mode for the named port profile.
		• *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.
		The type cannot be inherited.
		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 1	**inherit port-profile** *name*
	
	Example:
	`n1000v(config-port-prof)# inherit port-profile AllAccess1`
	`n1000v(config-port-prof)#`
		Adds the inherited configuration of the named profile as a default configuration.

	Command	Description
Step 2	**show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*] **Example:** n1000v(config-port-prof)# show port-profile AllAccess2	(Optional) Displays the configuration for verification.
Step 3	**copy running-config startup-config** **Example:** n1000v(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.

EXAMPLES

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

```
n1000v# config t
n1000v(config)# port-profile AllAccess2
n1000v(config-port-prof)# inherit port-profile AllAccess1
n1000v(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:
n1000v(config-port-prof)#
```

Removing Inherited Policies from a Port Profile

You can use this procedure to remove the inherited policies from a port profile.

BEFORE YOU BEGIN

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

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

SUMMARY STEPS

1. **config t**
2. (Optional) **show port-profile virtual usage name** *profile_name*

3. **no inherit port-profile** *profile_name*
4. (Optional) **show port-profile virtual usage name** *profile_name*
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Description
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	**show port-profile virtual usage name** *profile_name* **Example:** n1000v(config)# show port-profile virtual usage name AccessProf	(Optional) Displays the policies inherited in the named port profile.
Step 3	**port-profile** *name* **Example:** (config)# port-profile Access4 (config-port-prof)#	Enters port profile configuration mode for the named port profile.
Step 4	**no inherit port-profile** *profile_name* **Example:** (config-port-prof)# no inherit port-profile AccessProf	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	**show port-profile virtual usage name** *profile_name* **Example:** n1000v(config)# show port-profile virtual usage name AccessProf	(Optional) Displays the policies inherited for verification of the removal.
Step 6	**copy running-config startup-config** **Example:** n1000v(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.

CHAPTER 4

Configuring System Port Profiles

This chapter describes system port profiles and how to configure them.

This chapter includes the following sections:

- Information About System Port Profiles, page 4-1
- Guidelines and Limitations for System Port Profiles, page 4-2
- Creating a System Port Profile, page 4-2
- Deleting System VLANs from a Port, page 4-6
- Modifying the System VLANs in a Port Profile, page 4-6
- Feature History for System Port Profiles, page 4-10

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.

For more information about system port profiles and system VLANs, see the *Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(4)*.

For a summary of the default settings used with port profiles, see the "Default Settings" section on page 2-3.

Guidelines and Limitations for System Port Profiles

System port profiles and system VLANs are subject to the following guidelines and limitations:

- System VLANs must be used sparingly and only as described in the "Information About System Port Profiles" section on page 4-1.
- For maximum system port profiles per host and DVS, see the "Port Profile Configuration Limits" section on page A-1.
- 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

You can use this procedure to configure a system port profile for critical ports.

BEFORE YOU BEGIN

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

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

- A system port profile must be of the Ethernet type because it is used for physical ports. This procedure configures the Ethernet 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.
- Once a port profile is created, you cannot change its type (Ethernet or vEthernet).
- The MTU size you set must be less than or equal to the fixed **system jumbomtu** size of 9000.

  For more information, see the *Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4)*.
- When you configure MTU on an interface, it takes precedence over MTU configured on the port profile.

  For more information, see the *Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4)*.

SUMMARY STEPS

1. **config t**
2. **port-profile type ethernet** *profilename*
3. **description** *profiledescription*
4. **switchport mode trunk**
5. **switchport trunk allowed vlan** *vlan-id-list*
6. **no shutdown**
7. **system vlan** *vlan-id-list*
8. (Optional) **mtu** *mtu-size*
9. **show port-profil**e [**brief** | **expand-interface** | **usage**] [**name** *profilename*]
10. **copy running-config startup-config**

DETAILED STEPS

	Command	Description
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	**port-profile type ethernet** *profilename* **Example:** n1000v(config)# port-profile AccessProf n1000v(config-port-prof)#	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**—The port profile type for system port profiles must be Ethernet. 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. This is a requirement for system port profiles. 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	**description** *profiledescription* **Example:** n1000v(config-port-prof)# description System profile for critical ports n1000v(config-port-prof)#	Adds a description of up to 80 ASCII characters to the port profile. This description is automatically pushed to the vCenter Server.
Step 4	**switchport mode trunk** **Example:** n1000v(config-port-prof)# switchport mode trunk n1000v(config-port-prof)#	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	Description

Step 5	**switchport trunk allowed vlan** *vlan-id-list*
	
	Example:
	`n1000v(config-port-prof)# switchport trunk allowed vlan 114,115`
	`n1000v(config-port-prof)#`
		Designates the port profile as trunking and defines VLAN access to it as follows:
		• *allowed-vlans*—Defines VLAN IDs that are allowed on the port.
		• **add**—Lists VLAN IDs to add to the list of those allowed on the port.
		• **except**—Lists VLAN IDs that are not allowed on the port.
		• **remove**—Lists VLAN IDs whose access is to be removed from the port.
		• **all**—Indicates that all VLAN IDs are allowed on the port, unless exceptions are also specified.
		• **none**—Indicates that no VLAN IDs are allowed on the port.
		If you do not configure allowed VLANs, then the default VLAN 1 is used as the allowed VLAN.

Step 6	**no shutdown**
	
	Example:
	`n1000v(config-port-prof)# no shutdown`
	`n1000v(config-port-prof)#`
		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	**system vlan** *vlan-id-list*
	
	Example:
	`n1000v(config-port-prof)# system vlan 114,115`
	`n1000v(config-port-prof)#`
		Adds system VLANs to this port profile.

Step 8	**mtu** *mtu-size*
	
	Example:
	`n1000v(config-port-prof)# mtu 4000`
	`n1000v(config-port-prof)#`
		(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.

Step 9	**show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*] **Example:** `n1000v(config-port-prof)# show port-profile name AccessProf`	(Optional) Displays the configuration for verification.

EXAMPLE

This example shows how to create a system port profile:

```
n1000v# config t
n1000v(config)# port-profile AccessProf
n1000v(config-port-prof)# description "System profile for critical ports"
n1000v(config-port-prof)# system vlan 1
n1000v(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:
```

Deleting System VLANs from a Port

You can use this procedure to delete system VLANs from a port from vCenter server.

BEFORE YOU BEGIN

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

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

DETAILED STEPS

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

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

Modifying the System VLANs in a Port Profile

You can use the following procedures in this section to modify the system VLANs in a port profile without removing all system VLANs.

- Modifying the System VLANs in a Trunk Mode Port Profile, page 4-7
- Modifying System VLANs in an Access Mode Port Profile, page 4-8

Modifying the System VLANs in a Trunk Mode Port Profile

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

BEFORE YOU BEGIN

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

- 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 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.

DETAILED STEPS

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

The VEMs are disconnected from the VSM.

Step 2 From the Cisco Nexus 1000V, use the following commands to convert the port profile to an access profile with a system VLAN. It does not matter which system VLAN you use.

config t

port-profile *name*

no system vlan

switchport mode access

switchport access vlan *vlan-id*

no shutdown

system vlan *vlan-id*

```
Example:
n1000v# config t
n1000v(config)# port-profile Trunk_System_Prof
n1000v(config-port-prof)# no system vlan
n1000v(config-port-prof)# switchport mode access
n1000v(config-port-prof)# switchport access vlan 1
n1000v(config-port-prof)# system vlan 300
```

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

Step 3 From the Cisco Nexus 1000V, use the following commands to convert the port profile back to a trunk profile with the required system VLAN IDs.

config t

port-profile *name*

switchport mode trunk

system vlan *vlan-id-list*

show port-profile [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]

copy running-config startup-config

```
Example:
n1000v# config t
n1000v(config)# port-profile Trunk_System_Prof
n1000v(config-port-prof)# switchport mode trunk
n1000v(config-port-prof)# system vlan 114,115
n1000v(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:
n1000v(config-port-prof)# copy running-config startup-config
```

The port profile is changed back to a trunk profile with the required system VLANs, and the changes are saved in the running configuration.

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.

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

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

- 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.

DETAILED STEPS

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

The VEMs are disconnected from the VSM.

Step 2 From the Cisco Nexus 1000V, use the following commands to configure a new list of system VLANs in the port profile.

config t

port-profile *name*

system vlan *vlan-id-list*

show port-profile name *profile-name*]

copy running-config startup-config

```
Example:
n1000v# config t
n1000v(config)# port-profile Access_System_Prof
n1000v(config-port-prof)# system vlan 114,115
n1000v(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:
n1000v(config-port-prof)# copy running-config startup-config
```

The list of system VLANs is changed and saved in the running configuration.

Step 3 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.

Feature History for System Port Profiles

This section provides the feature history for system port profiles.

Feature Name	Releases	Feature Information
MTU	4.2(1)SV1(4)	The **system mtu** command is removed and replaced with the **mtu** command.
System Port Profiles	4.0(4)SV1(1)	This feature was introduced.
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.

CHAPTER 5

Configuring a Private VLAN in a Port Profile

This chapter describes how to create a port profile for a private VLAN (PVLAN).

This chapter includes the following sections:

- Information About Private VLANs, page 5-1
- Configuring a Port Profile as a Private VLAN, page 5-1
- Feature History for Private VLAN Port Profiles, page 5-4

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 PVLAN, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(4)*

Configuring a Port Profile as a Private VLAN

You can use this procedure to configure a port profile to be used as a private VLAN (PVLAN).

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 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. **config t**
2. **port-profile** [**type** {**ethernet** | **vethernet**}] *name*
3. **switchport mode private-vlan** {**host** | **promiscuous** | **trunk promiscuous**}

4. **switchport private-vlan host-association** *primary-vlan secondary-vlan*
5. **switchport private-vlan trunk allowed vlan** *vlan-range*
6. **switchport private-vlan mapping** *primary_vlan* [add | remove] *secondary_vlan*
7. **switchport private-vlan mapping trunk** *primary_vlan* [add | remove] *secondary_vlan*
8. **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
9. **copy running-config startup-config**

DETAILED STEPS

	Command	Description
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	**port-profile** [**type** {**ethernet** | **vethernet**}] *name* **Example:** n1000v(config)# port-profile AccessProf n1000v(config-port-prof)#	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	Description
Step 3	**switchport mode private-vlan** {**host**|**promiscuous**|**trunk promiscuous**} **Example:** n1000v(config-port-prof)# switchport mode private-vlan promiscuous n1000v(config-port-prof)#	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 – Isolated PVLAN host port • **promiscuous trunk**—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	**switchport private-vlan host-association** *primary-vlan secondary-vlan* **Example:** n1000v(config-port-prof)# switchport private-vlan host-association 3 300 n1000v(config-port-prof)#	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	**switchport private-vlan trunk allowed vlan** *vlan-range* **Example:** n1000v(config-port-prof)# switchport private-vlan trunk allowed vlan 155-156 n1000v(config-port-prof)#	Sets the allowed VLANs and VLAN IDs when interface is in private-vlan trunking mode.
Step 6	**switchport private-vlan mapping** *primary_vlan* [add | remove] *secondary_vlan* **Example:** n1000v(config-port-prof)# switchport private-vlan mapping 3 add 300 301 302 n1000v(config-port-prof)#	Maps the primary VLAN ID to the secondary VLAN ID for the port profile.
Step 7	**switchport private-vlan mapping trunk** *primary_vlan* [add | remove] *secondary_vlan* **Example:** n1000v(config-port-prof)# switchport private-vlan mapping trunk 3 add 300 301 302 n1000v(config-port-prof)#	
Step 8	**show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*] **Example:** n1000v(config-port-prof)# show port-profile name AccessProf	(Optional) Displays the configuration for verification.

	Command	Description
Step 9	**copy running-config startup-config** **Example:** n1000v(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.

```
switch# config t
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

This section provides the feature history for system port profiles.

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

CHAPTER 6

Restricting Port Profile Visibility

This chapter describes the commands used to restrict visibility of port profiles to a user or a group of users and includes the following sections:

- Information About Port Profile Visibility, page 6-1
- Guidelines and Limitations, page 6-2
- Defining DVS Access in vSphere Client, page 6-3
- Enabling the Port Profile Role Feature, page 6-5
- Restricting Port Profile Visibility on the VSM, page 6-6
- Removing a Port Profile Role, page 6-9
- Feature History for Restricting Port Profile Visibility, page 6-11

Information About Port Profile Visibility

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

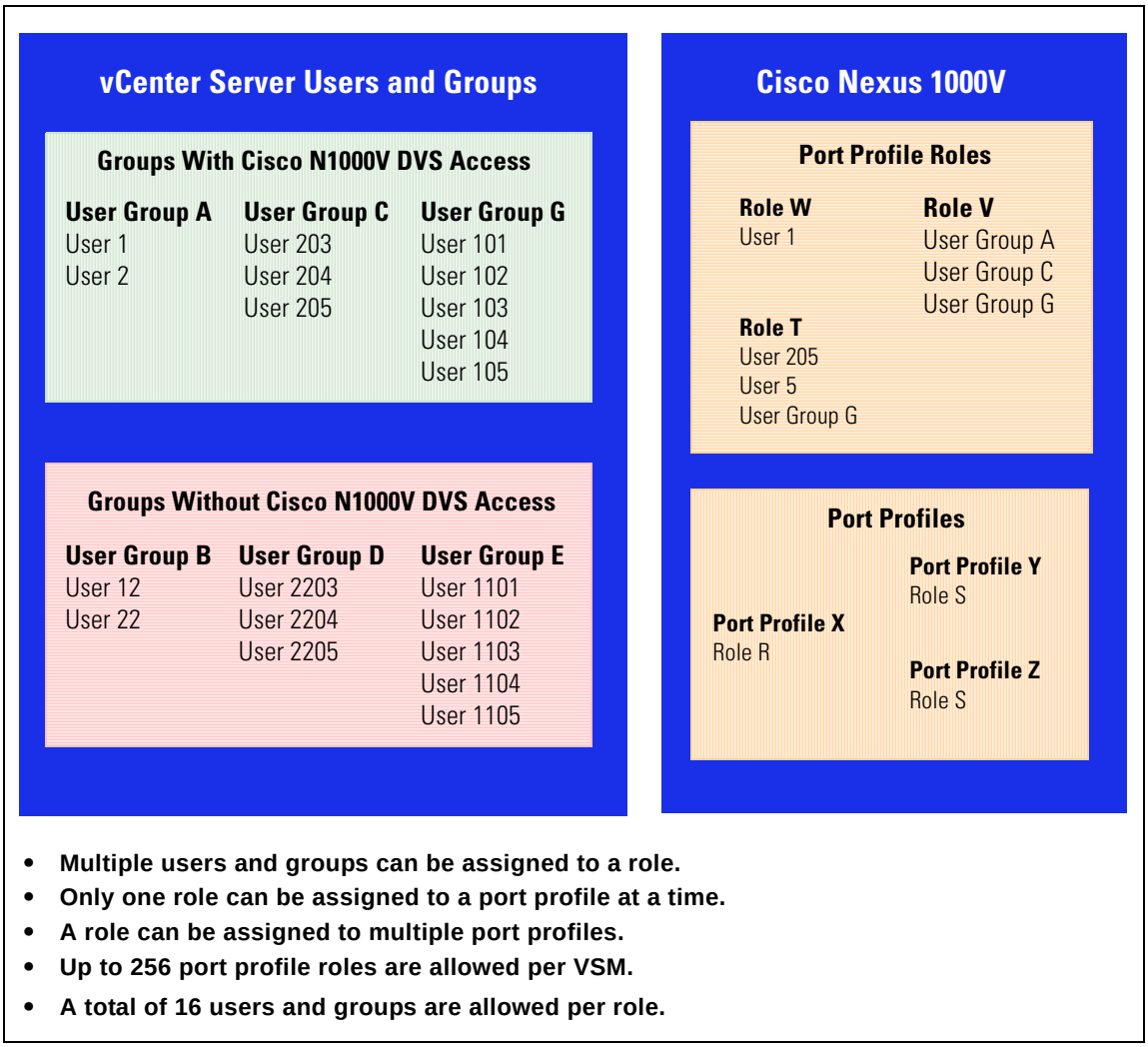
Before you can restrict the visibility of a port group, the server administrator must define which vCenter users and user groups have access to the Cisco Nexus 1000V DVS top level folder in vCenter server. Once this is done, the network administrator can further define the visibility of specific port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

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 vCenter where access is already defined. Group members defined in vCenter automatically gain access to the port groups defined for the group.

You can see in Figure 6-1 the relationship between users and groups in vCenter server and port profiles and port profile roles in Cisco Nexus 1000V.

Figure 6-1 Port Profile Visibility: Users, 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.**

Guidelines and Limitations

Use the following guidelines and limitations when 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 vCenter server.
- The Cisco Nexus 1000V VSM must be connected to the 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 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

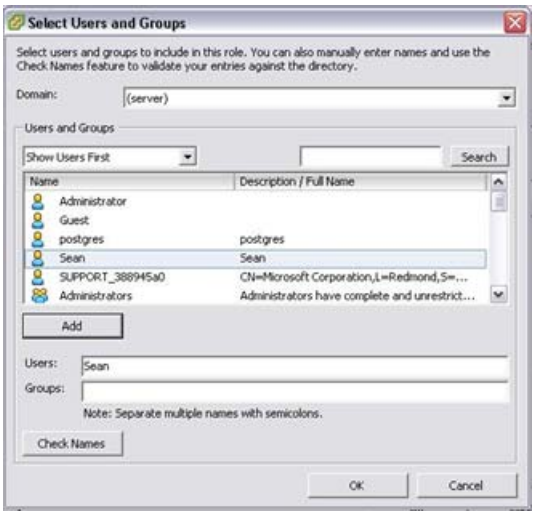
Before beginning this procedure, you must know or do the following:

- You are logged in to 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" procedure on page 6-6.

DETAILED STEPS

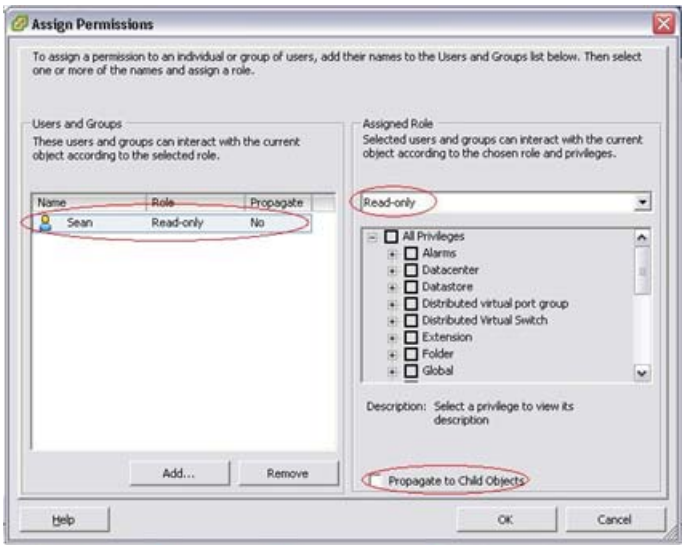
Step 1 From Inventory > Networking, right-click the Cisco Nexus 1000V DVS folder, and choose **Add Permission**.

The Select Users and Groups dialog box opens.



Step 2 Choose the name from the list of users and groups and click **Add**. Then click **OK**.

The Assign Permissions dialog box opens.



Step 3 From the Assigned Role selection list, choose a role for this user or group.

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.

Step 4 Make sure that the Propagate to Child Objects box is unchecked.

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

Step 5 Click **OK**.

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

Step 6 To restrict access to specific port groups, go to the "Restricting Port Profile Visibility on the VSM" procedure on page 6-6.

Enabling the Port Profile Role Feature

The network administrator can use this procedure to enable the port profile role feature on the VSM.

BEFORE YOU BEGIN

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

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

SUMMARY STEPS

1. **config t**
2. **feature port-profile-role**
3. (Optional) **show feature**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Description
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	**feature port-profile-role** **Example:** n1000v(config)# **feature port-profile-role adminUser** n1000v(config)#	Enables the port profile roles feature to restrict user and group access.

	Command	Description
Step 3	**show feature** **Example:** n1000v (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 n1000v(config)#	(Optional) Displays the configuration for verification.
Step 4	**copy running-config startup-config** **Example:** n1000v(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.

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

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

- 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" procedure on page 6-3.
- You have enabled the port profile role feature using the "Enabling the Port Profile Role Feature" procedure on page 6-5.
- 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. **config t**
2. **port-profile-role** *role-name*
3. (Optional) **description** *role-description*
4. (Optional) **show port profile role users**
5. (Optional) **user** *user-name*

   (Optional) **group** *group-name*
6. **exit**
7. **port-profile** [**type** {**ethernet** | **vethernet**}] *profile-name*
8. **assign port-profile-role** *role-name*
9. (Optional) **show port-profile-role** [**name** *role-name*]
10. **copy running-config startup-config**

DETAILED STEPS

	Command	Description
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	**port-profile-role** *role-name* **Example:** n1000v(config)# **port-profile-role adminUser** n1000v(config-port-prof-role)#	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	**description** *role-description* **Example:** n1000v(config-port-profile-role)# **description adminOnly** n1000v(config-port-profile-role)#	(Optional) Adds a description of up to 32 characters to the role. This description is automatically pushed to vCenter Server.

Step 4	**show port-profile-role users**
	
	Example:
	n1000v(config-port-profile-role)# **show port-profile-role users**
	Groups:
	  Administrators
	  TestGroupB
	Users:
	  dbaar
	  fgreen
	  suchen
	  mariofr
	n1000v(config-port-profile-role)#
		(Optional) Displays all the users on vCenter Server who have access to the DVS parent folder and who can be assigned to the role.

	Command	Description
Step 5	**Enter one or more of the following:** **user** *user-name* **group** *group-name* **Example:** n1000v(config-port-profile-role)# **user hdbaar** n1000v(config-port-profile-role)# **Example:** n1000v(config-port-profile-role)# **group credit** n1000v(config-port-profile-role)#	(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. **Note** Multiple users and groups can be assigned to a role. **Note** 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" procedure on page 6-3.
Step 6	**exit** **Example:** n1000v(config-port-profile-role)# **exit** n1000v(config)#	Exits port-profile-role configuration mode and returns you to global configuration mode.
Step 7	**port-profile** *profile-name* **Example:** n1000v(config)# **port-profile allaccess2** n1000v(config-port-prof)#	Enters port profile configuration mode for the named port profile.
Step 8	**assign port-profile-role** *role-name* **Example:** n1000v(config-port-prof)# **assign port-profile-role adminUser** n1000v(config-port-prof)#	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. **Note** A role can be assigned to multiple port profiles.
Step 9	**show port-profile-role** [**name** *role-name*] **Example:** n1000v(config-port-prof)# **show port-profile-role name adminUser** Name: adminUser Description: adminOnly Users: hdbaar (user) Assigned port-profiles: allaccess2 n1000v(config-port-prof)#	(Optional) Displays the configuration for verification.
Step 10	**copy running-config startup-config** **Example:** n1000v(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.

EXAMPLES

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

```
config t
port-profile-role adminUser
description adminOnly
user hdbaar
exit
port-profile allaccess2
assign port-profile-role adminUser
show port-profile-role name adminUser

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

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

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

DETAILED STEPS

	Command	Description
Step 1	**show port-profile-role** [**name** *role-name*] **Example:** n1000v(config-port-prof)# **show port-profile-role name adminUser** Name: adminUser Description: adminOnly Users: hdbaar (user) Assigned port-profiles: allaccess2 n1000v(config-port-prof)#	(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 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	**port-profile** *profile-name* **Example:** n1000v(config)# **port-profile allaccess2** n1000v(config-port-prof)#	Enters port profile configuration mode for the named port profile.
Step 3	**no assign port-profile-role** *role-name* **Example:** n1000v(config-port-prof)# **no assign port-profile-role adminUser** n1000v(config-port-prof)#	Removes the role from the port profile. The port group is updated in vCenter Server.
Step 4	**exit** **Example:** n1000v(config-port-profile)# **exit** n1000v(config)#	Exits port-profile configuration mode and returns you to global configuration mode.
Step 5	**no port-profile-role** *role-name* **Example:** n1000v(config)# **no port-profile-role adminUser** n1000v(config)#	Removes the role from the VSM.
Step 6	**show port-profile-role** [**name** *role-name*] **Example:** n1000v(config-port-prof)# **show port-profile-role name adminUser**	(Optional) Displays the configuration for verification.
Step 7	**copy running-config startup-config** **Example:** n1000v(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.

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 7

Verifying the Port Profile Configuration

This chapter describes the commands used to verify port profile configurations and includes the following sections:

- Verifying the Port Profile Configuration, page 7-1
- Feature History for Port Profile Verification, page 7-5

Verifying the Port Profile Configuration

You can use the following commands to verify the port profile configuration.

Command	Purpose
show port-profile [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]	Displays the port profile configuration. See Example 7-1 on page 7-2. See Example 7-2 on page 7-3. See Example 7-3 on page 7-3. See Example 7-5 on page 7-4. See Example 7-6 on page 7-4
show port-profile-role [**name** *port-profile-role-name*]	Displays the port profile role configuration, including role names, descriptions, assigned users, and assigned groups. See Example 7-9 on page 7-5.
show running-config port-profile [*profile-name*]	Displays the port profile configuration. See Example 7-8 on page 7-4.
show port-profile-role users	Displays available users and groups. See Example 7-10 on page 7-5.
show port-profile sync-status [**interface** *if-name*]	Displays interfaces that are out of sync with the port profile. See Example 7-7 on page 7-4.

Command	Purpose
show port-profile virtual usage [**name** *profile-name*]	Displays the port profile usage by interface. See Example 7-4 on page 7-3.
show running-config port-profile [*prof-name*]	Displays the port profile configuration, including interface assignments. See Example 7-8 on page 7-4.

For detailed information about the command output, see the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)*.

EXAMPLES

Example 7-1 show port-profile

```
n1000v# 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:n1000v#
```

Example 7-2 show port-profile name UpLinkProfile

```
n1000v# 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:
n1000v#
```

Example 7-3 show port-profile brief

```
n1000v# 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
n1000v#
```

Example 7-4 show port-profile virtual usage

```
n1000v# 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
n1000v#
```

Example 7-5 show port-profile expand-interface name UplinkProfile1

```
n1000v# show port-profile expand-interface name UplinkProfile1
port-profile UplinkProfile1
Ethernet2/2
    switchport mode trunk
    switchport trunk allowed vlan 110-119
    no shutdown
n1000v#
```

Example 7-6 show port-profile expand-interface

```
n1000v# 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
n1000v#
```

Example 7-7 show port-profile sync-status

```
n1000v# 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
n1000v#
```

Example 7-8 show running-config port-profile

```
n1000v# 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
n1000v#
```

Example 7-9 show port-profile-role

```
n1000v# show port-profile-role name adminUser

Name: adminUser
Description: adminOnly
Users:
    hdbaar (user)
Assigned port-profiles:
    allaccess2
n1000v#
```

Example 7-10 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

This section provides the 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.
show running-config command	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.

Feature Name	Releases	Feature Information
show port-profile *name* command	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 section lists the maximum configuration limits for port profile features.

Table A-1 Port Profile Maximum Configuration Limits

Port Profile Feature	Maximum Limit per DVS	Maximum Limit per Host
vEthernet interfaces	2000	216
vEthernet trunks	256	8
vEthernet interfaces per port profile	1024	—
Port Profiles	2048	—
System Profiles per host	32	16
Private VLAN	512	—

INDEX

A

atomic inheritance, about 1-3

C

capability uplink command
  new and changed information ii-iv
class-map limits A-1
clearing a policy 2-13, 4-2
community ports 5-2
configuration limits A-1

D

default command 2-14
description command 2-5, 4-4, 6-7
disabled state, about 2-1
documentation
  additional publications iv-xiii

E

enabled state, about 2-1
enabling
  port profiles 2-19
  ports in the profile 2-9, 2-12

F

feature port-profile-role command 6-5

H

host ports 5-2

I

inheritance
  removing a port profile 2-20
interface quarantine, about 1-3
isolated ports 5-2

L

limits, configuration A-1

M

MAC pinning
  new and changed information ii-iv
mapping PVLANs 5-3
match criteria limit A-1

N

no port-profile command 2-20
no shutdown command 2-9, 2-12, 4-5

O

options, designating group as VMware 2-5

P

policy map limits A-1
port binding
  default setting 2-15
  information about 2-2
  verify in vCenter 2-18
port-binding command 2-16, 2-17
port-profile command 2-4, 3-3, 6-7, 6-9
port-profile-role command 6-7, 6-10
port profiles
  configuring as private VLAN 5-1
  creating 2-4
  enabling 2-18
  mapping PVLANs 5-3
  removing 2-20
  type
    new and changed information ii-iv
  VLANs 2-7
  VMware tag 2-5
ports, private vlan 5-2
private VLANs
  See PVLANs.
promiscuous ports 5-2
PVLANs
  configuring port profiles as 5-1
PVLAN-switchport association 5-3

Q

quarantine, about 1-3

R

ranges, VLANs 2-7
related documents iv-xiii, iv-xv
removing a port profile 2-20
rollback to consistent config, about 1-3

S

service policy limits A-1
show feature command 6-6
show port-profile command
  new and changed information ii-v
show port-profile-role command 6-8, 6-10
show port-profile sync-status command 7-1
show port-profile virtual usage command 7-2
show running-config
  new and changed information ii-iv
shutdown command 2-14
state
  port profile, about 2-1
state enabled command 2-19
static pinning
  new and changed information ii-iv
switchport mode command 2-12, 2-14
switchport mode private-vlan command 5-2
switchport private-vlan host-association command 5-3
switchport private-vlan mapping command 5-3
switchport-PVLAN association 5-3
switchport trunk allowed vlan, command 2-9, 2-10
system port profiles
  information about 4-1
system vlan command 4-5

U

user command 6-8

V

vEthernet
  port binding 2-2
VLAN ranges 2-7
VLANs, private
  See PVLANs
VMware, identifying in port group 2-5

vmware port-group command 2-6
vPC-HM
new and changed information ii-iv
vPC-Host Mode, See vPC-HM.