CHAPTER 2

Setting Up the Software

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

Note To install the Cisco Nexus 1000V software on your ESX or ESXi 4.0 VMware server, see the *Cisco Nexus 1000V Software Installation Guide, Release 4.0(4)SV1(3)*.

This chapter includes the following topics:

- Prerequisites, page 2-3
- Software Configuration Process, page 2-6
- Verifying the Configuration, page 2-9
- Starting the VMs, page 2-10
- Implementation Guidelines, page 2-11

Information About Setting Up the Software

A setup configuration process helps you with your initial configuration of the Cisco Nexus 1000V.

Setting up a Configuration File

Whether you use the CLI or the GUI, the software prompts 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 netmas
- 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 include 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 4.0(4)SV1(3)*.

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

Caution The VSM VM configuration will fail unless the NICs are specified as shown in Table 2-1.

Table 2-1 Required NIC Configuration

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

1. See Figure 2-1Cisco Nexus 1000V Configuration Example, page 2-5.

Prerequisites

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

- You have already installed the Cisco Nexus 1000V software and configured the following using the *Cisco Nexus 1000V Software Installation Guide, Release 4.0(4)SV1(3)*.
  - 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 2-5 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.
- 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 2-11.
- You have already identified the HA role for this VSM from those listed in Table 2-2:

Table 2-2 VSM HA Roles

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

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

For more information about HA roles, see the *Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.0(4)SV1(3)*.

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

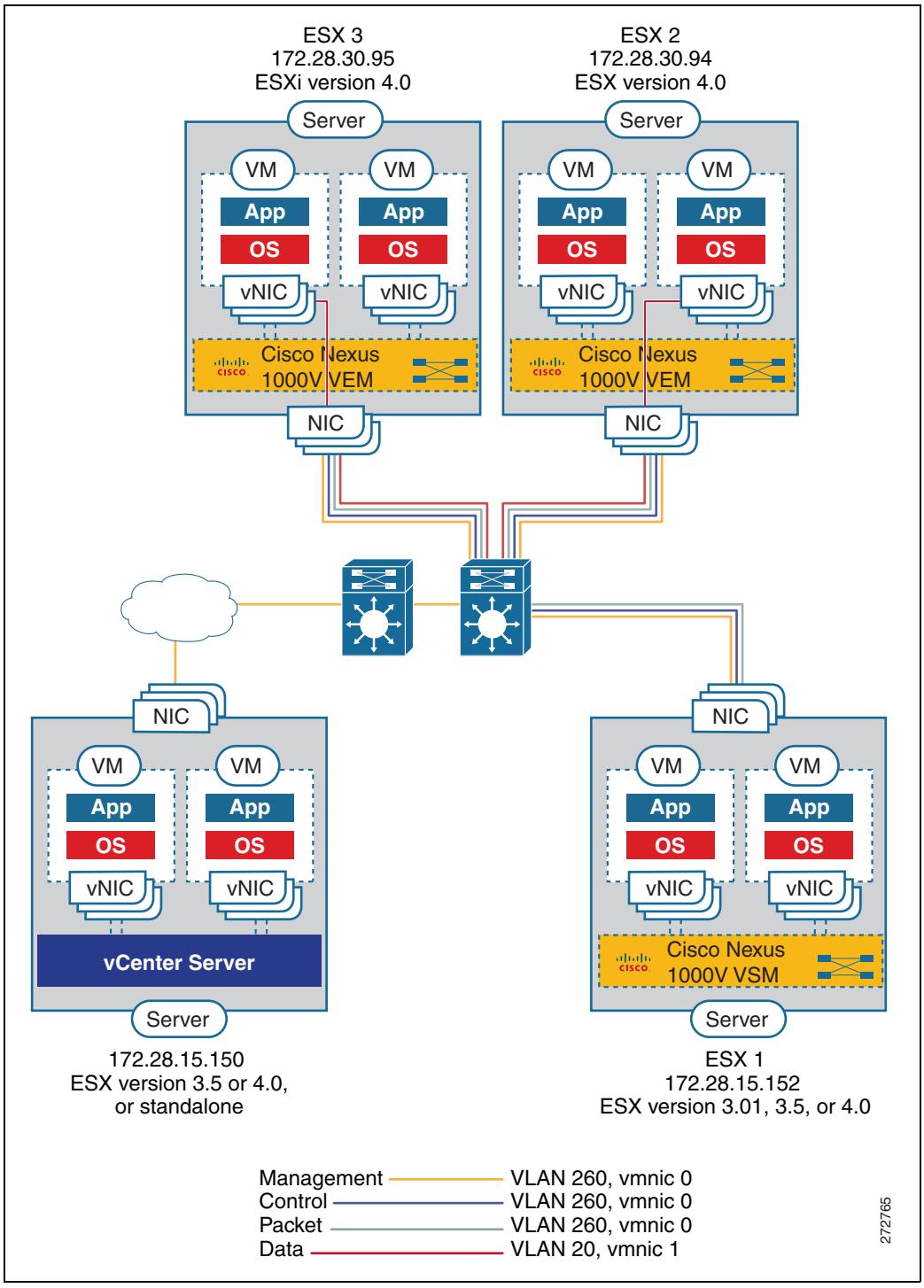
Table 2-3 Guidelines for strong passwords

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

- All ESX hosts within a Cisco Nexus 1000V VSM domain must have Layer 2 connectivity to each other.
- If you are using a set of switches, make sure that the inter-switch trunk links carry all relevant VLANs, including control and packet VLANs. The uplink should be a trunk port carrying all VLANs configured on the ESX host.
- The control traffic on the Cisco Nexus 1000V can be affected if you have configured storm control or storm suppression on an upstream switch. Since traffic storm control can drop the broadcast packets that the Cisco Nexus 1000V relies on for communication, be aware of the storm control settings on your upstream switch.
- On the host running the VSM VM, the control and packet VLANs are configured through the VMware switch and the VMNIC.
- 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



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

Step 2 Verify the configuration. See the "Verifying the Configuration" procedure on page 2-9.

Step 3 Start the VMs. See the "Starting the VMs" procedure on page 2-10.

Step 4 Do one of the following:

- If both the VSM and VEMs are working as expected, continue with the next step.
- If not, then see the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(3)*.

Step 5 Continue your implementation. See the "Implementation Guidelines" section on page 2-11.

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

Creating VLANs

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

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

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

BEFORE YOU BEGIN

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

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

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

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

- Cisco recommends that you use the same VLAN for control, packet, and management, but that you do not place data traffic on this VLAN. For flexibility, you can use separate VLANs.
- VLAN ranges used for control and packet port groups must be allowed on the upstream switch.
- Newly-created VLANs remain unused until Layer 2 ports are assigned to them.
- For information about the following, see the *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)*.
  - Assigning Layer 2 interfaces to VLANs (access or trunk ports).
  - Configuring ports as VLAN access or trunk ports and assigning ports to VLANs.
- For more information about configuring VLANs, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(3)*.

SUMMARY STEPS

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

DETAILED STEPS

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

Verifying the Configuration

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

BEFORE YOU BEGIN

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

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

DETAILED STEPS

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

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

Example:

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

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

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

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


* this terminal session
n1000v#
```

Example:

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

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

Step 2 Do one of the following:

- If the VSM and VEM are active and configured correctly, continue with the next step.
- If not, see the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(3)*.

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

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

Example:
```
n1000v# show port-profile usage

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

Example:
```
n1000v# show int brief

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

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

Step 4 You have completed this procedure.
Return to the Software Configuration Process, page 2-6.

Starting the VMs

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

BEFORE YOU BEGIN

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

- You have an IP address in the same subnet as the VMs to use for verifying VM connectivity.
- You have the VMware documentation for creating the VMs available.
- For a detailed description of the system, see the *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(3)*.

DETAILED STEPS

Step 1 Create the VMs.

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

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

Step 4 You have completed this procedure.
Return to Software Configuration Process, page 2-6.

Implementation Guidelines

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

- If two or more PNICs are required to carry the same VLANs then you must configure them in a port channel. For information about port channels, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(3)*.
- If PNICs on the same server are connected to different upstream switches, then you must configure the asymmetric port channel in host mode (vPC-HM). For more information, see the following documents:
  - *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)*
  - *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)*
- Cisco recommends that you run the VSM in HA mode. For more information about configuring HA, see the *Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.0(4)SV1(3)*.
- 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