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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Changed in Release</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting Up a Secondary  VSM</td>
<td>Modified the procedure.</td>
<td>4.2(1)SV1(4b)</td>
<td>“Configuring the Software Using the GUI”</td>
</tr>
<tr>
<td>Configuration Limits</td>
<td>Updated Cisco Nexus 1000V configuration limits.</td>
<td>4.2(1)SV1(4a)</td>
<td>Chapter 8, “Configuration Limits”</td>
</tr>
<tr>
<td>Configuration Limits</td>
<td>Updated Cisco Nexus 1000V configuration limits.</td>
<td>4.2(1)SV1(4)</td>
<td>Chapter 8, “Configuration Limits”</td>
</tr>
<tr>
<td>GUI Setup procedures</td>
<td>GUI application enhancements:</td>
<td>4.2(1)SV1(4)</td>
<td>“Configuring the Software Using the GUI”</td>
</tr>
<tr>
<td></td>
<td>• New configuration file option.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Secondary VSM configuration option.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• New Layer 3 configuration option.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• New HA configuration option.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CLI Setup procedures</td>
<td>CLI application enhancement:</td>
<td>4.2(1)SV1(4)</td>
<td>“Configuring the Software Using the CLI”</td>
</tr>
<tr>
<td></td>
<td>• New HTTP server option.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Displaying Available</td>
<td>Show command for displaying available features and whether they are enabled.</td>
<td>4.2(1)SV1(4)</td>
<td>“Understanding the CLI”</td>
</tr>
<tr>
<td>Features</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GUI Setup procedures</td>
<td>GUI application enhancements:</td>
<td>4.0(4)SV1(3)</td>
<td>“Configuring the Software Using the GUI”</td>
</tr>
<tr>
<td></td>
<td>• Migrates host, port groups, and PNICs.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Creates port profiles.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Migrates VSM to its own VEM.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Adds the host to the DVS.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 1  New and Changed Getting Started Information (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Changed in Release</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI Setup procedures</td>
<td>A new GUI application is added to set up the Cisco Nexus 1000V software.</td>
<td>4.0(4)SV1(2)</td>
<td>“Configuring the Software Using the GUI”</td>
</tr>
<tr>
<td>CLI Setup procedures</td>
<td>The procedures for setting up the Cisco Nexus 1000V using the CLI have been moved into this document from the <em>Cisco Nexus 1000V Software Installation Guide, Release 4.2(1)SV1(4b).</em></td>
<td>4.0(4)SV1(2)</td>
<td>“Configuring the Software Using the CLI”</td>
</tr>
<tr>
<td>Configuration Limits</td>
<td>Lists the Cisco Nexus 1000V configuration limits.</td>
<td>4.0(4)SV1(2)</td>
<td>Chapter 8, “Configuration Limits”</td>
</tr>
<tr>
<td>VSM Vmotion support</td>
<td>Support is added for Vmotion of the VSM VM.</td>
<td>4.0(4)SV1(2)</td>
<td>“Implementation Considerations”</td>
</tr>
</tbody>
</table>
CONTENTS

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 viii

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
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 3-18
    Preparing a Configuration File 3-18
    Example Configuration File 3-20
    Applying the Configuration File 3-21

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 4-19
      Configuring the Data Port Profile for VM Traffic 4-19
      Example Configuration: Data Profile for VM Traffic 4-22
      Adding an ESX 4.0 Host to the DVS 4-23

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
    Global Configuration Command Mode 6-3
    Accessing Interface Configuration Command Mode 6-3
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 viii**

**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 Port Profile Configuration Guide, Release 4.2(1)SV1(4a)*
- *Cisco Nexus 1000V Software Installation Guide, Release 4.2(1)SV1(4b)*
- *Cisco Nexus 1000V VEM Software Installation and Upgrade Guide, Release 4.2(1)SV1(4b) (server administrators)*
- *Cisco VN-Link: Virtualization-Aware Networking* white paper
Preface

**Document Organization**

This document is organized into the following chapters:

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

**Document Conventions**

Command descriptions use these conventions:

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

Screen examples use these conventions:

- **screen font**: Terminal sessions and information the device displays are in screen font.
- **boldface screen font**: Information you must enter is in boldface screen font.
- **italic screen font**: Arguments for which you supply values are in italic screen font.
- **< >**: Nonprinting characters, such as passwords, are in angle brackets.
Available Documents

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


General Information

Cisco Nexus 1000V Documentation Roadmap, Release 4.2(1)SV1(4a)
Cisco Nexus 1000V Release Notes, Release 4.2(1)SV1(4b)
Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(4b)
Cisco Nexus 1010 Management Software Release Notes, Release 4.2(1)SP1(4)

Install and Upgrade

Cisco Nexus 1000V Software Installation Guide, Release 4.2(1)SV1(4b)
Cisco Nexus 1000V Software Upgrade Guide, Release 4.2(1)SV1(4b)
Cisco Nexus 1000V VEM Software Installation and Upgrade Guide, Release 4.2(1)SV1(4b)
Cisco Nexus 1010 Virtual Services Appliance Hardware Installation Guide
Cisco Nexus 1010 Software Installation and Upgrade Guide, Release 4.2(1)SP1(4)

Configuration Guides

Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV1(4a)
Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(4b)
Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.2(1)SV1(4b)
Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4a)
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(4a)
Send document comments to nexus1k-docfeedback@cisco.com.

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(4b)
Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(4b)
Cisco Nexus 1010 Software Configuration Guide, Release 4.2(1)SP1(4)

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(4)

Troubleshooting and Alerts

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

Virtual Network Management Center

Cisco Virtual Network Management Center

Network Analysis Module Documentation

Cisco Prime Network Analysis Module Software Documentation Guide, 5.1
Cisco Prime Network Analysis Module (NAM) for Nexus 1010 Installation and Configuration Guide, 5.1
Cisco Prime Network Analysis Module Command Reference Guide 5.1
Cisco Prime Network Analysis Module Software 5.1 Release Notes
Cisco Prime Network Analysis Module Software 5.1 User Guide

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:


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.
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.

*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.

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

<table>
<thead>
<tr>
<th>x86 Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>*Virtual Machine 1</td>
</tr>
<tr>
<td>App</td>
</tr>
<tr>
<td>Operating System</td>
</tr>
<tr>
<td>CPU</td>
</tr>
<tr>
<td>Virtual Hardware</td>
</tr>
<tr>
<td>Memory</td>
</tr>
<tr>
<td>*Virtual Machine 2</td>
</tr>
<tr>
<td>App</td>
</tr>
<tr>
<td>Operating System</td>
</tr>
<tr>
<td>CPU</td>
</tr>
<tr>
<td>Virtual Hardware</td>
</tr>
<tr>
<td>Memory</td>
</tr>
<tr>
<td>Virtualization Layer</td>
</tr>
</tbody>
</table>
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.

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...
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
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(4a).

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

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>
<thead>
<tr>
<th>Table 1-1 Administrator Roles</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Administrator</strong></td>
<td><strong>Server Administrator</strong></td>
</tr>
<tr>
<td>• Creates, configures, and manages vSwitches.</td>
<td>• Assigns the following to port groups:</td>
</tr>
<tr>
<td>• Creates, configures, and manages port profiles, including the following:</td>
<td>– vNICs</td>
</tr>
<tr>
<td>– security</td>
<td>– vmkernel interfaces</td>
</tr>
<tr>
<td>– port channels</td>
<td>– service console interfaces</td>
</tr>
<tr>
<td>– QOS policies</td>
<td>• Assigns physical NICs (also called PNICS).</td>
</tr>
</tbody>
</table>

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.
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(4b) 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.
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.

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.

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
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(4b).

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

<table>
<thead>
<tr>
<th>NICs</th>
<th>Traffic</th>
<th>Description</th>
<th>VLAN numbering used in example¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>First</td>
<td>Control</td>
<td>e1000</td>
<td>260</td>
</tr>
</tbody>
</table>
**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(4b)*.
  - 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.

---

**Table 2-1 Required NIC Configuration (continued)**

<table>
<thead>
<tr>
<th>NICs</th>
<th>Traffic</th>
<th>Description</th>
<th>VLAN numbering used in example¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second</td>
<td>Management</td>
<td>e1000 The Management VLAN corresponds to the mgmt0 interface on the switch.</td>
<td>260</td>
</tr>
<tr>
<td>Third (last)</td>
<td>Packet</td>
<td>e1000</td>
<td>260</td>
</tr>
</tbody>
</table>

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(4a)*.
- Control VLANs, packet VLANs, and management VLANs must be configured as regular VLANs and not as private VLANs.

---

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.
Prerequisites

- 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>
<thead>
<tr>
<th>Role</th>
<th>Single Supervisor System</th>
<th>Dual Supervisor System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standalone</td>
<td>X</td>
<td>X³</td>
</tr>
<tr>
<td>Primary</td>
<td>X¹</td>
<td></td>
</tr>
<tr>
<td>Secondary</td>
<td>X²</td>
<td></td>
</tr>
</tbody>
</table>

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(4b).

- 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>
<thead>
<tr>
<th>Strong passwords have:</th>
<th>Strong passwords do NOT have:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• At least eight characters</td>
<td>• Consecutive characters, such as “abcd”</td>
</tr>
<tr>
<td>• Uppercase letters</td>
<td>• Repeating characters, such as “aaabbb”</td>
</tr>
<tr>
<td>• Lowercase letters</td>
<td>• Dictionary words</td>
</tr>
<tr>
<td>• Numbers</td>
<td>• Proper names</td>
</tr>
<tr>
<td>• Special characters</td>
<td></td>
</tr>
</tbody>
</table>

Note: Clear text passwords cannot include the dollar sign ($) special character.

- 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.
Prerequisites

- 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.
Figure 2-1 Cisco Nexus 1000V Configuration Example

Redundant Cisco Nexus 1000V VSMs
Primary and secondary VSMs form an HA Pair

Management VLAN 260, vmnic 0
Control VLAN 260, vmnic 0
Packet VLAN 260, vmnic 0
Data VLAN 20, vmnic 1
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:
- 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:
- If both the VSM and VEMs are working as expected, continue with the next step.
- If not, then see the Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(4b).

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.
Creating VLANs

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(4a).

- 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`

**VLAN Numbers**

<table>
<thead>
<tr>
<th>VLAN Numbers</th>
<th>Range</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Normal</td>
<td>Cisco Nexus 1000V default. You can use this VLAN, but you cannot modify or delete it.</td>
</tr>
<tr>
<td>2–1005</td>
<td>Normal</td>
<td>You can create, use, modify, and delete these VLANs.</td>
</tr>
<tr>
<td>1006–4094</td>
<td>Extended</td>
<td>You can create, name, and use these VLANs. You cannot change the following parameters:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• State is always active.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• VLAN is always enabled. You cannot shut down these VLANs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> The extended system ID is always automatically enabled.</td>
</tr>
<tr>
<td>3968–4047 and 4094</td>
<td>Internally allocated</td>
<td>You cannot use, create, delete, or modify these VLANs. You can display these VLANs. Cisco Nexus 1000V allocates these 80 VLANs, plus VLAN 4094, for features, like diagnostics, that use internal VLANs for their operation.</td>
</tr>
</tbody>
</table>
### Creating VLANs

#### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>config t</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Creates, and saves in the running configuration, a VLAN or a range or VLANs.</td>
</tr>
<tr>
<td>`vlan (vlan-id</td>
<td>vlan-range)`</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you enter a VLAN ID that is assigned to an internally allocated VLAN, the system returns an error message.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> From the VLAN configuration mode, you can also create and delete VLANs.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>This example shows VLAN 5 being created. The VLAN is activated and you are automatically placed into a submode for configuring VLAN 5.</td>
</tr>
<tr>
<td><code>n1000v# config t</code></td>
<td></td>
</tr>
<tr>
<td><code>n1000v(config)# vlan 5</code></td>
<td></td>
</tr>
<tr>
<td><code>n1000v(config-vlan)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>(Optional) Displays the VLAN configuration for verification purposes.</td>
</tr>
<tr>
<td><code>show vlan id 5</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>n1000v(config)# show vlan id 5</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>n1000v(config)# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

You have completed this procedure. Return to the configuration process that pointed you here:

- CLI Software Configuration Process, page 4-1
**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:**

```
show module
```

<table>
<thead>
<tr>
<th>Mod</th>
<th>Ports</th>
<th>Module-Type</th>
<th>Model</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>Virtual Supervisor Module</td>
<td>Nexus1000V</td>
<td>ha-standby</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>Virtual Supervisor Module</td>
<td>Nexus1000V</td>
<td>active *</td>
</tr>
<tr>
<td>3</td>
<td>248</td>
<td>Virtual Ethernet Module</td>
<td>NA</td>
<td>ok</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mod</th>
<th>Sw</th>
<th>Hw</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4.2(1)SV1(4)</td>
<td>0.0</td>
</tr>
<tr>
<td>2</td>
<td>4.2(1)SV1(4)</td>
<td>0.0</td>
</tr>
<tr>
<td>3</td>
<td>4.2(1)SV1(4) VMware ESXi 4.0.0 Releasebuild-208167 (2.0)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mod</th>
<th>MAC-Address(es)</th>
<th>Serial-Num</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8</td>
<td>NA</td>
</tr>
<tr>
<td>2</td>
<td>00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8</td>
<td>NA</td>
</tr>
<tr>
<td>3</td>
<td>02-00-0c-00-03-00 to 02-00-0c-00-03-80</td>
<td>NA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mod</th>
<th>Server-IP</th>
<th>Server-UUID</th>
<th>Server-Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>172.28.15.152</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>2</td>
<td>172.28.15.152</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>3</td>
<td>172.28.30.94</td>
<td>89130a67-e66b-3e57-ad25-547750bcfc7e</td>
<td>localhost.</td>
</tr>
</tbody>
</table>

* this terminal session

```
n1000v#
```

**Example:**

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

<table>
<thead>
<tr>
<th>Mod</th>
<th>Status</th>
<th>UUID</th>
<th>License Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>powered-up</td>
<td>0b0a1871-1fd9-3c1d-b3c6-a097c7ae714</td>
<td>licensed</td>
</tr>
</tbody>
</table>

**Step 2**

Do one of the following:
Chapter 2      Setting Up the Software

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(4b).

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.
Implementation Guidelines

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.

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

• 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(4b).

• 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.
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 3-18

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.
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(4a)
- If you are using the temporary licenses provided in the software, then continue with the next step. No action is required.

**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.

**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 3-18.

**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.

### 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(4a).
- 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:
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.
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.
Chapter 3 Configuring the Software Using the GUI

Setting Up a Primary or Standalone VSM VM Using the GUI

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.
Choose your VSM from the selection list.

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.

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.
**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.
  
  ![Interface Selection](image)

- 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

![GUI Configuration](image)
Setting Up a Primary or Standalone VSM VM Using the GUI

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.

Choose an interface for L3 Connectivity:
- mgmt0
- control0

L3 interface control0 IP address:
L3 interface control0 subnet mask:
L3 interface control0 gateway:
Enter L3 control0 interface Port Profile VI...
Please enter a valid L3 control IP address. (i.e. 192.168.0.10)

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
Step 14  Click **Next**.

The complete configuration for your VSM displays.

Step 15  Review the configuration.

Step 16  Do one of the following:
Setting Up a Primary or Standalone VSM VM Using the GUI

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.
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:

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

A summary screen displays the details of the proposed migration.
Step 20 Click **Finish**.

The migration starts and progress is displayed.
**Step 21**  A summary of the configuration displays with the migration details.

![Image](image1.png)

**Step 22**  A summary of the complete installed configuration displays.

![Image](image2.png)

**Step 23**  Click Close.
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.
Step 3 From the Configuration drop-down list, choose Nexus 1000V Secondary and click Next.
The Host/Cluster screen opens.

Step 4 Choose a host from the host’s list and click Next.
The Storage screen opens.

Step 5 Choose the storage on which the VSM is to be hosted and click Next.
The Disk Format screen opens.

Step 6 Validate the datastore chosen and if it is the correct value, click Next.
The Network Mapping screen opens.
Step 7  Click Next.

The Secondary Properties screen opens.
Step 8  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 9  Click Next.
The secondary VSM synchronizes with the primary VSM and the dual supervisors form an HA pair.

Step 10  You have completed the setup of the secondary VSM.
Return to the GUI Software Configuration Process, page 3-2.
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 3-18
- “Example Configuration File” section on page 3-20
- “Applying the Configuration File” procedure on page 3-21

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.
  - 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.
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:
Setting Up a VSM with a Copy of a Configuration File

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:

# 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
Setting Up a VSM with a Copy of a 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 3-18.

**DETAILED STEPS**

**Step 1**

In your local browser address field, enter the VSM IP address.

The Cisco Nexus 1000V home page opens.

```bash
# 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
```
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.
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.
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.
A summary screen displays the progress as the VSM configuration completes.
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**.
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.
Setting Up a VSM with a Copy of a Configuration File

Send document comments to nexus1k-docfeedback@cisco.com.
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(4b)*.

**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(4a)*, 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(4a)*.

**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.
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.

\[\text{Note}\] 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.

\[\text{Note}\] It may take up to 5 minutes for the VM to power on.
Chapter 4      Configuring the Software Using the CLI

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.
CLI Software Configuration Process

**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**.
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)SVI(4b)*.

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 svfs 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(4b),
Do you want to reconfigure? (yes/no) [n] yes
  Current vem feature level is set to 4.2(1)SV1(4b)
  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
  svfs-domain
  svfs 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.
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(4b).

**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(4b).

**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.
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 config t</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>n1000v# config t</td>
<td></td>
</tr>
<tr>
<td>n1000v(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 2 svs connection name</td>
<td>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.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>n1000v (config#) svs connection VC</td>
<td></td>
</tr>
<tr>
<td>n1000v(config-svs-conn#)</td>
<td></td>
</tr>
</tbody>
</table>
# CLI Software Configuration Process

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Step 3** | protocol vmware-vim [http]  
Example: n1000v(config-svs-conn#) protocol vmware-vim  
n1000v(config-svs-conn#)  
| Specifies that this connection uses the VIM protocol. This command is stored locally.  
- **http**: Specifies that the VIM protocol runs over HTTP. The default is to use HTTP over SSL (HTTPS). |
| **Step 4** | remote ip address ipaddress  
Example: n1000v(config-svs-conn#) remote ip address  
172.28.15.150  
n1000v(config-svs-conn#)  
| Specifies the IP address of the ESX server or vCenter Server for this connection. This command is stored locally. |
| **Step 5** | vmware dvs datacenter-name name  
Example: n1000v(config-svs-conn#) vmware dvs datacenter-name  
Hamilton-DC  
n1000v(config-svs-conn#)  
| Identifies the datacenter name in the vCenter Server where Cisco Nexus 1000V is to be created as a distributed virtual switch (DVS). You can use this command before or after connecting. The datacenter name is stored locally. |
| **Step 6** | connect  
Example: n1000v(config-svs-conn#) connect  
| Initiates the connection.  
**Note**: It may take up to 10 seconds to connect the first time.  
If the username and password have not been configured for this connection, the user is prompted for a username and password.  
There can be only one active connection at a time. If a previously-defined connection is up, an error message displays and the command is rejected until you close the previous connection using the no connect command.  
**Note**: If the connection is not initiated, see the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(4b)*. |
| **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,  

```mmdm
no connect  
connect
``` |
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
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(4a).

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(4a).
- 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`
Chapter 4  Configuring the Software Using the CLI

CLI Software Configuration Process

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

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> config t</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:**  
n1000v# config t  
n1000v(config)# |             |
| **Step 2** port-profile type ethernet name | Enters port profile configuration mode for the named port profile. If the port profile does not already exist, it is created using the following characteristics:  
  - name—The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V.  
  - type—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.  
  Defining a port profile type as Ethernet allows the port profile to be used for physical (Ethernet) ports. In the vCenter Server, the corresponding port group can be selected and assigned to physical ports (PNICs).  
**Note** If a port profile is configured as an Ethernet type, then it cannot be used to configure VMware virtual ports. |
| **Example:**  
n1000v(config)# port-profile type ethernet system-uplink  
n1000v(config-port-prof)# |             |
| **Step 3** description profile_description | Adds a description to the port profile. This description is automatically pushed to the vCenter Server.  
**profile description:** up to 80 ASCII characters  
**Note** If the description includes spaces, it must be surrounded by quotations. |
| **Example:**  
n1000v(config-port-prof)# description "System profile for critical ports"  
n1000v(config-port-prof)# |             |
| **Step 4** switchport mode trunk | Designates that the new port profile is used as a trunk port, |
| **Example:**  
n1000v(config-port-prof)# switchport mode trunk  
n1000v(config-port-prof)# |             |
| **Step 5** switchport trunk allowed vlan vlan_IDs | Specifies the VLANs allowed on the trunk port for the new port profile. |
| **Example:**  
n1000v(config-port-prof)# switchport trunk allowed vlan 260 |             |
| **Step 6** no shutdown | Administratively enables all ports in the new port profile. |
| **Example:**  
n1000v(config-port-prof)# no shutdown  
n1000v(config-port-prof)# |             |
## CLI Software Configuration Process

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

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>system vlan vlan_ID_list</strong></td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
| **Example:** | n1000v(config-port-prof)# system vlan 260  
n1000v(config-port-prof)# |
| **Note** | If you defined separate control and packet VLANs, then add another system VLAN. |

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>mtu mtu-size</strong></td>
<td>(Optional) Designates the MTU size.</td>
<td></td>
</tr>
</tbody>
</table>
| **Example:** | n1000v(config-port-prof)# mtu 4000  
n1000v(config-port-prof)# |
| - | 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. |

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>vmware port-group [portgroup_name]</strong></td>
<td>Designates the port profile as a VMware port group of the same name.</td>
<td></td>
</tr>
</tbody>
</table>
| **Example:** | n1000v(config-port-prof)# vmware port-group  
system-uplink  
n1000v(config-port-prof)# |
| 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. |

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>state enabled</strong></td>
<td>Enables the new system port profile.</td>
<td></td>
</tr>
</tbody>
</table>
| **Example:** | n1000v(config-port-prof)# state enabled  
n1000v(config-port-prof)# |
| 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. |
| A Distributed Virtual Port Group is now visible under the VSM Name on the vSphere Client Inventory > Networking > DataCenter tab. |
Example Configuration: System Profile for Critical Ports

```plaintext
config t
port-profile type ethernet system-uplink
description "System profile for critical ports"
switchport mode trunk
switchport trunk allowed vlan 260
no shutdown
system vlan 260
vmware port group system-uplink
state enabled
```
Configuring the Uplink Port Profile for VM Traffic

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

BEFORE YOU BEGIN

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

- You 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 4-19.
- 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 trunk`
5. `switchport trunk allowed vlan vlan_IDs`
6. `channel-group auto [mode {on | active | passive}] [mac-pinning]`
7. `vmware port-group [portgroup_name]`
8. `no shutdown`
9. `state enabled`
10. `show port-profile [brief | expand-interface | usage] [name profile-name]`
11. `copy running-config startup-config`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>config t</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

Example:

```
n1000v# config t
n1000v(config)#
```
**Step 2**

```plaintext
port-profile type ethernet name
```

Example:
```plaintext
n1000v(config)# port-profile type ethernet
vm-uplink
n1000v(config-port-prof)#
```

- **type**: Defines the port-profile as Ethernet or vEthernet type. Once configured, this setting cannot be changed. The default is vEthernet type.

- **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**

```plaintext
description profile_description
```

Example:
```plaintext
n1000v(config-port-prof)# description "Uplink profile for VM Traffic"
n1000v(config-port-prof)#
```

- **profile description**: up to 80 ASCII characters

**Step 4**

```plaintext
switchport mode trunk
```

Example:
```plaintext
n1000v(config-port-prof)# switchport mode
trunk
n1000v(config-port-prof)#
```

- **profile description**: up to 80 ASCII characters

**Step 5**

```plaintext
switchport trunk allowed vlan vlan_IDs
```

Example:
```plaintext
n1000v(config-port-prof)# trunk allowed vlan
260
n1000v(config-port-prof)#
```

- **profile description**: up to 80 ASCII characters

**Step 6**

```plaintext
channel-group auto [mode {on {active | passive}} [mac-pinning]]
```

Example:
```plaintext
n1000v(config-port-prof)# channel-group auto
mode on
n1000v(config-port-prof)#
```

- **mode**—Sets the port channel mode to on, active, or passive (active and passive use LACP).
- **mac-pinning**—If the upstream switch does not support port channels, this designates that one subgroup per Ethernet member port must be automatically assigned.
## CLI Software Configuration Process

### Step 7

**Command**
```
vmware port-group [portgroup_name]
```

**Example:**
```
n1000v(config-port-prof)# vmware port-group
vm-uplink
n1000v(config-port-prof)#
```

**Description:**
Designates the port profile as a VMware port group of the same name. The port profile is mapped to a VMware port group. When a vCenter Server connection is established, this port group is then distributed to the virtual switch on the vCenter Server.

### Step 8

**Command**
```
no shutdown
```

**Example:**
```
n1000v(config-port-prof)# no shutdown
n1000v(config-port-prof)#
```

**Description:**
Administratively enables all ports in the new port profile.

### Step 9

**Command**
```
state enabled
```

**Example:**
```
n1000v(config-port-prof)# state enabled
n1000v(config-port-prof)#
```

**Description:**
Enables the new uplink port profile for VM traffic. 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. A Distributed Virtual Port Group is now visible under the VSM Name on the vSphere Client Inventory > Networking > DataCenter tab.

### Step 10

**Command**
```
show port-profile name profile-name
```

**Example:**
```
n1000v(config-port-prof)# show port-profile name vm-uplink
port-profile vm-uplink
description: 'Uplink profile for VM traffic

type: ethernet
status: enabled
capability l3control: no
pinning control-vlan: -
pinning packet-vlan: -
system vlans: none
port-group: vm-uplink
max ports: -
inherit:
config attributes:
  switchport mode access
  switchport access vlan 260
  no shutdown
evaluated config attributes:
  switchport mode access
  switchport access vlan 260
  no shutdown
assigned interfaces:
n1000v(config-port-prof)#
```

**Description:**
(Optional) Displays the vm-uplink port profile configuration.

### Step 11

**Command**
```
copy running-config startup-config
```

**Example:**
```
n1000v(config-port-prof)# copy running-config
startup-config
[########################################]
100%
```

**Description:**
Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

**Caution**
If you do not copy this configuration to the startup configuration, then in the event of a VSM reboot, this port group will continue to exist on the vCenter Server but not on the VSM.

### Step 12

You have completed this procedure.

Return to the CLI Software Configuration Process, page 4-1 to continue setting up your VSM.
Example Configuration: Uplink Profile for VM Traffic

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

Configuring the Data Port Profile for VM Traffic

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

BEFORE YOU BEGIN

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

- You 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 4-22. For more information about using scripts, see the Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(4b).

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config t</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

Example:
```
n1000v# config t
n1000v(config)#
```
Chapter 4  Configuring the Software Using the CLI

### Command Description

<table>
<thead>
<tr>
<th>Step 2</th>
<th>port-profile {type {ethernet | vethernet}} name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>n1000v(config)# port-profile type vethernet data20 n1000v(config-port-prof)#</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>- <strong>name</strong>—The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V.</td>
</tr>
<tr>
<td></td>
<td>- <strong>type</strong>—(Optional) The port profile type can be Ethernet or vEthernet. Once configured, the type cannot be changed. The default is the vEthernet type.</td>
</tr>
<tr>
<td></td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If a port profile is configured as an Ethernet type, then it cannot be used to configure VMware virtual ports.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>description profile_description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>n1000v(config-port-prof)# description &quot;Data profile for VM Traffic&quot; n1000v(config-port-prof)#</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Adds a description of up to 80 ASCII characters to the port profile. This description is automatically pushed to the vCenter Server.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>switchport mode access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>n1000v(config-port-prof)# switchport mode access n1000v(config-port-prof)#</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Designates that the new port profile is used as an access port.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>switchport access vlan vlan_ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>n1000v(config-port-prof)# switchport access vlan 20</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Specifies the access VLAN for the new port profile.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>no shutdown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>n1000v(config-port-prof)# no shutdown n1000v(config-port-prof)#</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Administratively enables all ports in the new port profile.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>vmware port-group {portgroup_name}</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>n1000v(config-port-prof)# vmware port-group data20 n1000v(config-port-prof)#</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
### 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.

**Caution**
If you do not copy this configuration to the startup
configuration, then in the event of a VSM reboot,
this port group will continue to exist on the
vCenter Server but not on the VSM

### Step 11
You have completed this procedure.

Return to the CLI Software Configuration Process, page 4-1 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
```

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:

<table>
<thead>
<tr>
<th>Traffic</th>
<th>VMNIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control VLAN</td>
<td>system-uplink VMNIC</td>
</tr>
<tr>
<td>Packet VLAN</td>
<td>system-uplink VMNIC</td>
</tr>
<tr>
<td>VM data</td>
<td>VM-uplink Port Group</td>
</tr>
</tbody>
</table>

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 VEM Software Installation and Upgrade Guide, Release 4.2(1)SV1(4b)*.
- 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(4a)*.
- 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.
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(4b)*.

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.
CLI Software Configuration Process

Chapter 4 Configuring the Software Using the CLI

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(4a)*.

**Step 6** Click Next.
Step 7: Verify the port group assignment and click **Finish**.

Step 8: Do one of the following:
- If the host is successfully added to the DVS, continue with the next step.
- If the operation fails, see the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(4b)*.

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

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

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

BEFORE YOU BEGIN

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

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

Step 1 On the ESX server host where the VSM is installed, add the VEM software using your VMware documentation and the Cisco Nexus 1000V VEM Software Installation and Upgrade Guide, Release 4.2(1)SV1(4b).

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

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

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

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

Step 6 Remove the vSwitches.
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
```
domain id 4
control vlan 101
packet vlan 103
svs mode L2
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.
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.

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

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.
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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>n1000v# configure terminal</td>
<td></td>
</tr>
<tr>
<td>n1000v(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 2 interface type number</td>
<td>Enters interface configuration mode for the interface you want to configure.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>n1000v(config)# interface</td>
<td></td>
</tr>
<tr>
<td>ethernet 3/2</td>
<td></td>
</tr>
<tr>
<td>n1000v(config-if)#</td>
<td></td>
</tr>
</tbody>
</table>

For details about interface commands and configuration, see the document, *Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4a)*.
### Exiting a Configuration Mode

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **exit** | Exits from the current configuration command mode and return to the previous configuration command mode.  
Example:  
svs(config-if)# exit  
svs(config)# |
| **end** | Exits from the configuration command mode and returns to EXEC mode.  
Example:  
svs(config)# end  
svs# |
| **Ctrl-z** | Exits the current configuration command mode and returns to EXEC mode.  
Example:  
svs(config)# ^z  
svs# |

**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.
# Command Mode Summary

Table 6-1 summarizes information about command modes.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC</td>
<td>From the login prompt, enter your username and password.</td>
<td>n1000v#</td>
<td>To exit to the login prompt, use the <code>exit</code> command.</td>
</tr>
<tr>
<td>Global Configuration</td>
<td>From EXEC mode, enter the command, <code>configure terminal</code>.</td>
<td>n1000v(config)#</td>
<td>To exit to EXEC mode, use the <code>end</code> or <code>exit</code> command or press Ctrl-Z.</td>
</tr>
<tr>
<td>Port Profile Configuration</td>
<td>From Global Configuration mode, enter the command, <code>port-profile name</code>.</td>
<td>n1000v(config-port-prof)#</td>
<td>To exit to Port Profile Configuration mode, use the <code>exit</code> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To exit to EXEC mode, use the <code>end</code> command or press Ctrl-Z.</td>
</tr>
<tr>
<td>Interface Configuration</td>
<td>From Global Configuration mode, enter the <code>interface</code> command for a specific interface, for example, <code>interface veth 2</code></td>
<td>n1000v(config-if)#</td>
<td>To exit to Interface Configuration mode, use the <code>exit</code> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To exit to EXEC mode, use the <code>end</code> command or press Ctrl-Z.</td>
</tr>
<tr>
<td>VLAN Configuration</td>
<td>Use a <code>vlan</code> command.</td>
<td>n1000v(config-vlan)#</td>
<td>To exit to VLAN Configuration mode, use the <code>exit</code> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To exit to EXEC mode, use the <code>end</code> command or press Ctrl-Z.</td>
</tr>
<tr>
<td>Console Configuration</td>
<td>From Global Configuration mode, use the <code>line console</code> command.</td>
<td>n1000v(config-console)</td>
<td>To exit to Console Configuration mode, use the <code>exit</code> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To exit to EXEC mode, use the <code>end</code> command or press Ctrl-Z.</td>
</tr>
<tr>
<td>Virtual Terminal Line Configuration</td>
<td>From Global Configuration mode, use the <code>line vty</code> command.</td>
<td>n1000v(config-line)#</td>
<td>To exit to Line Configuration mode, use the <code>exit</code> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To exit to EXEC mode, use the <code>end</code> command or press Ctrl-Z.</td>
</tr>
<tr>
<td>SVS Domain Configuration</td>
<td>From Global Configuration mode, use the <code>svs-domain</code> command.</td>
<td>n1000v(config-svs-domain)#</td>
<td>To exit to SVS Domain Configuration mode, use the <code>exit</code> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To exit to EXEC mode, use the <code>end</code> command or press Ctrl-Z.</td>
</tr>
<tr>
<td>Policy Map QoS Configuration</td>
<td>From Global Configuration mode, use the <code>policy-map</code> command.</td>
<td>n1000v(config-pmap-qos)#</td>
<td>To exit to Policy Map QoS Configuration mode, use the <code>exit</code> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To exit to EXEC mode, use the <code>end</code> command or press Ctrl-Z.</td>
</tr>
</tbody>
</table>
Chapter 6  Understanding the CLI

**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.

---

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

<table>
<thead>
<tr>
<th>Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Map Class QoS</td>
<td>From Policy-Map QoS Configuration mode, use the class command.</td>
<td>n1000v(config-pmap-c-qos)#</td>
<td>To exit to Policy Map Class QoS Configuration mode, use the <code>exit</code> command.</td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
<td></td>
<td>To exit to EXEC mode, use the <code>end</code> command or press Ctrl-Z.</td>
</tr>
<tr>
<td>Class Map QoS</td>
<td>From Global Configuration mode, use the <code>class-map</code> command.</td>
<td>n1000v(config-cmap-qos)#</td>
<td>To exit to Class Map QoS Configuration mode, use the <code>exit</code> command.</td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
<td></td>
<td>To exit to EXEC mode, use the <code>end</code> command or press Ctrl-Z.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\</td>
<td>Vertical bar</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Less than or greater than</td>
</tr>
</tbody>
</table>

Keystroke Shortcuts

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

<table>
<thead>
<tr>
<th>Key(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-A</td>
<td>Moves the cursor to the beginning of the line</td>
</tr>
<tr>
<td>Ctrl-B</td>
<td>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.</td>
</tr>
<tr>
<td>Ctrl-C</td>
<td>Cancels the command and returns to the command prompt.</td>
</tr>
<tr>
<td>Ctrl-D</td>
<td>Deletes the character at the cursor.</td>
</tr>
<tr>
<td>Ctrl-E</td>
<td>Moves the cursor to the end of the line.</td>
</tr>
<tr>
<td>Ctrl-F</td>
<td>Moves the cursor one character to the right.</td>
</tr>
<tr>
<td>Ctrl-G</td>
<td>Exits to the previous command mode without removing the command string.</td>
</tr>
<tr>
<td>Ctrl-K</td>
<td>Deletes all characters from the cursor to the end of the command line.</td>
</tr>
<tr>
<td>Ctrl-L</td>
<td>Redisplays the current command line.</td>
</tr>
<tr>
<td>Ctrl-R</td>
<td>Redisplays the current command line.</td>
</tr>
</tbody>
</table>
Send document comments to nexus1k-docfeedback@cisco.com.

### Table 6-3 Keystroke Shortcuts (continued)

<table>
<thead>
<tr>
<th>Key(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-T</td>
<td>Transposes the character to the left of the cursor with the character located to the right of the cursor.</td>
</tr>
<tr>
<td>Ctrl-U</td>
<td>Deletes all characters from the cursor to the beginning of the command line.</td>
</tr>
<tr>
<td>Ctrl-W</td>
<td>Deletes the word to the left of the cursor.</td>
</tr>
<tr>
<td>Ctrl-X, H</td>
<td>List history. When using this key combination, press and release the Ctrl and X keys together before pressing H.</td>
</tr>
<tr>
<td>Ctrl-Y</td>
<td>Recalls the most recent entry in the buffer (press keys simultaneously).</td>
</tr>
<tr>
<td>Ctrl-Z</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>↑</td>
<td>Displays the previous command in the command history.</td>
</tr>
<tr>
<td>↓</td>
<td>Displays the next command in the command history.</td>
</tr>
<tr>
<td>←→</td>
<td>Moves your cursor through the command history directionally to locate a command string.</td>
</tr>
<tr>
<td>?</td>
<td>Displays a list of available commands.</td>
</tr>
<tr>
<td>Tab</td>
<td>Completes the word for you after entering the first characters of the word, and then pressing the Tab key. All options that match are presented. Used to complete:</td>
</tr>
<tr>
<td></td>
<td>• command names</td>
</tr>
<tr>
<td></td>
<td>• scheme names in the file system</td>
</tr>
<tr>
<td></td>
<td>• server names in the file system</td>
</tr>
<tr>
<td></td>
<td>• file names in the file system</td>
</tr>
</tbody>
</table>

**Example**

```
n1000v(config)# xm<Tab>  
n1000v(config)# xml <Tab>  
n1000v(config)# xml server
```

**Example**

```
n1000v(config)# c<Tab>  
callhome class-map clock cts  
cdp cli control-plane
```

```
n1000v(config)# cl<Tab>  
class-map cli clock
```

```
n1000v(config)# cla<Tab>  
class-map
```
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>conf t</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>copy run start</td>
</tr>
<tr>
<td>interface ethernet 1/2</td>
<td>int e 1/2</td>
</tr>
<tr>
<td>show running-config</td>
<td>sho run</td>
</tr>
</tbody>
</table>

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(SV1(4a))* 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:

```bash
n1000v(config)# boot system bootflash: svs1.bin
n1000v(config)# no boot system bootflash: svs1.bin
```
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)
mgmt 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.
The following example removes a user-defined CLI persistent variable.

```plaintext
n1000v# config t
n1000v(config)# cli no var name mgmtp
```

### 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:**

```plaintext
n1000v# show running-config > rcfg.$(TIMESTAMP)
n1000v# dir
```

### 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.

```plaintext
n1000v# show file bootflash:testfile
conf t
show interface mgmt 0
```
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.4dac)
  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
```
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)`
```

<table>
<thead>
<tr>
<th>Ethernet</th>
<th>VLAN</th>
<th>Type</th>
<th>Mode</th>
<th>Status</th>
<th>Reason</th>
<th>Speed</th>
<th>Port Ch #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth2/45</td>
<td>--</td>
<td>eth</td>
<td>routed</td>
<td>down</td>
<td>Administratively</td>
<td>auto(D)</td>
<td>--</td>
</tr>
</tbody>
</table>

**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.

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

The following example describes how to use syntax error isolation and context-sensitive help.
### Chapter 6  Understanding the CLI

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

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>show interface virtual ?</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>n1000v# show interface virtual ?</td>
</tr>
<tr>
<td></td>
<td>&lt;CR&gt;</td>
</tr>
<tr>
<td></td>
<td>module</td>
</tr>
<tr>
<td></td>
<td>vm</td>
</tr>
<tr>
<td></td>
<td>vmk</td>
</tr>
<tr>
<td></td>
<td>vswif</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

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

**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 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
```

**Command** | **Purpose**
--- | ---
**Step 6** show module ? | Displays the optional parameters for the show module command.
**Step 7** show module | Displays module information.

**Example 6-1** show interface virtual

```
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 virtual module ?
^% invalid command detected at '^' marker.
n1000v# <Ctrl-P>
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
```
**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

```bash
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
sshsServer                        1           enabled
tacacs                            1           enabled
telnetServer                      1           enabled
n1000v#
```
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.
Chapter 7      Configuring the Terminal

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>terminal length number of lines</td>
<td>Configures the number of lines to display on the screen for the current console session.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>n1000v# terminal length 20 n1000v#</td>
<td>Range = 0 to 511 lines</td>
</tr>
<tr>
<td></td>
<td>Default = 24 lines</td>
</tr>
<tr>
<td></td>
<td>Disable = 0 (scrolls continuously)</td>
</tr>
</tbody>
</table>

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.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>terminal terminal-type type</td>
<td>Configures a terminal type for the switch.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>n1000v# terminal terminal-type vt100 n1000v#</td>
<td>Valid types = vt100, xterm, etc.</td>
</tr>
<tr>
<td></td>
<td>Default = vt100</td>
</tr>
<tr>
<td></td>
<td>Maximum string length = 80 characters</td>
</tr>
<tr>
<td></td>
<td>If an unknown terminal type is used for a Telnet or SSH session, then the switch uses the default, vt100.</td>
</tr>
</tbody>
</table>
**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**

**Step 1**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>terminal width</strong></td>
<td>Configures the number of characters to display on each line for the current console session.</td>
</tr>
</tbody>
</table>
| **number of characters** | - Range = 24 to 511 characters  
                     | - Default = 88 characters                                                  |

**Example:**

n1000v# terminal width 86
n1000v#

**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.
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> config t</td>
<td>Places you into the CLI Global Configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>n1000v # config t</td>
<td></td>
</tr>
<tr>
<td>n1000v(config)#</td>
<td></td>
</tr>
</tbody>
</table>

| Step 2                  |                                                                         |
| line console            | Places you into the Console Configuration mode.                          |
| Example:                |                                                                         |
| n1000v(config)# line console |                                                       |
| n1000v(config-console)# |                                                                         |

| Step 3                  |                                                                         |
| exec-timeout minutes    | 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. |
| Example:                |                                                                         |
| n1000v(config-console)# exec-timeout 60 |                                                |
| n1000v(config-console)# |                                                                         |

- 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.
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 clear line aux</td>
<td>Closes a line connection.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>n1000v# clear line aux</td>
<td></td>
</tr>
<tr>
<td>n1000v #</td>
<td></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2 line vty</td>
<td>Places you into the Virtual Terminal Line Configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>n1000v(config)# line vty</td>
<td></td>
</tr>
<tr>
<td>n1000v(config-line)#</td>
<td></td>
</tr>
<tr>
<td>Step 3 exec-timeout minutes</td>
<td>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.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>n1000v(config-line)# exec-timeout 60</td>
<td></td>
</tr>
<tr>
<td>n1000v(config-line)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Range = 0 to 525, 600 minutes</td>
</tr>
<tr>
<td></td>
<td>Default = 30 minutes</td>
</tr>
<tr>
<td></td>
<td>Disable (no timeout) = 0 minutes</td>
</tr>
<tr>
<td></td>
<td>If you set the timeout to zero, then the line connection remains alive until you close it.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 clear line aux</td>
<td>Closes a line connection.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>n1000v# clear line aux</td>
<td></td>
</tr>
<tr>
<td>n1000v #</td>
<td></td>
</tr>
</tbody>
</table>
## Setting a Timeout for the Current Session

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

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1 | `terminal session minutes` | Configures the duration of time, in minutes, that the current terminal session can remain open before the switch shuts it down.  
   - Range = 0 to 525, 600 minutes  
   - Disable (no timeout) = 0 minutes  
   This change is not saved in the configuration file since it only applies to the current session. |

**Example:**

```
n1000v# terminal session 600
n1000v#
```
# Configuration Limits

**Table 8-1  Configuration Limits for Cisco Nexus 1000V**

<table>
<thead>
<tr>
<th>Component</th>
<th>Supported Limits for Cisco Nexus 1000V in the Same Datacenter</th>
<th>Supported Limits for Cisco Nexus 1000V Across Two Datacenters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Modules</td>
<td>66</td>
<td>34</td>
</tr>
<tr>
<td>Virtual Ethernet Module(VEM)</td>
<td>64</td>
<td>32</td>
</tr>
<tr>
<td>Virtual Supervisor Module (VSM)</td>
<td>2 in an HA Pair (active-standby hosted in the same datacenter)</td>
<td>2 in an HA Pair (active-standby hosted in the same datacenter)</td>
</tr>
<tr>
<td>vCenter Server Datacenters per VSM</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Hosts</td>
<td>64</td>
<td>32</td>
</tr>
<tr>
<td>Active VLANs across all VEMs</td>
<td>2048</td>
<td>1024</td>
</tr>
<tr>
<td>MACs per VEM</td>
<td>32000</td>
<td>32000</td>
</tr>
<tr>
<td>MACs per VLAN per VEM</td>
<td>4000</td>
<td>4000</td>
</tr>
<tr>
<td>vEthernet interfaces per port profile</td>
<td>1024</td>
<td>1024</td>
</tr>
<tr>
<td>PVLAN</td>
<td>512</td>
<td>128</td>
</tr>
<tr>
<td>Distributed Virtual Switches (DVSes) per vCenter</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>vCenter Server connections</td>
<td>1 per VSM HA Pair&lt;sup&gt;1&lt;/sup&gt;</td>
<td>1 per VSM HA Pair&lt;sup&gt;1&lt;/sup&gt;</td>
</tr>
<tr>
<td>Maximum latency between VSMs and VEMs</td>
<td>—</td>
<td>5 ms</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Per DVS</th>
<th>Per Host</th>
<th>Per DVS</th>
<th>Per Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service Domains (VSDs)</td>
<td>64</td>
<td>6</td>
<td>32</td>
</tr>
<tr>
<td>VSD interfaces</td>
<td>2048</td>
<td>216</td>
<td>1024</td>
</tr>
<tr>
<td>vEthernet interfaces</td>
<td>2048</td>
<td>216</td>
<td>1024</td>
</tr>
<tr>
<td>Port profiles</td>
<td>2048</td>
<td>—</td>
<td>1024</td>
</tr>
<tr>
<td>System port profiles</td>
<td>32</td>
<td>32</td>
<td>16</td>
</tr>
<tr>
<td>Port channels</td>
<td>256</td>
<td>8</td>
<td>128</td>
</tr>
<tr>
<td>Physical trunks</td>
<td>512</td>
<td>—</td>
<td>256</td>
</tr>
<tr>
<td>Physical NICs</td>
<td>—</td>
<td>32</td>
<td>—</td>
</tr>
</tbody>
</table>
### Table 8-1  Configuration Limits for Cisco Nexus 1000V (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Supported Limits for Cisco Nexus 1000V in the Same Datacenter</th>
<th>Supported Limits for Cisco Nexus 1000V Across Two Datacenters</th>
</tr>
</thead>
<tbody>
<tr>
<td>vEthernet trunks</td>
<td>256 8</td>
<td>128 4</td>
</tr>
<tr>
<td>ACLs</td>
<td>128 16&lt;sup&gt;2&lt;/sup&gt;</td>
<td>64 8&lt;sup&gt;2&lt;/sup&gt;</td>
</tr>
<tr>
<td>ACEs per ACL</td>
<td>128 128&lt;sup&gt;2&lt;/sup&gt;</td>
<td>64 64&lt;sup&gt;2&lt;/sup&gt;</td>
</tr>
<tr>
<td>ACL interfaces</td>
<td>2048 256</td>
<td>1024 128</td>
</tr>
<tr>
<td>NetFlow policies</td>
<td>32 8</td>
<td>16 4</td>
</tr>
<tr>
<td>NetFlow interfaces</td>
<td>256 32</td>
<td>128 16</td>
</tr>
<tr>
<td>SPAN/ERSPAN sessions</td>
<td>64 64</td>
<td>32 32</td>
</tr>
<tr>
<td>QoS policy maps</td>
<td>128 128</td>
<td>64 64</td>
</tr>
<tr>
<td>QoS class maps</td>
<td>1024 1024</td>
<td>512 512</td>
</tr>
<tr>
<td>QoS interfaces</td>
<td>2048 256</td>
<td>1024 128</td>
</tr>
<tr>
<td>Port security</td>
<td>2048 216</td>
<td>1024 108</td>
</tr>
<tr>
<td>Multicast groups</td>
<td>512 512</td>
<td>256 256</td>
</tr>
<tr>
<td>DHCP snoop binding entries (static + dynamic)</td>
<td>2048 2048</td>
<td>1024 1024</td>
</tr>
</tbody>
</table>

1. Only one connection to vCenter server is permitted at a time.
2. This number can be exceeded if VEM has available memory.
List of Terms

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

<table>
<thead>
<tr>
<th>Table 9-1</th>
<th><strong>Cisco Nexus 1000V Terminology</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Term</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Control VLAN</td>
<td>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.</td>
</tr>
<tr>
<td>Distributed Resource Scheduler (DRS)</td>
<td>Balances the workload across your defined resources (hosts, shared storage, network presence, and resource pools) in a cluster.</td>
</tr>
<tr>
<td>Distributed Virtual Switch (DVS)</td>
<td>This is a logical switch that spans one or more VMware ESX 4.0 servers. It is controlled by one VSM instance.</td>
</tr>
<tr>
<td>ESX/ESXi</td>
<td>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.</td>
</tr>
<tr>
<td>Managed Object Browser (MOB)</td>
<td>A tool that enables you to browse managed objects on VirtualCenter Server and ESX Server systems.</td>
</tr>
<tr>
<td>Network Interface Card (NIC)</td>
<td>Network Interface Card. PNIC: physical network interface card vNIC:</td>
</tr>
<tr>
<td>Open Virtual Appliance or Application (OVA) file</td>
<td>The package that contains the following files used to describe a virtual machine and saved in a single archive using .TAR packaging.</td>
</tr>
<tr>
<td></td>
<td>- Descriptor file (.OVF)</td>
</tr>
<tr>
<td></td>
<td>- Manifest (.MF) and certificate files (optional)</td>
</tr>
<tr>
<td>Packet VLAN</td>
<td>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.</td>
</tr>
</tbody>
</table>
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)  
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.

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.

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)  
The software application that manages Cisco Nexus 1000V software installation and VEM upgrades.

Note  
VUM is not a requirement. Software can be installed manually without using VUM.

vSphere Client  
The user interface that lets users connect remotely to the vCenter Server or ESX/ESXi from any windows PC. The primary interface for creating, managing, and monitoring virtual machines, their resources, and their hosts. It also provides console access to virtual machines.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Profile</td>
<td>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.</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>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).</td>
</tr>
<tr>
<td>Virtual Ethernet Interface (vEth)</td>
<td>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.</td>
</tr>
<tr>
<td>Virtual Ethernet Module (VEM)</td>
<td>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. 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.</td>
</tr>
<tr>
<td>Virtual Machine (VM)</td>
<td>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.</td>
</tr>
<tr>
<td>VMotion</td>
<td>The practice of migrating virtual machines live from server to server.</td>
</tr>
<tr>
<td>Virtual NIC (vNIC)</td>
<td>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.</td>
</tr>
<tr>
<td>Virtual Supervisor Module (VSM)</td>
<td>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.</td>
</tr>
<tr>
<td>VMware Infrastructure Bundle (VIB)</td>
<td>The package format used by VMware ESX 4.0 release.</td>
</tr>
<tr>
<td>VMware update manager (VUM)</td>
<td>The software application that manages Cisco Nexus 1000V software installation and VEM upgrades. Note VUM is not a requirement. Software can be installed manually without using VUM.</td>
</tr>
<tr>
<td>vSphere Client</td>
<td>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.</td>
</tr>
</tbody>
</table>
INDEX

Symbols

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

A

add host to DVS
   CLI setup  4-23
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, 4-21
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
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 4-23
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, 3-22
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-viii
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
Index

**U**

uplink port profile
   CLI setup  **4-16**

**V**

vCenter identification, GU setup  **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
      credentials
         CLI setup  **4-3**
         GUI setup  **3-4, 3-22**
   host, GUI setup  **3-5**