



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



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

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-22813-01

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 4.2(1) SV1(4)
© 2011 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 by release.

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

- [Release Notes](#).
- [Command Reference](#).

Table 1 *New and Changed Getting Started Information*

Feature	Description	Changed in Release	Where Documented
Configuration Limits	Updated Cisco Nexus 1000V configuration limits.	4.2(1)SV1(4)	Chapter 8, “Configuration Limits”
GUI Setup procedures	GUI application enhancements: <ul style="list-style-type: none"> • New configuration file option. • Secondary VSM configuration option. • New Layer 3 configuration option. • New HA configuration option. 	4.2(1)SV1(4)	“Configuring the Software Using the GUI”
CLI Setup procedures	CLI application enhancement: <ul style="list-style-type: none"> • New HTTP server option. 	4.2(1)SV1(4)	“Configuring the Software Using the CLI”
Displaying Available Features	Show command for displaying available features and whether they are enabled.	4.2(1)SV1(4)	“Understanding the CLI”
GUI Setup procedures	GUI application enhancements: <ul style="list-style-type: none"> • Migrates host, port groups, and PNICs. • Creates port profiles. • Migrates VSM to its own VEM. • Adds the host to the DVS. 	4.0(4)SV1(3)	“Configuring the Software Using the GUI”
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”

[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

Table 1 ***New and Changed Getting Started Information (continued)***

Feature	Description	Changed in Release	Where Documented
CLI Setup procedures	The procedures for setting up the Cisco Nexus 1000V using the CLI have been moved into this document from the <i>Cisco Nexus 1000V Software Installation Guide, Release 4.2(1)SV1(4)</i> .	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”



C O N T E N T S

New and Changed Information iii

Preface v

Audience v

Recommended Reading v

Document Organization vi

Document Conventions vi

Available Documents vii

Obtaining Documentation and Submitting a Service Request ix

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

Information About Setting Up the Software 2-1

 Setting up a Configuration File 2-1

Guidelines and Limitations 2-2

Prerequisites 2-3

Software Configuration Process 2-7

 Creating VLANs 2-7

Verifying the Configuration 2-10

Starting the VMs 2-11

Implementation Guidelines 2-12

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

Configuring the Software Using the GUI 3-1

- Information About the GUI Application 3-1
- GUI Software Configuration Process 3-2
- Guidelines and Limitations 3-2
- Setting Up a Primary or Standalone VSM VM Using the GUI 3-3
- Setting Up a Secondary VSM 3-14
- Setting Up a VSM with a Copy of a Configuration File 3-17
 - Preparing a Configuration File 3-17
 - Example Configuration File 3-19
 - Applying the Configuration File 3-20

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 4-7
 - Connecting to the vCenter Server 4-9
 - Creating Required Port Profiles 4-11
 - Configuring the System Port Profile for VSM-VEM Communication 4-12
 - Example Configuration: System Profile for Critical Ports 4-15
 - Configuring the Uplink Port Profile for VM Traffic 4-16
 - Example Configuration: Uplink Profile for VM Traffic 4-18
 - Configuring the Data Port Profile for VM Traffic 4-19
 - Example Configuration: Data Profile for VM Traffic 4-21
 - Adding an ESX 4.0 Host to the DVS 4-22

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
- Example Configuration for VSM and VEM on the Same Host 5-4

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

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

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
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
Displaying Available Features	6-17
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

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



Preface

This Getting Started Guide shows you how to create a configuration file for your Cisco Nexus 1000V, and provides enough information about the system to get you started configuring and using it in your datacenter.

This preface describes the following aspects of this document:

- [Audience, page v](#)
- [Recommended Reading, page v](#)
- [Document Organization, page vi](#)
- [Document Conventions, page vi](#)
- [Available Documents, page vii](#)
- [Obtaining Documentation and Submitting a Service Request, page ix](#)

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 4.2(1) SV1(4)* (this document)
- *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4)*
- *Cisco Nexus 1000V Software Installation Guide, Release 4.2(1)SV1(4)*
- *Cisco Nexus 1000V Virtual Ethernet Module Software Installation Guide, Release 4.2(1)SV1(4)* (server administrators)

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

- *Cisco VN-Link: Virtualization-Aware Networking* white paper

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 how to use the GUI Application to setup a configuration file.
Chapter 4, “Configuring the Software Using the CLI”	Describes how to use 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 9, “List of Terms”	Lists and defines terminology used in the Cisco Nexus 1000V implementation.
Chapter 8, “Configuration Limits”	Lists the Cisco Nexus 1000V configuration limits.

Document Conventions

Command descriptions use these conventions:

boldface font	Commands and keywords are in boldface.
<i>italic font</i>	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:

<code>screen font</code>	Terminal sessions and information the device displays are in screen font.
<code>boldface screen font</code>	Information you must enter is in boldface screen font.

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

<i>italic screen font</i>	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions for notes and cautions:



Note

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



Caution

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

Available Documents

This section lists the documents used with the Cisco Nexus 1000 and available on [Cisco.com](http://www.cisco.com) at the following url:

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

General Information

[Cisco Nexus 1000V Documentation Roadmap, Release 4.2\(1\)SV1\(4\)](#)

[Cisco Nexus 1000V Release Notes, Release 4.2\(1\)SV1\(4\)](#)

[Cisco Nexus 1000V Compatibility Information, Release 4.2\(1\)SV1\(4\)](#)

[Cisco Nexus 1010 Management Software Release Notes, Release 4.2\(1\)SP1\(2\)](#)

Install and Upgrade

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

[Cisco Nexus 1000V Software Upgrade Guide, Release 4.2\(1\)SV1\(4\)](#)

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

[Cisco Nexus 1010 Virtual Services Appliance Hardware Installation Guide](#)

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

Configuration Guides

[Cisco Nexus 1000V License Configuration Guide, Release 4.2\(1\)SV1\(4\)](#)

[Cisco Nexus 1000V Getting Started Guide, Release 4.2\(1\)SV1\(4\)](#)

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

[Cisco Nexus 1000V Interface Configuration Guide, Release 4.2\(1\)SV1\(4\)](#)

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

[Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2\(1\)SV1\(4\)](#)
[Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2\(1\)SV1\(4\)](#)
[Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.2\(1\)SV1\(4\)](#)
[Cisco Nexus 1000V Security Configuration Guide, Release 4.2\(1\)SV1\(4\)](#)
[Cisco Nexus 1000V System Management Configuration Guide, Release 4.2\(1\)SV1\(4\)](#)
[Cisco Nexus 1010 Software Configuration Guide, Release 4.2\(1\)SP1\(2\)](#)

Programming Guide

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

Reference Guides

[Cisco Nexus 1000V Command Reference, Release 4.2\(1\)SV1\(4\)](#)
[Cisco Nexus 1000V MIB Quick Reference](#)
[Cisco Nexus 1010 Command Reference, Release 4.2\(1\)SP1\(2\)](#)

Troubleshooting and Alerts

[Cisco Nexus 1000V Troubleshooting Guide, Release 4.2\(1\)SV1\(4\)](#)
[Cisco Nexus 1000V Password Recovery Guide](#)
[Cisco NX-OS System Messages Reference](#)

Virtual Security Gateway Documentation

[Cisco Virtual Security Gateway for Nexus 1000V Series Switch Release Notes, Release 4.2\(1\)VSG\(1\)](#)
[Cisco Virtual Security Gateway, Release 4.2\(1\)VSG1\(1\) and Cisco Virtual Network Management Center, Release 1.0.1 Installation Guide](#)
[Cisco Virtual Security Gateway for Nexus 1000V Series Switch License Configuration Guide, Release 4.2\(1\)VSG1\(1\)](#)
[Cisco Virtual Security Gateway for Nexus 1000V Series Switch Configuration Guide, Release 4.2\(1\)VSG1\(1\)](#)
[Cisco Virtual Security Gateway for Nexus 1000V Series Switch Command Reference, Release 4.2\(1\)VSG1\(1\)](#)

Virtual Network Management Center

[Release Notes for Cisco Virtual Network Management Center, Release 1.0.1](#)
[Cisco Virtual Security Gateway, Release 4.2\(1\)VSG1\(1\) and Cisco Virtual Network Management Center, Release 1.0.1 Installation Guide](#)
[Cisco Virtual Network Management Center CLI Configuration Guide, Release 1.0.1](#)
[Cisco Virtual Network Management Center GUI Configuration Guide, Release 1.0.1](#)
[Cisco Virtual Network Management Center XML API Reference Guide, Release 1.0.1](#)

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

Network Analysis Module Documentation

[Cisco Network Analysis Module Software Documentation Guide, 4.2](#)

[Cisco Nexus 1000V NAM Virtual Service Blade Installation and Configuration Guide](#)

[Network Analysis Module Command Reference Guide, 4.2](#)

[User Guide for the Cisco Network Analysis Module Virtual Service Blades, 4.2](#)

[Cisco Network Analysis Module Software Release Notes, 4.2](#)

Obtaining Documentation and Submitting a Service Request

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

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

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

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



CHAPTER 1

Overview

This chapter provides an overview of 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.

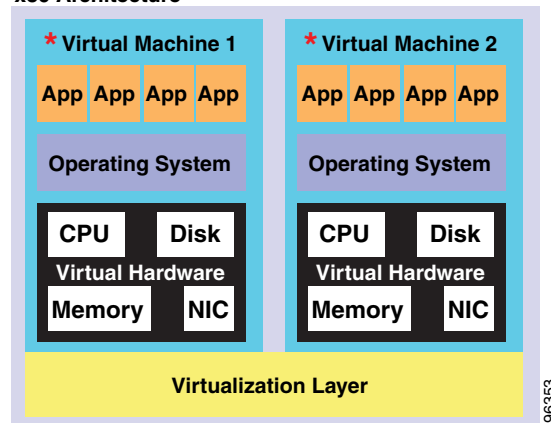
Virtual machines are encapsulated into files, for rapid saving, copying and provisioning. Full systems (fully configured applications, operating systems, BIOS and virtual hardware) can be moved, within seconds, from one physical server to another for zero-downtime maintenance and continuous workload 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 consistent, normalized set of hardware.
- Both hardware and software are encapsulated in a single file for rapid copying, provisioning, and moving between physical servers.

x86 Architecture



196353

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](#)

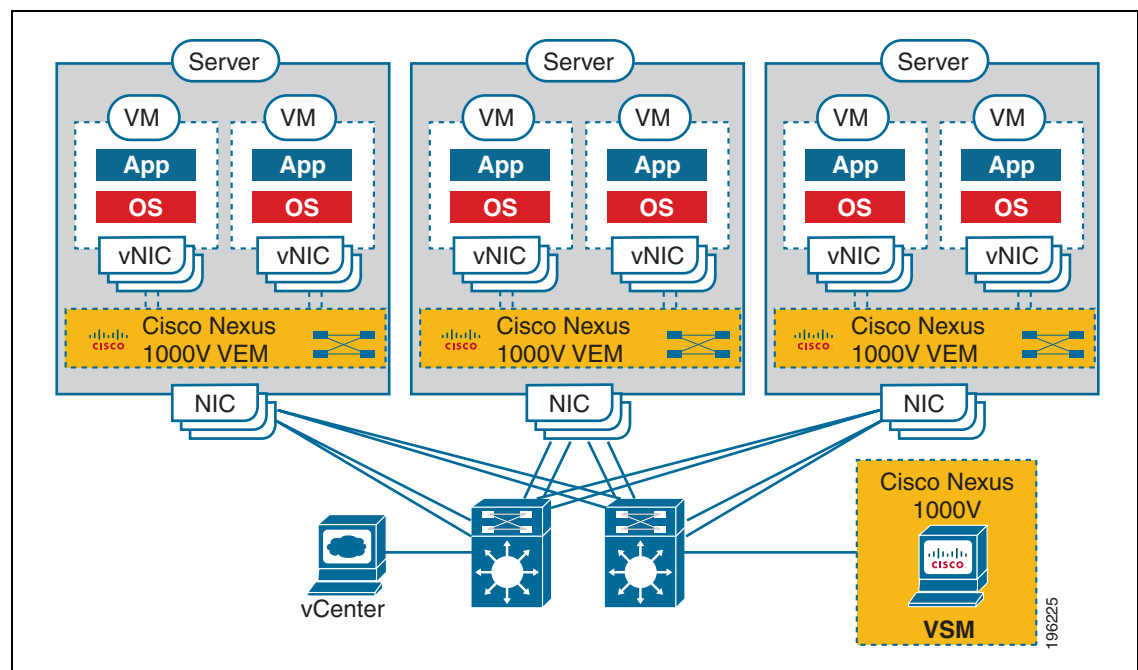
System Description

The Cisco Nexus 1000V is a virtual access software switch that works with VMware vSphere 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.

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 system login, configuration, and corresponds to the mgmt0 interface. The management interface 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 VLANs are used as follows:

- 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.
 - VSM active to standby synchronization for high availability.

You can use the same VLAN for control, packet, and management, but if needed for flexibility, you can use separate VLANs. Make sure that the network segment has adequate bandwidth and latency.

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 specifies a set of attributes that can include the following:

- VLAN
- port channels
- private VLAN (PVLAN),
- ACL
- port security
- NetFlow
- rate limiting
- QoS marking

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

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 4.2(1)SV1(4)*.

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.



Note

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

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

To delete a system VLAN, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4)*.

Administrator Roles

The Cisco Nexus 1000V enables network and server administrators to collaborate 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
<ul style="list-style-type: none"> Creates, configures, and manages vSwitches. Creates, configures, and manages port profiles, including the following: <ul style="list-style-type: none"> security port channels QOS policies 	<ul style="list-style-type: none"> Assigns the following to port groups: <ul style="list-style-type: none"> vNICs vmkernel interfaces service console interfaces Assigns physical NICs (also called PNICs).

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.](mailto: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.
- Using a VSM VM snapshot is not recommended. VSM VM snapshots do not contain unsaved configuration changes.
- 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 and 4.1. (requires Enterprise Plus license edition of vSphere 4)

For detailed information, see the *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(4)* 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 create and save an initial Cisco Nexus 1000V configuration file using either the GUI or CLI setup dialog.



Note

To install the Cisco Nexus 1000V software on your ESX or ESXi VMware server, see the *Cisco Nexus 1000V Software Installation Guide, Release 4.2(1)SV1(4)*.

This chapter includes the following topics:

- [Prerequisites, page 2-3](#)
- [Software Configuration Process, page 2-7](#)
- [Verifying the Configuration, page 2-10](#)
- [Starting the VMs, page 2-11](#)
- [Implementation Guidelines, page 2-12](#)

Information About Setting Up the Software

After you have installed the Cisco Nexus 1000V software and powered on the VM, a setup configuration dialog starts automatically. This setup configuration dialog is available in either the CLI or GUI and helps you configure the initial configuration file that was created during installation of the software. You can use the procedures in this document and the setup configuration to complete the Cisco Nexus 1000V configuration.



Note

To install the Cisco Nexus 1000V software on your ESX or ESXi VMware server, see the *Cisco Nexus 1000V Software Installation Guide, Release 4.2(1)SV1(4)*.

Setting up a Configuration File

Both the CLI and GUI setup dialog prompt you to create an initial configuration file that includes the following minimal configuration:

- Administrative user and password
- Domain ID
- HA Role

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

- Switch name
- Management 0 interface IP address and netmask
- Telnet and SSH
- VEM feature level
- VLAN for system login and configuration, and control and packet traffic

If you use the configuration GUI, the software also prompts you to do the following in the initial configuration file:

- Create port profiles for the following:
 - control, management, and packet port groups
 - uplinks
 - VMware kernel NICs
- Migrate the following:
 - VMware port group or kernel NICs to the correct port-profile.
 - PNIC from the VMware vSwitch to the correct uplink on the DVS.
- Create and register a Cisco Nexus 1000V plug-in on the vCenter server.
- Add the host to the Cisco Nexus 1000V DVS.

Guidelines and Limitations

The following guidelines and limitations apply to setting up the Cisco Nexus 1000V.

- 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 4.2(1)SV1(4)*.



Caution

A disruption in the broadcast packets between the VSM and VEMs can occur if the following are improperly configured on the ports that carry control or packet traffic:

storm-control broadcast
storm-control multicast



Caution

The VSM VM configuration will fail unless the NICs are specified as shown in [Table 2-1](#).

Table 2-1 Required NIC Configuration

NICs	Traffic	Description	VLAN numbering used in example ¹
First	Control	e1000	260

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

Table 2-1 Required NIC Configuration (continued)

NICs	Traffic	Description	VLAN numbering used in example ¹
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 2-6](#).

- When installing the Cisco Nexus 1000 in a VMware cluster with DRS enabled, all ESX hosts must be migrated to the Cisco Nexus 1000 DVS. If only some hosts are migrated it is possible that VMs could be installed or moved to hosts in which the vSwitch is missing VLANs, physical adapters, or both.
- For a complete list of port profile guidelines and limitations, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4)*.

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 4.2(1)SV1(4)*.
 - 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 2-6](#) illustrating a sample Cisco Nexus 1000V setup.
- 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.

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

- 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 2-12.
- You have already identified the HA role for this VSM from those listed in [Table 2-2](#):

Table 2-2 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 4.2(1)SV1(4)*.

- When you set up the Cisco Nexus 1000V software, you are required to create an administrator password. [Table 2-3](#) lists password strength guidelines:

Table 2-3 Guidelines for strong passwords

Strong passwords have:	Strong passwords do NOT have:
<ul style="list-style-type: none"> • At least eight characters • Uppercase letters • Lowercase letters • Numbers • Special characters <p>Note Clear text passwords cannot include the dollar sign (\$) special character.</p>	<ul style="list-style-type: none"> • 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.
- 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 physical NIC.

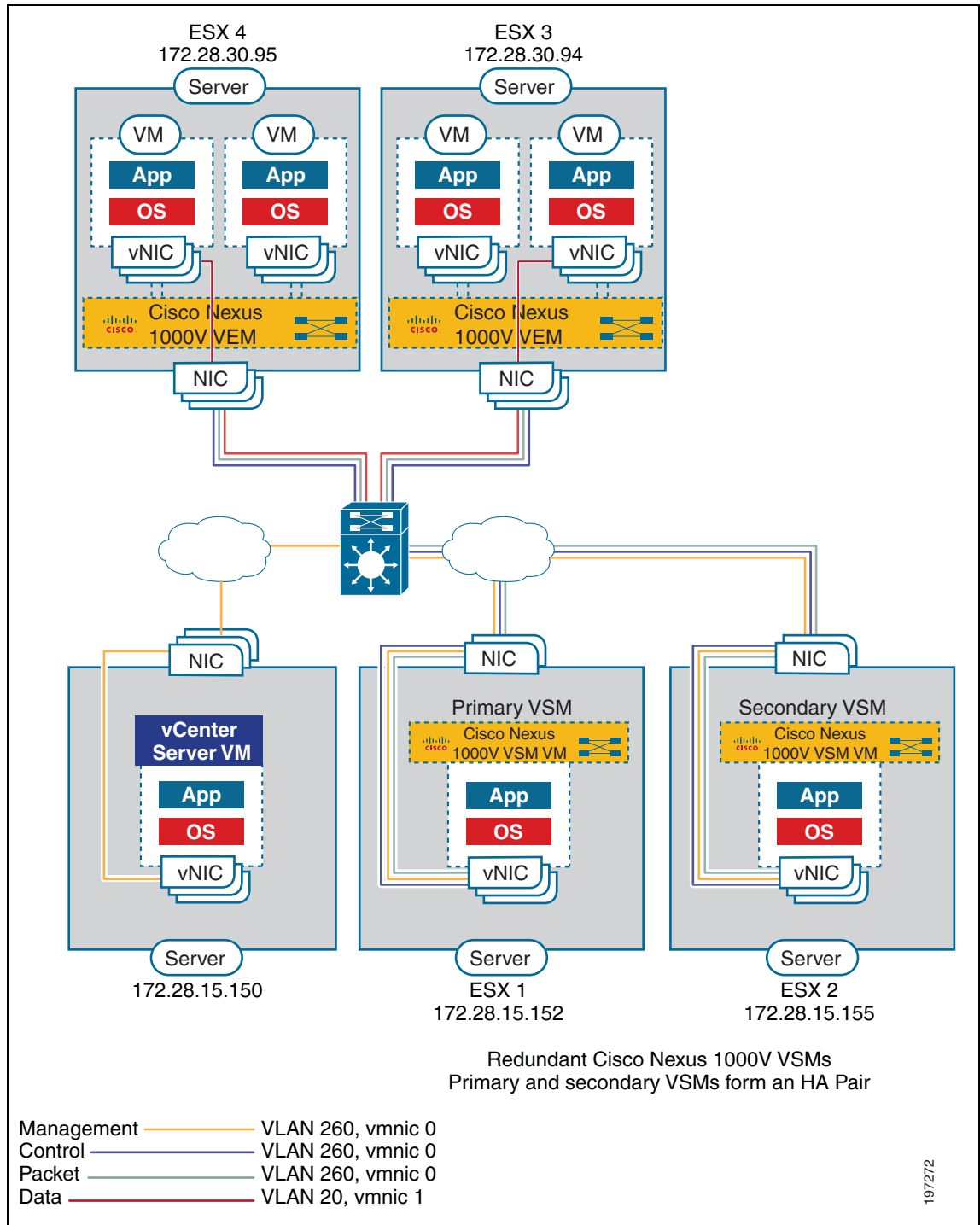
Send document comments to nexus1k-docfeedback@cisco.com.

- In an installation where multiple Ethernet port profiles are active on the same VEM, it is recommended that they do not carry the same VLAN(s). The allowed VLAN list should be mutually exclusive. Overlapping VLANs can be configured but may cause duplicate packets to be received by virtual machines in the network.
- 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.

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 guides you through the setup 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: <ul style="list-style-type: none">• If you are using the GUI application to set up your software, then see the “GUI Software Configuration Process” section on page 3-2.• 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 2-10 . |
| Step 3 | Start the VMs. See the “Starting the VMs” procedure on page 2-11 . |
| Step 4 | Do one of the following: <ul style="list-style-type: none">• If both the VSM and VEMs are working as expected, continue with the next step.• If not, then see the <i>Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(4)</i>. |
| Step 5 | Continue your implementation. See the “Implementation Guidelines” section on page 2-12 . |
| 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-VEM 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	<p>You can create, name, and use these VLANs. You cannot change the following parameters:</p> <ul style="list-style-type: none"> • State is always active. • VLAN is always enabled. You cannot shut down these VLANs. <p>Note The extended system ID is always automatically enabled.</p>
3968–4047 and 4094	Internally allocated	<p>You cannot use, create, delete, or modify these VLANs. You can display these VLANs.</p> <p>Cisco Nexus 1000V allocates these 80 VLANs, plus VLAN 4094, for features, like diagnostics, that use internal VLANs for their operation.</p>

- You can use the same VLAN for control, packet, and management, but if needed for flexibility, you can use separate VLANs. Make sure that the network segment has adequate bandwidth and latency.
- 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 4.2(1)SV1(4)*.
 - 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 4.2(1)SV1(4)*.

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} Example: n1000v(config)# vlan 5 n1000v(config-vlan)# Example: n1000v# config t n1000v(config)# vlan 15-20 n1000v(config-vlan)#	<p>Creates, and saves in the running configuration, a VLAN or a range of VLANs.</p> <p>Note If you enter a VLAN ID that is already assigned, you are placed into the VLAN configuration mode for that VLAN.</p> <p>Note If you enter a VLAN ID that is assigned to an internally allocated VLAN, the system returns an error message.</p> <p>Note From the VLAN configuration mode, you can also create and delete VLANs.</p> <p>To configure the VLAN further, see the <i>Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SVI(4)</i>.</p> <p>This example shows VLAN 5 being created.</p> <p>The VLAN is activated and you are automatically placed into a submode for configuring VLAN 5.</p> <p>This example shows the range, VLAN 15-20, being created.</p> <p>The VLANs in the range are activated, and you are automatically placed into a submode for configuring VLAN 15-20.</p> <p>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.</p>
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.
<p>You have completed this procedure. Return to the configuration process that pointed you here:</p> <ul style="list-style-type: none"> • GUI Software Configuration Process, page 3-2. • 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          ha-standby
2    0      Virtual Supervisor Module  Nexus1000V          active *
3    248    Virtual Ethernet Module    NA                   ok

Mod  Sw                Hw
---  ---
1    4.2(1)SV1(4)      0.0
2    4.2(1)SV1(4)      0.0
3    4.2(1)SV1(4)      VMware ESXi 4.0.0 Releasebuild-208167 (2.0)

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

Mod  Server-IP          Server-UUID                Server-Name
---  ---
1    172.28.15.152      NA                          NA
2    172.28.15.152      NA                          NA
3    172.28.30.94       89130a67-e66b-3e57-ad25-547750bcfc7e  localhost.

* this terminal session
n1000v#
  
```

```

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

Mod  Status          UUID                                License Status
---  ---
3    powered-up      0b0a1871-1fd9-3c1d-b3c6-a097c7a1e714  licensed
  
```

Step 2 Do one of the following:

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

- 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 4.2(1)SV1(4)*.

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 virtual usage
```

Port Profile	Port	Adapter	Owner
nlkv-uplink0	Po1		
Eth3/2	vmnic1		localhost.
Eth3/3	vmnic2		localhost.
vlan1767	Veth7	Net Adapter 1	all-tool-7
Veth8		Net Adapter 1	all-tool-8
aipc1765	Veth4	Net Adapter 1	bl-h-s
inband1766	Veth6	Net Adapter 3	bl-h-s
mgmt1764	Veth5	Net Adapter 2	bl-h-s
vpc-mac-uplink	Po7		
Eth5/2	vmnic1		localhost.
Eth5/3	vmnic2		localhost.
ch-vpc-mac-uplink	Po2 Po3		
ch-aipc1765	Veth1	Net Adapter 1	bl-h-p
ch-mgmt1764	Veth2	Net Adapter 2	bl-h-p
ch-inband1766	Veth3	Net Adapter 3	bl-h-p

```
n1000v#
```

Step 4 You have completed this procedure.
Return to the [Software Configuration Process, page 2-7](#).

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.
- For a detailed description of the system, see the *Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(4)*.

DETAILED STEPS

Step 1 Create the VMs for the datacenter servers which get their connectivity through the Cisco Nexus 1000V.

Step 2 Edit VM settings on the vSphere Client so that their network adapters are in the port profile 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 2-7](#).

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 4.2(1)SV1(4)*.
- 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 4.2(1)SV1(4)*
 - *Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4)*
- 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 4.2(1)SV1(4)*.
- 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
- When installing the Cisco Nexus 1000 in a VMware cluster with DRS enabled, all ESX hosts must be migrated to the Cisco Nexus 1000 DVS. If only some hosts are migrated it is possible that VMs could be installed or moved to hosts in which the vSwitch is missing VLANs, physical adapters, or both.



CHAPTER 3

Configuring the Software Using the GUI

This chapter describes how to use the GUI application to complete the Cisco Nexus 1000V configuration, and includes the following sections.

- [GUI Software Configuration Process, page 3-2](#)
- [Guidelines and Limitations, page 3-2](#)
- [Setting Up a Primary or Standalone VSM VM Using the GUI, page 3-3](#)
- [Setting Up a Secondary VSM, page 3-14](#)
- [Setting Up a VSM with a Copy of a Configuration File, page 3-17](#)

Information About the GUI Application

You can use the GUI application, after the software is installed, to complete the following Cisco Nexus 1000V configuration for a standalone, or primary and secondary VSM. The GUI application uses the options you chose during VSM installation to determine which configuration steps are required.

- Create port profiles for the Control, Management, and Packet port groups:
- Create uplink port profiles.
- Create port profiles for VMware kernel NICs.
- Specify a VLAN to be used for system login and configuration, and control and packet traffic.



Note

You can use the same VLAN for control, packet, and management, but if needed for flexibility, you can use separate VLANs. If you use the same VLAN, make sure that the network segment where it resides has adequate bandwidth and latency.

- Enable Telnet and SSH and configure an SSH connection.
- Create a Cisco Nexus 1000V plug-in and register it on the vCenter server.
- Migrate each VMware port group or kernel NIC to the correct port-profile.
- Migrate each PNIC from the VMware vSwitch to the correct uplink on the DVS.
- Add the host to the DVS.

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

**Note**

If you install the Cisco Nexus 1000 in a VMware cluster with DRS enabled, all ESX hosts must be migrated to the Cisco Nexus 1000 DVS. If only some hosts are migrated it is possible that VMs could be installed or moved to hosts in which the vSwitch is missing VLANs, physical adapters, or both.

- Save the configuration to a file as a backup or for use as a template in creating subsequent VSMs.

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 primary or standalone VSM virtual machine using the [“Setting Up a Primary or Standalone VSM VM Using the GUI” procedure on page 3-3](#).
- Step 2** Set up the secondary VSM virtual machine using the [“Setting Up a Secondary VSM” procedure on page 3-14](#).
- Step 3** Do one of the following:
- If you have purchased licenses, add them to the Cisco Nexus 1000V using the following document:
 - *Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV1(4)*
 - If you are using the temporary licenses provided in the software, then continue with the next step. No action is required.
-
- Step 4** Set up the additional VSM virtual machines using the [“Setting Up a VSM with a Copy of a Configuration File” section on page 3-17](#).
- Step 5** You have completed this process. Return to the [“Software Configuration Process” section on page 2-7](#) to continue setting up your VSM software.
-

**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.

Guidelines and Limitations

This configuration process has the following guidelines and limitations:

- To prevent a disruption in connectivity, all port profiles are created with a system VLAN. You can change this after migration if needed.
- For a complete list of port profile guidelines and limitations, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4)*.
- The host and adapter migration process moves all PNICs used by the VSM from the vSwitches to the Cisco Nexus 1000V DVS.
- The following must be in place if you migrate the host and adapters:

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

- The host must have one or more physical NICs on each vSwitch in use.
- The vSwitch does not have any active VMs.

To prevent a disruption in connectivity during migration, any VMs that share a vSwitch with port groups used by the VSM must be powered off.

- The host must use a VUM-enabled vCenter server.
- You must also configure the VSM connection to the vCenter server datacenter where the host resides.
- The migration process supports Layer 2 and Layer 3.
- No VEMs were previously installed on the host where the VSM resides.

**Caution**

Host management connectivity may be interrupted if VMware kernel 0, vSwitch interface 0 are migrated and the native VLAN is not correctly specified in the setup process.

- The following modification is required to the uplink port profile created by the GUI application if you are installing Cisco Nexus 1000V in an environment where the upstream switch does not support static port channels, such as UCS. The GUI application creates the uplink port profile with **channel group auto mode on** which must be changed to:

channel group auto mode on mac-pinning

This change is required before adding VMNICs in the DVS using this profile.

Setting Up a Primary or Standalone VSM VM Using the GUI

You can use this section and the software GUI to configure the following:

BEFORE YOU BEGIN

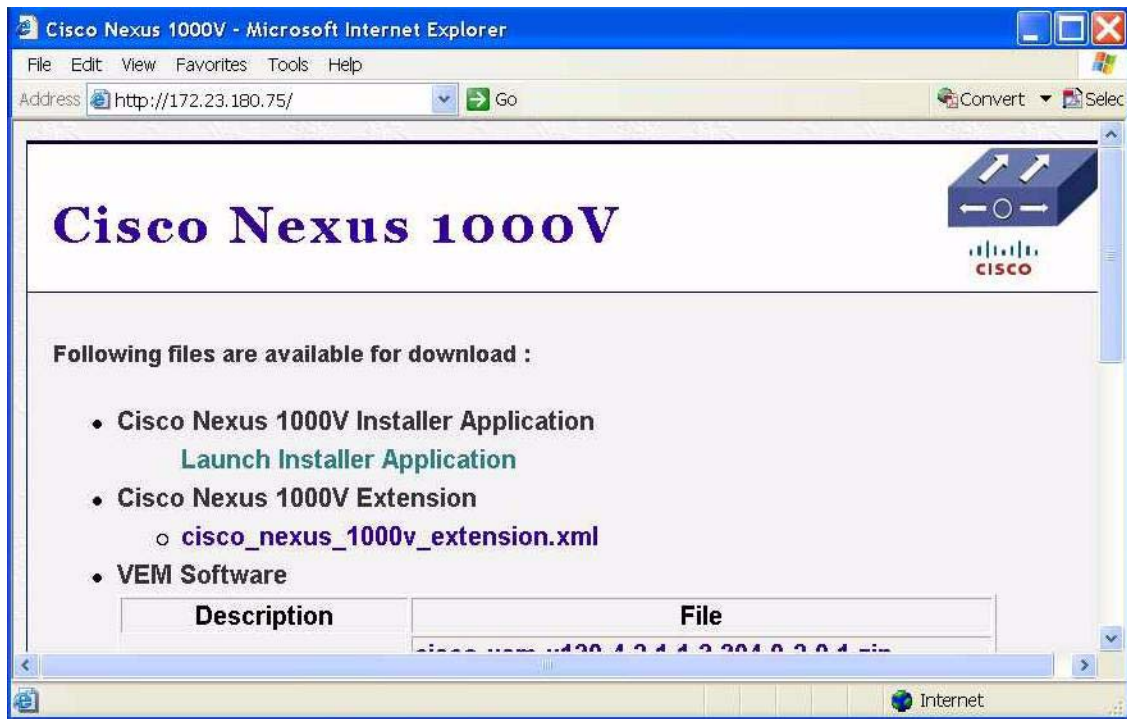
Before beginning this procedure, you must know or do the following:

- You have the following domain information:
 - Control VLAN ID
 - Packet VLAN ID
 - Domain ID

DETAILED STEPS

-
- Step 1** In your local browser address field, enter the VSM IP address.
The Cisco Nexus 1000V home page opens.

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



Step 2 Click **Launch Installer Application**.

The application is downloaded and a security screen opens asking if you want to run it.

Step 3 Click **Run**.

The Enter VSM Credentials screen opens.



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

The 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 In the Use a configuration file field, choose **No** and then click **Next**.

The VSM Host screen opens.



Step 7 Choose a host or cluster where the VSM resides 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 Click one of the following configuration options:

- To use the default Layer 2 configuration, click **Next**, and go to [Step 13](#).
This configures one VLAN (the management VLAN) for use in the control, management, and packet port profiles.
- To configure a different vSwitch port group for each VSM network adapter, click **Advanced L2** and then continue with the next step.
- To configure Layer 3 connectivity, click **Advanced L3** and go to [Step 11](#).

Step 10 In the Advanced Layer 2 configuration screen, do the following:

- Choose your port groups from the selection lists.
- Add VLAN IDs.
- Click **Next**, and then go to [Step 13](#).

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

Nexus 1000V Installation Management Center

Steps

1. Enter VSM Credentials
2. Enter vCenter Credentials
3. Select the VSM's host
- 4. Select the VSM VM & Port groups**
5. Provide VSM Config Options
6. Summary: Please Review Configurations
7. Configure DVS Migration Options
8. Summary: Migrate DVS

Select the VSM VM & Port groups

Choose VSM Virtual Machine: **vsm1**

Please choose a configuration option:

☐ Default L2: Choose the Management vlan for all port groups.

☒ **Advanced L2: Configure each port group individually.**

☐ Advanced L3: Configure configure through L3

Control Port Group: ☒ Choose Control Port Group: ☐ Create Control Port Group:

Port Group: **VLAN108, VLAN: 108** Port Group Name:

Vswitch: **vSwitch0, pnics: vmnic4** VLAN id:

Vswitch: **vSwitch0, pnics...**

Management Port Group: ☒ Choose Management Port Group:

Port Group: **VM Network, VLAN: 0** Port Group Name:

Vswitch: **vSwitch0, pnics: vmnic4** VLAN id:

Vswitch: **vSwitch0, pnics...**

Packet Port Group: ☒ Choose Packet Port Group: ☐ Create Packet Port Group:

Port Group: **VLAN109, VLAN: 109** Port Group Name:

Vswitch: **vSwitch0, pnics: vmnic4** VLAN id:

Vswitch: **vSwitch0, pnics...**

< Prev Next > Finish Cancel

Step 11 In the Advanced Layer 3 port group configuration screen, add the following information:

- Control port group configuration.
- Management port group configuration.

Step 12 For Layer 3 connectivity, choose either mgmt0 or control0 and then do one the following:

- If you chose mgmt0, add the following information and then click **Next**.
 - Layer 3 mgmt0 interface port profile VLAN ID.

Choose an interface for L3 Connectivity: ☒ **mgmt0** ☐ control0

Enter L3 mgmt0 Interface Port Profile Vl...

Please enter a valid L3 management vlan id (range 1-3967, 4048-4093).

< Prev Next > Finish Cancel

- If you chose control0, add the following information and then click **Next**.
 - Layer 3 interface control0 IP address, subnet mask, and gateway
 - Layer 3 control0 interface port profile VLAN ID

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

**Note**

Control and management IP addresses must be in different subnets. This command will fail if the control and management IP addresses are not in different subnets.

Step 13 In the VSM Configuration Options screen, add the following for your VSM and then click **Next**.

- Switch name
- 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.

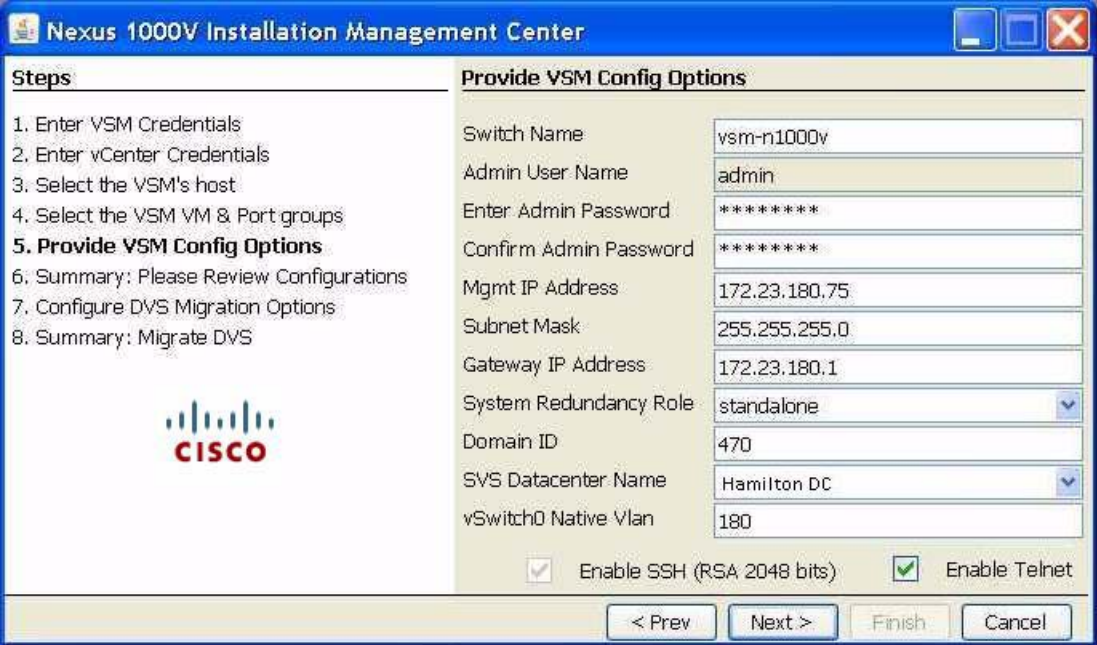
- System Redundancy Role
- Domain ID
- Datacenter name
- vSwitch native VLAN

**Caution**

Host management connectivity may be interrupted if VMware kernel 0, vSwitch interface 0 are migrated and the native VLAN is not correctly specified here.

- Whether to enable Telnet

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



Nexus 1000V Installation Management Center

Steps:

1. Enter VSM Credentials
2. Enter vCenter Credentials
3. Select the VSM's host
4. Select the VSM VM & Port groups
- 5. Provide VSM Config Options**
6. Summary: Please Review Configurations
7. Configure DVS Migration Options
8. Summary: Migrate DVS

Provide VSM Config Options

Switch Name	vsm-n1000v
Admin User Name	admin
Enter Admin Password	*****
Confirm Admin Password	*****
Mgmt IP Address	172.23.180.75
Subnet Mask	255.255.255.0
Gateway IP Address	172.23.180.1
System Redundancy Role	standalone
Domain ID	470
SVS Datacenter Name	Hamilton DC
vSwitch0 Native Vlan	180

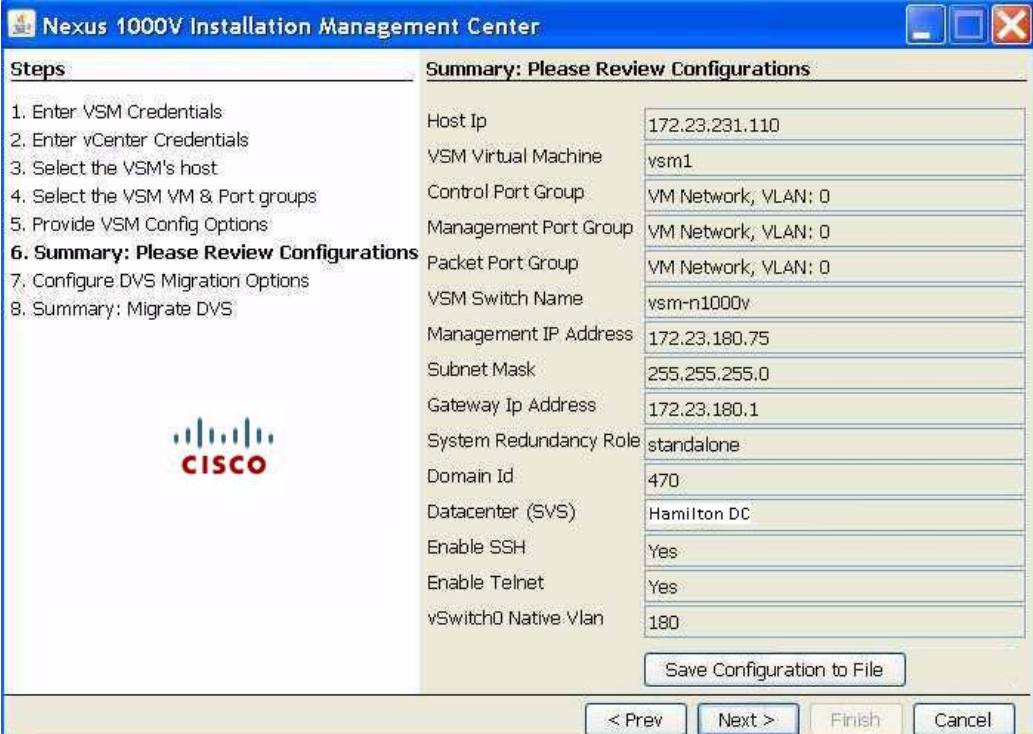
☒ Enable SSH (RSA 2048 bits) ☒ Enable Telnet

< Prev Next > Finish Cancel

Step 14 Click **Next**.

The complete configuration for your VSM displays.

Step 15 Review the configuration.



Nexus 1000V Installation Management Center

Steps:

1. Enter VSM Credentials
2. Enter vCenter Credentials
3. Select the VSM's host
4. Select the VSM VM & Port groups
5. Provide VSM Config Options
- 6. Summary: Please Review Configurations**
7. Configure DVS Migration Options
8. Summary: Migrate DVS

Summary: Please Review Configurations

Host Ip	172.23.231.110
VSM Virtual Machine	vsm1
Control Port Group	VM Network, VLAN: 0
Management Port Group	VM Network, VLAN: 0
Packet Port Group	VM Network, VLAN: 0
VSM Switch Name	vsm-n1000v
Management IP Address	172.23.180.75
Subnet Mask	255.255.255.0
Gateway Ip Address	172.23.180.1
System Redundancy Role	standalone
Domain Id	470
Datacenter (SVS)	Hamilton DC
Enable SSH	Yes
Enable Telnet	Yes
vSwitch0 Native Vlan	180

Save Configuration to File

< Prev Next > Finish Cancel

Step 16 Do one of the following:

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

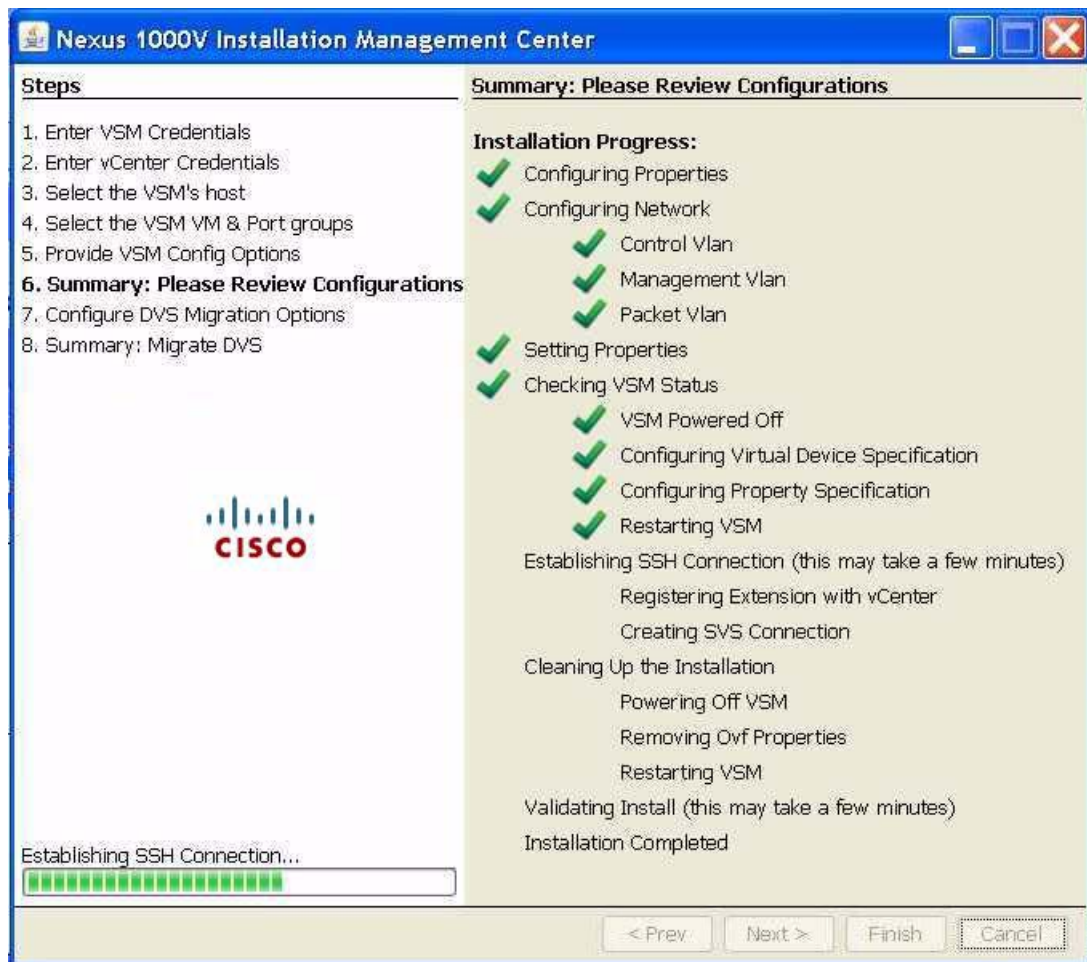
- To make corrections, click **Prev**, go back to the previous screens, and make corrections.
- If the configuration is correct, continue with the next step.

Step 17 Do one of the following:

- To save the configuration to a file as a back up (recommended) or for use in creating another VSM later, click **Save Configuration to File**, and specify a filename and location.
- If not, continue with the next step.

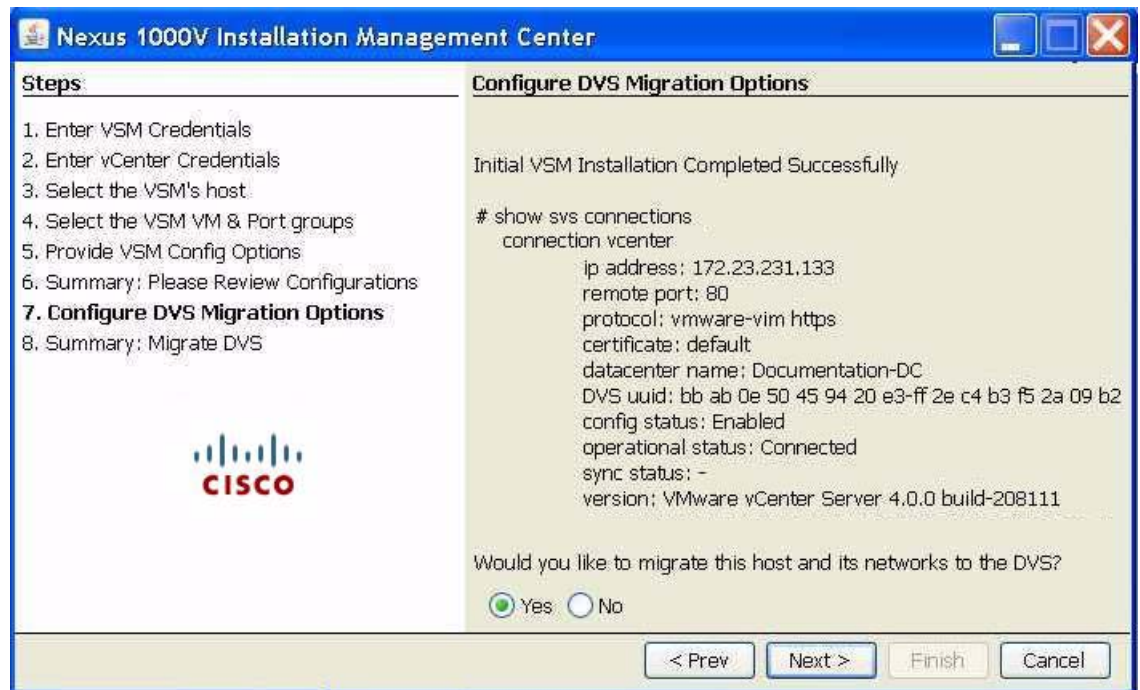
Step 18 Click **Next**.

As the configuration is applied to the VSM, a summary screen displays the progress.



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

The completed VSM configuration is displayed and you are then prompted to migrate the host and networks to the new DVS.



Step 19 Do one of the following:

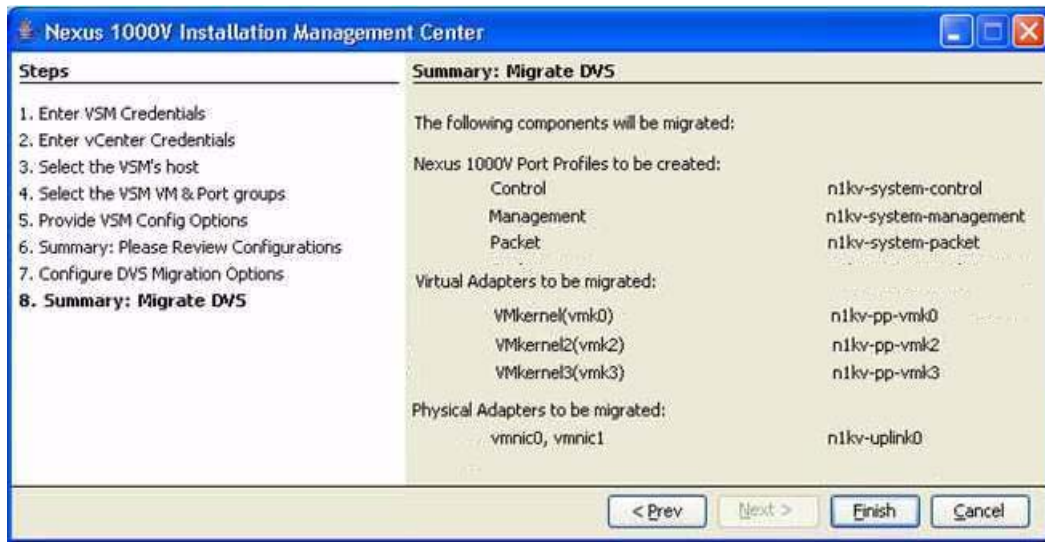
- To continue without migrating the host and networks, click **No**. Then click **Finish** and go to [Step 22](#). If you do not migrate the host now, you can migrate it later manually.
- To have the host and networks automatically migrated to the new DVS, click **Yes** and then click **Next**.

When you click **Yes**, one of the following is configured on the uplink port profile during migration:

Port Channel created during migration	For vSwitch Teaming policy in use:
A static port channel channel-group auto mode on	Route based on IP Hash or Route based on the originating virtual port ID
A vPC host mode port channel with mac-pinning channel-group auto mode on mac-pinning	MAC Hash

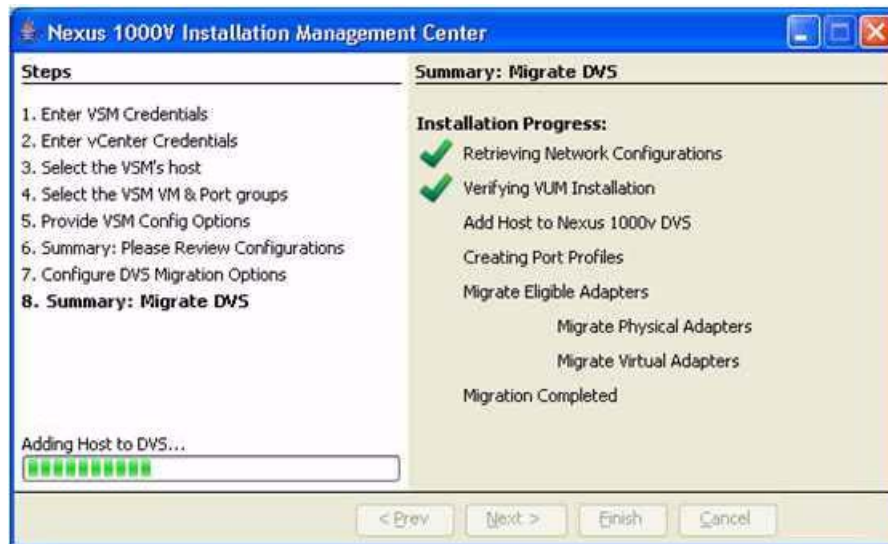
A summary screen displays the details of the proposed migration.

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



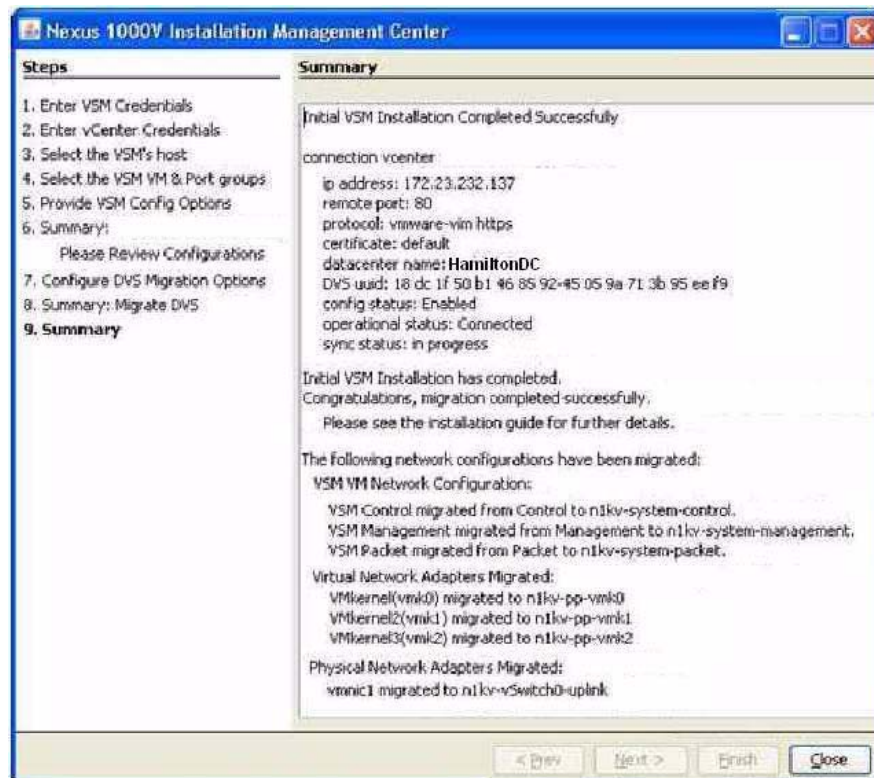
Step 20 Click **Finish**.

The migration starts and progress is displayed.

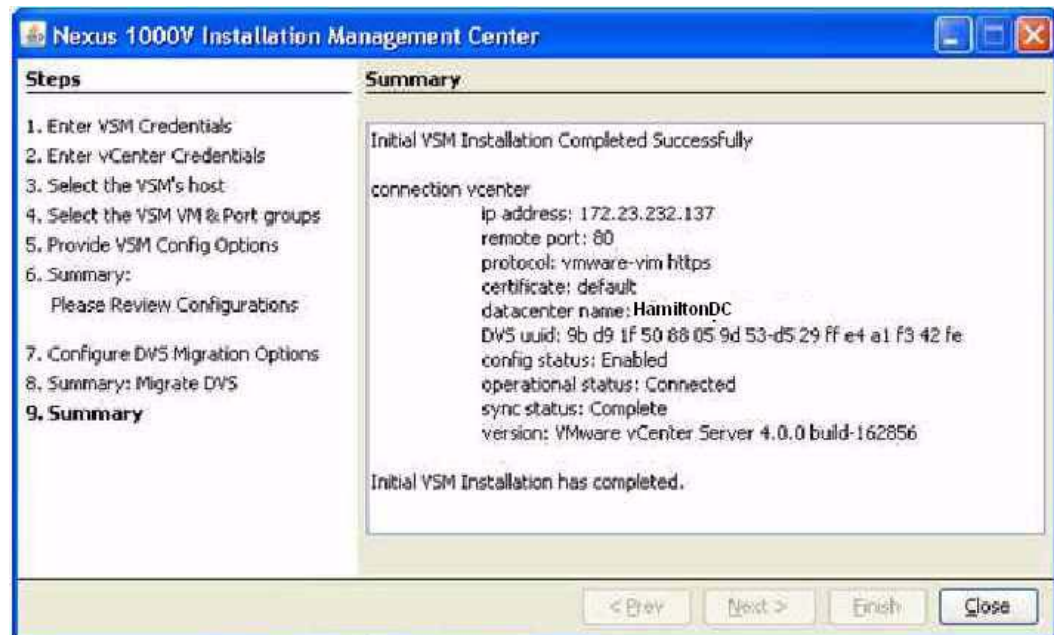


Send document comments to nexus1k-docfeedback@cisco.com.

Step 21 A summary of the configuration displays with the migration details.



Step 22 A summary of the complete installed configuration displays.



Step 23 Click Close.

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

You have completed the setup of the Cisco Nexus 1000V software.
Return to the [GUI Software Configuration Process, page 3-2](#).

Setting Up a Secondary VSM

You can use this procedure to set up the secondary VSM in an HA pair.

BEFORE YOU BEGIN

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

- You have already created the primary VSM in the HA pair using the “[Setting Up a Primary or Standalone VSM VM Using the GUI](#)” procedure on page 3-3.
- If you have not saved a backup copy of your primary VSM configuration file, do so now, using the following command:

copy system:running-config [*destination filesystem:*] *filename*

Example:

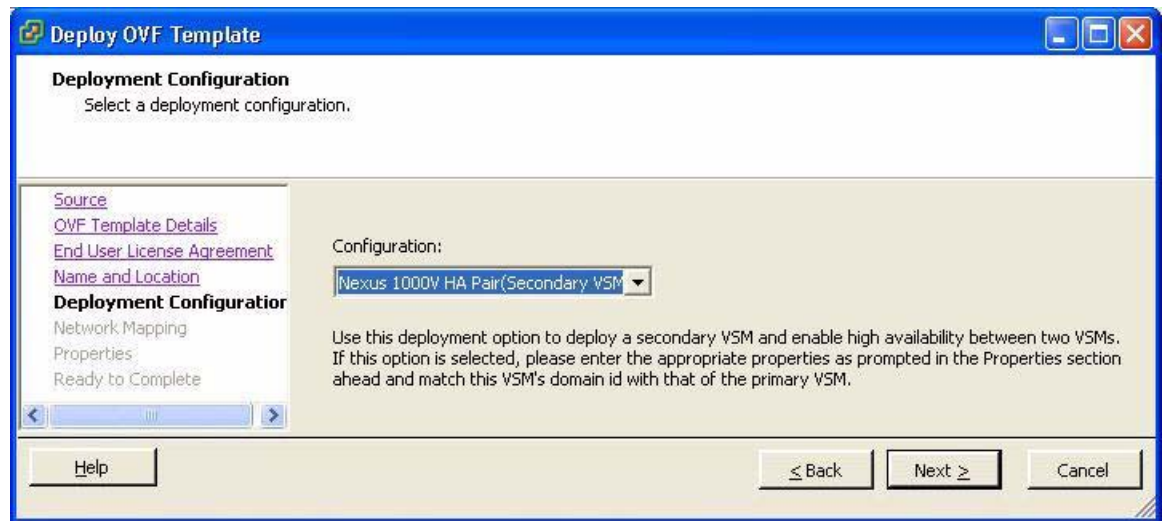
```
n1000v# copy system:running-config tftp://10.10.1.1/home/configs/switch3-run.cfg
```

- You have the following information available. This is the same information used for the primary VSM:
 - Domain ID
 - Password for the Admin user

DETAILED STEPS

- Step 1** In your browser address field, enter the VSM IP address.
The Cisco Nexus 1000V home page opens.
- Step 2** Click **Deployment Configuration**.
The Deploy OVF Template screen opens.

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



Step 3 From the Configuration list, choose **Nexus 1000V HA Pair (Secondary VSM)**.

Step 4 Click **Next**.

The Secondary Properties screen opens.

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

Deploy OVF Template

Properties
Customize the software solution for this deployment.

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)
[Deployment Configuration](#)
[Datastore](#)
[Network Mapping](#)
Properties
 Ready to Complete

a. VSM Domain Id
DomainId
 Enter the Domain Id (1-4095).

 Enter an integer value between 1 and 4095.

b. Nexus 1000V Admin User Password
Password
 Enter the password.
 Must contain at least one capital, one lowercase, one number.

 Enter a string value with 8 to 64 characters.

c. Management IP Address
ManagementIpV4
 Enter the VSM Ip in the following form: 192.168.0.10
 . . .

d. Management IP Subnet Mask
ManagementIpV4Subnet
 Enter the Subnet Mask in the following form: 255.255.255.0
 . . .

e. Management IP Gateway
GatewayIpV4
 Enter the gateway in the following form: 192.168.0.1
 . . .

Not all properties have valid values.
 The vApp will not be able to power on.

≤ Back Next ≥ Cancel

Step 5 Add the following information for the secondary VSM. Use the same values used for the primary VSM.

- Domain ID
- Password for the Admin user



Note If you add information in other fields, it will be ignored.

Step 6 Click Next.

The secondary VSM synchronizes with the primary VSM and the dual supervisors form an HA pair.

Step 7 You have completed the setup of the secondary VSM.
 Return to the [GUI Software Configuration Process, page 3-2](#).

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

Setting Up a VSM with a Copy of a Configuration File

You can use this section and a configuration file to set up a VSM. This section includes the following procedures:

- “Preparing a Configuration File” procedure on page 3-17
- “Example Configuration File” section on page 3-19
- “Applying the Configuration File” procedure on page 3-20

Preparing a Configuration File

You can use this procedure to create a new VSM by editing a copy of the configuration file exported while creating another VSM.

BEFORE YOU BEGIN

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

- You have saved a previous VSM configuration to file and you know the location of this file.
- You have the following information about the new VSM you are creating:
 - Datacenter name
 - Virtual Machine name
 - Virtual switch port group name(s)

You can use the same port group for management, control, and packet; or you can specify separate port groups.



Note Port group names must match those in the vSwitch of the ESX host where the VSM is installed.

- Layer 3 interface and VLAN ID

This information is only needed if you are configuring Layer 3 connectivity.

- Host name
- Management IP, subnet mask, gateway IP
- Domain ID
- SVS connection datacenter name
- HA role
- Native VLAN ID

This is the upstream switch native VLAN for the physical NIC which will be added to the DVS. The native VLAN is used only if you are migrating your configuration.

DETAILED STEPS

Step 1 In a text editor, open the configuration file you intend to use as a template.

This will be a file you exported from a previous VSM configuration. You will edit this file using the following steps.

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

Step 2 Add the name of the datacenter where your VSM resides.

Example:
 # The datacenter name
 Datacenter=**AutomationDC**

Step 3 Add the name of the VM for your VSM.

Example:
 # The virtual machine name
 VirtualMachine=**upgrade1**

Step 4 Do one of the following:

- Go to [Step 5](#) to configure one VLAN (the management VLAN) for use in the control, management, and packet port profiles.
- Go to [Step 6](#) to configure a VLAN for each port profile separately.
- Go to [Step 7](#) to configure Layer 3 connectivity.

Step 5 Specify that you are using the basic configuration.

In this case, you are configuring the management VLAN for use in the control, management, and packet vSwitch port groups.

Example:
 # Basic: All on preconfigured Management Port Group. No other config necessary
 NetConf=**Basic**

The port group assigned to the VSM mgmt interface is now also assigned for control and packet and the VSM VM is reconfigured to use the same port group for mgmt, control, and packet.

Go to [Step 9](#).

Step 6 Specify that you are configuring a VLAN for each port profile separately; and then add the VLAN IDs for this VSM.

Example:
 # Advanced: Must specify Control/Management/Packet
 NetConf=**Advanced**

 # Port group names (names must match the name in the VC)
 Control=**control-portgroup**
 Management=**management-portgroup**
 Packet=**packet-portgroup**

Go to [Step 9](#).

Step 7 Specify that you are configuring Layer 3 connectivity.

Example:
 # L3: Must specify L3Interface/Control/Management
 NetConf=**L3**

Step 8 Do one of the following:

- Specify VSM to VEM communication over the VSM control interface and control port group. Then add the port groups and IP addresses.



Note Control and management IP addresses must be in different subnets. This command will fail if the control and management IP addresses are not in different subnets.

Example:

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

```
# L3Interface (2 options): control0/mgmt0
L3Interface=control0
Control=control-portgroup
Management=management-portgroup
L3Vlan=233
ControlIPv4=192.168.0.100
ControlIPv4Subnet=255.255.255.0
ControlIPv4Gateway=192.168.0.1
```

- Specify VSM to VEM communication over the management interface. The control portgroup will still be used for VSM HA. Then add the port groups and VLAN ID.

Example:

```
# L3Interface (2 options): control0/mgmt0
L3Interface=mgmt0
Control=control-portgroup
Management=management-portgroup
L3Vlan=233
```

Step 9 Add the following information for this VSM:

- Host name
- Management IP, subnet mask, Gateway IP
- Domain ID
- SVS connection datacenter name
- Whether to enable Telnet.

Example:

```
#####
# VSM Config #
#####
HostName=configSwitch
ManagementIPv4=172.23.233.64
ManagementIPv4Subnet=255.255.255.0
GatewayIPv4=172.23.233.1
DomainId=470
SvsDatacenter=AutomationDC
#EnableTelnet: True/False
EnableTelnet=True
```

Step 10 Add the HA role (standalone or primary) for this VSM.

Example:

```
#HARole: standalone/primary
HARole=standalone
```

Step 11 Add the native VLAN for this VSM.

Example:

```
#NativeVlan: native vlan ID
NativeVlan=233
```

Step 12 Save the configuration file.

You have completed this procedure.

Example Configuration File

The following example shows a configuration file for a VSM with the following options:

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

- Datacenter is named AutomationDC
- Virtual Machine is named upgrade1.
- One VLAN (the management VLAN) is used for control, management, and packet port profiles.
- This VSM has the primary HA role.

```
# The datacenter name
Datacenter=AutomationDC
# The virtual machine name
VirtualMachine=upgrade1
# Basic: All on preconfigured Management Port Group. No other config necessary
NetConf=Basic
#####
# VSM Config #
#####
HostName=configSwitch
ManagementIPv4=172.23.233.64
ManagementIPv4Subnet=255.255.255.0
GatewayIPv4=172.23.233.1
DomainId=470
SvsDatacenter=AutomationDC
#EnableTelnet: True/False
EnableTelnet=True
#HARole: standalone/primary
HARole=primary
#NativeVlan: native vlan ID
NativeVlan=233
```

Applying the Configuration File

You can use this procedure to create a VSM using a prepared configuration file and the GUI application.

BEFORE YOU BEGIN

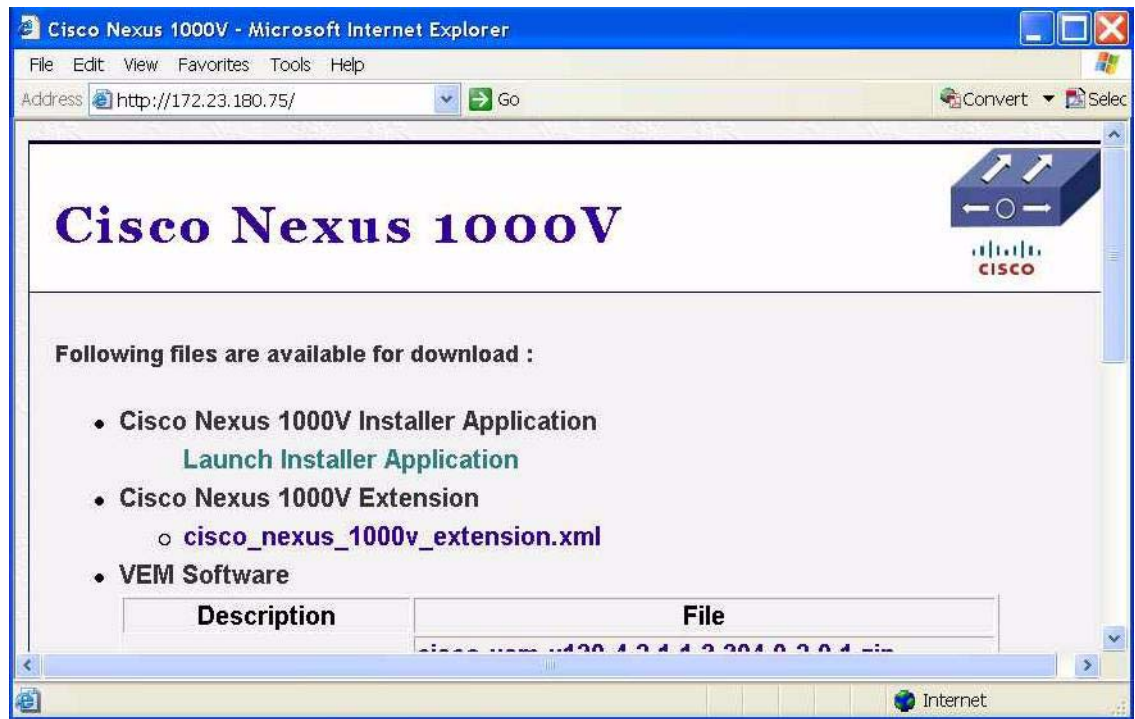
Before beginning this procedure, you must know or do the following:

- You have prepared the configuration file and you know its location.
- To prepare a configuration file, see the [“Preparing a Configuration File” procedure on page 3-17](#).

DETAILED STEPS

-
- Step 1** In your local browser address field, enter the VSM IP address.
- The Cisco Nexus 1000V home page opens.

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



Step 2 Click **Launch Application**.

The application is downloaded and a security screen opens asking if you want to run it.

Step 3 Click **Run**.

The Enter VSM Credentials screen opens.



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

The vCenter Credentials screen opens.

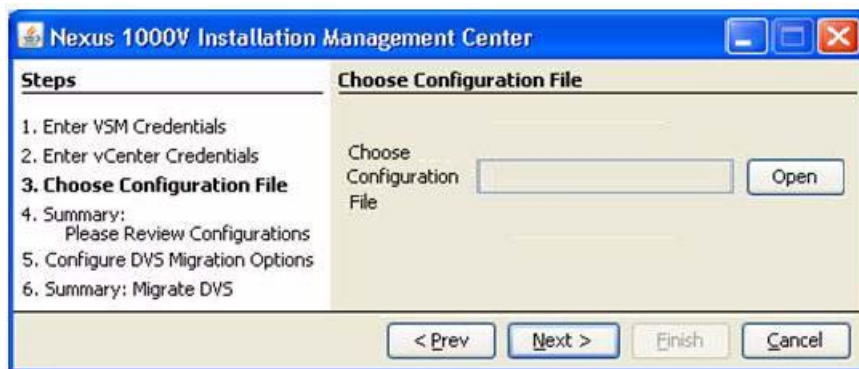
Send document comments to nexus1k-docfeedback@cisco.com.



Step 5 In the Use Configuration file field, click **Yes** and then click **Next**.

The Choose Configuration File screen opens.

Step 6 Click **Open**, browse to the configuration file you want to use as a template, and click **Next**.



The configuration is loaded from your configuration file.

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

The screenshot shows the 'Nexus 1000V Installation Management Center' window. On the left, a 'Steps' list shows the progression from entering credentials to migrating DVS. Step 6, 'Summary: Please Review Configurations', is highlighted. The main area displays a summary of the configuration parameters in a table-like format. At the bottom, there are navigation buttons: '< Prev', 'Next >', 'Finish', and 'Cancel'. A 'Save Configuration to File' button is also present.

Summary: Please Review Configurations	
Host Ip	172.23.231.110
VSM Virtual Machine	vsm1
Control Port Group	VM Network, VLAN: 0
Management Port Group	VM Network, VLAN: 0
Packet Port Group	VM Network, VLAN: 0
VSM Switch Name	n1000v
Management IP Address	172.23.180.75
Subnet Mask	255.255.255.0
Gateway Ip Address	172.23.180.1
System Redundancy Role	Primary
Domain Id	470
Datacenter (SVS)	Hamilton DC
Enable SSH	Yes
Enable Telnet	Yes
vSwitch0 Native Vlan	180

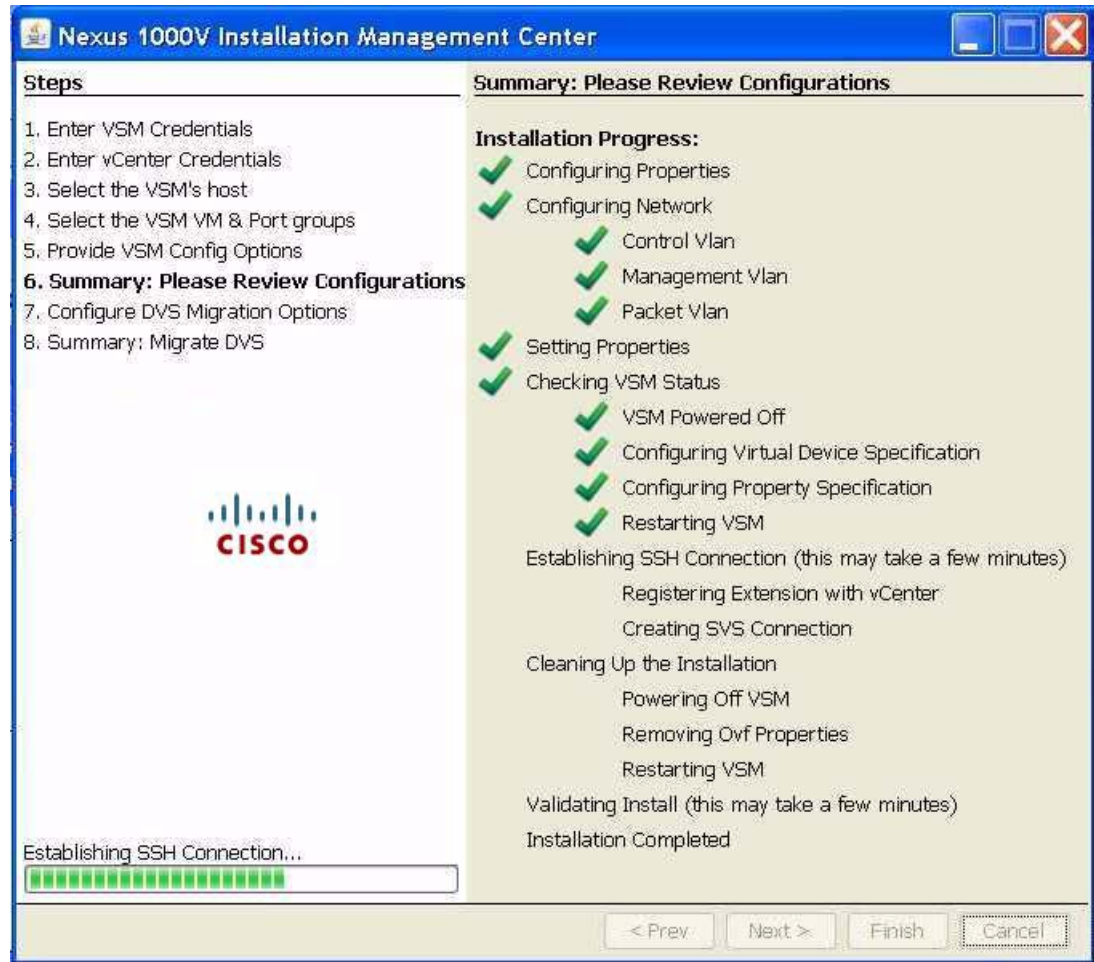
Save Configuration to File

< Prev Next > Finish Cancel

- Step 7** Review the configuration and do one of the following:
- If the configuration is correct, continue with the next step.
 - If not, click **Previous** to revise the contents.
- Step 8** Do one of the following:
- To save the new configuration to a file, click **Save Configuration to File**. This saves the configuration you have just created to a file.
 - Otherwise, continue with the next step.
- Step 9** Click **Next**.
- The configuration is applied to the VSM.

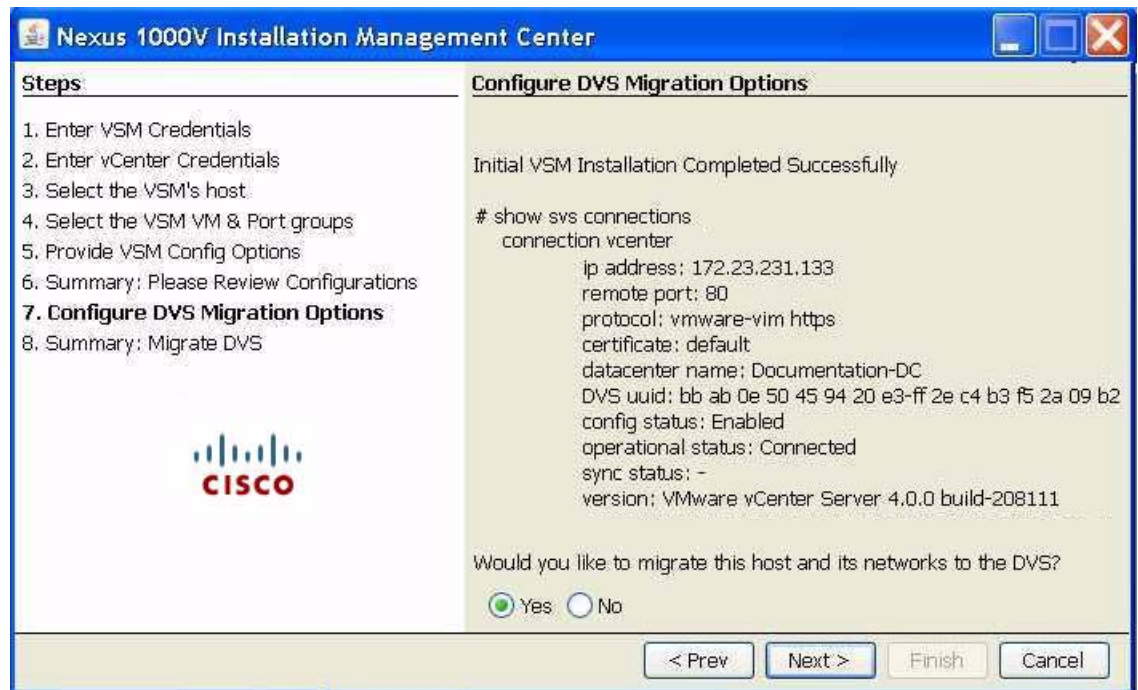
Send document comments to nexus1k-docfeedback@cisco.com.

A summary screen displays the progress as the VSM configuration completes.



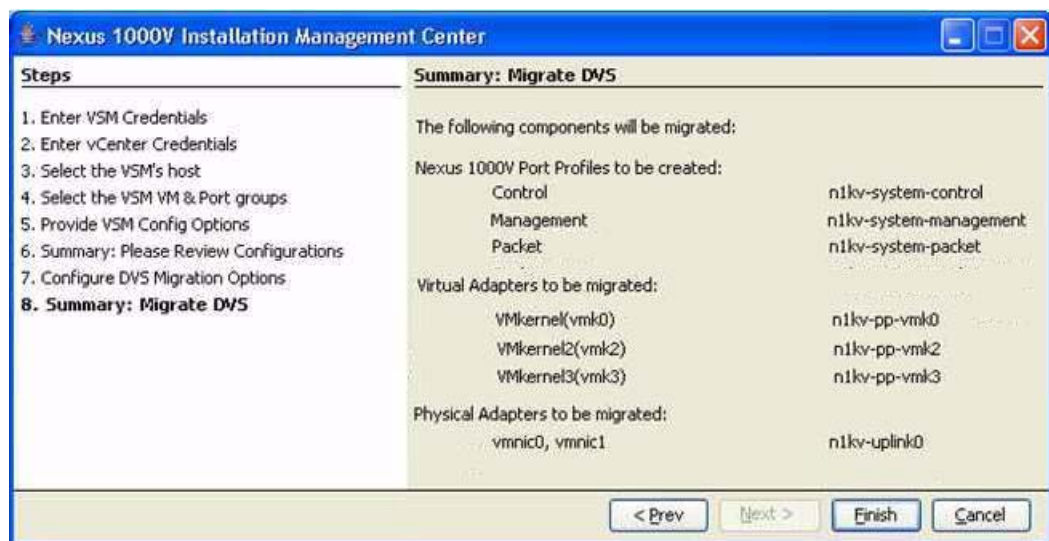
Send document comments to nexus1k-docfeedback@cisco.com.

The completed VSM configuration is displayed and you are prompted to migrate the host and networks to the new DVS.



Step 10 Do one of the following:

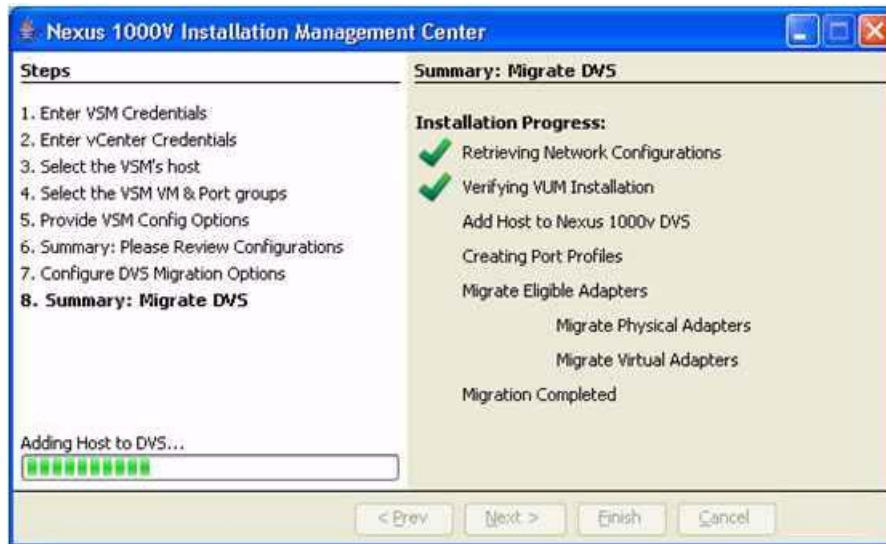
- To continue without migrating the host and networks, click **No**. Then click **Finish** and go to [Step 12](#).
If you do not migrate the host now, you can migrate it later manually.
- To have the host automatically migrated to the new DVS, click **Yes** and then click **Next**.
A summary screen displays the details of the proposed migration.



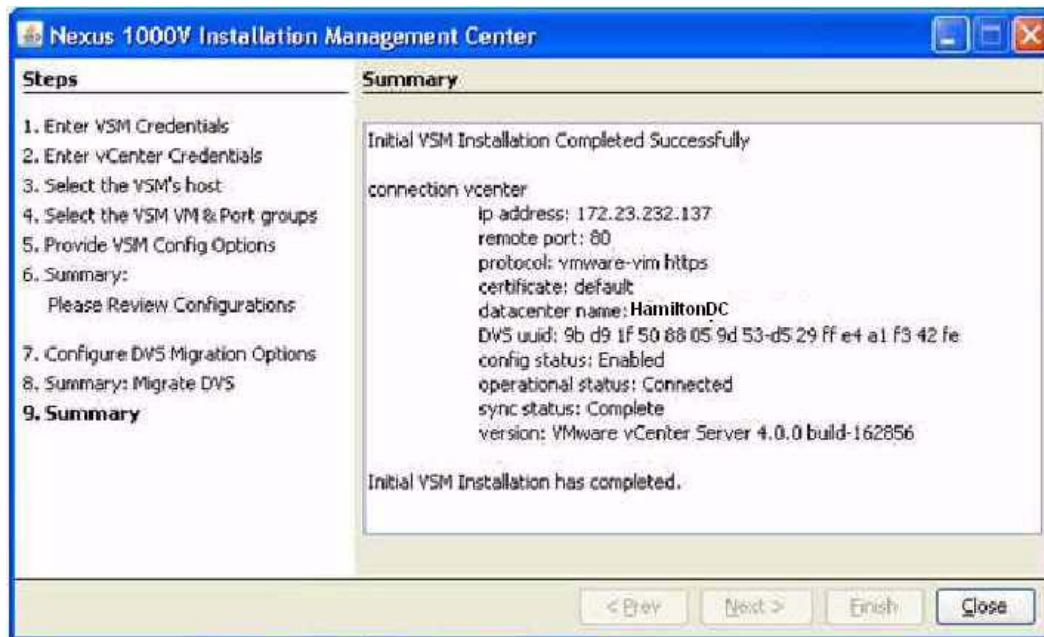
Step 11 Click **Finish**.

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

The migration starts and progress is displayed, followed by a summary of the configuration.



Step 12 A summary of the configuration displays.



Step 13 Click Close.

You have completed the setup of the Cisco Nexus 1000V software.
Return to the [GUI Software Configuration Process, page 3-2](#).



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 4.2(1)SV1(4)*.

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 4.2(1)SV1(4)*, 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 4.2(1)SV1(4)*.

- 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 4-7](#).
- 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 2-7](#).

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 4-12.
 - “Configuring the Uplink Port Profile for VM Traffic” procedure on page 4-16
 - “Configuring the Data Port Profile for VM Traffic” procedure on page 4-19
- Step 9** Add the host to the DVS using the “Adding an ESX 4.0 Host to the DVS” procedure on page 4-22.
- Step 10** You have completed this process. Return to the “Software Configuration Process” section on page 2-7
-

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 information for configuring this Cisco Nexus 1000V VSM:
 - The administrator password.
 - The domain ID.
 - The HA role.
 - Primary for the first VSM in a redundant pair.
 - Secondary for the second VSM in a redundant pair.
 - A switch name.
 - The Management 0 IP address and network mask.
 - The type of SSH key to generate and the number of key bits.
 - The SVS control mode (Layer 2 or Layer 3).
 - The control VLAN ID.
 - The packet VLAN ID.



Note

You can use the same VLAN ID for control, packet, and management, but if needed for flexibility, you can use separate VLAN IDs. Make sure that the network segment has adequate bandwidth and latency.

DETAILED STEPS

- Step 1** Power on the VM, choose **Install Cisco Nexus 1000V**.
The Cisco Nexus 1000V software starts.

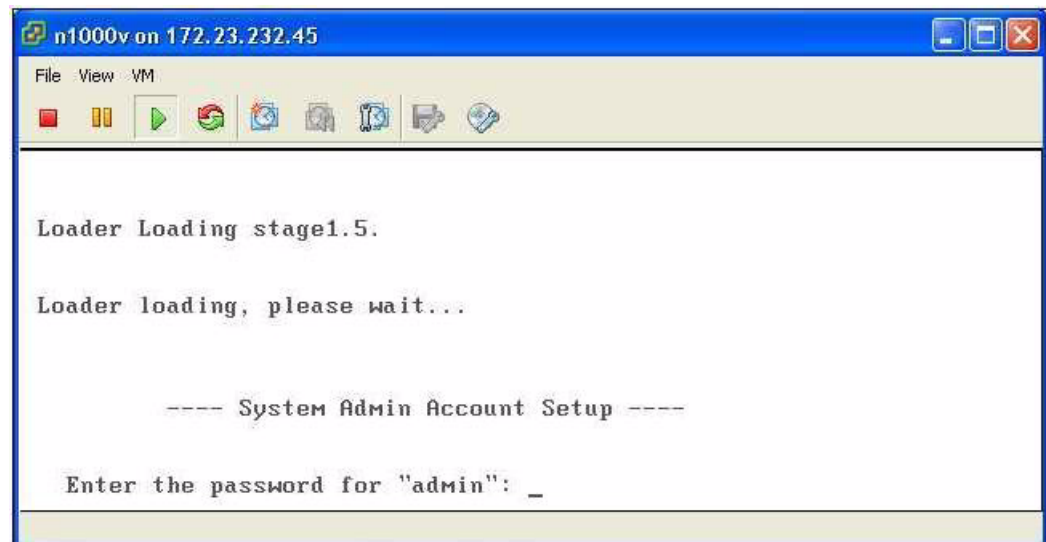
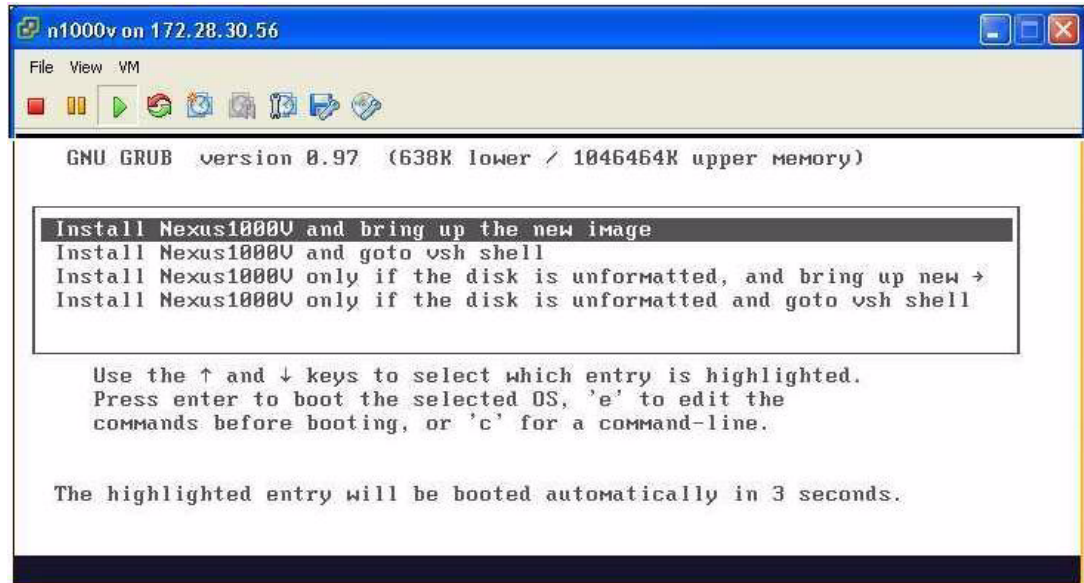


Note

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

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

One of the following displays.



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.

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

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 have set the up the VSM VM to boot from the CD-ROM, and are installing the secondary VSM from the ISO image attached to your CD-ROM, remove the virtual CD-ROM now, so 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.

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**.

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

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 **yes**.

Example:

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

IPv4 address of the default gateway : 172.23.233.1

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 4.2(1)SV1(4)*.

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 enable the HTTP server, answer **yes**.

Example:

Enable the http-server? (yes/no) [y]: **yes**

Step 19 When asked to configure the NTP server, answer **no**.

Example:

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

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

- Step 20** When asked to configure the SVS domain parameters, answer **yes**, and then enter the mode (L2 or L3), and the control and packet VLAN IDs.

Example:

```
Configure svcs domain parameters? (yes/no) [y]: yes
Enter SVS Control mode (L2 / L3) : L2
Enter control vlan <1-3967, 4048-4093> : 100
Enter packet vlan <1-3967, 4048-4093> : 101
```

- Step 21** When asked to configure the VEM feature level, answer **yes** and then enter 0 or 1.

Example:

```
Vem feature level will be set to 4.2(1)SV1(4),
Do you want to reconfigure? (yes/no) [n] yes
    Current vem feature level is set to 4.2(1)SV1(4)
    You can change the feature level to:
        vem feature level is set to the highest value possible
```

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
no telnet server enable
ssh key rsa 1024 force
ssh server enable
feature http-server
svcs-domain
svcs mode L2
control vlan 100
packet vlan 101
domain id 101
vlan 100
vlan 101
```

- Step 22** 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 23** 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%
```

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

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

**Note**

You can use the setup routine to update the configuration done in [Step 8](#) through [Step 23](#) 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 24** 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](#).

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 know the IP address of the active VSM.

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

- You have already downloaded a copy of the following file from the VSM home page.
 - cisco_nexus1000v_extension.xml



Note To go to your VSM home page, point your browser to the IP address of the active VSM.

- 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.

- 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 *Resolving a Plug-In Conflict* procedure in the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(4)*.

DETAILED STEPS

Step 1 Start 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 *Resolving a Plug-In Conflict* procedure in the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(4)*.

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.

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

- Step 10** You have completed this procedure.
Return to the [CLI Software Configuration Process, page 4-1](#) to continue setting up your VSM.

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**


DETAILED STEPS

	Command	Description
Step 1	config t Example: n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	svs connection <i>name</i> 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.

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

	Command	Description
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. <ul style="list-style-type: none"> 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 <i>Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(4)</i> .
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

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

Command	Description
Step 8 copy running-config startup-config Example: <pre>n1000v(config-svs-connn#) copy running-config startup-config [#####] 100% n1000v(config-port-prof)#</pre>	<p>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.</p> <div>  <p>Caution If you do not copy this configuration to the startup configuration, then in the event of a VSM reboot, this configured connection is discarded.</p> </div>
Step 9 You have completed this procedure. Return to the CLI Software Configuration Process, page 4-1 to continue setting up your VSM.	

Creating Required Port Profiles

Use the procedures in this section to create the port profiles required for the VSM.

BEFORE YOU BEGIN

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

- A port profile is a set of interface configuration commands that can be dynamically applied to either the physical (uplink) or virtual interfaces. 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. Specific attributes that can be applied to a port profile include VLAN IDs and VMware port groups.
- You have already added the VLANs that will be applied to these port profiles to the VSM using the [“Creating VLANs” procedure on page 2-7](#).
- You are logged in to the standalone or active VSM in EXEC mode.
- You don’t need to configure the port profiles on the secondary VSM. Once this configuration is made in the primary VSM, it automatically synchronizes with the secondary VSM.
- In an installation where multiple Ethernet port profiles are active on the same VEM, it is recommended that they do not carry the same VLAN(s). The allowed VLAN list should be mutually exclusive. Overlapping VLANs can be configured but may cause duplicate packets to be received by virtual machines in the network.
- You can save the commands used to create a port profile in a file, copy the file to bootflash, and run it as a script. An example configuration is provided after each procedure in this section for this purpose.

For more information about using scripts, see the [“Working with Command Scripts” section on page 6-12](#).

- The port profile name you designate in these procedures is your choice.
- For more information about port profiles, see the following:
 - [“Port Profiles” section on page 1-3](#)
 - [“System Port Profiles and System VLANs” section on page 1-4](#)

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

- For a complete list of the port profile guidelines and limitations, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4)*.

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:

- 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 4.2(1)SV1(4)*.
- System port profiles in this case must be of the Ethernet type because they are used for physical ports. This procedure includes steps for designating the port profile as Ethernet type.
- The system VLANs used in this procedure establish a communication link between the VSM and VEM.



Caution

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

- The VLANs used in the trunk configuration in the system port profile must also be defined in the trunk configuration in the attached physical switchport.
- 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.
- You can save the commands used here in a file, copy the file to bootflash, and run it as a script. An example configuration is provided for this purpose in the [“Example Configuration: System Profile for Critical Ports” section on page 4-15](#).

SUMMARY STEPS

1. **config t**
2. **port-profile type ethernet** *profile_name*
3. **description** *profile_description*
4. **switchport mode trunk**
5. **switchport trunk allowed vlan** *vlan_IDs*
6. **no shutdown**
7. **system vlan** *vlan_ID_list*
8. (Optional) **mtu** *mtu_size*
9. **vmware port-group** [*portgroup_name*]
10. **state enabled**

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

11. `show port-profile [brief | expand-interface | usage] [name profile_name]`
12. `copy running-config startup-config`


DETAILED STEPS

	Command	Description
Step 1	config t Example: <pre>n1000v# config t n1000v(config)#</pre>	Enters global configuration mode.
Step 2	port-profile type ethernet <i>name</i> Example: <pre>n1000v(config)# port-profile type ethernet system-uplink n1000v(config-port-prof)#</pre>	<p>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:</p> <ul style="list-style-type: none"> name—The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V. type—The port profile type for system port profiles in this case must be Ethernet. Once configured, the type cannot be changed. The default is the vEthernet type. <p>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).</p> <p>Note If a port profile is configured as an Ethernet type, then it cannot be used to configure VMware virtual ports.</p>
Step 3	description <i>profile_description</i> Example: <pre>n1000v(config-port-prof)# description "System profile for critical ports" n1000v(config-port-prof)#</pre>	<p>Adds a description to the port profile. This description is automatically pushed to the vCenter Server.</p> <p>profile description: up to 80 ASCII characters</p> <p>Note If the description includes spaces, it must be surrounded by quotations.</p>
Step 4	switchport mode trunk Example: <pre>n1000v(config-port-prof)# switchport mode trunk n1000v(config-port-prof)#</pre>	Designates that the new port profile is used as a trunk port.
Step 5	switchport trunk allowed vlan <i>vlan_IDs</i> Example: <pre>n1000v(config-port-prof)# switchport trunk allowed vlan 260</pre>	Specifies the VLANs allowed on the trunk port for the new port profile.
Step 6	no shutdown Example: <pre>n1000v(config-port-prof)# no shutdown n1000v(config-port-prof)#</pre>	Administratively enables all ports in the new port profile.

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

	Command	Description
Step 7	system vlan <i>vlan_ID_list</i> Example: n1000v(config-port-prof)# system vlan 260 n1000v(config-port-prof)#	<p>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.</p> <p>Note If you defined separate control and packet VLANs, then add another system VLAN.</p>
Step 8	mtu <i>mtu-size</i> Example: n1000v(config-port-prof)# mtu 4000 n1000v(config-port-prof)#	<p>(Optional) Designates the MTU size.</p> <ul style="list-style-type: none"> • If you do not set the MTU size here, the default of 1500 is used. • Must be an even number between 1500 and 9000. • Must be less than the size of the system jumbomtu on the interface.
Step 9	vmware port-group [<i>portgroup_name</i>] Example: n1000v(config-port-prof)# vmware port-group system-uplink n1000v(config-port-prof)#	<p>Designates the port profile as a VMware port group of the same name.</p> <p>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.</p>
Step 10	state enabled Example: n1000v(config-port-prof)# state enabled n1000v(config-port-prof)#	<p>Enables the new system port profile.</p> <p>The configuration for this new system port profile is applied to the assigned ports. The VMware port group is created in the vSwitch on the vCenter Server.</p> <p>A Distributed Virtual Port Group is now visible under the VSM Name on the vSphere Client Inventory > Networking > DataCenter tab.</p>

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

	Command	Description
Step 11	<p>show port-profile name <i>profile-name</i></p> <p>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)#</p>	(Optional) Displays the system-uplink port profile configuration.
Step 12	<p>copy running-config startup-config</p> <p>Example: n1000v(config-port-prof)# copy running-config startup-config [#####] 100% n1000v(config-port-prof)#</p>	<p>Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.</p> <div data-bbox="841 1066 922 1144">  Caution </div> <p>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.</p>
Step 13	<p>You have completed this procedure.</p> <p>Return to the CLI Software Configuration Process, page 4-1 to continue setting up your VSM.</p>	

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

```

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

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 can save the commands used here in a file, copy it to bootflash, and run it as a script. An example configuration is provided for this purpose in the [“Example Configuration: Uplink Profile for VM Traffic”](#) section on page 4-18.
- If you want to use the system-uplink port profile to carry your data traffic, then add the data VLAN ID to the system-uplink port profile and make the corresponding changes on the upstream switch.

SUMMARY STEPS

1. **config t**
2. **port-profile** [type {**ethernet** | **vethernet**}] *name*
3. **description** *profile_description*
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.

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

	Command	Description
Step 2	port-profile type ethernet <i>name</i> Example: <pre>n1000v(config)# port-profile type ethernet vm-uplink n1000v(config-port-prof)#</pre>	<p>Enters port profile configuration mode for the specified port profile.</p> <ul style="list-style-type: none"> type: Defines the port-profile as Ethernet or vEthernet type. Once configured, this setting cannot be changed. The default is vEthernet type. <p>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).</p> <p>Note If a port profile is configured as an Ethernet type, then it cannot be used to configure VMware virtual ports.</p> <ul style="list-style-type: none"> 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 <i>profile_description</i> Example: <pre>n1000v(config-port-prof)# description "Uplink profile for VM Traffic" n1000v(config-port-prof)#</pre>	<p>Adds a description to the port profile. This description is automatically pushed to the vCenter Server.</p> <p>profile description: up to 80 ASCII characters</p> <p>Note If the description includes spaces, it must be surrounded by quotations.</p>
Step 4	switchport mode access Example: <pre>n1000v(config-port-prof)# switchport mode access n1000v(config-port-prof)#</pre>	Designates that the new port profile is used as an access port,
Step 5	switchport access vlan <i>vlan_ID</i> Example: <pre>n1000v(config-port-prof)# switchport access vlan 260</pre>	Specifies the access VLAN for the new port profile.
Step 6	vmware port-group [<i>portgroup_name</i>] Example: <pre>n1000v(config-port-prof)# vmware port-group vm-uplink n1000v(config-port-prof)#</pre>	<p>Designates the port profile as a VMware port group of the same name.</p> <p>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.</p>
Step 7	no shutdown Example: <pre>n1000v(config-port-prof)# no shutdown n1000v(config-port-prof)#</pre>	Administratively enables all ports in the new port profile.

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

	Command	Description
Step 8	state enabled Example: <pre>n1000v(config-port-prof)# state enabled n1000v(config-port-prof)#</pre>	<p>Enables the new uplink port profile for VM traffic.</p> <p>The configuration for this new uplink port profile is applied to the assigned ports. The VMware port group is created in the vSwitch on the vCenter Server.</p> <p>A Distributed Virtual Port Group is now visible under the VSM Name on the vSphere Client Inventory > Networking > DataCenter tab.</p>
Step 9	show port-profile name profile-name Example: <pre>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)#</pre>	<p>(Optional) Displays the vm-uplink port profile configuration.</p>
Step 10	copy running-config startup-config Example: <pre>n1000v(config-port-prof)# copy running-config startup-config [#####] 100% n1000v(config-port-prof)#</pre>	<p>Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.</p> <div>  <p>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</p> </div>
Step 11	<p>You have completed this procedure.</p> <p>Return to the CLI Software Configuration Process, page 4-1 to continue setting up your VSM.</p>	

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
```

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

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 can save the commands used here in a file, copy the file to bootflash, and run it as a script. An example configuration is provided for this purpose in the [“Example Configuration: Data Profile for VM Traffic” section on page 4-21](#). For more information about using scripts, see the *Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(4)*.

SUMMARY STEPS

- config t**
- port-profile** [type {ethernet | vethernet}] *name*
- description** *profile_description*
- switchport mode access**
- switchport access vlan** *vlan_ID*
- vmware port-group** [*portgroup_name*]
- no shutdown**
- state enabled**
- show port-profile** [brief | expand-interface | usage] [*name profile-name*]
- copy running-config startup-config**


DETAILED STEPS

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

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

	Command	Description
Step 2	port-profile [type { ethernet vethernet }] <i>name</i> 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: <ul style="list-style-type: none"> 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). <p>Note If a port profile is configured as an Ethernet type, then it cannot be used to configure VMware virtual ports.</p>
Step 3	description <i>profile_description</i> 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.
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 <i>vlan_ID</i> 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 [<i>portgroup_name</i>] 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.

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

	Command	Description
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 this 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.
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. <div style="display: flex; align-items: center;">  <div> <p>Caution</p> <p>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</p> </div> </div>
Step 11	You have completed this procedure. Return to the CLI Software Configuration Process, page 4-1 to continue setting up your VSM.	

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

```


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

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 that are 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.

- 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 4.2(1)SV1(4)*.
- 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 4.2(1)SV1(4)*.
- When installing the Cisco Nexus 1000 in a VMware cluster with DRS enabled, all ESX hosts must be migrated to the Cisco Nexus 1000 DVS. If only some hosts are migrated it is possible that VMs could be installed or moved to hosts in which the vSwitch is missing VLANs, physical adapters, or both.

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

DETAILED STEPS

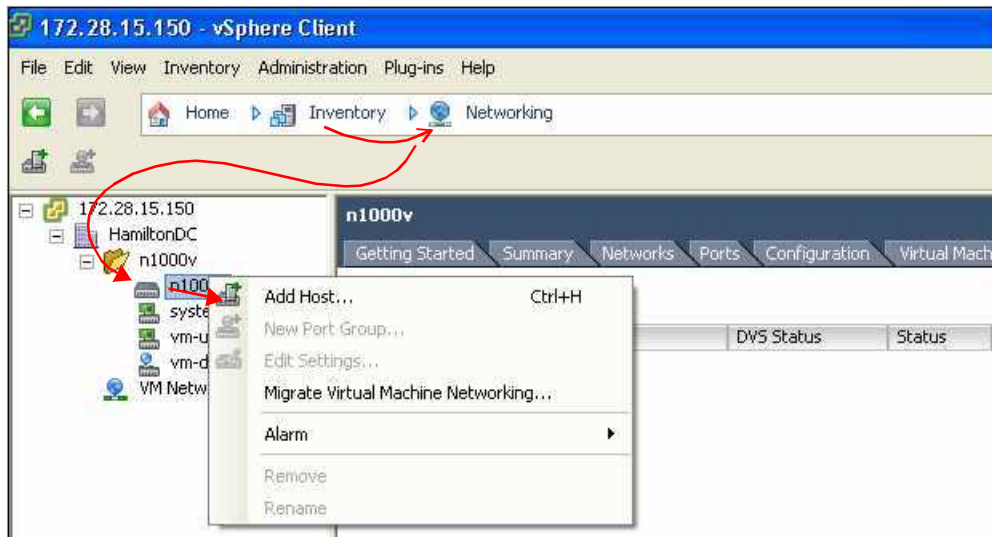
Step 1 In the vSphere Client, click Inventory → Networking.

You should see the following:

- 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 4.2(1)SV1(4)*.



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

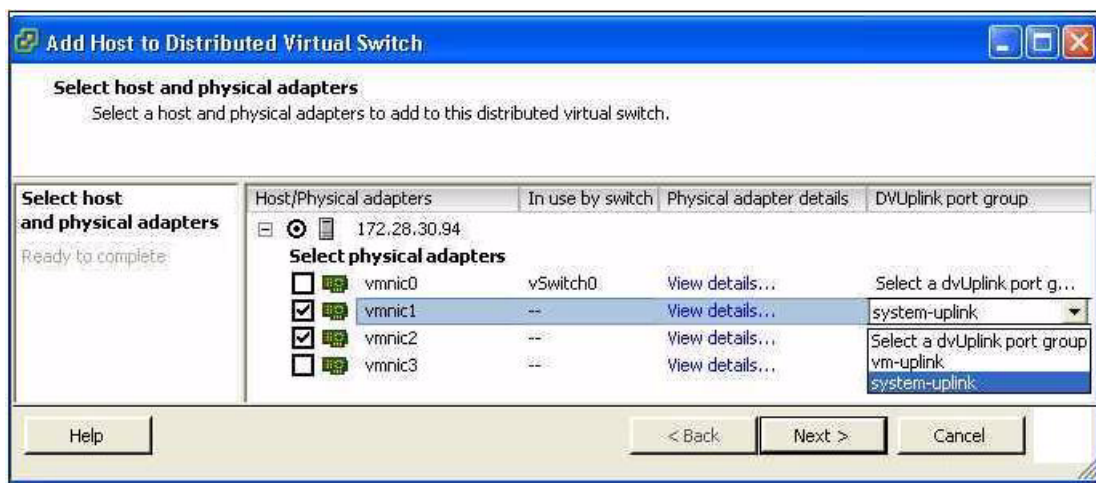
The Add Host to Distributed Virtual Switch Wizard opens.



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.

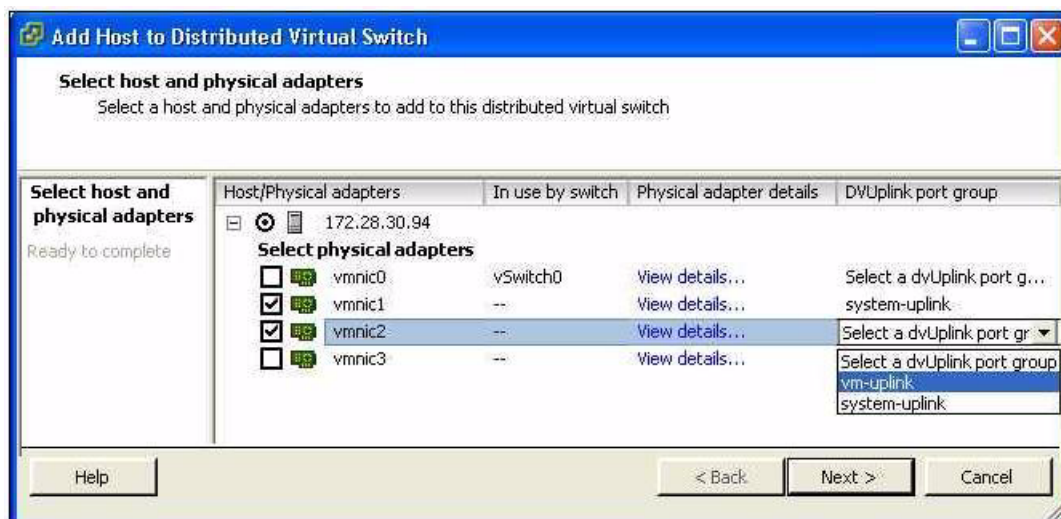
Send document comments to nexus1k-docfeedback@cisco.com.



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, click the check box for the next vmnic that is not attached to the VMware vSwitch, for example vmnic1, click the down arrow and then choose the Uplink Port Group **system-uplink**.



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 4.2(1)SV1(4)*.

Step 6 Click Next.

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

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 4.2(1)SV1(4)*.

Step 9 You have completed this procedure.

Return to the [CLI Software Configuration Process, page 4-1](#) to continue configuring your VSM.

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



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](#)
- [Example Configuration for VSM and VEM on the Same Host, page 5-4](#)

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.

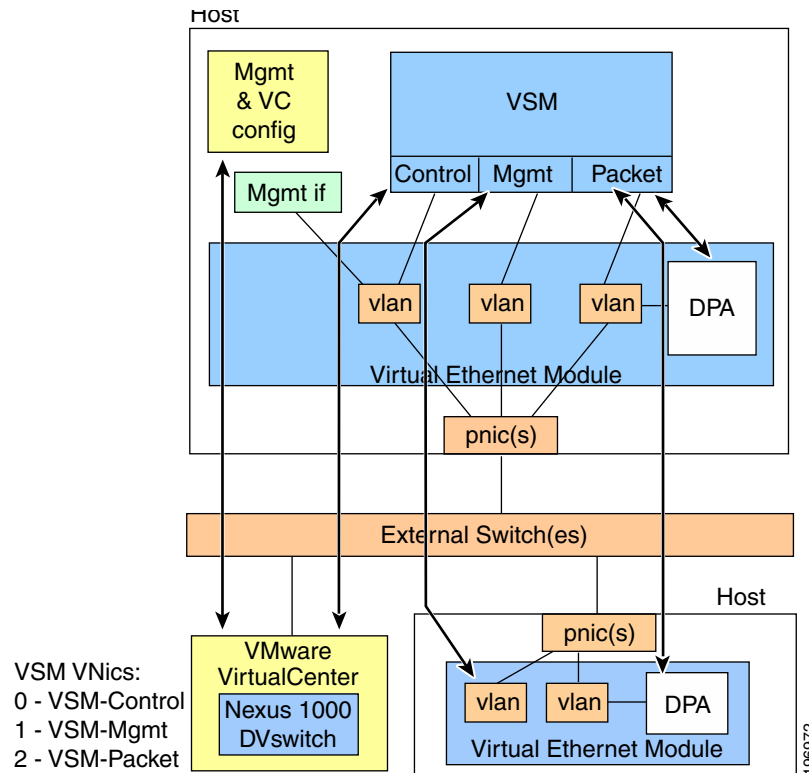
The following are examples of networks where you are advised to run your VSM on a separate host from its VEMs:

- 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 vmknics 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 <i>Cisco Nexus 1000V Virtual Ethernet Module Software Installation Guide, Release 4.2(1)SV1(4)</i> . |
| 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.

Example Configuration for VSM and VEM on the Same Host

The following example shows the port profile and domain configuration for a VSM and VEM on the same host .

In this example the following VLANs are used:

- Service Console: VLAN 100
- Control traffic: VLAN 101
- Management traffic: VLAN 102
- Packet traffic: VLAN 103

In this example, the ServiceConsole is not configured for VLAN tagging. The vethernet port profile could easily be changed to trunking if required.

vlan 1,100,101,102,103

```
port-profile type ethernet system-uplink
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 100, 101, 102, 103
  no shutdown
  system vlan 100,101,102,103
  state enabled
port-profile type vethernet control
  vmware port-group
  switchport mode access
  switchport access vlan 101
  no shutdown
  system vlan 101
  state enabled
port-profile type vethernet management
  vmware port-group
  switchport mode access
  switchport access vlan 102
  no shutdown
  system vlan 102
  state enabled
port-profile type vethernet packet
  vmware port-group
  switchport mode access
  switchport access vlan 103
  no shutdown
  system vlan 103
  state enabled
port-profile type vethernet ServiceConsole
  vmware port-group
  switchport mode access
  switchport access vlan 100
  no shutdown
  system vlan 100
  state enabled
svs-domain
```

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

```
domain id 4
control vlan 101
packet vlan 103
svs mode L2
```

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



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](#)
- [Displaying Available Features, page 6-17](#)

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#	<ul style="list-style-type: none"> • Connect to remote devices. • Temporarily change terminal line settings. • Perform basic tests. • List system information (show).
Global Configuration	n1000v(config)#	<ul style="list-style-type: none"> • Configure features, such as the following: <ul style="list-style-type: none"> – port profile – VLANs – Interfaces • Includes access to EXEC commands. <ul style="list-style-type: none"> – 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 4.2(1)SV1(4)*.

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: <pre>svs(config-if)# exit svs(config)#</pre>	Exits from the current configuration command mode and return to the previous configuration command mode.
end Example: <pre>svs(config)# end svs#</pre>	Exits from the configuration command mode and returns to EXEC mode.
Ctrl-z Example: <pre>svs(config)# ^z svs#</pre>	<p>Exits the current configuration command mode and returns to EXEC mode.</p> <div>  <p>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.</p> </div>

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, <code>interface veth 2</code>	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	<p>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.</p> <p>Used to complete:</p> <ul style="list-style-type: none"> • command names • scheme names in the file system • server names in the file system • file names in the file system <p>Example</p> <pre>n1000v(config)# xm<Tab> n1000v(config)# xml <Tab> n1000v(config)# xml server</pre> <p>Example</p> <pre>n1000v(config)# c<Tab> callhome class-map clock cts cdp cli control-plane</pre> <p>n1000v(config)# cl<Tab> class-map cli clock n1000v(config)# cla<Tab> n1000v(config)# class-map</p>

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 4.2(1)SV1(4)* 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: svsl.bin
n1000v(config)# no boot system bootflash: svsl.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 file named *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: <pre>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</pre> <pre>n1000v# show interface virtual</pre>	Displays the optional parameters used with the show interface virtual command in EXEC mode.
Step 2	show interface module ? Example: <pre>n1000v# show interface module ? ^ % invalid command detected at '^' marker. n1000v#</pre>	Displays an invalid command error message and points (^) to the syntax error.
Step 3	Ctrl-P or the Up Arrow Example: <pre>n1000v# <Ctrl-P> n1000v# show interface virtual ?</pre>	Displays the previous command you entered so that you can correct the error.
Step 4	show interface virtual module ? Example: <pre>n1000v# show interface virtual module ? <1-256> Enter module number</pre> <pre>n1000v# show interface virtual module</pre>	Displays the syntax for showing a virtual interface module.
Step 5	show interface virtual module 3 Example: <pre>n1000v# show interface virtual module 3</pre> <pre>----- Port Adapter Owner Mod Host ----- n1000v#</pre>	Displays the virtual interface module 3.

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

	Command	Purpose
Step 6	show module ? Example: <pre>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</pre>	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

Displaying Available Features

To display a list of available features in Cisco Nexus 1000V and whether they are enabled on your device, use the **show feature** command from any command mode.

Example 6-2 Displaying Available Features

```

n1000v# show feature
Feature Name      Instance  State
-----
dhcp-snooping     1         enabled
http-server       1         enabled
ippool            1         enabled
lacp              1         enabled
netflow           1         disabled
port-profile-roles 1         enabled
private-vlan      1         disabled
sshServer         1         enabled
tacacs            1         enabled
telnetServer      1         enabled
n1000v#

```

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

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 <i>type</i> Example: <pre>n1000v# terminal terminal-type vt100 n1000v#</pre>	Configures a terminal type for the switch. <ul style="list-style-type: none"> 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

Use this procedure to set the number of lines to display on the screen 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 length automatically.
- You are logged in to a terminal session with the CLI in EXEC mode.

DETAILED STEPS

	Command	Purpose
Step 1	terminal length <i>number of lines</i> Example: <pre>n1000v# terminal length 20 n1000v#</pre>	Configures the number of lines to display on the screen for the current console session. <ul style="list-style-type: none"> Range = 0 to 511 lines Default = 24 lines Disable = 0 (scrolls continuously)

Setting the Screen Width for the Console Terminal

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 <i>number of characters</i> Example: n1000v# terminal width 86 n1000v#	Configures the number of characters to display on each line for the current console session. <ul style="list-style-type: none">• Range = 24 to 511 characters• Default = 88 characters

Displaying Terminal Settings

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

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)#	Places you into the CLI Global Configuration mode.
Step 2	line console Example: n1000v(config)# line console n1000v(config-console)#	Places you into the Console Configuration mode.
Step 3	exec-timeout <i>minutes</i> 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. <ul style="list-style-type: none"> • 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

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)#	Places you into the CLI 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)#	Places you into the Virtual Terminal Line Configuration mode.
Step 3	exec-timeout <i>minutes</i> 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. <ul style="list-style-type: none"> • 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

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

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 <i>minutes</i> 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. <ul style="list-style-type: none">• Range = 0 to 525, 600 minutes• Disable (no timeout) = 0 minutes This change is not saved in the configuration file since it only applies to the current session.



CHAPTER 8

Configuration Limits

Table 8-1 Configuration Limits for Cisco Nexus 1000V

Component	Supported Limit	
Maximum Modules	66	
Virtual Ethernet (VEM)	64	
Virtual Supervisor (VSM)	2	
Data Center per VSM	1	
Hosts	64	
Active VLANs across all VEMs	2048 (2K)	
MACs per VEM	16000 (16K)	
MACs per VLAN per VEM	4000 (4K)	
vEthernet interfaces per port profile	1024 (1K)	
PVLAN	512	
vCenter Server connections	1 per VSM ¹	
	Per DVS	Per Host
Virtual Service Domains (VSDs)	64	6
VSD interfaces	2048	214
vEthernet interfaces	2K	216
Port profiles	2048	—
System port profiles	32	16
Port channel	256	8
Physical trunks	512	—
Physical NICs	—	32
vEthernet trunks	256	8
ACL	128	16 ²
ACEs per ACL	128	16 ²
ACL Interfaces	2048	256
NetFlow policies	32	8
NetFlow interfaces	256	32

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

Table 8-1 Configuration Limits for Cisco Nexus 1000V (continued)

Component	Supported Limit	
SPAN/ERSPAN sessions	64	64
QoS policy map	128	16
QoS class map	1024	128
QoS interfaces	2048	256
Port security	2000	216
MultiCast groups	512	512

1. Only one connection to vCenter server is permitted at a time.
2. 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 (DRS)	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. PNIC: physical network interface card vNIC:
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. <ul style="list-style-type: none"> • 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.

[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

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

Term	Description
Port Profile	A collection of interface configuration commands that can be dynamically applied at either physical or virtual interfaces. A port profile can define a collection of attributes such as VLAN ID, private VLAN (PVLAN), access control list (ACL), and port security. Port profiles are integrated with the management layer for the virtual machines and allow virtual machine administrators to choose from profiles as they create virtual machines. When a virtual machine is powered on or off, its corresponding profiles are used to dynamically configure the vEth interface.
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).
Virtual Ethernet Interface (vEth)	Virtual equivalent of physical network access ports. vEths are dynamically provisioned based on network policies stored in the switch as the result of virtual machine provisioning operations at the hypervisor management layer.
Virtual Ethernet Module (VEM)	<p>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.</p> <p>This software replaces the vSwitch in each hypervisor. It performs switching between directly attached virtual machines, and provides uplink capabilities to the rest of the network.</p>
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 NIC (vNIC)	Logically connects a virtual machine to the vSwitch and allows the virtual machine to send and receive traffic through that interface. If two vNICs attached to the same vSwitch need to communicate with each other, the vSwitch performs the Layer 2 switching function directly, without any need to send traffic to the physical network.
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)	<p>The software application that manages Cisco Nexus 1000V software installation and VEM upgrades.</p> <p>Note VUM is not a requirement. Software can be installed manually without using VUM.</p>
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 [4-22](#)

authentication, vCenter Server, GUI setup [3-5](#)

C

class-map limits [8-1](#)

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](#)

configuration limits [8-1](#)

connectivity, verify [4-7](#)

connect to vCenter Server

CLI setup [4-9](#)

context-sensitive help, check syntax for [6-14](#)

control VLAN

CLI setup [4-6](#)

D

data port profile, setup CLI [4-19](#)

default gateway

CLI setup [4-5](#)

description command [4-13, 4-17, 4-20](#)

documentation

additional publications [1-vii](#)

domain

CLI setup [4-6](#)

domain ID, VSM

CLI setup [4-3](#)

E

end command [6-4](#)

EXEC commands [6-3](#)

exit a command mode [6-4](#)

exit command [6-4](#)

extended system ID

VLAN [2-8](#)

F

features, new and changed (table) [1-iii](#)

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

G

global configuration mode, about [6-3](#)
 GUI, software setup [3-1](#)

H

HA role
 CLI setup [4-3](#)
 host, add to DVS
 CLI setup [4-22](#)
 HTTP
 CLI setup [4-5](#)

I

IP connectivity, verify [4-7](#)

L

limits, configuration [8-1](#)

M

match criteria limit [8-1](#)
 mgmt0
 CLI setup [4-5](#)
 modes, command [6-5](#)

N

no command form [6-9](#)
 NTP
 CLI setup [4-5](#)

P

packet VLAN

CLI setup [4-6](#)

password

vCenter Server, GUI setup [3-5](#)

VSM setup, GUI [3-4, 3-21](#)

plug-in, create on vCenter Server, CLI setup [4-7](#)

policy map limits [8-1](#)

prompt, command [6-1](#)

prompts, command [6-5](#)

R

related documents [1-vii, 1-ix](#)

reserved VLANs [2-7](#)

roles

network administrator [1-5](#)

server administrator [1-5](#)

S

same host for VEM and VSM [5-1](#)

secure http, GUI setup [3-5](#)

service policy limits [8-1](#)

software setup

CLI [4-1](#)

GUI [3-1](#)

SSH

CLI setup [4-5](#)

switch name

CLI setup [4-5](#)

syntax check [6-14](#)

system port profile

CLI setup [4-12](#)

T

Telnet

CLI setup [4-5](#)

time

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

setting delay in CLI [6-14](#)

U

uplink port profile

CLI setup [4-16](#)

V

vCenter identification, GU setupI [3-5](#)

VEM

feature level

CLI setup [4-6](#)

VEM and VSM on same host [5-1](#)

verify IP connectivity [4-7](#)

VLAN

extended system ID [2-8](#)

reserved range of [2-7](#)

setup, GUI [3-6](#)

VMotion [1-6](#)

VSM

and VEM on same host [5-1](#)

configuration file, setup [3-22](#)

credentials

CLI setup [4-3](#)

GUI setup [3-4, 3-21](#)

host, GUI setup [3-5](#)

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