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

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

April 8, 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-20463-06

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

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

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(2)
© 2010 Cisco Systems, Inc. All rights reserved.

New and Changed Information

This section describes the information in this document that is either new or has changed with Release 4.0(4)SV1(2).

To find additional information about new features or command changes in Release 4.0(4)SV1(2), see the following:

- Release Notes.
- Command Reference.

Table 1 New and Changed Getting Started Information in Release 4.0(4)SV1(2)

Feature	Description	Changed in Release	Where Documented
GUI Setup procedures	A new GUI application is added to set up the Cisco Nexus 1000V software.	4.0(4)SV1(2)	"Configuring the Software Using the GUI"
CLI Setup procedures	The procedures for setting up the Cisco Nexus 1000V using the CLI have been moved into this document from the *Cisco Nexus 1000V Software Installation Guide, Release 4.0(4)SV1(2)*.	4.0(4)SV1(2)	"Configuring the Software Using the CLI"
Configuration Limits	Lists the Cisco Nexus 1000V configuration limits.	4.0(4)SV1(2)	Chapter 8, "Configuration Limits"
VSM Vmotion support	Support is added for Vmotion of the VSM VM.	4.0(4)SV1(2)	"Implementation Considerations"
System VLANs	Revixed the description of system VLANs and system port profiles.	4.0(4)SV1(2)	"System Port Profiles and System VLANs" section on page 4

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

CONTENTS

New and Changed Information iii

Preface ix

- Audience ix
- Recommended Reading ix
- Document Organization x
- Document Conventions x
- Related Documentation xi
- Obtaining Documentation and Submitting a Service Request xii

Overview 1-1

- Information about Virtualization 1-1
- Information About Cisco Nexus 1000V 1-2
  - System Description 1-2
    - Management, Control, and Packet VLANs 1-3
    - Port Profiles 1-3
    - System Port Profiles and System VLANs 1-4
  - Administrator Roles 1-5
  - Contrasting the Cisco Nexus 1000V with a Physical Switch 1-5
  - Implementation Considerations 1-6
  - Software Compatibility 1-6
  - Configuring Cisco Nexus 1000V with CLI 1-6

Setting Up the Software 2-1

- Prerequisites 2-1
- Software Configuration Process 2-5
- Creating VLANs 2-5
- Verifying the Configuration 2-8
- Starting the VMs 2-9
- Implementation Guidelines 2-10

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

Configuring the Software Using the GUI 3-1

GUI Software Configuration Process 3-1

Setting Up the VSM Virtual Machine Using the GUI 3-2

Configuring the VSM HA Role 3-9

Configuring the Software Using the CLI 4-1

CLI Software Configuration Process 4-1

Setting Up the VSM Virtual Machine Using the CLI 4-2

Verifying VSM Connectivity 4-7

Creating a Cisco Nexus 1000V Plug-In on the vCenter Server 4-8

Connecting to the vCenter Server 4-9

Configuring the System Port Profile for VSM-VEM Communication 4-11

Example Configuration: System Profile for Critical Ports 4-15

Configuring the Uplink Port Profile for VM Traffic 4-15

Example Configuration: Uplink Profile for VM Traffic 4-18

Configuring the Data Port Profile for VM Traffic 4-18

Example Configuration: Data Profile for VM Traffic 4-21

Adding an ESX 4.0 Host to the DVS 4-21

Running a VSM and VEM on the Same Host 5-1

Information About a VSM and VEM on the Same Host 5-1

Guidelines and Limitations 5-2

Configuring a VSM and its VEM on the Same Host 5-3

Understanding the CLI 6-1

Information About the CLI Prompt 6-1

Command Modes 6-2

About Command Modes 6-2

EXEC Command Mode 6-3

Global Configuration Command Mode 6-3

Accessing Interface Configuration Command Mode 6-3

Exiting a Configuration Mode 6-4

Command Mode Summary 6-5

Saving CLI Configuration Changes 6-6

Running Configuration 6-6

Startup Configuration 6-6

Copying the Running Configuration to the Startup Configuration 6-7

Special Characters 6-7

Keystroke Shortcuts 6-7

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

Abbreviating Commands 6-9
Using the No Form of a Command 6-9
Using CLI Variables 6-10
User-Defined CLI Session Variables 6-10
User-Defined CLI Persistent Variables 6-11
System-Defined Variables 6-12
Working with Command Scripts 6-12
Running a Script 6-12
Using CLI Variables in Scripts 6-13
Delaying Command Action 6-14
Using Help 6-14

Configuring the Terminal 7-1
Information about the Terminal 7-1
Defining a Terminal Type 7-1
Setting the Screen Length for the Console Terminal 7-2
Setting the Screen Width for the Console Terminal 7-2
Displaying Terminal Settings 7-3
Setting the Timeout for Console Connections 7-3
Setting the Timeout for SSH and Telnet Connections 7-4
Clearing a Line Connection to the Switch 7-5
Setting a Timeout for the Current Session 7-5

Configuration Limits 8-1

List of Terms 9-1

INDEX

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

Preface

This document, *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(2)*, is designed to provide enough information about the system to get you started configuring and using the Cisco Nexus 1000Vin your datacenter.

This preface includes the following topics:

- Audience, page ix
- Recommended Reading, page ix
- Document Organization, page x
- Document Conventions, page x
- Related Documentation, page xi

Audience

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

- An understanding of virtualization
- Using VMware tools to create a virtual machine and configure a vswitch

Note Knowledge of VMware vNetwork Distributed Switch is not required.

Recommended Reading

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

- *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(2)* (this document)
- *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)*
- *Cisco Nexus 1000V Software Installation Guide, Release 4.0(4)SV1(2)*
- *Cisco Nexus 1000V Virtual Ethernet Module Software Installation Guide, Release 4.0(4)SV1(2)* (server administrators)
- *Cisco VN-Link: Virtualization-Aware Networking* white paper

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

Document Organization

This document is organized into the following chapters:

Chapter and Title	Description
Chapter 1, "Overview"	Provides an overview of the Cisco Nexus 1000V product and features.
Chapter 2, "Setting Up the Software"	Describes how, after installing the Cisco Nexus 1000V software, to setup a configuration.
Chapter 3, "Configuring the Software Using the GUI"	Describes howuse the GUI Application to setup a configuration file.
Chapter 4, "Configuring the Software Using the CLI"	Describes howuse the CLI to setup a configuration file.
Chapter 5, "Running a VSM and VEM on the Same Host"	Describes how, after installing the Cisco Nexus 1000V software, to configure a VEM on the same host.
Chapter 6, "Understanding the CLI"	Describes how to use the CLI, including command modes, prompts, keystroke shortcuts, variables, scripts, and so forth.
Chapter 7, "Configuring the Terminal"	Describes how to configure the terminal that is used to communicate with the Cisco Nexus 1000V.
Chapter 8, "Configuration Limits"	Lists the Cisco Nexus 1000V configuration limits.
Chapter 9, "List of Terms"	Lists and defines terminology used in the Cisco Nexus 1000V implementation.

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.

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

[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions for notes and cautions:

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

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

Related Documentation

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

General Information

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

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

Install and Upgrade

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

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

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

Configuration Guides

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

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

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

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

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

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

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

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

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

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

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

Programming Guide

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

Reference Guides

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

Cisco Nexus 1000V MIB Quick Reference

Troubleshooting and Alerts

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

Cisco Nexus 1000V Password Recovery Guide

Cisco NX-OS System Messages Reference

Obtaining Documentation and Submitting a Service Request

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

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

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

CHAPTER 1

Overview

This chapter provides an overview of the product, Cisco Nexus 1000V, and includes the following sections:

- Information about Virtualization, page 1-1
- Information About Cisco Nexus 1000V, page 1-2

Information about Virtualization

Virtualization allows the creation of multiple virtual machines to run in isolation, side-by-side on the same physical machine.

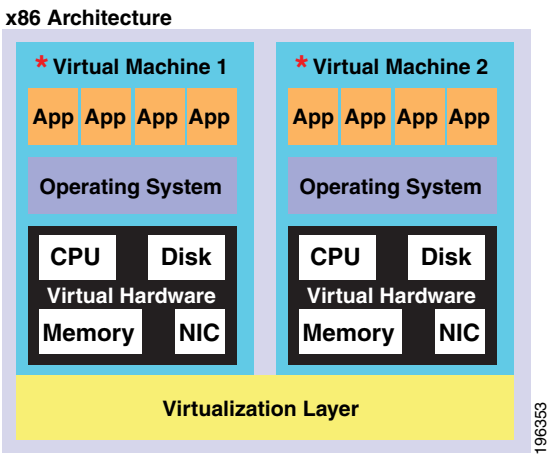
Each virtual machine has its own set of virtual hardware (RAM, CPU, NIC) upon which an operating system and applications are loaded. The operating system sees a consistent, normalized set of hardware regardless of the actual physical hardware components.

Virtual machines are encapsulated into files, for rapid saving, copying and provisioning. Full systems (fully configured applications, operating systems, BIOS and virtual hardware) can be moved, within seconds, from one physical server to another for zero-downtime maintenance and continuous workload consolidation.

Figure 1-1 Two virtual machines running in isolation side-by-side on the same physical machine

* Virtual Machine

- Virtual software (both application and OS) that once ran on a dedicated physical server.
- Virtual hardware replaces physical cards, disks, and NICs.
- OS see virtual hardware as a consistant, normalized set of hardware.
- Both hardware and software are encapsulated in a single file for rapid copying, provisioning, and moving between physical servers.



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

Information About Cisco Nexus 1000V

This section includes the following topics:

- System Description, page 1-2
- Administrator Roles, page 1-5
- Contrasting the Cisco Nexus 1000V with a Physical Switch, page 1-5
- Implementation Considerations, page 1-6
- Configuring Cisco Nexus 1000V with CLI, page 1-6

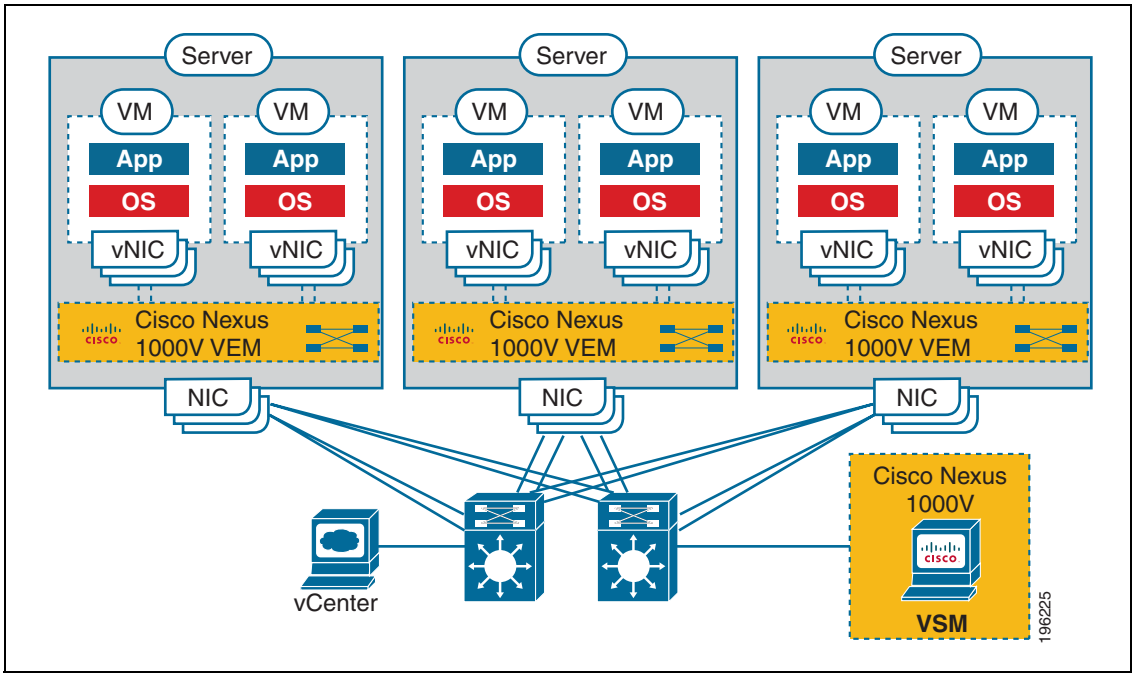
System Description

The Cisco Nexus 1000V is a virtual access software switch that works with VMware vSphere 4.0 and has the following components:

- The Virtual Supervisor Module (VSM)— the control plane of the switch and a virtual machine that runs NX-OS.
- The Virtual Ethernet Module (VEM) —a virtual line card embedded in each VMware vSphere (ESX) host. The VEM is partly inside the kernel of the hypervisor and partly in a user world process, called the VEM Agent.

Figure 1-2 shows the relationship between the Cisco Nexus 1000V components.

Figure 1-2 Cisco Nexus 1000V Distributed Virtual Switch



The VSM uses an external network fabric to communicate with the VEMs. The physical NICs on the VEM server are uplinks to the external fabric. VEMs switch traffic between the local virtual Ethernet ports connected to VM vNICs, but do not switch traffic to other VEMs. Instead, a source VEM switches

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

packets to uplinks that the external fabric then delivers to the target VEM. The VSM runs the control plane protocols and configures the state of each VEM, but it never takes part in the actual forwarding of packets.

A single VSM can control up to 64 VEMs.Cisco recommends that you install two VSMs in an active-standby configuration for high availability. With the 64 VEMs and the redundant supervisors, the Cisco Nexus 1000V can be viewed as a 66-slot modular switch.

The VSM(s) and the VEMs must be in the same Layer 2 network. The VMware vCenter server can be separated from the VSM(s) and the VEM by a Layer 3 router.

A single Cisco Nexus 1000V instance, including dual redundant VSMs and managed VEMs, forms a switch domain. Each Cisco Nexus 1000V domain within a VMware vCenter Server needs to be distinguished by a unique integer called the Domain Identifier.

Management, Control, and Packet VLANs

The Management VLAN is used for sytem login, configuration. this vlan corresponds to mgmt0 interface. The management interface is the interface that appears as the mgmt0 port on a Cisco switch, and is assigned an IP address. Although the management interface is not used to exchange data between the VSM and VEM, it is used to establish and maintain the connection between the VSM and VMware vCenter Server.

The management interface is always the second interface on the VSM and is usually labeled **Network Adapter 2** in the virtual machine network properties.

The Control VLAN and the Packet VLAN are used for communication between the VSM and the VEMs within a switch domain:

- The Packet VLAN is used by protocols such as CDP, LACP, and IGMP.
- The Control VLAN is used for the following:
  - VSM configuration commands to each VEM, and their responses
  - VEM notifications to the VSM, for example a VEM notifies the VSM of the attachment or detachment of ports to the DVS
  - VEM NetFlow exports are sent to the VSM, where they are then forwarded to a NetFlow Collector.

Cisco recommends that you use the same VLAN for control, packet, and management, but that you do not place data traffic on this VLAN. For flexibility, you can configure separate VLANs.

Port Profiles

A port profile is a set of interface configuration commands that can be dynamically applied to either the physical (uplink) or virtual interfaces. A port profile can define a set of attributes including the following:

- VLAN
- port channels
- private VLAN (PVLAN),
- ACL
- port security
- NetFlow

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

- rate limiting
- QoS marking

The network administrator defines port profiles in the VSM. When the VSM connects to vCenter Server, it creates a distributed virtual switch (DVS) and each port profile is published as a port group on the DVS. The server administrator can then apply those port groups to specific uplinks, VM vNICs, or management ports, such as virtual switch interfaces or VM kernel NICs.

A change to a VSM port profile is propagated to all ports associated with the port profile. The network administrator uses the Cisco NX-OS CLI to change a specific interface configuration from the port profile configuration applied to it. For example, a specific uplink can be shut down or a specific virtual port can have ERSPAN applied to it, without affecting other interfaces using the same port profile.

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

System Port Profiles and System VLANs

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

When a server administrator first adds a host to the DVS, its VEM must be able to contact the VSM. Since the ports and VLANs used for this communication are not yet in place, the VSM sends a minimal configuration, including system port profiles and system VLANs, to the vCenter Server, which then propagates it to the VEM.

When configuring a system port profile, you assign VLANs and designate them as system VLANs. In doing so, the port profile becomes a system port profile and included in the Cisco Nexus 1000V opaque data. Interfaces using the system port profile, and that are members of one of the defined system VLANs, are automatically enabled and forwarding traffic when the VMware ESX starts, even if the VEM does not have communication with the VSM. By doing so, the critical host functions are enabled even if the VMware ESX host starts and cannot communicate with the VSM.

Caution VMkernel connectivity can be lost if the relevant VLANs are not configured as system VLANs.

A system VLAN must be defined in both the Ethernet and vEth port profiles to automatically enable a specific virtual interface to forward traffic on a physical interface. If the system VLAN is configured only on the Ethernet port profile, the VMware VMkernel interface that inherits this port profile is not enabled by default and does not forward traffic.

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 port profiles (that is, the Ethernet and vEthernet ports) 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.

Note System VLANs must be used sparingly and only as described here.

After a system port profile has been applied to one or more ports, you can add more system VLANs, but you can only delete a system VLAN after removing the port profile from service. This is to prevent accidentally deleting a critical VLAN, such as a host management VLAN, or a VSM storage VLAN.

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

Note One VLAN can be a system VLAN on one port but a regular VLAN on another in the same ESX host.

To delete a system VLAN, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)*.

Administrator Roles

The Nexus 1000V enables collaboration between the network and server administrators in managing the switch. The network administrator is responsible for the VSM, including its creation, configuration and maintenance. The server administrator manages the hosts and the VMs, including the connection of specific VM ports and host uplinks to specific port groups, which are published in the vCenter Server by the network administrator. The VEMs are part of the network administrator's domain, but the server administrator has a say in the installation, upgrade, or deletion of a VEM.

The following table describes the administrator roles.

Table 1-1 Administrator Roles

Network Administrator	Server Administrator
• Creates, configures, and manages vswitches. • Creates, configures, and manages port profiles, including the following: – security – port channels – QOS policies	• Assigns the following to port groups: – VNICs – vmkernel interfaces – service console interfaces • Assigns physical NICs (also called PNICs) to vswitches on each host.

Contrasting the Cisco Nexus 1000V with a Physical Switch

The following are the differences between the Cisco Nexus 1000V and a physical switch:

- **Joint management by network and server administrators**
- **External fabric**
  The supervisor(s) and line cards in a physical switch have a shared internal fabric over which they communicate. The Cisco Nexus 1000V uses the external fabric.
- **No switch backplane**
  Line cards in a physical switch can forward traffic to each other on the switch's backplane. Since the Nexus 1000V lacks such a backplane, a VEM cannot directly forward packets to another VEM. Instead, it has to forward the packet via some uplink to the external fabric, which then switches it to the destination.
- **No Spanning Tree Protocol**
  The Nexus 1000V does not run STP because it will deactivate all but one uplink to an upstream switch, preventing full utilization of uplink bandwidth. Instead, each VEM is designed to prevent loops in the network topology.
- **Port channels only for uplinks**
  The uplinks in a host can be bundled in a port channel for load balancing and high availability. The virtual ports cannot be bundled into a port channel, since there is no reason to.

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

Implementation Considerations

The following are things to consider when implementing Cisco Nexus 1000V:

- VMotion of a VSM is supported for both the active and standby VSM VMs. For high availability, it is recommended that the active VSM and standby VSM reside on separate hosts. To achieve this, and prevent a host failure resulting in the loss of both the active and standby VSM, it is recommended that distributed resource scheduling (DRS) be disabled for both the active and standby VSMs.

  If you do not disable DRS, then you must use the VMware anti-affinity rules to ensure that the two virtual machines are never on the same host, and that a host failure cannot result in the loss of both the active and standby VSM.
- VMware Fault Tolerance is not supported for the VSM VM. It is supported for other VMs connected to Cisco Nexus 1000V.
- The snapshot of the VSM VM will not contain the configuration changes made since the snapshot was taken. So, restoring the VSM VM from a snapshot may require some care.
- The server administrator should not assign more than one uplink on the same VLAN without port channels. Assigning more than one uplink on the same host is not supported for the following:
  - A profile without port channels.
  - Port profiles that share one or more VLANs.

Software Compatibility

Cisco Nexus 1000V VSM can be implemented as a virtual machine in the following VMware environments:

- VMware ESX/i 3.5U2 or higher
- ESX/i 4.0. (requires Enterprise Plus edition of vSphere 4)

For detailes information, see the *Cisco Nexus 1000V Compatibility Information, Release 4.0(4)SV1(2)* document.

Configuring Cisco Nexus 1000V with CLI

Cisco Nexus 1000V is configured using a command line interface (CLI) from any of the following:

- an SSH session (SSH provides a secure connection.)
- a Telnet Session
- a service console for the VM running the VSM

For information about the CLI, see the "Understanding the CLI" section on page 6-1.

CHAPTER 2

Setting Up the Software

This chapter describes how, after installing the Cisco Nexus 1000V software, to setup a configuration by using either the GUI application or the CLI.

Note To install the Cisco Nexus 1000V software on your ESX or ESXi 4.0 VMware server, see the *Cisco Nexus 1000V Software Installation Guide, Release 4.0(4)SV1(2)*.

This chapter includes the following topics:

- Prerequisites, page 2-1
- Software Configuration Process, page 2-5
- Verifying the Configuration, page 2-8
- Starting the VMs, page 2-9
- Implementation Guidelines, page 2-10

Prerequisites

Before beginning the setup of the Cisco Nexus 1000V software, you must know or do the following:

- You have already installed the Cisco Nexus 1000V software and configured the following using the *Cisco Nexus 1000V Software Installation Guide, Release 4.0(4)SV1(2)*.
  - A name for the new VSM that is unique within the inventory folder and up to 80 characters in length.
  - The name of the host where the VSM is installed in the inventory folder.
  - The name of the datastore in which the VM files are stored.
  - The names of the network port groups used for the VM.
  - The Cisco Nexus 1000V VSM IP address.
- You are familiar with the "Understanding the CLI" section on page 6-1.
- You are familiar with the "List of Terms" section on page 9-1.
- You are familiar with Figure 2-1Cisco Nexus 1000V Configuration Example, page 2-4 illustrating a sample Cisco Nexus 1000V setup.

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

- If you are installing redundant VSMs, make sure you have first completed the following before installing the software on the secondary VSM:
  - Install the software on the primary VSM.
  - Set up the primary VSM using this document.
- It is highly recommended that you install redundant VSMs. For more information about configuring redundant VSMs, see the *Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.0(4)SV1(2)*.
- To improve redundancy, install primary and secondary VSM virtual machines in separate hosts connected to different upstream switches. For other recommendations, see the "Implementation Guidelines" section on page 2-10.
- You have already identified the HA role for this VSM from those listed in Table 2-1:

Table 2-1 VSM HA Roles

Role	Single Supervisor System	Dual Supervisor System
Standalone	X	
Primary		X[1]
Secondary		X[2]

1. If this is the first VSM of a dual supervisor pair, install it as primary.
2. If this is the second VSM of a dual supervisor pair, install it as secondary.

For more information about HA roles, see the *Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.0(4)SV1(2)*.

- When you set up the Cisco Nexus 1000V software, you are required to create an administrator password. Table 2-2 lists password strength guidelines:

Table 2-2 Guidelines for strong passwords

Strong passwords have:	Strong passwords do NOT have:
• At least eight characters • Uppercase letters • Lowercase letters • Numbers • Special characters **Note** Clear text passwords cannot include the dollar sign ($) special character.	• Consecutive characters, such as "abcd" • Repeating characters, such as "aaabbb" • Dictionary words • Proper names

- All ESX hosts within a Cisco Nexus 1000V VSM domain must have Layer 2 connectivity to each other.

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

- If you are using a set of switches, make sure that the inter-switch trunk links carry all relevant VLANs, including control and packet VLANs. The uplink should be a trunk port carrying all VLANs configured on the ESX host.
- The control traffic on the Cisco Nexus 1000V can be affected if you have configured storm control or storm suppression on an upstream switch. Since traffic storm control can drop the broadcast packets that the Cisco Nexus 1000V relies on for communication, be aware of the storm control settings on your upstream switch.
- On the host running the VSM VM, the control and packet VLANs are configured through the VMware switch and the VMNIC.
- The VSM VM must be run on the same IP subnet as the ESX 4.0 hosts that it manages.
- If you are planning to run the VSM and the VEM on the same ESX host, refer to the "Running a VSM and VEM on the Same Host" section on page 5-1.
- On the ESX host for the VSM VM, make sure that you have created the following three VMware vSwitch port groups:
  - Control VLAN
  - Packet VLAN
  - Management VLAN

  Make sure to associate them with the corresponding VLANs within the physical LAN.

Caution The VSM VM configuration will fail unless the NICs are specified as shown in Table 2-3 on page 2-3.

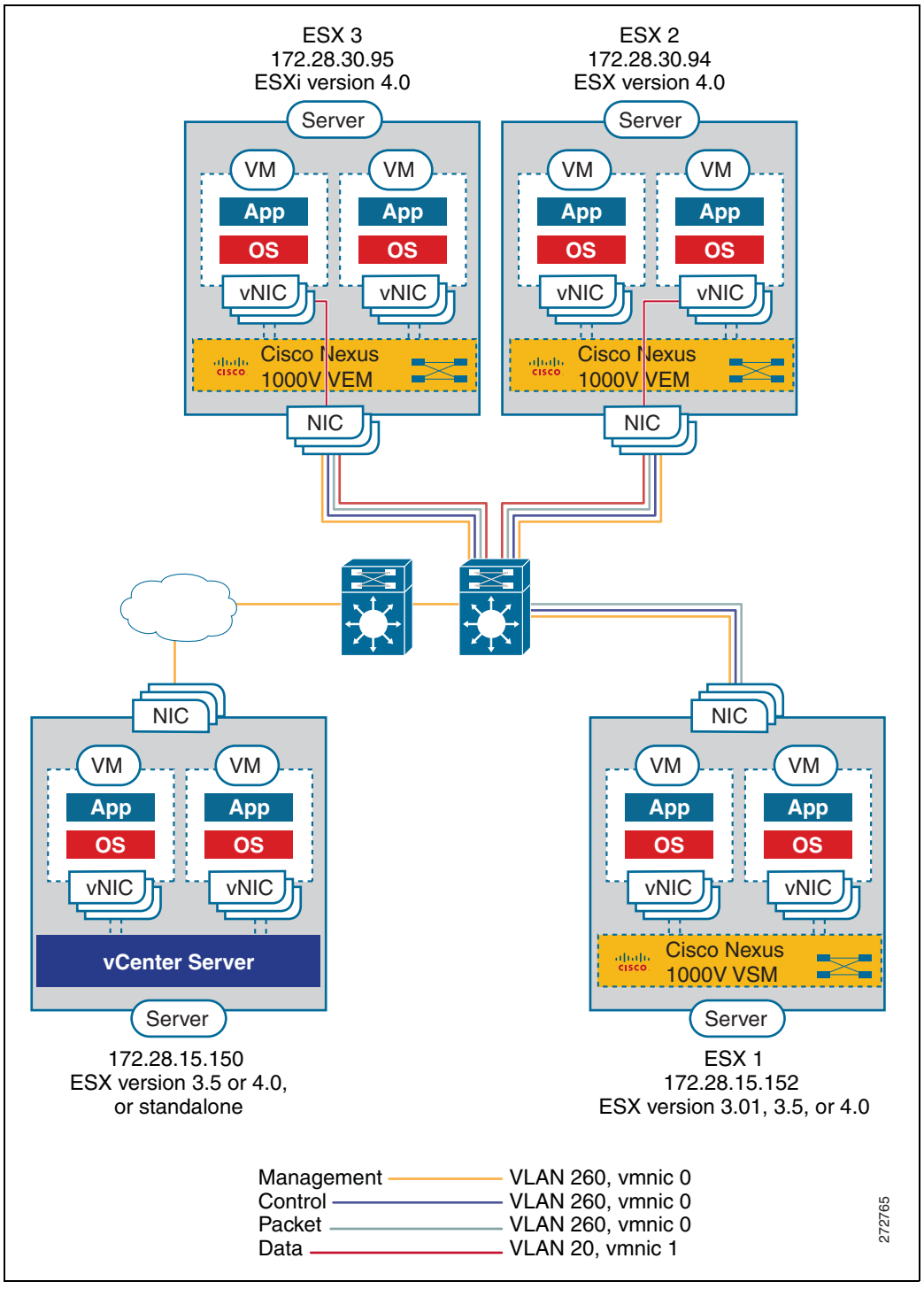
Table 2-3 Required NIC Configuration

NICs	VLAN	Description	VLAN numbering used in example[1]
First	Control	e1000	260
Second	Management	e1000 The Management VLAN corresponds to the mgmt0 interface on the switch.	260
Third (last)	Packet	e1000	260

1. See Figure 2-1Cisco Nexus 1000V Configuration Example, page 2-4.

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

Figure 2-1 Cisco Nexus 1000V Configuration Example



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

Software Configuration Process

The following section will guide you through this process. After completing each procedure, return to this section to make sure you complete all required procedures in the correct sequence.

Step 1 Do one of the following:

- If you are using the GUI application to set up your software, then see the "GUI Software Configuration Process" section on page 3-1.
- If you are using the CLI to set up your software, then see the "CLI Software Configuration Process" section on page 4-1.

Step 2 Verify the configuration. See the "Verifying the Configuration" procedure on page 2-8.

Step 3 Start the VMs. See the "Starting the VMs" procedure on page 2-9.

Step 4 Do one of the following:

- If both the VSM and VEMs are working as expected, continue with the next step.
- If not, then see the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(2)*.

Step 5 Continue your implementation. See the "Implementation Guidelines" section on page 2-10.

Step 6 You have completed the Cisco Nexus 1000V software configuration process.

Creating VLANs

You can use this procedure to create a single VLAN or a range of VLANs to be used in the following port profiles:

- The system port profile for VSM-VM communication
- The uplink port profile for VM traffic
- The data port profile for VM traffic

Port profiles are created when setting up the software using the CLI or GUI.

BEFORE YOU BEGIN

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

Note All interfaces and all ports configured as switchports are in VLAN 1 by default.

- You are logged in to the CLI in EXEC mode.
- For an illustration of how VLANs are used in the Cisco Nexus 1000V, see the "Cisco Nexus 1000V Configuration Example"on page 2-1.
- In accordance with the IEEE 802.1Q standard, up to 4094 VLANs (numbered 1-4094) are supported in Cisco Nexus 1000V, and are organized as shown in the following table.

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

VLAN Numbers	Range	Usage
1	Normal	Cisco Nexus 1000V 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. **Note** The extended system ID is always automatically enabled.
3968-4047 and 4094	Internally allocated	You cannot use, create, delete, or modify these VLANs. You can display these VLANs. Cisco Nexus 1000V allocates these 80 VLANs, plus VLAN 4094, for features, like diagnostics, that use internal VLANs for their operation.

- Cisco recommends that you use the same VLAN for control, packet, and management, but that you do not place data traffic on this VLAN. For flexibility, you can use separate VLANs.
- VLAN ranges used for control and packet port groups must be allowed on the upstream switch.
- Newly-created VLANs remain unused until Layer 2 ports are assigned to them.
- For information about the following, see the *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(2)*.
  - Assigning Layer 2 interfaces to VLANs (access or trunk ports).
  - Configuring ports as VLAN access or trunk ports and assigning ports to VLANs.
- For more information about configuring VLANs, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(2)*.

SUMMARY STEPS

1. **config t**
2. **vlan** {*vlan-id* | *vlan-range*}
3. **show vlan id** <*vlan-id*>
4. **copy running-config startup-config**

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

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	**vlan** {*vlan-id* | *vlan-range*}	Creates, and saves in the running configuration, a VLAN or a range or VLANs. **Note** If you enter a VLAN ID that is already assigned, you are placed into the VLAN configuration mode for that VLAN. **Note** If you enter a VLAN ID that is assigned to an internally allocated VLAN, the system returns an error message. **Note** From the VLAN configuration mode, you can also create and delete VLANs. To configure the VLAN further, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(2)*.
	Example: n1000v(config)# vlan 5 n1000v(config-vlan)#	This example shows VLAN 5 being created. The VLAN is activated and you are automatically placed into a submode for configuring VLAN 5.
	Example: n1000v# **config t** n1000v(config)# **vlan 15-20** n1000v(config-vlan)#	This example shows the range, VLAN 15-20, being created. The VLANs in the range are activated, and you are automatically placed into a submode for configuring VLAN 15-20. **Note** If you create a range of VLANs that includes an unusable VLAN, all VLANs in the range are created except those that are unusable; and Cisco Nexus 1000V returns a message listing the failed VLANs.
Step 3	**show vlan id 5** **Example:** n1000v(config)# show vlan id 5	(Optional) Displays the VLAN configuration for verification purposes.
Step 4	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.
	You have completed this procedure. Return to the configuration process that pointed you here: • GUI Software Configuration Process, page 3-1. • CLI Software Configuration Process, page 4-1	

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

Verifying the Configuration

You can use this procedure to verify that the software is installed and working as expected.

BEFORE YOU BEGIN

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

- Once the host is added to DVS, the Server-Name is displayed in the **show module** command output. This should happen within 5 minutes of the module coming up on VSM. The server name is the equivalent of the host object name seen in vCenter Server and is fetched from the vCenter Server-VSM connection.

DETAILED STEPS

Step 1 On the VSM, verify that the VEM appears as expected.

- **show module**
- **show module vem mapping**

Example:

```
n1000v# show module
Mod  Ports  Module-Type                      Model              Status
---  -----  -------------------------------- ------------------ ------------
1    0      Virtual Supervisor Module        Nexus1000V         active *
3    248    Virtual Ethernet Module          NA                 ok

Mod  Sw               Hw
---  ---------------  ------
1    4.0(4)SV1(1)     0.0
3    4.0(4)SV1(1)     0.4

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
3    02-00-0c-00-03-00 to 02-00-0c-00-03-80  NA

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
1    172.28.15.152    NA                                    NA
3    172.28.30.94      89130a67-e66b-3e57-ad25-547750bcfc7e  srvr-94


* this terminal session
n1000v#
```

Example:

```
n1000v(config-port-prof)# show module vem mapping

Mod     Status          UUID
---     -----------     ----
  3      powered-up     8f2aa4d8-1f1a-34d8-90ee-9ca7ace00ad3
```

Step 2 Do one of the following:

- If the VSM and VEM are active and configured correctly, continue with the next step.
- If not, see the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(2)*.

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

Step 3 On the VSM, use the following commands to verify that the interfaces are up and are assigned to the correct port-groups.

- **show port-profile usage**
- **show interface brief**

Example:

```
n1000v# show port-profile usage

------------------------------------------------------------------------------
Port Profile               Port        Adapter        Owner
------------------------------------------------------------------------------
system-uplink              Eth3/2      vmnic1         172.28.30.94
vm-uplink                  Eth3/3      vmnic2         172.28.30.94
n1000v#
```

Example:

```
n1000v# show int brief

------------------------------------------------------------------------------
Port     VRF          Status IP Address                       Speed    MTU
------------------------------------------------------------------------------
mgmt0     --           up     172.23.232.141                   1000     1500

------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                   Ch #
------------------------------------------------------------------------------
Eth3/2        1      eth  trunk  up      none                       1000(D) --
Eth3/3        1      eth  access up      none                       1000(D) --
n1000v#
```

Step 4 You have completed this procedure.
Return to the Software Configuration Process, page 2-5.

Starting the VMs

You can use this procedure to start the VMs and verify their connectivity to the network.

BEFORE YOU BEGIN

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

- You have an IP address in the same subnet as the VMs to use for verifying VM connectivity.
- You have the VMware documentation for creating the VMs available.
- For a detailed description of the system, see the *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(2)*.

DETAILED STEPS

Step 1 Create the VMs.

Step 2 Edit VM settings on the vSphere Client so that their network adapters are in port profile data262, as defined when you configured the data port profile for VM traffic.

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

Step 3 Power on the VMs and verify the traffic as you would normally.

Step 4 You have completed this procedure.
Return to Software Configuration Process, page 2-5.

Implementation Guidelines

After completing the installation procedures in this document, use the following guidelines as you configure the Cisco Nexus 1000V.

- If two or more PNICs are required to carry the same VLANs then you must configure them in a port channel. For information about port channels, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(2)*.
- If PNICs on the same server are connected to different upstream switches, then you must configure the asymmetric port channel in host mode (vPC-HM). For more information, see the following documents:
  - *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)*
  - *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(2)*
- Cisco recommends that you run the VSM in HA mode. For more information about configuring HA, see the *Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.0(4)SV1(2)*.
- Cisco recommends that you migrate the following from the VMware vSwitch to the Cisco Nexus 1000V:
  - uplinks
  - virtual switch interfaces
  - vmkernel NICs (including the management ports)
  - VSM VM

CHAPTER 3

Configuring the Software Using the GUI

This chapter describes how use the GUI application to configure your new Cisco Nexus 1000V software.

GUI Software Configuration Process

The following section will guide you through this process. After completing each procedure, return to this section to make sure you complete all required procedures in the correct sequence.

Step 1 Set up the VSM virtual machine using the "Setting Up the VSM Virtual Machine Using the GUI" procedure on page 3-2.

Step 2 Add the Cisco Nexus 1000V licenses.

Note The software provides licenses for 16 CPU sockets for a period of 60 days. These licenses are used only if there are no permanent licenses installed on the VSM. The evaluation period of 60 days starts when you install the software.

If you have purchased licenses, see the *Cisco Nexus 1000V License Configuration Guide, Release 4.0(4)SV1(2)*.

Step 3 Do one of the following:

- If you are adding dual VSMs, continue with the next step.
- If this VSM is a standalone VSM, its HA role has been automatically configured. Go to Step 5.

Step 4 Configure the HA role for this VSM using the "Configuring the VSM HA Role" procedure on page 3-9.

Step 5 You have completed this process. Return to the "Software Configuration Process" section on page 2-5 to continue setting up your VSM software.

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

Setting Up the VSM Virtual Machine Using the GUI

You can use this procedure to configure the VSM as follows:

- Create the following port profiles:
  - System port profile
  - Data port profile
  - Uplink port profile
- Create the following VLANs:
  - Control VLAN
  - Packet VLAN
  - Management VLAN
- Enable SSH and configure an SSH connection.
- Create a Cisco Nexus 1000V plug-in and register it on the vCenter server.
- Power off and then restart the VSM.

BEFORE YOU BEGIN

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

- You have the following Cisco Nexus 1000V domain information:
  - Control VLAN ID
  - Packet VLAN ID
  - Domain ID
- The Cisco Nexus 1000V GUI supports the configuration of the control, management, and packet port groups for a single common vswitch—not for multiple vswitches.

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

DETAILED STEPS

Step 1 In your browser address field, enter the VSM IP address.

The Cisco Nexus 1000V home page opens.

Step 2 Click **Launch Application**.

A security screen opens asking if you want to run this application.

Step 3 Click **Run**.

The Enter VSM Credentials screen opens.

Step 4 Enter a password for the Adminisrator and then click **Next**.

The Enter vCenter Credentials screen opens.

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

Step 5 Enter the following vCenter credentials.

- vCenter IP address
- Secure HTTP port

  Port 443 is configured by default, but you can change this if needed.
- vCenter User ID (for a vCenter user with administrator-level privileges)
- vCenter Password (for a vCenter user with administrator-level privileges)

Step 6 Click **Next**.

The VSM Host screen opens.

Step 7 Choose the host for the VSM and click **Next**.

The VSM VM and Port Groups screen opens.

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

Step 8 Choose your VSM from the selection list.

Step 9 Do one of the following:

- Click **Default** to use the default configuration and continue with the next step.

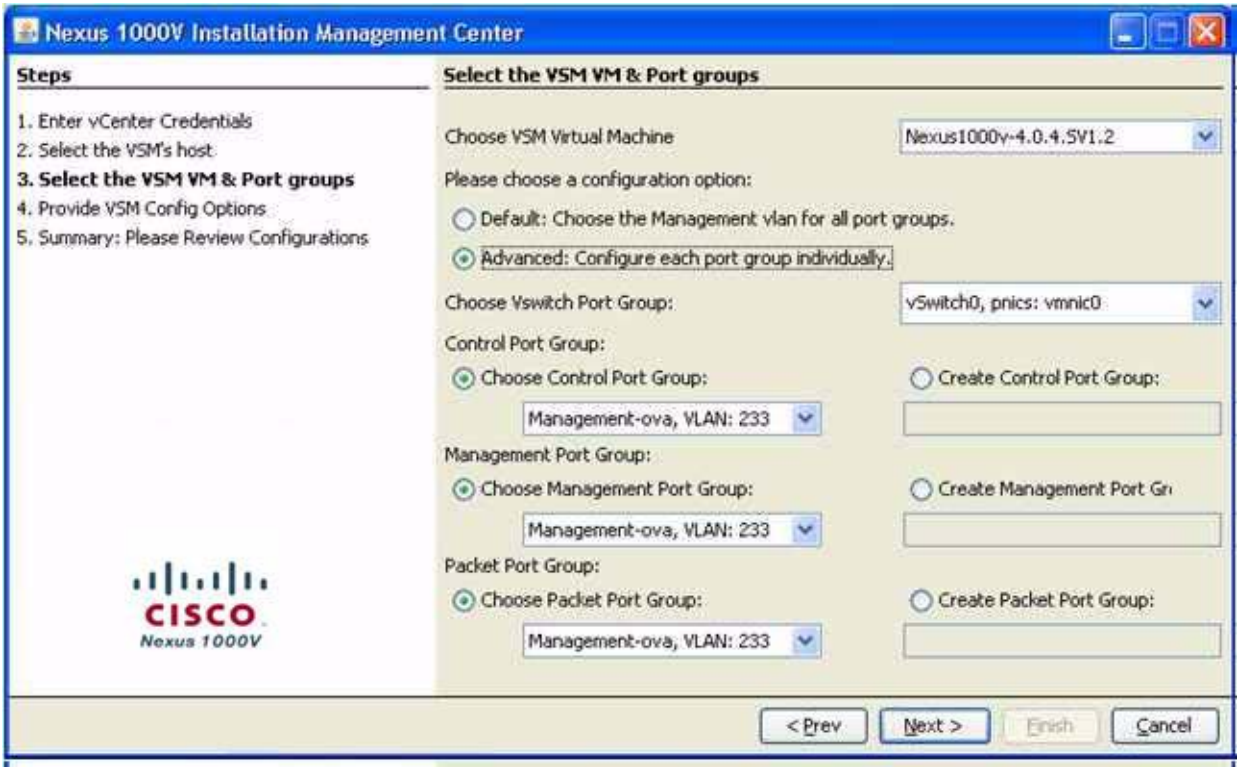
  The default option configures the management VLAN for all port profiles (system, data, and uplink).
- Click **Advanced** to configure each port profile and go to Step 11.

Step 10 Enter the management VLAN ID to be used for control and packet traffic, click **Next**, and then go to Step 12.

Step 11 Choose your port groups from the selection lists, enter VLAN IDs when prompted, and then click **Next**.

- Control VLAN
- Management VLAN
- Packet VLAN

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

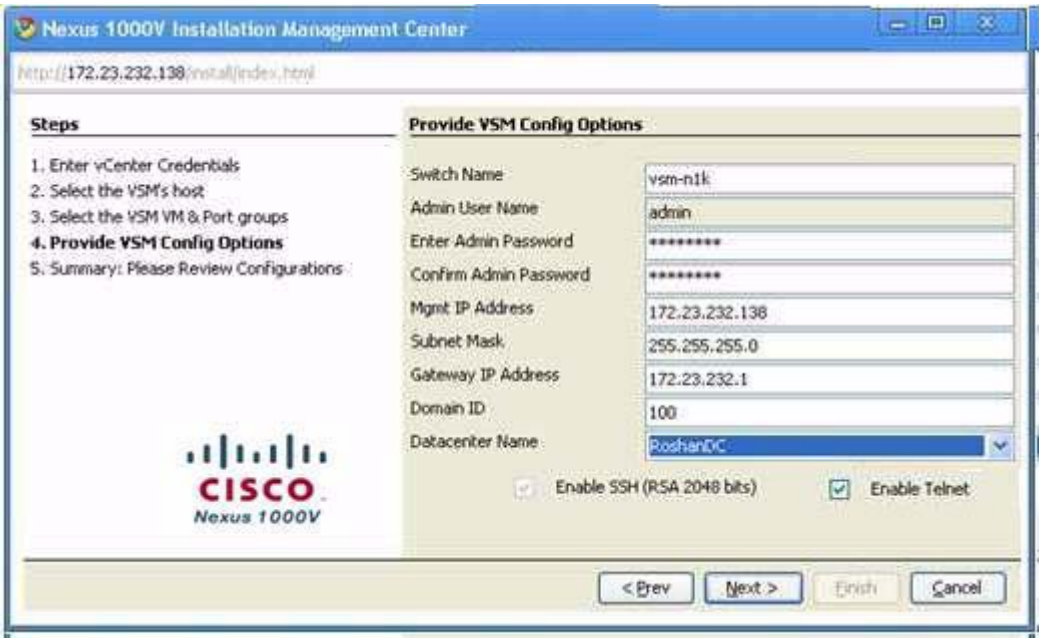


Step 12 In the VSM Config Options screen, configure the following for your VSM and click **Next**.

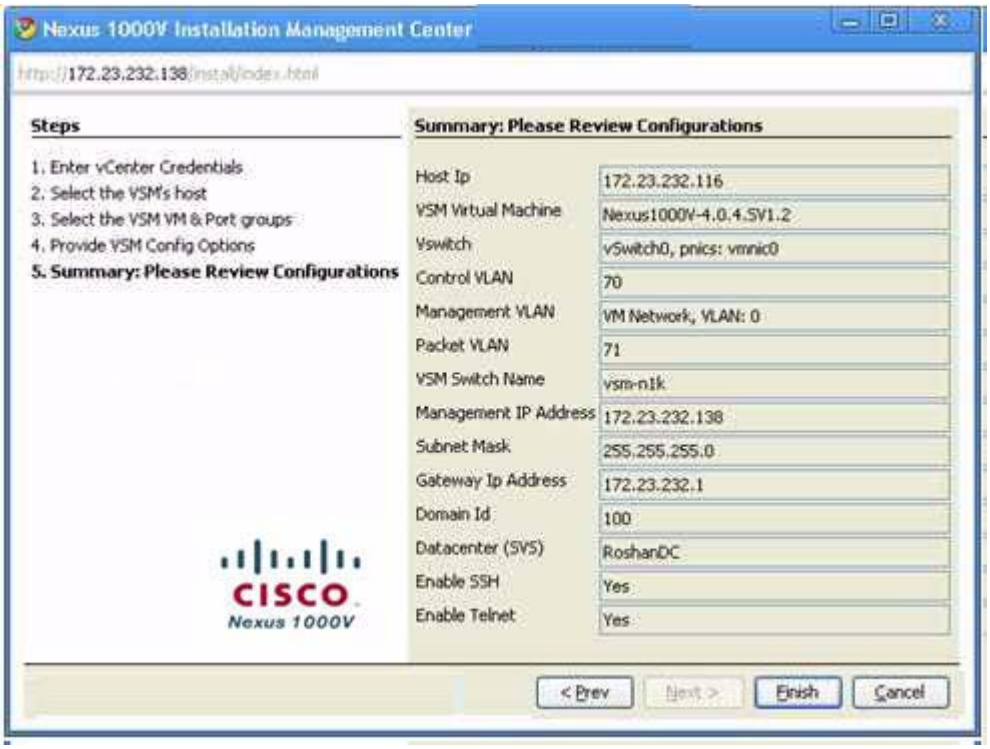
- Administrator user name and password
- Management IP address, subnet mask, and gateway IP address

  The VSM VM must be run on the same IP subnet as the ESX 4.0 hosts that it manages.
- Domain ID
- Datacenter name
- Whether to enable telnet

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



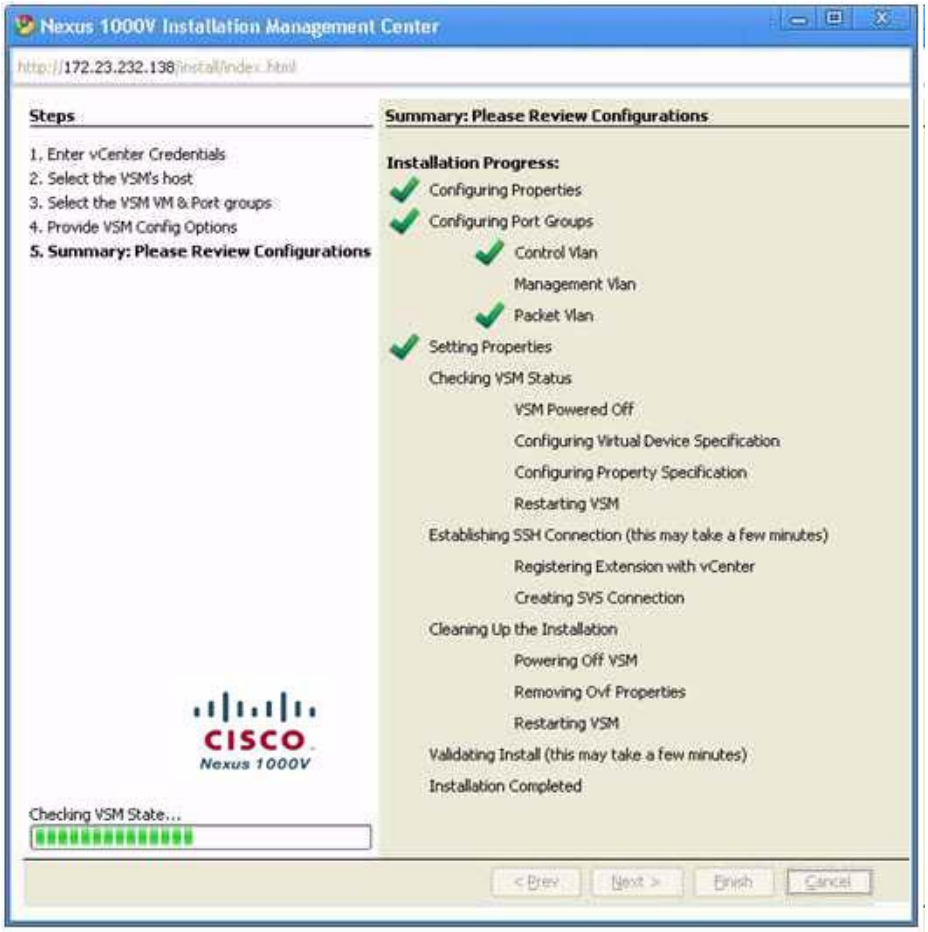
Step 13 In the VSM Summary Screen, review the configuration for accuracy. To make corrections, click **Prev** and go back to the previous screens. When the configuration is accurate, click **Finish**.



The configuration is applied to the VSM.

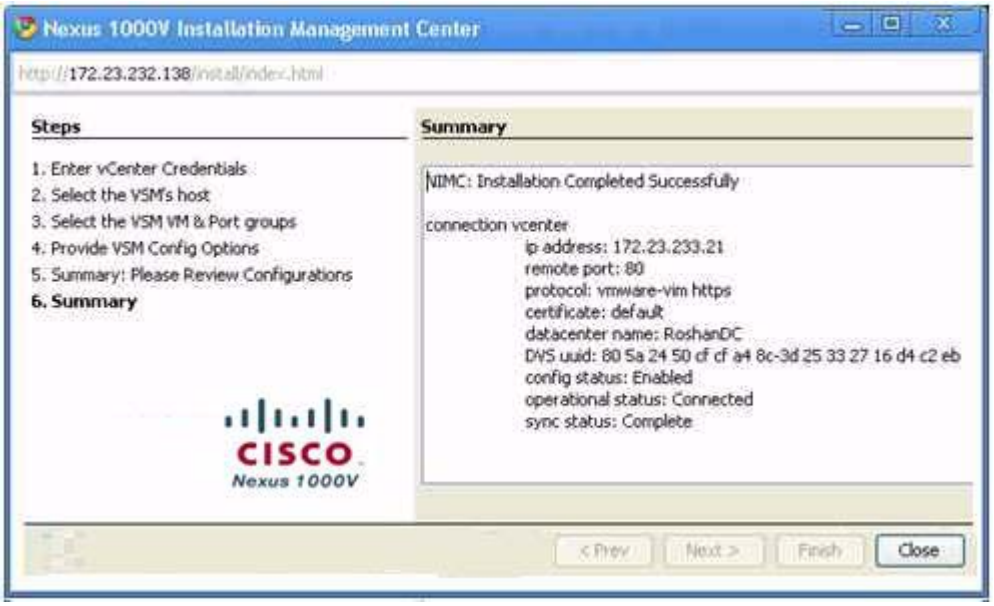
Send document comments to nexus1k-docfeedback@cisco.com.

Step 14 A second summary screen opens displaying the progress as each configuration completes on the VSM.



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

A third summary screen opens displayingthe completed VSM configuration.



Step 15 Click **Close**.

Step 16 You have completed this procedure.
Return to the GUI Software Configuration Process, page 3-1.

Configuring the VSM HA Role

You can use this procedure to change the role of a VSM to one of the following after it is already in service:

- standalone
- primary
- secondary

BEFORE YOU BEGIN

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

- If you are changing a standalone VSM to a primary or secondary VSM, be sure to first isolate it from the other VSM in the pair as follows:
  - Disconnect the VSM VM management and control ports from the switch.
  - Stop the control and management VLAN in the upstream switch.

  This prevents any interaction between the two VSMs during the change. Then power the VM off from the vSphere Client before reconnecting it as standby.
- You are logged in to the CLI in EXEC mode.
- The HA redundancy states are active and standby.

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

- A change from a standalone to a primaryVSM takes effect immediately.

SUMMARY STEPS

1. **show system redundancy status**
2. **system redundancy role** {**standalone** | **primary** | **secondary**}
3. **show system redundancy status**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**show system redundancy status**
	Example:
	`switch# show system redundancy status`
	`Redundancy role`
	`---------------`
	`administrative: standalone`
	`operational: standalone`
	
	`Redundancy mode`
	`---------------`
	`administrative: HA`
	`operational: None`
	
	`This supervisor (sup-1)`
	`------------------------`
	`Redundancy state: Active`
	`Supervisor state: Active`
	`Internal state: Active with no standby`
	
	`Other supervisor (sup-2)`
	`------------------------`
	`Redundancy state: Not present`
	`switch#`
		Displays the current redundancy status for the VSM(s).

Step 2	**system redundancy role [standalone | primary | secondary]**
	Example:
	`n1000v# system redundancy role primary`
	`n1000v#`
		Designates the HA role of the VSM.

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

	Command	Purpose

Step 3	**show system redundancy status**
	Example:
	`show system redundancy status`
	`Redundancy role`
	`---------------`
	`administrative: primary`
	`operational: primary`
	
	`Redundancy mode`
	`---------------`
	`administrative: HA`
	`operational: None`
	
	`This supervisor (sup-1)`
	`-----------------------`
	`Redundancy state: Active`
	`Supervisor state: Active`
	`Internal state: Active with no standby`
	
	`Other supervisor (sup-2)`
	`-----------------------`
	`Redundancy state: Not present`
	`switch#`
		(Optional) Displays the current redundancy status for the VSM(s).

Step 4	**copy running-config startup-config** **Example:** `n1000v(config)# copy running-config startup-config`	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

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

CHAPTER 4

Configuring the Software Using the CLI

This chapter describes how to use the CLI to configure your Cisco Nexus 1000V software after it is installed on your ESX or ESXi 4.0 VMware server.

Note To install the Cisco Nexus 1000V software on your ESX or ESXi 4.0 VMware server, see the *Cisco Nexus 1000V Software Installation Guide, Release 4.0(4)SV1(2)*.

CLI Software Configuration Process

The following section will guide you through this process. After completing each procedure, return to this section to make sure you complete all required procedures in the correct sequence.

Step 1 Set up the VSM virtual machine using the "Setting Up the VSM Virtual Machine Using the CLI" procedure on page 4-2.

Step 2 Do one of the following:

- If you are configuring Layer 3 control, see the Domain Configuration section in the *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(2)*, and then continue with the next step.
- If you are not configuring Layer 3 control, continue with the next step.

Step 3 Verify VSM connectivity using the "Verifying VSM Connectivity" procedure on page 4-7.

Step 4 Add the Cisco Nexus 1000V license.

Note The software provides licenses for 16 CPU sockets for a period of 60 days. These licenses are used only if there are no permanent licenses installed on the VSM. The evaluation period of 60 days starts when you install the software.

If you have purchased licenses, see the *Cisco Nexus 1000V License Configuration Guide, Release 4.0(4)SV1(2)*.

Step 5 Create a Cisco Nexus 1000V plug-in using the "Creating a Cisco Nexus 1000V Plug-In on the vCenter Server" procedure on page 4-8.

Step 6 Connect to vCenter Server using the "Connecting to the vCenter Server" procedure on page 4-9.

Step 7 Create the required VLANs using the "Creating VLANs" procedure on page 2-5.

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

Step 8 Use the following procedures to create the required port profiles.

- "Configuring the System Port Profile for VSM-VEM Communication" procedure on page 4-11.
- "Configuring the Uplink Port Profile for VM Traffic" procedure on page 4-15
- "Configuring the Data Port Profile for VM Traffic" procedure on page 4-18

Step 9 Add the host to the DVS using the "Adding an ESX 4.0 Host to the DVS" procedure on page 4-21.

Step 10 You have completed this process. Return to the "Software Configuration Process" section on page 2-5

Setting Up the VSM Virtual Machine Using the CLI

You can use this procedure to set up and save the VSM management access configuration with the CLI.

BEFORE YOU BEGIN

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

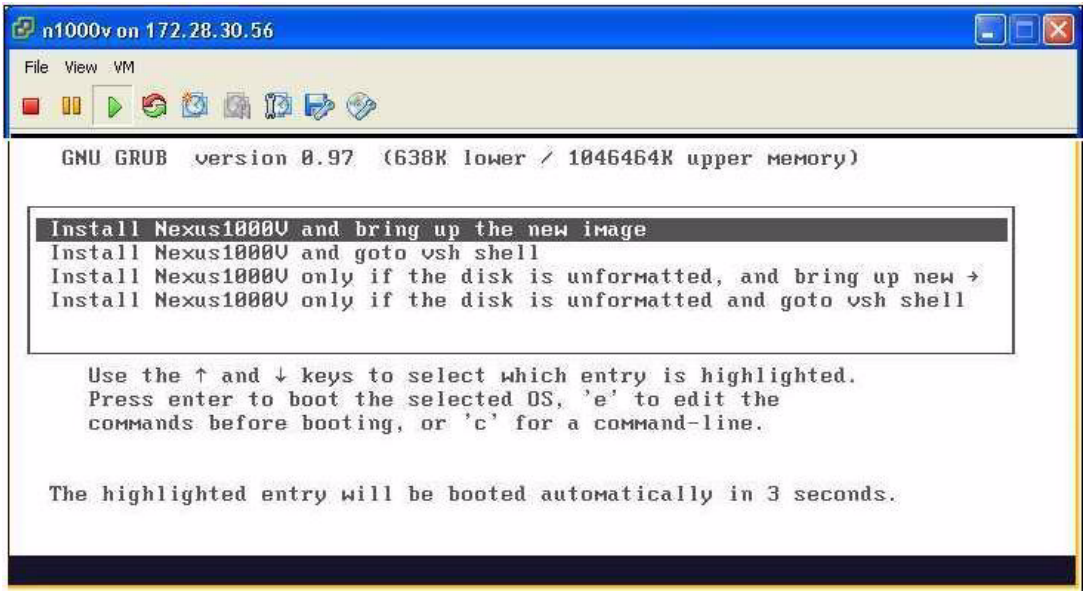
- You have the following Cisco Nexus 1000V domain information:
  - Control VLAN ID
  - Packet VLAN ID
  - Domain ID
- Cisco recommends that you use the same VLAN for control, packet, and management, but that you do not place data traffic on this VLAN. For flexibility, you can use separate VLANs.

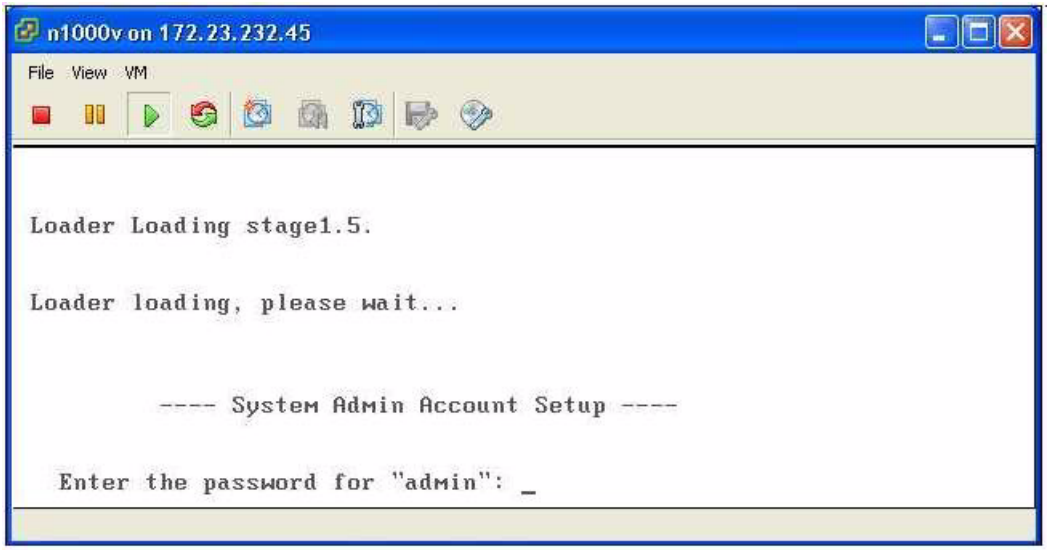
Send document comments to nexus1k-docfeedback@cisco.com.

DETAILED STEPS

Step 1 Power on the VM, choose **Install Cisco Nexus 1000V**, and bring up the new image.

One of the following screens displays.





Note It may take up to 5 minutes for the VM to power on.

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

Step 2 When asked, enter and confirm the Administrator password.

Example:

```
---- System Admin Account Setup ----
Enter the password for "admin":
Confirm the password for "admin":
```

Step 3 When asked, enter the domain ID.

Example:

```
Enter the domain id<1-4095>: 152
```

Step 4 When asked, enter the HA role.

If you do not specify a role, standalone is assigned by default.

Example: standalone or primary

```
Enter HA role[standalone/primary/secondary]: primary


[########################################] 100%

         ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no):
```

Example: Secondary

```
Enter HA role[standalone/primary/secondary]: secondary


  Setting HA role to secondary will cause a system reboot. Are you sure (yes/no) ? :
```

Step 5 Do one of the following:

- If you are setting up the primary/active VSM, go to Step 8.
- If you are setting up the secondary/standby VSM, then continue with the next step.

Step 6 If you are installing the secondary VSM from the ISO image attached to your CD-ROM, unmount the virtual CD-ROM now, so that that VSM does not boot from the CD.

This is necessary if you have set up the VSM VM to boot from the CD-ROM before the hard drive.

Step 7 If you are setting up the secondary/standby VSM, when prompted to reboot the VSM, answer **yes**.

The secondary VSM VM is rebooted and brought up in standby mode.

The password on the secondary VSM is synchronized with the password on the active/primary VSM.

Any configuration made on the active/primary VSM is now automatically synchronized with the standby.

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

Example: Secondary

```
Setting HA role to secondary will cause a system reboot. Are you sure (yes/no) ? :y

[########################################] 100%

  HA mode set to secondary. Rebooting now...
```

You have completed this procedure for the secondary VSM. Return to the "CLI Software Configuration Process" section on page 4-1 to proceed with the configuration.

Step 8 When asked if you want to enter the basic configuration dialog, answer **yes**.

Example:

```
Would you like to enter the basic configuration dialog (yes/no): yes
```

Step 9 When asked to create another Login account, answer **no**.

Example:

```
Create another login account (yes/no) [n]: no
```

Step 10 When asked to configure a read-only SNMP community string, answer **no**.

Example:

```
Configure read-only SNMP community string (yes/no) [n]: no
```

Step 11 When asked to configure a read-write SNMP community string, answer **no**.

Example:

```
Configure read-write SNMP community string (yes/no) [n]: no
```

Step 12 Enter a name for the switch.

Example:

```
Enter the switch name: n1000v
```

Step 13 When asked to configure out-of-band management, answer **yes** and then enter the mgmt0 IPv4 address and subnet mask.

Example:

```
Continue with Out-of-band (mgmt0) management configuration? [yes/no] [y]: yes
Mgmt0 IPv4 address: 172.28.15.152
Mgmt0 IPv4 netmask: 255.255.255.0
```

Step 14 When asked to configure the default gateway, answer **no**.

Example:

```
Configure the default-gateway: (yes/no) [y]: no
```

Step 15 When asked to configure advanced IP options, answer **no**.

Example:

```
Configure Advanced IP options (yes/no)? [n]: no
```

Step 16 When asked to enable the Telnet service, answer **yes**.

Example:

```
Enable the telnet service? (yes/no) [y]: yes
```

Step 17 When asked to enable the SSH service, answer **yes** and then enter the key type and number of key bits. For more information, see the document,*Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(2)*.

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

Example:
```
Enable the ssh service? (yes/no) [y]: yes
Type of ssh key you would like to generate (dsa/rsa) : rsa
Number of  key bits <768-2048> : 1024
```

Step 18 When asked to configure the NTP server, answer **no**.

Example:
```
Configure NTP server? (yes/no) [n]: no
```

Step 19 When asked to configure the VEM feature level, answer **yes** and then enter 0 or 1.

Example:
```
Configure vem feature level? (yes/no) [n]: yes
Current vem feature level is set to 4.0.(4)SV1(1)
You can change the feature level to:
  1 4.0(4)SV1(2)
Enter an index from the list above <1-1> or 0 if you don't want to change:
```

Step 20 When asked to configure Cisco Nexus 1000V domain parameters, answer **yes** and then enter them.

Example:
```
Configure n1000v domain parameters (yes/no) [y]: yes
Enter control vlan <1-3967, 4048-4093>: 260
Enter packet vlan  <1-3967, 4048-4093>: 260

The system now summarizes the complete configuration and asks if you want to edit it.
```

Example:
```
The following configuration will be applied:
 Switchname n1000v
interface Mgmt0
ip address 172.28.15.152 255.255.255.0
no shutdown
telnet server enable
 ssh key rsa 1024 force
 ssh server enable
svs-domain
 control vlan 260
 packet vlan 260
 domain id 152
```

Step 21 Do one of the following:

- If you do not want to edit the configuration answer **no** and continue with the next step.
- If you want to edit the configuration, answer **yes** and return to Step 9 to revisit each command.

Example:
```
Would you like to edit the configuration? (yes/no) [n]:no
```

Step 22 When asked to use and save this configuration, answer **yes**.

Caution If you do not save the configuration now, then none of your changes are part of the configuration the next time the switch is rebooted. Enter **yes** to save the new configuration. This ensures that the kickstart and system images are also automatically configured.

Example:
```
Use this configuration and save it? (yes/no) [y]: yes
[########################################] 100%
```

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

The new configuration is saved into nonvolatile storage, after which the running and the startup copies of the configuration are identical.

Note You can use the setup routine to update the configuration done in Step 8 through Step 22 at any time by entering the **setup** command in EXEC mode. Once setup begins, press Enter to skip a command. Use ctrl-c to skip the remaining commands.

Step 23 You have completed this procedure.
Return to the "CLI Software Configuration Process" section on page 4-1.

Verifying VSM Connectivity

You can use this procedure to verify the IP connectivity to the active VSM.

BEFORE YOU BEGIN

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

- You are logged in to the active VSM in EXEC mode.

DETAILED STEPS

Step 1 Verify IP connectivity with the active VSM.

ping *ip_address*

Example:

```
n1000v# ping 172.28.15.1
PING 172.28.15.1 (172.28.15.1): 56 data bytes
Request 0 timed out
64 bytes from 172.28.15.1: icmp_seq=1 ttl=63 time=0.799 ms
64 bytes from 172.28.15.1: icmp_seq=2 ttl=63 time=0.597 ms
64 bytes from 172.28.15.1: icmp_seq=3 ttl=63 time=0.711 ms
64 bytes from 172.28.15.1: icmp_seq=4 ttl=63 time=0.67 ms
--- 172.28.15.1 ping statistics ---
5 packets transmitted, 4 packets received, 20.00% packet loss
round-trip min/avg/max = 0.597/0.694/0.799 ms
```

Connectivity is now verified to the VSM and you can use SSH for a secure connection.

Step 2 You have completed this procedure.
Return to the CLI Software Configuration Process, page 4-1.

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

Creating a Cisco Nexus 1000V Plug-In on the vCenter Server

Use the following guidelines and your VMware documentation to install and register the Cisco Nexus 1000V plug-in (extension) on the vCenter Server.

BEFORE YOU BEGIN

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

- You have already downloaded a copy of the following file from the VSM home page (point your browser to the IP address of the active VSM):
  - cisco_nexus1000v_extension.xml
- Using an old or corrupt version of the cisco_nexus1000v_extension.xml file could result in an error message.

Note To avoid downloading an obsolete cached copy of the file, make sure to first refresh your browser window.

- You know the IP address of the active VSM.
- A plug-in must be added to the vCenter Server for every VSM connecting to it.

  If you have dual supervisors, both use the same plug-in.

Note If you see the error, "The specified parameter was not correct," then you have tried to register a plugin that is already registered. See the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(2)*.

DETAILED STEPS

Step 1 Open the vSphere Client.

The local host—VMware Infrastructure Client dialog box opens.

Step 2 From the Plug-Ins menu, choose **Manage Plug-Ins**.

The Plug-In Manager dialog box opens.

Step 3 Right-click the white space within the dialog box, and choose **New Plug-In** from the popup menu.

The Register Plug-In dialog box opens.

Step 4 Click **Browse** and choose the cisco_nexus1000v_extension.xml file that you downloaded from the VSM home page.

Step 5 Click **Register Plug-In**.

Note If you see the error, "The specified parameter was not correct," then you have tried to register a plugin that is already registered. See the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(2)*.

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

Step 6 In the Security Warning dialog box, click **Ignore** to continue using the certificate.

Step 7 In the Register Plug-in dialog box, click **OK**.

The plug-in is created and registered.

Step 8 Verify that the extension now shows up in the Plug-in Manager window.

Step 9 Close the window.

Step 10 You have completed this procedure.
Return to the CLI Software Configuration Process, page 4-1.

Connecting to the vCenter Server

You can use this procedure to configure the connection between the VSM and the vCenter Server and then save the configuration in persistent memory across reboots and restarts.

BEFORE YOU BEGIN

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

- You are logged in to the standalone or active VSM in EXEC mode.
- The extension for the Cisco Nexus 1000V is already registered as a plug-in on the vCenter Server.
- You know the datacenter name, which is case-sensitive.
- The datacenter already exists on the vCenter Server.
- You know the IP address of the vCenter Server.

SUMMARY STEPS

1. **config t**
2. **svs connection** *connection_name*
3. **vmware dvs datacenter-name** *dc_name*
4. **protocol vmware-vim**
5. **remote ip address** *ip_address*
6. **connect**
7. **show svs connections**
8. **copy running-config startup-config**

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

DETAILED STEPS

	Command	Description
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	**svs connection** *name* **Example:** n1000v (config#) svs connection VC n1000v(config-svs-conn#)	Enters connection configuration mode for adding this connection between Cisco Nexus 1000V and the vCenter Server. By using a name, information for multiple connections can be stored in the configuration.
Step 3	**protocol vmware-vim** [http] **Example:** n1000v(config-svs-conn#) protocol vmware-vim n1000v(config-svs-conn#)	Specifies that this connection uses the VIM protocol. This command is stored locally. • **http**: Specifies that the VIM protocol runs over HTTP. The default is to use HTTP over SSL (HTTPS).
Step 4	**remote ip address** *ipaddress* **Example:** n1000v(config-svs-conn#) remote ip address 172.28.15.150 n1000v(config-svs-conn#)	Specifies the IP address of the ESX server or vCenter Server for this connection. This command is stored locally.
Step 5	**vmware dvs datacenter-name** *name* **Example:** n1000v(config-svs-conn#) vmware dvs datacenter-name Hamilton-DC n1000v(config-svs-conn#)	Identifies the datacenter name in the vCenter Server where Cisco Nexus 1000V is to be created as a distributed virtual switch (DVS). You can use this command before or after connecting. The datacenter name is stored locally.
Step 6	**connect** **Example:** n1000v(config-svs-conn#) connect	Initiates the connection. **Note** It may take up to 10 seconds to connect the first time. If the username and password have not been configured for this connection, the user is prompted for a username and password. There can be only one active connection at a time. If a previously-defined connection is up, an error message displays and the command is rejected until you close the previous connection using the **no connect** command. **Note** If the connection is not initiated, see the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(2).*

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

	Command	Description
Step 7	**show svs connections** [*name*] **Example:** n1000v(config-svs-conn#) show svs connections vc connection VC: hostname: 172.28.15.150 protocol: vmware-vim https certificate: default datacenter name: HamiltonDC DVS uuid: 6d fd 37 50 37 45 05 64-b9 a4 90 4e 66 eb 8c f5 config status: Enabled operational status: Connected n1000v(config-svs-conn#)	Displays the current connections to the Cisco Nexus 1000V for verification. A Cisco Nexus 1000V DVS is created on vCenter Server and is visible through vSphere Client under Inventory > Networking. **Note** If your connection to the vCenter Server is shut down unexpectedly, the Cisco Nexus 1000V does not automatically restore it. In this case, you must restore the connection manually using the following command sequence, **no connect** **connect**
Step 8	**copy running-config startup-config** **Example:** n1000v(config-svs-conn#) copy running-config startup-config [##] 100% n1000v(config-port-prof)#	The connection to the vCenter Server is setup and copied from the running configuration to the startup configuration where it is saved persistently through reboots and restarts. **Caution** If you do not copy this configuration to the startup configuration, then in the event of a VSM reboot, this connection configuration is discarded.
Step 9	You have completed this procedure. Return to the CLI Software Configuration Process, page 4-1.	

Configuring the System Port Profile for VSM-VEM Communication

You can use this procedure to define the uplink port profile with system VLANs to establish communication between the VSM and VEM.

BEFORE YOU BEGIN

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

- You have already added the required VLANs using the "Creating VLANs" procedure on page 2-5.
- You are logged in to the standalone or active VSM in EXEC mode.
- You don't need to configure the system port profile on the secondary VSM. Once this configuration is made in the primary VSM, it automatically synchronizes with the secondary VSM.
- You can save the commands used here in a file, copy it to bootflash, and run it as a script. For more information about using scripts, see the "Working with Command Scripts" section on page 6-12.
- The system VLANs defined in this procedure establish a communication link between the VSM and VEM.

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

- The VLANs defined in the trunk configuration in the system port profile must also be defined in the trunk configuration in the attached physical switchport.
- The port profile name you designate in this procedure is your choice.
- Cisco recommends that you use the same VLAN for control, packet, and management, but that you do not place data traffic on this VLAN. For flexibility, you can use separate VLANs.
- In this example, a single system VLAN 260 is used for both control and packet traffic. You can use separate VLANs.
- The port mode (access or trunk), allowed VLANs, and shut state are defined before the system VLANS.
- The list of allowed VLANs has to be a superset of (or the same as) the list of system VLANs.
- For more information about system VLANs and system port profiles, see the following:
  - "System Port Profiles and System VLANs" section on page 1-4
  - *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2).*

Caution You must store the port profiles in the Cisco Nexus 1000V startup configuration so that they are saved in the event of a restart or reboot. Otherwise, in the event of a VSM reboot, port groups continue to exist on the vCenter Server but not on the VSM.

SUMMARY STEPS

1. **config t**
2. **port-profile** [**type** {**ethernet** | **vethernet**}] *name*
3. **description** *profiledescription*
4. **switchport mode trunk**
5. **switchport trunk allowed vlan** *vlan_IDs*
6. **no shutdown**
7. **system vlan** *vlan_ID_list*
8. **vmware port-group** [*portgroup_name*]
9. **state enabled**
10. **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
11. **copy running-config startup-config**

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

DETAILED STEPS

	Command	Description

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

Step 2	**port-profile** [**type** {**ethernet** | **vethernet**}] *name*
	
	Example:
	`n1000v(config)# port-profile type ethernet system-uplink`
	`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	**description** *profiledescription*
	
	Example:
	`n1000v(config-port-prof)# description "System profile for critical ports"`
	`n1000v(config-port-prof)#`
		Adds a description to the port profile. This description is automatically pushed to the vCenter Server.
		profile description: up to 80 ASCII characters
		Note If the description includes spaces, it must be surrounded by quotations.

Step 4	**switchport mode trunk**
	
	Example:
	`n1000v(config-port-prof)# switchport mode trunk`
	`n1000v(config-port-prof)#`
		Designates that the new port profile is used as a trunk port,

Step 5	**switchport trunk allowed vlan** *vlan_IDs* **Example:** `n1000v(config-port-prof)# switchport trunk allowed vlan 260`	Specifies the VLANs allowed on the trunk port for the new port profile.

Step 6	**no shutdown**
	
	Example:
	`n1000v(config-port-prof)# no shutdown`
	`n1000v(config-port-prof)#`
		Administratively enables all ports in the new port profile.

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

	Command	Description
Step 7	**system vlan** *vlan_ID_list* **Example:** n1000v(config-port-prof)# system vlan 260 n1000v(config-port-prof)#	Adds the system vlan to this port profile. A system vlan is used to configure and bring up physical or vEthernet ports before the VSM has established communication with the VEM. **Note** If you defined separate control and packet VLANs, then add another system VLAN.
Step 8	**vmware port-group** [*portgroup_name*] **Example:** n1000v(config-port-prof)# vmware port-group system-uplink n1000v(config-port-prof)#	Designates the port profile as a VMware port group of the same name. The port profile is mapped to a VMware port group of the same name. When a vCenter Server connection is established, this port group is then distributed to the virtual switch on the vCenter Server.
Step 9	**state enabled** **Example:** n1000v(config-port-prof)# state enabled n1000v(config-port-prof)#	Enables the new system port profile. The configuration for ths new system port profile is applied to the assigned ports. The VMware port group is created in the vswitch on the vCenter Server. A Distributed Virtual Port Group is now visible under the VSM Name on the vSphere Client Inventory > Networking > DataCenter tab.

Step 10	**show port-profile name** *profile-name*
	
	Example:
	n1000v(config-port-prof)# show port-profile name system-uplink
	port-profile system-uplink
	  description: "System profile for critical ports"
	  type: ethernet
	  status: enabled
	  capability l3control: no
	  pinning control-vlan: -
	  pinning packet-vlan: -
	  system vlans: 260
	  port-group: system-uplink
	  max ports: -
	  inherit:
	  config attributes:
	  switchport mode trunk
	  switchport trunk allowed vlan 260
	  no shutdown
	  evaluated config attributes:
	  switchport mode trunk
	  switchport trunk allowed vlan 260
	  no shutdown
	  assigned interfaces:
	n1000v(config-port-prof)#
		(Optional) Displays the system-uplink port profile configuration.

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

	Command	Description

Step 11	**copy running-config startup-config**
	
	Example:
	`n1000v(config-port-prof)# copy running-config startup-config`
	`[########################################]`
	`100%`
	`n1000v(config-port-prof)#`
		Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.
		
		Caution If you do not copy this configuration to the startup configuration, then in the event of a VSM reboot, this port group will continue to exist on the vCenter Server but not on the VSM

Step 12	You have completed this procedure. Return to the CLI Software Configuration Process, page 4-1.	

Example Configuration: System Profile for Critical Ports

```
config t
port-profile type ethernet system-uplink
description "System profile for critical ports"
switchport mode trunk
switchport trunk allowed vlan 260
no shutdown
system vlan 260
vmware port group system-uplink
state enabled
```

Configuring the Uplink Port Profile for VM Traffic

You can use this procedure to define the uplink port profile that the physical interface uses to carry the VM traffic.

BEFORE YOU BEGIN

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

- You have already added the required VLANs using the "Creating VLANs" procedure on page 2-5.
- You are logged in to the standalone or active VSM in EXEC mode.
- You don't need to configure the system port profile on the secondary VSM. Once this configuration is made, the primary VSM automatically synchronizes with the secondary VSM.
- You can save the commands used here in a file, copy it to bootflash, and run it as a script. For more information about using scripts, see the *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(2)*.
- The port profile name you designate in this procedure is your choice.
- If you want to use the system-uplink port profile to carry your data traffic, then add the data VLAN to the system-uplink port profile and make the corresponding changes on the upstream switch.
- For more information about port profiles, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)*.

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

SUMMARY STEPS

1. **config t**
2. **port-profile** [**type** {**ethernet** | **vethernet**}] *name*
3. **description** *profiledescription*
4. **switchport mode access**
5. **switchport access vlan** *vlan_ID*
6. **vmware port-group** [*portgroup_name*]
7. **no shutdown**
8. **state enabled**
9. **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-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 type ethernet** *name*
	
	Example:
	`n1000v(config)# port-profile type ethernet vm-uplink`
	`n1000v(config-port-prof)#`
		Enters port profile configuration mode for the specified port profile.
		• **type**: Defines the port-profile as Ethernet or vEthernet type. Once configured, this setting cannot be changed. The default is vEthernet type.
		Defining a port-profile as an Ethernet type allows the port to be used as an uplink port. In 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.
		• **name**: The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V.

Step 3	**description** *profiledescription*
	
	Example:
	`n1000v(config-port-prof)# description "Uplink profile for VM Traffic"`
	`n1000v(config-port-prof)#`
		Adds a description to the port profile. This description is automatically pushed to the vCenter Server.
		profile description: up to 80 ASCII characters
		Note If the description includes spaces, it must be surrounded by quotations.

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

	Command	Description

Step 4	**switchport mode access**
	
	Example:
	`n1000v(config-port-prof)# switchport mode access`
	`n1000v(config-port-prof)#`
		Designates that the new port profile is used as an access port,

Step 5	**switchport access vlan** *vlan_ID* **Example:** `n1000v(config-port-prof)# switchport access vlan 260`	Specifies the access VLAN for the new port profile.

Step 6	**no shutdown**
	
	Example:
	`n1000v(config-port-prof)# no shutdown`
	`n1000v(config-port-prof)#`
		Administratively enables all ports in the new port profile.

Step 7	**vmware port-group** [*portgroup_name*]
	
	Example:
	`n1000v(config-port-prof)# vmware port-group vm-uplink`
	`n1000v(config-port-prof)#`
		Designates the port profile as a VMware port group of the same name.
		
		The port profile is mapped to a VMware port group. When a vCenter Server connection is established, this port group is then distributed to the virtual switch on the vCenter Server.

Step 8	**state enabled**
	
	Example:
	`n1000v(config-port-prof)# state enabled`
	`n1000v(config-port-prof)#`
		Enables the new uplink port profile for VM traffic.
		
		The configuration for ths new uplink port profile is applied to the assigned ports. The VMware port group is created in the vswitch on the vCenter Server.
		
		A Distributed Virtual Port Group is now visible under the VSM Name on the vSphere Client Inventory > Networking > DataCenter tab.

Step 9	**show port-profile name** *profile-name*
	
	Example:
	`n1000v(config-port-prof)# show port-profile name vm-uplink`
	`port-profile vm-uplink`
	`  description: "Uplink profile for VM traffic`
	`  type: ethernet`
	`  status: enabled`
	`  capability l3control: no`
	`  pinning control-vlan: -`
	`  pinning packet-vlan: -`
	`  system vlans: none`
	`  port-group: vm-uplink`
	`  max ports: -`
	`  inherit:`
	`  config attributes:`
	`  switchport mode access`
	`  switchport access vlan 260`
	`  no shutdown`
	`  evaluated config attributes:`
	`  switchport mode access`
	`  switchport access vlan 260`
	`  no shutdown`
	`  assigned interfaces:`
	`n1000v(config-port-prof)#`
		(Optional) Displays the vm-uplink port profile configuration.

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

	Command	Description
Step 10	**copy running-config startup-config** **Example:** n1000v(config-port-prof)# copy running-config startup-config [##] 100% n1000v(config-port-prof)#	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration. **Caution** If you do not copy this configuration to the startup configuration, then in the event of a VSM reboot, this port group will continue to exist on the vCenter Server but not on the VSM
Step 11	You have completed this procedure. Return to the CLI Software Configuration Process, page 4-1.	

Example Configuration: Uplink Profile for VM Traffic

```
config t
port-profile type ethernet vm-uplink
description "Uplink profile for VM traffic
switchport mode access
switchport access vlan 260
no shutdown
vmware port-group vm-uplink
state enabled
```

Configuring the Data Port Profile for VM Traffic

You can use this procedure to define the data port profile that will be presented to the VM as a network adapter to carry traffic to and from the guest VM.

BEFORE YOU BEGIN

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

- You have already added the required VLANs using the "Creating VLANs" procedure on page 2-5.
- Cisco recommends that you use the same VLAN for control, packet, and management, but that you do not place data traffic on this VLAN. For flexibility, you can configure separate VLANs.
- You are logged in to the standalone or active VSM in EXEC mode.
- You don't need to configure the data port profile on the secondary VSM. Once this configuration is made in the primary VSM, it automatically synchronizes with the secondary VSM.
- You can save the commands used here in a file, copy it to bootflash, and run it as a script. For more information about using scripts, see the *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(2)*.
- The port profile name you designate in this procedure is your choice.
- For more information about port profiles, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)*.

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

SUMMARY STEPS

1. **config t**
2. **port-profile** [**type** {**ethernet** | **vethernet**}] *name*
3. **description** *profiledescription*
4. **switchport mode access**
5. **switchport access vlan** *vlan_ID*
6. **vmware port-group** [*portgroup_name*]
7. **no shutdown**
8. **state enabled**
9. **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-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** [**type** {**ethernet** | **vethernet**}] *name*
	
	Example:
	`n1000v(config)# port-profile type vethernet data20`
	`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	**description** *profiledescription*
	
	Example:
	`n1000v(config-port-prof)# description "Data profile for VM Traffic"`
	`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.

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

	Command	Description

Step 4	**switchport mode access**
	
	Example:
	`n1000v(config-port-prof)# switchport mode access`
	`n1000v(config-port-prof)#`
		Designates that the new port profile is used as an access port,

Step 5	**switchport access vlan** *vlan_ID* **Example:** `n1000v(config-port-prof)# switchport access vlan 20`	Specifies the access VLAN for the new port profile.

Step 6	**no shutdown**
	
	Example:
	`n1000v(config-port-prof)# no shutdown`
	`n1000v(config-port-prof)#`
		Administratively enables all ports in the new port profile.

Step 7	**vmware port-group** [*portgroup_name*]
	
	Example:
	`n1000v(config-port-prof)# vmware port-group data20`
	`n1000v(config-port-prof)#`
		Designates the port profile as a VMware port group.
		
		The port profile is mapped to a VMware port group. When a vCenter Server connection is established, this port group is then distributed to the virtual switch on the vCenter Server.

Step 8	**state enabled**
	
	Example:
	`n1000v(config-port-prof)# state enabled`
	`n1000v(config-port-prof)#`
		Enables the new data port profile for VM traffic.
		
		The configuration for ths new data port profile is applied to the assigned ports. The VMware port group is created in the vswitch on the vCenter Server.
		
		A Distributed Virtual Port Group is now visible under the VSM Name on the vSphere Client Inventory > Networking > DataCenter tab.

Step 9	**show port-profile name** *profile-name*
	
	Example:
	`n1000v(config-port-prof)# show port-profile name data260`
	`port-profile data20`
	`  description: "Data profile for VM traffic"`
	`  type: vethernet`
	`  status: enabled`
	`  capability l3control: no`
	`  pinning control-vlan: -`
	`  pinning packet-vlan: -`
	`  system vlans: none`
	`  port-group: data20`
	`  max ports: -`
	`  inherit:`
	`  config attributes:`
	`  switchport mode access`
	`  switchport access vlan 20`
	`  no shutdown`
	`  evaluated config attributes:`
	`  switchport mode access`
	`  switchport access vlan 20`
	`  no shutdown`
	`  assigned interfaces:`
	`n1000v(config-port-prof)#`
		(Optional) Displays the port profile configuration that will be bound to the physical NIC for VM traffic.

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

	Command	Description
Step 10	**copy running-config startup-config** **Example:** n1000v(config-port-prof)# copy running-config startup-config [##] 100% n1000v(config-port-prof)#	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration. **Caution** If you do not copy this configuration to the startup configuration, then in the event of a VSM reboot, this port group will continue to exist on the vCenter Server but not on the VSM
Step 11	You have completed this procedure. Return to the CLI Software Configuration Process, page 4-1.	

Example Configuration: Data Profile for VM Traffic

```
config t
port-profile type vethernet data20
description "Data profile for VM traffic"
switchport mode access
switchport access vlan 20
no shutdown
vmware port-group data20
state enabled
```

Adding an ESX 4.0 Host to the DVS

Use this procedure and your VMware documentation to add the host to the DVS.

Note If you are using VUM, then this procedure also installs the Cisco Nexus 1000V software onto the VEM automatically when the host is added to the switch.

BEFORE YOU BEGIN

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

- The corresponding interface on the upstream switch must already be configured to allow the same VLANs as configured in the system-uplink port profile.
- In the example in this procedure, the traffic flow is set up as follows:

Traffic	VMNIC
Control VLAN	system-uplink VMNIC
Packet VLAN	system-uplink VMNIC
VM data	VM-uplink Port Group

Note If you use the system-uplink profile to carry data traffic and the system-uplink profile has already been defined, then you do not need to assign the vm-uplink profile to another vmnic.

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

- If you are not using VUM, you have already installed the VEM software on the host using the *Cisco Nexus 1000V Virtual Ethernet Module Software Installation Guide, Release 4.0(4)SV1(2)*.
- If you are using VUM, this procedure triggers VUM to install the Cisco Nexus 1000V VEM package.
- If you are using VUM, you have already loaded VUM and created a database for patches on the vCenter Server using the VMware instructions.

Caution The automatic VEM software installation by VUM might fail with a proxy server enabled in VUM. This is due to a VMware limitation. The workaround is to disable the proxy during the software installation.

- The VMware Enterprise Plus license must already be installed on the host before the host can be added to the DVS. If not, then the host will not show up in the **Add Host to Distributed Virtual Switch** dialog box and you cannot add it.
- The VSM is already connected to the vCenter Server.
- To add multiple uplinks to the DVS and form a port channel with them, see the *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(2)*.

DETAILED STEPS

Step 1 In the vSphere Client, click Inventory → Networking.

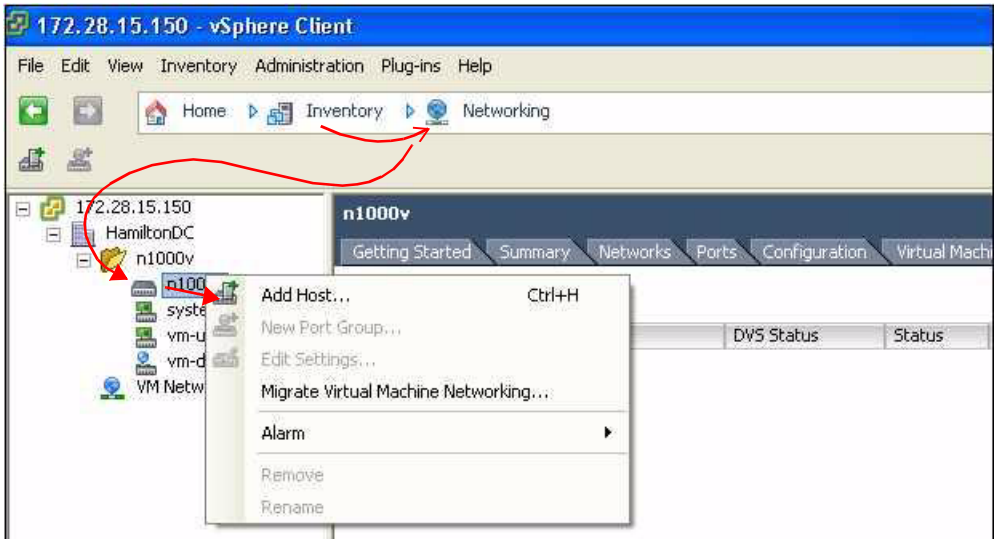
You should see the following that you create when :

- A DVS with the switch name that you configured.
- The port profiles that you created.

Step 2 Do one of the following:

- If the DVS and the port profiles are present, continue with the next step.
- Otherwise, see the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(2)*.

Figure 4-1 Adding a Host to a DVS



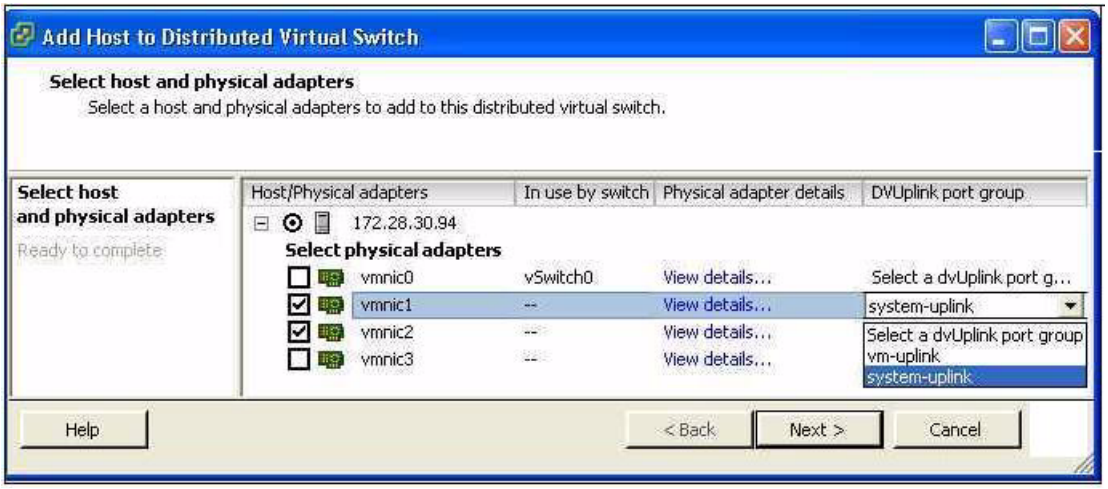
Send document comments to nexus1k-docfeedback@cisco.com.

Step 3 Right-click the switch name, and choose **Add Host**.

The Add Host to Distributed Virtual Switch Wizard opens.

Note If the Add Host to Distributed Virtual Switch dialog box is empty, then check to make sure the host has an Enterprise Plus license for VMware ESX 4.0 servers.

Figure 4-2 Choosing the VM System NIC for the Host



Note If using VUM, the Cisco Nexus 1000V software is now loaded onto the DVS by VUM.

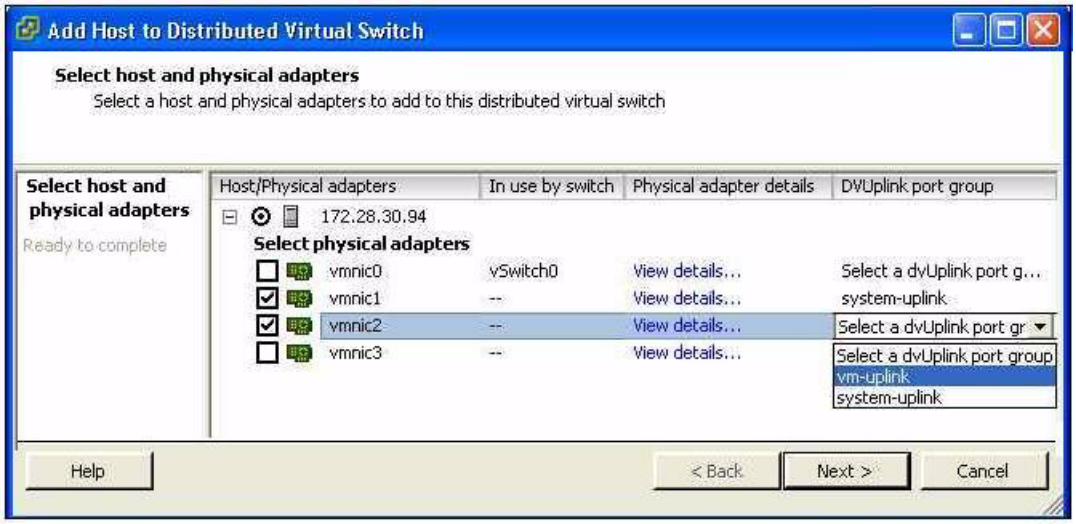
Step 4 Do one of the following:

- If you use the system-uplink profile to carry data traffic and the system-uplink profile has already been defined, then you do not need to assign the vm-uplink profile to another vmnic.
- If not, choose the next vmnic that is not attached to the VMware vSwitch, for example vmnic1.

  It should be linked to the Uplink Port Group system-uplink.

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

Figure 4-3 Choosing the VM Uplink NIC for the Host



Note If the Add Host to Distributed Virtual Switch dialog box is empty, then check to make sure the host has an Enterprise Plus license for VMware ESX 4.0 servers.

Step 5 Choose the next vmnic that is not attached to the VMware vSwitch, for example vmnic2.

It should be linked to the Uplink Port Group vm-uplink.

Note To add multiple uplinks to the DVS and form a port channel with them, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2).*

Step 6 Click **Next**.

Step 7 Verify the port group assignment and click **Finish**.

Step 8 Do one of the following:

- If the host is successfully added to the DVS, continue with the next step.
- If the operation fails, see the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(2).*

Step 9 You have completed this procedure.
Return to the CLI Software Configuration Process, page 4-1.

CHAPTER 5

Running a VSM and VEM on the Same Host

This chapter describes how a VSM and VEM can run on the same host.

This chapter includes the following topics:

- Information About a VSM and VEM on the Same Host, page 5-1
- Guidelines and Limitations, page 5-2
- Configuring a VSM and its VEM on the Same Host, page 5-3

Information About a VSM and VEM on the Same Host

The VSM and VEM can run on the same host. In this case, the VSM communicates with the co-located VEM and other VEMs in the network using its own switch.

The following are examples of networks where you could run a VSM on its own host:

- Environments where the server administrator can guarantee that the VSM VM will not be mistakenly powered down or reconfigured.
- Test and demonstration setups.

To avoid any possibility of losing communication with its VEMs, it is recommended that the VSM be installed on a separately-managed server.

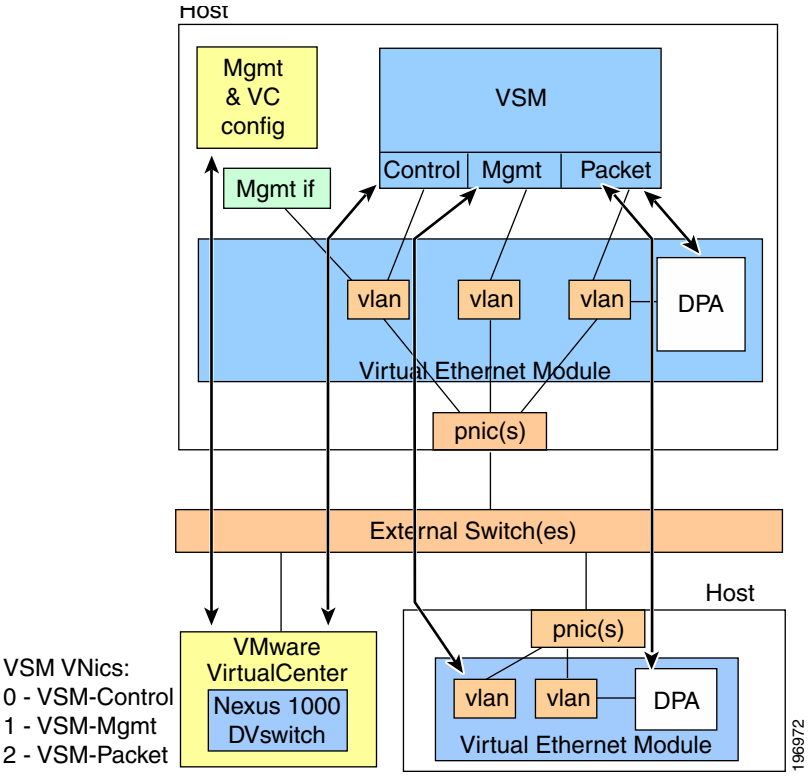
The following are examples of networks where you are advised to run your VSM on a separate host from its VEMs:

- Environments where the server administrator cannot guarantee the virtual machine for the VSM will be available and will not be modified.
- Environments where server resources (CPU, memory, network bandwidth) cannot be guaranteed for the VSM.
- Environments where network administrators have their own ESX server hosts to run network services.
- Environments where network administrators need to quickly create, destroy, and move VSMs without server administrator interaction.

Figure 5-1 shows a VSM and VEM running on the same host.

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

Figure 5-1 Running a VSM and VEM on the Same Host



Guidelines and Limitations

When running a VSM and its VEM on the same server host, use the following guidelines and limitations:

- When the virtual NICs for a VSM are attached to one of its own VEMs, both network and server administrator must ensure that their actions do not interfere with the configuration that enables the VSM to communicate, including the following:
  - The management port must use a system port profile.
  - The control port must use a system port profile.
  - It is recommended that the packet port use a system port profile.
  - To bring up a new VSM on a server using its own VEM, it must have at least 2 physical ports.
- If the virtual disk for the VSM is accessed via iSCSI or NFS, the storage vmknic on every host that may run the active/standby VSMs must use a system profile.
- The server administrator must not detach the VSM from its networks, including the following:
  - Do not stop the host server.
  - Do not remove the host server virtual NICs or change their port groups.
  - Do not remove any physical ports in use by VLANs that are needed by the host server virtual NICs.

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

- Since the critical management and control ports for the VSM must use system port profiles, these networks will be available on any host that supports the correct VLANs on its physical ports. Therefore, VMotion of either the primary or standby VSM is supported on these hosts.
- Since the VSM depends on itself for configuring the VEM on which it is running, it must first be brought up using normal vswitches to connect to VC and its server host. This is a transitory state that is only required the first time the VSM is brought up.

Configuring a VSM and its VEM on the Same Host

Use this procedure to configure a VSM and its VEM on the same physical server host.

BEFORE YOU BEGIN

Before configuring the VSM and its VEM on a single ESX server, you must know or do the following:

- You have already installed and set up the Cisco Nexus 1000V software on the ESX server using the "Setting Up the Software" section on page 2-1, including the following:
  - Installing the VSM on an ESX server with vswitches for the following:
    - management
    - packet traffic
    - control traffic
  - Configuring physical ports on the vswitches for control, management, and packet VLANs.
  - Configuring the system, uplink, and data port profiles.
  - Connecting with vCenter.
- The ESX server host has at least two physical ports.
- The standby VSM can be directly added to Cisco Nexus 1000V when it is created, and will not require the following procedure.
- A VSM that is already running in a vswitch environment on the same host can also be migrated to a VEM solution using this procedure. By reversing this procedure, a VSM can be moved from the VEM back onto vswitches if needed.

Step 1 On the ESX server host where the VSM is installed, add the VEM software using your VMware documentation and the *Cisco Nexus 1000V Virtual Ethernet Module Software Installation Guide, Release 4.0(4)SV1(2)*.

Step 2 Assign the VSM management port to the corresponding port group on the Cisco Nexus 1000V.

VSM management traffic is now using Cisco Nexus 1000V.

Step 3 Assign the ESX server host management port to the corresponding port group on the Cisco Nexus 1000V.

vCenter now uses Cisco Nexus 1000V to talk to the server host.

Step 4 Assign the VSM control port to the corresponding port group on the Cisco Nexus 1000V.

The VSM and VEM control traffic (and that of other VEMs in the network) now use Cisco Nexus 1000V.

Step 5 Assign the VSM packet port to the corresponding port group on the Cisco Nexus 1000V.

Protocols such as CDP, LACP, and IGMP, now communicate using the Cisco Nexus 1000V.

Step 6 Remove the vswitches.

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

You may now reuse the old physical port for Cisco Nexus 1000V.

You have completed configuring a VSM and its VEM running on the same server host.

CHAPTER 6

Understanding the CLI

This chapter provides information about the CLI in the following sections:

- Information About the CLI Prompt, page 6-1
- Command Modes, page 6-2
- Special Characters, page 6-7
- Keystroke Shortcuts, page 6-7
- Abbreviating Commands, page 6-9
- Using the No Form of a Command, page 6-9
- Using CLI Variables, page 6-10
- Working with Command Scripts, page 6-12
- Using Help, page 6-14

Information About the CLI Prompt

Once you have successfully accessed the system, the CLI prompt displays in the terminal window of your console port or remote workstation, as follows.

```
switch#
```

You can change this switch prompt to another name or leave it as it is.

Example:

```
switch# config t
switch(config)# switchname n1000v
n1000v(config)# exit
n1000v#
```

From the CLI prompt, you can do the following:

- Use CLI commands for configuring features.
- Access the command history.
- Use command parsing functions.

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

Command Modes

This section includes the following topics:

- About Command Modes, page 6-2
- EXEC Command Mode, page 6-3
- Global Configuration Command Mode, page 6-3
- Accessing Interface Configuration Command Mode, page 6-3
- Exiting a Configuration Mode, page 6-4
- Command Mode Summary, page 6-5

About Command Modes

Cisco Nexus 1000V CLI is divided into command modes which define the actions available to the user. Command modes are “nested” and are accessed in sequence. When you first log in, you are placed in CLI EXEC mode.

As you navigate from EXEC mode to global configuration mode, a larger set of commands are available to you. To transition to global configuration mode, enter the following command:

config t

The following table shows how command access builds from user EXEC to global configuration mode.

Command Mode	Prompt	Description
Exec	n1000v#	• Connect to remote devices. • Temporarily change terminal line settings. • Perform basic tests. • List system information (show).
Global Configuration	n1000v(config)#	• Configure features, such as the following: – port profile – VLANs – Interfaces • Includes access to EXEC commands. – Connect to remote devices. – Temporarily change terminal line settings. – Perform basic tests. – List system information (show).

All commands in EXEC command mode are accessible from the global configuration command mode. For example, the **show** commands are available from any command mode.

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

EXEC Command Mode

When you first log in, you are placed into EXEC mode. The commands available in EXEC mode include the **show** commands that display device status and configuration information, the **clear** commands, and other commands that perform actions that you do not save in the device configuration.

Global Configuration Command Mode

Global configuration mode provides access to the most broad range of commands, including those used to make configuration changes that are saved by the device, and can be stored and applied when the device is rebooted.

Commands entered in global configuration mode update the running configuration file as soon as they are entered, but must also be saved into the startup configuration file by using the following command:

copy running-config startup-config

In global configuration mode, you can access a number of protocol-specific, platform-specific, and feature-specific configuration modes.

Accessing Interface Configuration Command Mode

To access and list the interface configuration commands, follow these steps:

	Command	Purpose

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

Step 2	**interface** *type number*
	
	Example:
	`n1000v(config)# interface ethernet 3/2`
	`n1000v(config-if)#`
		Enters interface configuration mode for the interface you want to configure.

For details about interface commands and configuration, see the document, *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(2).*

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

Exiting a Configuration Mode

To exit from any Configuration mode, use any of the following commands:

Command	Purpose

exit
 	
Example:
`svs(config-if)# exit`
`svs(config)#`
	Exits from the current configuration command mode and return to the previous configuration command mode.

end
 	
Example:
`svs(config)# end`
`svs#`
	Exits from the configuration command mode and returns to EXEC mode.

Ctrl-z
 	
Example:
`svs(config)# ^z`
`svs#`
	Exits the current configuration command mode and returns to EXEC mode.
	
	Caution If you use Ctrl-Z at the end of a command line in which a valid command has been typed, the CLI adds the command to the running configuration file. We recommend that you exit a configuration mode using the **exit** or **end** command.

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

Command Mode Summary

Table 6-1 summarizes information about command modes.

Table 6-1 Command Mode Summary

Mode	Access Method	Prompt	Exit Method
EXEC	From the login prompt, enter your username and password.	`n1000v#`	To exit to the login prompt, use the **exit** command.
Global Configuration	From EXEC mode, enter the command, **configure terminal**.	`n1000v(config)#`	To exit to EXEC mode, use the **end** or **exit** command or press **Ctrl-Z**.
Port Profile Configuration	From Global Configuration mode, enter the command, **port-profile** *name*.	`n1000v(config-port-prof)#`	To exit to Port Profile Configuration mode, use the **exit** command. To exit to EXEC mode, use the **end** command or press **Ctrl-Z**.
Interface Configuration	From Global Configuration mode, enter the **interface** command for a specific interface, for example, `interface veth 2`	`n1000v(config-if)#`	To exit to Interface Configuration mode, use the **exit** command. To exit to EXEC mode, use the **end** command or press **Ctrl-Z**.
VLAN Configuration	Use a **vlan** command.	`n1000v(config-vlan)#`	To exit to VLAN Configuration mode, use the **exit** command. To exit to EXEC mode, use the **end** command or press **Ctrl-Z**.
`Console Configuration`	From Global Configuration mode, use the **line console** command.	`n1000v(config-console)`	To exit to Console Configuration mode, use the **exit** command. To exit to EXEC mode, use the **end** command or press **Ctrl-Z**.
Virtual Terminal Line Configuration	From Global Configuration mode, use the **line vty** command.	`n1000v(config-line)#`	To exit to Line Configuration mode, use the **exit** command. To exit to EXEC mode, use the **end** command or press **Ctrl-Z**.
SVS Domain Configuration	From Global Configuration mode, use the **svs-domain** command.	`n1000v(config-svs-domain)#`	To exit to SVS Domain Configuration mode, use the **exit** command. To exit to EXEC mode, use the **end** command or press **Ctrl-Z**.
Policy Map QoS Configuration	From Global Configuration mode, use the **policy-map** command.	`n1000v(config-pmap-qos)#`	To exit to Policy Map QoS Configuration mode, use the **exit** command. To exit to EXEC mode, use the **end** command or press **Ctrl-Z**.

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

Table 6-1 (continued)Command Mode Summary (continued)

Mode	Access Method	Prompt	Exit Method
Policy Map Class QoS Configuration	From Policy-Map QoS Configuration mode, use the class command.	`n1000v(config-pmap-c-qos)#`	To exit to Policy Map Class QoS Configuration mode, use the **exit** command. To exit to EXEC mode, use the **end** command or press **Ctrl-Z**.
Class Map QoS Configuration	From Global Configuration mode, use the **class-map** command.	`n1000v(config-cmap-qos)#`	To exit to Class Map QoS Configuration mode, use the **exit** command. To exit to EXEC mode, use the **end** command or press **Ctrl-Z.**

Saving CLI Configuration Changes

This section describes how changes you make using the CLI are saved and includes the following topics:

- Running Configuration, page 6-6
- Startup Configuration, page 6-6
- Copying the Running Configuration to the Startup Configuration, page 6-7

Running Configuration

The running configuration is the configuration that is currently running on the device. It includes configuration changes from commands entered since the last time the device was restarted. If the device is restarted, the running configuration is replaced with a copy of the startup configuration. Any changes that were made to the running configuration but were not copied to the startup configuration are discarded.

Startup Configuration

The startup configuration is the configuration that is saved and that will be used by the device when you restart it. When you make configuration changes to the device, they are automatically saved in the running configuration. If you want configuration changes saved permanently, you must copy them to the startup configuration so that they are preserved when the device is rebooted or restarted.

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

Copying the Running Configuration to the Startup Configuration

You can use this procedure to copy changes you have made to the running configuration into the startup configuration so that they are saved persistently through reboots and restarts.

	Command	Purpose

Step 1	`copy running-config startup-config`
	
	Example:
	`n1000v(config)# copy running-config startup-config`
		(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Special Characters

Table 6-2 lists the characters that have special meaning in Cisco Nexus 1000V text strings and should be used only in regular expressions or other special contexts.

Table 6-2 Special Characters

Character	Description
|	Vertical bar
< >	Less than or greater than

Keystroke Shortcuts

Table 6-3 lists command key combinations that can be used in both EXEC and configuration modes:

Table 6-3 Keystroke Shortcuts

Key(s)	Description
Ctrl-A	Moves the cursor to the beginning of the line
Ctrl-B	Moves the cursor one character to the left. When you enter a command that extends beyond a single line, you can press the Left Arrow or Ctrl-B keys repeatedly to scroll back toward the system prompt and verify the beginning of the command entry, or you can press the Ctrl-A key combination.
Ctrl-C	Cancels the command and returns to the command prompt.
Ctrl-D	Deletes the character at the cursor.
Ctrl-E	Moves the cursor to the end of the line.
Ctrl-F	Moves the cursor one character to the right.
Ctrl-G	Exits to the previous command mode without removing the command string.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.
Ctrl-L	Redisplays the current command line.
Ctrl-R	Redisplays the current command line.

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

Table 6-3 Keystroke Shortcuts (continued)

Key(s)	Description
Ctrl-T	Transposes the character to the left of the cursor with the character located to the right of the cursor.
Ctrl-U	Deletes all characters from the cursor to the beginning of the command line.
Ctrl-W	Deletes the word to the left of the cursor.
Ctrl-X, H	List history. When using this key combination, press and release the Ctrl and X keys together before pressing H.
Ctrl-Y	Recalls the most recent entry in the buffer (press keys simultaneously).
Ctrl-Z	Ends a configuration session, and returns you to EXEC mode. When used at the end of a command line in which a valid command has been typed, the resulting configuration is first added to the running configuration file.
↑	Displays the previous command in the command history.
↓	Displays the next command in the command history.
→ ←	Moves your cursor through the command history directionally to locate a command string.
?	Displays a list of available commands.

Tab	Completes the word for you after entering the first characters of the word, and then pressing the Tab key. All options that match are presented.
	Used to complete:
	• command names
	• scheme names in the file system
	• server names in the file system
	• file names in the file system
	Example
	`n1000v(config)# xm<Tab>`
	`n1000v(config)# xml <Tab>`
	`n1000v(config)# xml server`
	
	Example
	`n1000v(config)# c<Tab>`
	`callhome  class-map  clock  cts`
	`cdp  cli  control-plane`
	
	`n1000v(config)# cl<Tab>`
	`class-map  cli  clock`
	`n1000v(config)# cla<Tab>`
	`n1000v(config)# class-map`

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

Table 6-3 Keystroke Shortcuts (continued)

Key(s)	Description
	Example n1000v# **cd bootflash:<Tab>** bootflash: bootflash://sup-1/ bootflash://sup-remote/ bootflash:/// bootflash://sup-2/ bootflash://sup-standby/ bootflash://module-5/ bootflash://sup-active/ bootflash://module-6/ bootflash://sup-local/ **Example** n1000v# **cd bootflash://mo<Tab>** bootflash://module-5/ bootflash://module-6/ n1000v# **cd bootflash://module-**

Abbreviating Commands

You can abbreviate commands and keywords by entering the first few characters of a command. The abbreviation must include sufficient characters to make it unique from other commands or keywords. If you are having trouble entering a command, check the system prompt and enter the question mark (?) for a list of available commands. You might be in the wrong command mode or using incorrect syntax.

Table 6-4 lists examples of command abbreviations.

Table 6-4 Examples of Command Abbreviations

Command	Abbreviation
configure terminal	**conf t**
copy running-config startup-config	**copy run start**
interface ethernet 1/2	**int e 1/2**
show running-config	**sho run**

Using the *No* Form of a Command

Almost every configuration command has a **no** form that can be used to disable a feature or function. For example, to remove a VLAN, use the **no vlan** command. To reenable it, use the plain **vlan** command form. The *Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(2)* describes the **no** form of a command when available.

For example, if you use the **boot** command in global configuration mode, you can then use the **no boot** command undo the results:

```
n1000v(config)# boot system bootflash: svs1.bin
n1000v(config)# no boot system bootflash: svs1.bin
```

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

Using CLI Variables

The Cisco Nexus 1000V supports the definition and use of variables in CLI commands. You can use CLI variables as follows:

- Entered directly on the command line.
- Passed to the child script initiated using the **run-script** command. The variables defined in the parent shell are available for use in the child **run-script** command process (the "Running a Script" section on page 6-12).
- Passed as command line arguments to the **run-script** command (the "Running a Script" section on page 6-12).

CLI variables have the following characteristics:

- Cannot have nested references through another variable.
- Can persist across switch reloads.
- Can exist only for the current session

The Cisco Nexus 1000V software provides one predefined system variable, the TIMESTAMP variable.

User-Defined CLI Session Variables

You can define CLI session variables to persist only for the duration of your CLI session using the **cli var name** command in EXEC mode. CLI session variables are useful for scripts that you execute periodically.

The following example shows how to create a user-defined CLI session variable.

```
svs# cli var name testinterface ethernet 3/2
```

You can reference a variable using the syntax **$**(variable**)**.

The following example shows how to reference a user-defined CLI session variable.

```
n1000v# show interface $(testinterface)
Ethernet3/2 is up
    Hardware is Ethernet, address is 0050.565a.2341 (bia 0050.565a.2341)
    MTU 1500 bytes, BW -332641784 Kbit, DLY 10 usec,
       reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA
    Port mode is trunk
    full-duplex, 1000 Mb/s
    Beacon is turned off
    Auto-Negotiation is turned on
    Input flow-control is off, output flow-control is off
    Rx
    222045 Input Packets 24263 Unicast Packets
    89347 Multicast Packets 108435 Broadcast Packets
    22529316 Bytes
    Tx
    33710 Output Packets 31393 Unicast Packets
    1898 Multicast Packets 419 Broadcast Packets 461 Flood Packets
    5221175 Bytes
    91323 Input Packet Drops 0 Output Packet Drops

n1000v#
```

```
Use the show cli variables command to display user-defined CLI session variables.
The following example displays user-defined CLI session variables.
```

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

```
n1000v# show cli variables
VSH Variable List
-----------------
TIMESTAMP="2008-07-02-13.45.15"
testinterface="ethernet 3/1"
n1000v#
```

Use the **cli no var name** command to remove user-defined CLI session variables.

The following example removes a user-defined CLI session variable.

```
n1000v# cli no var name testinterface
```

User-Defined CLI Persistent Variables

You can define CLI variables that persist across CLI sessions and switch reloads using the **cli var name** command in configuration mode. These CLI persistent variables are defined in configuration mode and are saved in the running configuration file.

The following example shows how to create a user-defined CLI persistent variable.

```
n1000v# config t
n1000v(config)# cli var name mgmtport mgmt 0
n1000v(config)# exit
n1000v#
```

You can reference a variable using the syntax **$**(variable).

The following example shows how to reference a user-defined CLI persistent variable.

```
n1000v# show interface $(mgmtport)
mgmt0 is up
    Hardware is GigabitEthernet, address is 0000.0000.0000 (bia 0050.5681.5578)
    Internet Address is 10.78.1.63/24
    MTU 1500 bytes, BW 0 Kbit, DLY 0 usec,
       reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA
    full-duplex, 1000 Mb/s
    Beacon is turned off
    Auto-Negotiation is turned on
    Input flow-control is off, output flow-control is off
    321949 packets input, 67199373 bytes
    0 multicast frames, 0 compressed
    0 input errors, 0 frame, 0 overrun, 0 fifo
    30178 packets output, 7071526 bytes
    0 underrun, 0 output errors, 0 collisions
    0 fifo, 0 carrier errors

n1000v#
```

Use the **show cli variables** command to display user-defined CLI persistent variables.

The following example displays user-defined CLI persistent variables.

```
n1000v# show cli variables
VSH Variable List
-----------------
TIMESTAMP="2005-10-24-21.37.13"
mgmtport="mgmt 0"
```

Use the **no cli var name** command in configuration mode to remove user-defined CLI persistent variables.

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

The following example removes a user-defined CLI persistent variable.

```
n1000v# config t
n1000v(config)# cli no var name mgmtport
```

System-Defined Variables

Cisco Nexus 1000V supports one predefined variable: TIMESTAMP. This variable refers to the time of execution of the command in the format YYYY-MM-DD-HH.MM.SS.

Note The TIMESTAMP variable name is case sensitive. All letters must be uppercase.

The following example uses $(TIMESTAMP) when redirecting **show** command output to a file.

```
Example:
n1000v# show running-config > rcfg.$(TIMESTAMP)
n1000v# dir
       5718     Jul 02 14:09:58 2008  rcfg.2008-07-02-14.09.58

Usage for volatile://
       8192 bytes used
   20963328 bytes free
   20971520 bytes total
n1000v#
```

Working with Command Scripts

This section includes the following sections:

- Running a Script, page 6-12
- Using CLI Variables in Scripts, page 6-13
- Delaying Command Action, page 6-14

Running a Script

The **run-script** command executes the commands specified in a file. To use this command, be sure to create the file and specify commands in the required order.

Note You cannot create the script files at the switch prompt. You can create the script file on an external machine and copy it into the bootflash: directory. This section assumes that the script file resides in the bootflash: directory.

The syntax for this command is **run-script** *filename*.

This example displays the CLI commands specified in the testfile that resides in bootflash.

```
n1000v# show file bootflash:testfile
conf t
show interface mgmt 0
```

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

This file output is in response to the **run-script** command executing the contents in the testfile file:

```
pvk-s33# run-script bootflash:testfile
`conf t`
`show interface mgmt 0`
mgmt0 is up
Hardware: Ethernet, address: 0050.5682.4ace (bia 0050.5682.4ace)
Internet Address is 10.78.1.99/24
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA
full-duplex, 1000 Mb/s
Auto-Negotiation is turned on
25427 packets input, 2602757 bytes
0 multicast frames, 0 compressed
0 input errors, 0 frame, 0 overrun, 0 fifo
9077 packets output, 2433391 bytes
0 underrun, 0 output errors, 0 collisions
0 fifo, 0 carrier errors
...
```

Using CLI Variables in Scripts

You can use CLI variables defined by the **cli var** command or passed as arguments in the **run-script** command. For more information about the **cli var** command, see the "Using CLI Variables" section on page 6-10.

The following example shows how to use CLI session variables in a script file used by the **run-script** command.

```
n1000v# cli var name testinterface e 3/1

n1000v# show file bootflash:test1.vsh
show interface $(testvar)

n1000v# run-script bootflash:test1.vsh
`show interface $(testvar)`
Ethernet3/1 is down (Administratively down)
  Hardware is 10/100/1000 Ethernet, address is 0000.0000.0000 (bia 0019.076c.4da
c)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  auto-duplex, auto-speed
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned on
  Switchport monitor is off
  Last clearing of "show interface" counters never
  5 minute input rate 0 bytes/sec, 0 packets/sec
  5 minute output rate 0 bytes/sec, 0 packets/sec
  L3 in Switched:
    ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
  L3 out Switched:
    ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
  Rx
    0 input packets 0 unicast packets 0 multicast packets
    0 broadcast packets 0 jumbo packets 0 storm suppression packets
    0 bytes
```

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

```
Tx
  0 output packets 0 multicast packets
  0 broadcast packets 0 jumbo packets
  0 bytes
  0 input error 0 short frame 0 watchdog
  0 no buffer 0 runt 0 CRC 0 ecc
  0 overrun  0 underrun 0 ignored 0 bad etype drop
  0 bad proto drop 0 if down drop 0 input with dribble
  0 input discard
  0 output error 0 collision 0 deferred
  0 late collision 0 lost carrier 0 no carrier
  0 babble
  0 Rx pause 0 Tx pause 0 reset
```

The following example shows how you can pass CLI session variable as arguments to a child **run-script** command process.

```
n1000v# show file bootflash:test1.vsh
show interface $(var1) $(var2)

n1000v# run bootflash:test2.vsh var1="e3/1" var2="brief"
`show interface $(var1) $(var2)`
--------------------------------------------------------------------------------
Ethernet      VLAN    Type Mode   Status  Reason                   Speed     Port
Interface                                                                    Ch #
--------------------------------------------------------------------------------
Eth2/45       --      eth  routed down    Administratively down      auto(D) --
```

Delaying Command Action

The **sleep** command delays an action by a specified number of seconds, and is particularly useful within a script.

The syntax for this command is **sleep** *seconds*.

```
n1000v# sleep 30
```

You will the switch prompt return after 30 seconds.

Using Help

The CLI provides the following help features.

Feature	Description
?	You can type the question mark (?) to list the valid input options
^	The CLI prints the caret (^) symbol below a line of syntax to point to an input error in the command string keyword, or argument.
↑	You can use the up arrow to have the CLI display the previous command you entered so that you can correct an error.

The following example describes how to use syntax error isolation and context-sensitive help.

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

	Command	Purpose
Step 1	**show interface virtual ?** **Example:** `n1000v# show interface virtual ?` `  <CR>` `  >  Redirect it to a file` `  module  Limit display to interfaces on module` `  vm  Show interfaces owned by a Virtual Machine` `  vmk  Show interfaces owned by the Virtual Machine Kernel` `  vswif  Show interfaces owned by the Virtual Service Console` `	Pipe command output to filter`  `n1000v# show interface virtual`	Displays the optional parameters used with the **show interface virtual** command in EXEC mode.

Step 2	**show interface module ?**
	Example:
	`n1000v# show interface module ?`
	`  ^`
	`% invalid command detected at '^' marker.`
	`n1000v#`
		Displays an invalid command error message and points (^) to the syntax error.

Step 3	**Ctrl-P** or the Up Arrow
	
	Example:
	`n1000v# <Ctrl-P>`
	`n1000v# show interface virtual ?`
		Displays the previous command you entered so that you can correct the error.

Step 4	**show interface virtual module ?**
	Example:
	`n1000v# show interface virtual module ?`
	`  <1-256>  Enter module number`
	
	`n1000v# show interface virtual module`
		Displays the syntax for showing a virtual interface module.

Step 5	**show interface virtual module 3**
	Example:
	`n1000v# show interface virtual module 3`
	
	`------------------------------------------`
	`Port  Adapter  Owner  Mod  Host`
	`------------------------------------------`
	`n1000v#`
		Displays the virtual interface module 3.

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

	Command	Purpose

Step 6	**show module ?**
	Example:
	`n1000v# show module ?`
	`  <CR>`
	`  <1-66>  Enter module number`
	`  >  Redirect it to a file`
	`  internal  Show line card manager related info`
	`  uptime  Show how long the module has been up and running`
	`  vem  Show Virtual Ethernet Module information`
	`  |  Pipe command output to filter`
		Displays the optional parameters for the show module command.

Step 7	**show module** **Example:** Example 6-1 on page 6-16.	Displays module information.

Example 6-1 Using Help

```
n1000v# show interface virtual ?
  <CR>
  >              Redirect it to a file
  module         Limit display to interfaces on module
  port-mapping   Show hypervisor port mapping
  vm             Show interfaces owned by a Virtual Machine
  vmk            Show interfaces owned by the Virtual Machine Kernel
  vswif          Show interfaces owned by the Virtual Service Console
  |              Pipe command output to filter
n1000v# show interface module ?
                              ^
% invalid command detected at '^' marker.
n1000v# <Ctrl-P>
n1000v# show interface virtual ?
n1000v# show interface virtual module ?
  <1-256>  Enter module number

n1000v# show interface virtual module ?
  <1-256>  Enter module number

n1000v# show interface virtual module 3

------------------------------------------------------------------------------
Port        Adapter        Owner                    Mod Host
------------------------------------------------------------------------------
n1000v# show module ?
  <CR>
  <1-32>    Enter module number
  >         Redirect it to a file
  internal  Show line card manager related info
  uptime    Show how long the module has been up and running
  |         Pipe command output to filter

n1000v# show module
show module
Mod  Ports  Module-Type                      Model              Status
---  -----  --------------------------------- ------------------ ------------
```

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

```
1    0      Virtual Supervisor Module        Nexus1000V         ha-standby
2    0      Virtual Supervisor Module        Nexus1000V         active *
3    248    Virtual Ethernet Module          NA                 ok
4    248    Virtual Ethernet Module          NA                 ok

Mod  Sw               Hw
---  ---------------  ------
1    4.0(4)SV1(0.33)  0.0
2    4.0(4)SV1(0.33)  0.0
3    4.0(4)SV1(0.33)  0.4
4    4.0(4)SV1(0.33)  0.4

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
2    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
3    02-00-0c-00-03-00 to 02-00-0c-00-03-80  NA
4    02-00-0c-00-04-00 to 02-00-0c-00-04-80  NA

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
1    10.78.1.99       NA                                    NA
2    10.78.1.99       NA                                    NA
3    10.78.1.92       8aca99de-16b7-300b-b572-730ea83c3de7  10.78.1.92
4    10.78.1.93       44454c4c-4800-104e-804d-b7c04f563153  10.78.1.93


* this terminal session
```

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

CHAPTER 7

Configuring the Terminal

This chapter provides information about configuring the terminal in the following topics:

- Information about the Terminal, page 7-1
- Setting the Screen Length for the Console Terminal, page 7-2
- Setting the Screen Width for the Console Terminal, page 7-2
- Displaying Terminal Settings, page 7-3
- Setting the Timeout for Console Connections, page 7-3
- Setting the Timeout for SSH and Telnet Connections, page 7-4
- Clearing a Line Connection to the Switch, page 7-5
- Setting a Timeout for the Current Session, page 7-5

Information about the Terminal

You can configure the terminal type, display, timeout, and other settings for the console terminal.

Defining a Terminal Type

You can use this procedure to define the type of terminal to use for the switch.

BEFORE YOU BEGIN

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

- You are logged in to a terminal session with the CLI in EXEC mode.

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

DETAILED STEPS

	Command	Purpose

Step 1	**terminal terminal-type** *type*
	Example:
	`n1000v# terminal terminal-type vt100`
	`n1000v#`
		Configures a terminal type for the switch.
		• Valid types = vt100, xterm, etc.
		• Default = vt100
		• Maximum string length = 80 characters
		If an unknown terminal type is used for a Telnet or SSH session, then the switch uses the default, vt100.

Setting the Screen Length for the Console Terminal

You can use this procedure to set the number of lines to display on the screen duirng the current console session.

BEFORE YOU BEGIN

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

- This procedure only applies to the console port. Telnet and SSH sessions set the terminal length automatically.
- You are logged in to a terminal session with the CLI in EXEC mode.

DETAILED STEPS

	Command	Purpose

Step 1	**terminal length** *number of lines*
	Example:
	`n1000v# terminal length 20`
	`n1000v#`
		Configures the number of lines to display on the screen for the current console session.
		• Range = 0 to 511 lines
		• Default = 24 lines
		• Disable = 0 (scrolls continuously)

Setting the Screen Width for the Console Terminal

You can use this procedure to set the number of characters to display on a screen line during the current console session.

BEFORE YOU BEGIN

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

- This procedure only applies to the console port. Telnet and SSH sessions set the terminal width automatically.

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

- You are logged in to a terminal session with the CLI in EXEC mode.

DETAILED STEPS

	Command	Purpose

Step 1	**terminal width** *number of characters*
	Example:
	`n1000v# terminal width 86`
	`n1000v#`
		Configures the number of characters to display on each line for the current console session.
		• Range = 24 to 511 characters
		• Default = 88 characters

Displaying Terminal Settings

You can use this procedure to display the terminal settings for the current session.

BEFORE YOU BEGIN

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

- You are logged in to a terminal session with the CLI in any command mode.

DETAILED STEPS

	Command	Purpose

Step 1	**show terminal**
	Example:
	`n1000v# show terminal`
	`TTY: /dev/pts/8 type: "vt100"`
	`Length: 24 lines, Width: 88 columns`
	`Session Timeout: None`
	`n1000v#`
		Displays the terminal settings for the current session.

Setting the Timeout for Console Connections

You can use this procedure to specify the duration of time, in minutes, that an inactive console session remains open.

BEFORE YOU BEGIN

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

- You are logged in to a terminal session with the CLI in EXEC mode.

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

DETAILED STEPS

	Command	Purpose

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

Step 2	**line console**
	Example:
	`n1000v(config)# line console`
	`n1000v(config-console)#`
		Enters the Console Configuration mode.

Step 3	**exec-timeout** *minutes*
	Example:
	`n1000v(config-console)# exec-timeout 60`
	`n1000v(config-console)#`
		Configures the duration of time, in minutes, that an inactive console session remains open. If the session remains inactive longer than this specified time period, then it is automatically closed.
		• Range = 0 to 525, 600 minutes
		• Default = 30 minutes
		• Disable (no timeout) = 0 minutes
		If you set the timeout to zero, then the console connection remains alive until you close it.

Setting the Timeout for SSH and Telnet Connections

You can use this procedure to specify the duration of time, in minutes, that an inactive SSH or Telnet session remains open.

BEFORE YOU BEGIN

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

- You are logged in to a terminal session with the CLI in EXEC mode.

DETAILED STEPS

	Command	Purpose

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

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

	Command	Purpose

Step 2	**line vty**
	Example:
	`n1000v(config)# line vty`
	`n1000v(config-line)#`
		Enters the Virtual Terminal Line Configuration mode.

Step 3	**exec-timeout** *minutes*
	Example:
	`n1000v(config-line)# exec-timeout 60`
	`n1000v(config-line)#`
		Configures the duration of time, in minutes, that an inactive Telnet or SSH session remains open. If the session remains inactive longer than this specified time period, then it is automatically closed.
		• Range = 0 to 525, 600 minutes
		• Default = 30 minutes
		• Disable (no timeout) = 0 minutes
		If you set the timeout to zero, then the line connection remains alive until you close it.

Clearing a Line Connection to the Switch

You can use this procedure to close a specific line connection to the switch.

BEFORE YOU BEGIN

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

- You are logged in to a terminal session with the CLI in EXEC mode.

DETAILED STEPS

	Command	Purpose

Step 1	**clear line aux**
	Example:
	`n1000v# clear line aux`
	`n1000v #`
		Closes a line connection.

Setting a Timeout for the Current Session

You can use this procedure to establish a maximum duration of time, in minutes, that the current terminal session can remain open before the switch shuts it down.

BEFORE YOU BEGIN

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

- You are logged in to a terminal session with the CLI in EXEC mode.

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

DETAILED STEPS

	Command	Purpose

Step 1	**terminal session** *minutes*
	
	Example:
	`n1000v# terminal session 600`
	`n1000v#`
		Configures the duration of time, in minutes, that the current terminal session can remain open before the switch shuts it down.
		• Range = 0 to 525, 600 minutes
		• Disable (no timeout) = 0 minutes
		This change is not saved in the configuration file since it only appies to the current session.

CHAPTER 8

Configuration Limits

This section lists the Cisco Nexus 1000V configuration limits.

Component	Supported Limit	
Maximum Modules	66	
Virtual Ethernet (VEM)	64	
Virtual Supervisor (VSM)	2	
Hosts	64	
Active VLANs across all VEMs	512	
MACs over VLAN within a VEM	1024 (1K)	
vEthernet interfaces per port profile	1024 (1K)	
PVLAN	512	
	Per DVS	**Per Host**
Virtual Service Domains (VSD)	64	6
VSD Interfaces	2048	214
vEthernet interfaces	2K	216
Port Profiles	256	—
System Port Profiles	—	16
Port Channel	256	8
Physical Trunks	512	—
Physical NICs	—	32
vEthernet Trunks	256	8
ACL	128	16[1]
ACEs per ACL	128	16[1]
ACL Interfaces	2048	256
NetFlow Policies	32	8
NetFlow Interfaces	256	32
SPAN/ERSPAN Sessions	64	4
QoS Policy-Map	128	16

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

Component	Supported Limit	
QoS Class-Map	1024	128
QoS Interfaces	2048	256
Port Security	1600	216
MultiCast Groups	512	64

1. This number can be exceeded if VEM has available memory.

CHAPTER 9

List of Terms

The following terminology is used in the Cisco Nexus 1000V implementation.

Table 9-1 Cisco Nexus 1000V Terminology

Term	Description
Control VLAN	One of two VLANs for the communication between VSM and VEM. The control VLAN is used to exchange control messages. The network administrator configures the control VLAN. See packet VLAN.
Distributed Resource Scheduler (DVS)	Balances the workload across your defined resources (hosts, shared storage, network presence, and resource pools) in a cluster.
Distributed Virtual Switch (DVS)	This is a logical switch that spans one or more VMware ESX 4.0 servers. It is controlled by one VSM instance.
ESX/ESXi	A virtualization platform used to create the virtual machines as a set of configuration and disk files that together perform all the functions of a physical machine. Each ESX/ESXi host has a VI Client available for management use. If your ESX/ESXi host is registered with the vCenter Server, a VI Client that accommodates the vCenter Server features is available.
Managed Object Browser (MOB)	A tool that enables you to browse managed objects on VirtualCenter Server and ESX Server systems.
Network Interface Card (NIC)	Network Interface Card.
Open Virtual Appliance or Application (OVA) file	The package that contains the following files used to describe a virtual machine and saved in a single archive using .TAR packaging. • Descriptor file (.OVF) • Manifest (.MF) and certificate files (optional)
Open Virtual Machine Format (OVF)	A platform independent method of packaging and distributing virtual machines.
Packet VLAN	One of two VLANs for the communication between VSM and VEM. The packet VLAN forwards relevant data packets, such as CDP, from the VEM to the VSM. The network administrator configures the packet VLAN. See control VLAN.
vCenter Server	A service that acts as a central administrator for VMware ESX/ESXi hosts that are connected on a network. vCenter Server directs actions on the virtual machines and the virtual machine hosts (the ESX/ESXi hosts).

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

Table 9-1 Cisco Nexus 1000V Terminology (continued)

Term	Description
Virtual Ethernet Module (VEM)	This is the part of Cisco Nexus 1000V that actually switches data traffic. It runs on a VMware ESX 4.0 host. Up to 64 VEMs are controlled by one VSM. All the VEMs that form a switch domain should be in the same virtual Data Center as defined by VMware vCenter Server.
Virtual Machine (VM)	A virtualized x86 PC environment in which a guest operating system and associated application software can run. Multiple virtual machines can operate on the same host system concurrently.
Vmotion	The practice of migrating virtual machines live from server to server.
Virtual Supervisor Module (VSM)	This is the control software of the Cisco Nexus 1000V distributed virtual switch. It runs on a virtual machine (VM) and is based on Cisco NX-OS.
VMware Infrastructure Bundle (VIB)	The package format used by VMware ESX 4.0 release.
VMware update manager (VUM)	The software application that manages Cisco Nexus 1000V software installation and VEM upgrades. **Note** VUM is not a requirement. Software can be installed manually without using VUM.
vSphere Client	The user interface that lets users connect remotely to the vCenter Server or ESX/ESXi from any windows PC. The primary interface for creating, managing, and monitoring virtual machines, their resources, and their hosts. It also provides console access to virtual machines.

INDEX

Symbols

^Z to exit current command mode and return to exec 6-4

A

add host to DVS
    CLI setup 4-21
authentication, vCenter Server, GUI setup 3-4

C

CLI
    command modes 6-2
    command prompt 6-1
    setting delay time 6-14
    software setup 4-1
    variables
        in command scripts 6-13
        persistent variables 6-11
        session-only variables 6-10
        system-defined variables 6-12
command
    mode
        EXEC 6-3
        global configuration 6-3
        how to exit 6-4
        information about 6-2
        summary of all 6-5
    no 6-9
    prompts 6-5
    scripts 6-13
connectivity, verify 4-7
connect to vCenter Server
    CLI setup 4-9
context-sensitive help, check syntax for 6-14
control and packet VLAN
    CLI setup 4-6

D

data port profile, CLI setup 4-18
default gateway
    CLI setup 4-5
default VLAN 2-6
description command 4-13, 4-16, 4-19
documentation
    additional publications 1-xi
domain ID, VSM
    CLI setup 4-4

E

end command 6-4
EXEC commands 6-3
exit a command mode 6-4
exit command 6-4

F

features, new and changed (table) 1-iii

G

global configuration mode, about 6-3
GUI, software setup 3-1

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

H

HA role
CLI setup 4-4
host, add to DVS
CLI setup 4-21

I

IP connectivity, verify 4-7

M

mgmt0
CLI setup 4-5
modes, command 6-5

N

network administrator role 1-5
no command form 6-9
NTP
CLI setup 4-6
numbering, VLANs 2-6

P

password
vCenter Server, GUI setup 3-4
VSM setup, GUI 3-3
plug-in, create on vCenter Server, CLI setup 4-8
primary role, VSM 3-9
prompt, command 6-1
prompts, command 6-5

R

related documents 1-xi
reserved VLANs 2-6
role
HA (standalone, primary, secondary) 3-9
network administrator 1-5
server administrator 1-5

S

same host for VEM and VSM 5-1
secondary role, VSM 3-9
secure http, GUI setup 3-4
server administrator role 1-5
software setup
CLI 4-1
GUI 3-1
SSH
CLI setup 4-5
standalone role, VSM 3-9
supervisor modules
role- primary, secondary, standalone 3-9
switch name
CLI setup 4-5
syntax check 6-14
system port profile
CLI setup 4-11

T

Telnet
CLI setup 4-5
time
setting delay in CLI 6-14

U

unusable VLANs 2-6
uplink port profile
CLI setup 4-15

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

V

vCenter identification, GU setupI 3-4
VEM
  and VSM on same host 5-1
  feature level
    CLI setup 4-6
verify IP connectivity 4-7
VLAN
  how to create 2-5
  numbering 2-6
  setup, GUI 3-5
VMotion 1-6
VSM
  and VEM on same host 5-1
  credentials
    CLI setup 4-4
    GUI setup 3-3
  host, GUI setup 3-4

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