Cisco Nexus 1000V InterCloud System Management Configuration Guide, Release 5.2(1)IC1(1.2)

First Published: October 11, 2013

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

Text Part Number: OL-30323-01

CONTENTS

Preface

This preface contains the following sections:

Audience

This publication is for network administrators who configure and maintain Cisco Nexus devices.

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

- An understanding of virtualization
- Using Virtual Machine Manager (VMM) software to create a virtual machine and configure a VMware vSwitch
- Ability to create an account on provider cloud such as Amazon Web Services (AWS).
- Knowledge of VMware vNetwork Distributed Switch is not required.

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.

Convention	Description
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

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

This document uses the following conventions:

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

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

Related Documentation for Cisco Nexus 1000V InterCloud

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

http://www.cisco.com/en/US/partner/products/ps12904/tsd_products_support_series_home.html

General Information

Cisco Nexus 1000V InterCloud Release Notes

Install and Upgrade

Cisco Nexus 1000V InterCloud Installation Guide

Configuration Guides

Cisco Nexus 1000V InterCloud License Configuration Guide

Cisco Nexus 1000V InterCloud High Availability and Redundancy Configuration Guide

Cisco Nexus 1000V InterCloud Interface Configuration Guide

Cisco Nexus 1000V InterCloud Layer 2 Configuration Guide

Cisco Nexus 1000V InterCloud Port Profile Configuration Guide

Cisco Nexus 1000V InterCloud Security Configuration Guide

Cisco Nexus 1000V InterCloud System Management Configuration Guide

Reference Guides

Cisco Nexus 1000V InterCloud Command Reference

Cisco Nexus 1000V InterCloud Verified Scalability Reference

Cisco Nexus 1000V MIB Quick Reference

Troubleshooting and Alerts

Cisco Nexus 1000V Password Recovery Procedure

Cisco Nexus 1000V Documentation

Cisco Nexus 1000V for VMware vSphere Documentation

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

Cisco Prime Network Services Controller Documentation

http://www.cisco.com/en/US/products/ps13213/tsd_products_support_series_home.html

Documentation Feedback

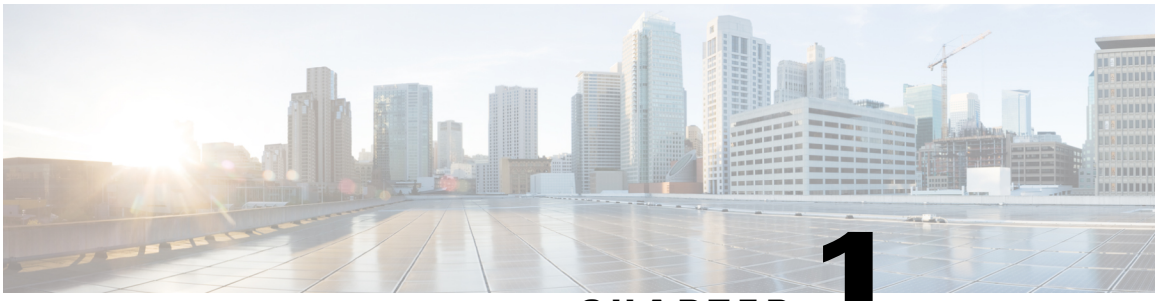
To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus1k-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

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

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

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



CHAPTER 1

New and Changed Information

This chapter contains the following sections:

New and Changed Information

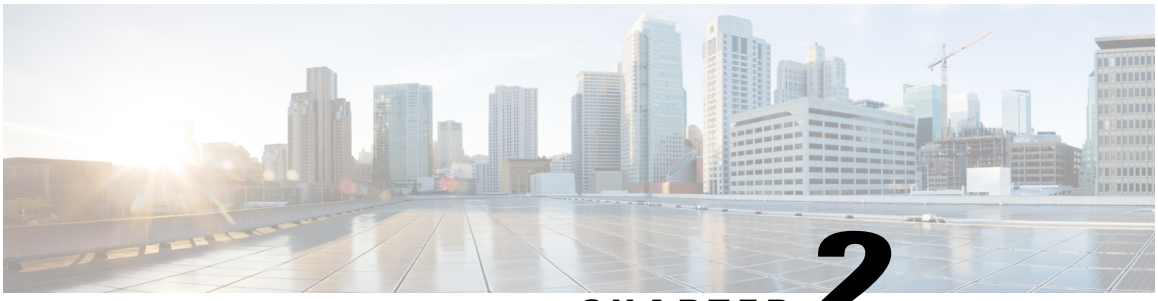
This section lists new and changed content in this document by software release.

To find additional information about new features, see the *Cisco Nexus 1000V InterCloud Release Notes*.

Table 1: New and Changed Features for the Cisco Nexus 1000V InterCloud System Management Configuration Guide

Feature	Description	Changed in Release	Where Documented
Netflow	Added support for Netflow.	5.2(1)IC1(1.2)	Configuring NetFlow, on page 65

New and Changed Information



CHAPTER 2

Overview

This chapter contains the following sections:

System Management Overview

Domains

You must create a domain ID for Cisco Nexus 1000V. This process is part of the initial setup of the Cisco Nexus 1000V when installing the software. If you need to create a domain ID later, use the **saves-domain** command to configure.

You can establish Layer 3 Control in your VSM domain so that your VSM is Layer 3 accessible and able to control hosts that reside in a separate Layer 2 network.

Server Connections

In order to connect to or an ESX server, you must first define the connection in the Cisco Nexus 1000V. Managing Server Connections describes how to connect and disconnect with and viewing connections.

Configuration Management

The Cisco Nexus 1000V provides you with the capability to change the switch name, configure messages of the day, and display, save, and erase configuration files.

File Management

Using a single interface, you can manage the file system including:

- Flash memory file systems

- Network file systems (TFTP and FTP)
- Any other endpoint for reading or writing data (such as the running configuration).

User Management

You can identify the users currently connected to the device and send a message to either a single user or all users.

NTP

The Network Time Protocol (NTP) synchronizes timekeeping among a set of distributed time servers and clients. This synchronization allows you to correlate events when you receive system logs and other time-specific events from multiple network devices.

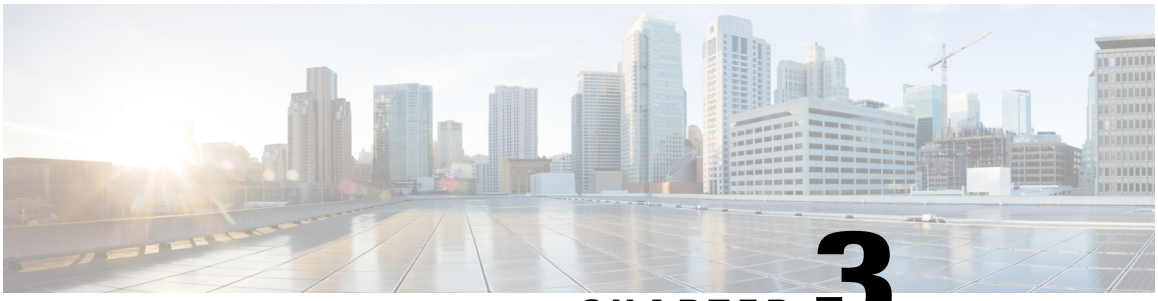
SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

System Messages

You can use system message logging to control the destination and to filter the severity level of messages that system processes generate. You can configure logging to a terminal session, a log file, and syslog servers on remote systems. System message logging is based on RFC 3164.

For more information about the system message format and the messages that the device generates, see the *Cisco Nexus 1000V Series NX-OS System Messages Reference*.



CHAPTER 3

Configuring the Domain

This chapter contains the following sections:

Information About the Domain

You must create a domain for the Cisco Nexus 1000V and then add control and packet VLANs for communication and management. This process is part of the initial setup of the a Cisco Nexus 1000V when installing the software. If you need to create a domain later, you can do so by using the **setup** command or the procedures described in this chapter.

Layer 3 Control

Layer 3 control, or IP connectivity, is supported between the Virtual Supervisor Module (VSM) and the Virtual Ethernet Module (VEM) for control and packet traffic. With Layer 3 control, a VSM can be Layer 3 accessible and can control hosts that reside in a separate Layer 2 network. In the Layer 3 mode, all the VEMs (hosts) managed by VSM and the VSM can be in different networks.

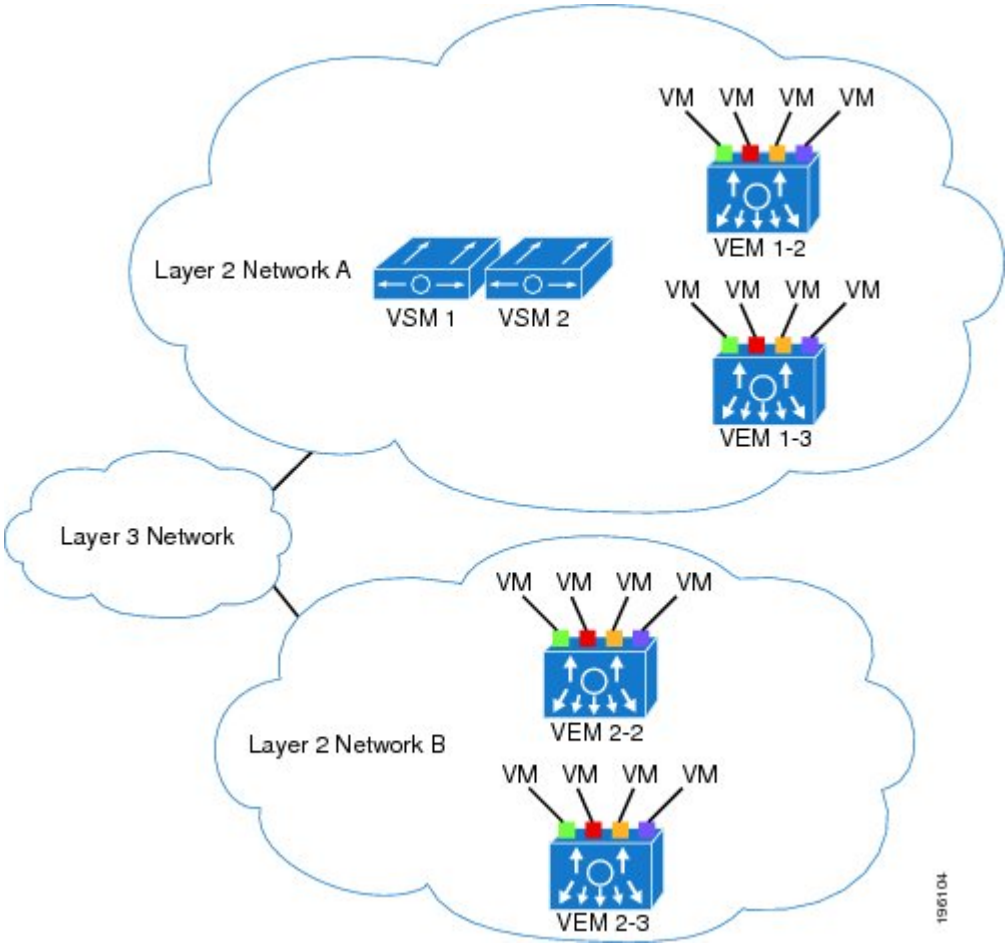
Another VSM cannot control a host that is outside of the Layer 2 network it controls, the host on which it resides must be controlled by another VSM.

To implement Layer 3 control, you must make the following configuration:

- Configure the VSM in L3 control mode.

In this figure, VSM 1 controls VEMs in Layer 2 Network A and VSM 2 controls VEMs in Layer 2 Network B.

Figure 1: Example of Layer 3 Control IP Connectivity



Guidelines and Limitations

- UDP port 4785 is required for Layer 3 communication between the VSM and VEM. If you have a firewall in your network and are configuring Layer 3 control, make sure that UDP port 4785 is open on your upstream switch or firewall device. For more information, see the documentation for your upstream switch or firewall device.
- The capability attribute (Layer 3 control) cannot be inherited from the port profile.
- Different hosts can use different VLANs for Layer 3 control.
- A port profile used for Layer 3 control must be an access port profile. It cannot be a trunk port profile.
- We recommend that if you are using the VMware kernel NIC for Layer 3 Control, you do not use it for any other purpose. For example, do not also use the Layer 3 Control VMware kernel NIC for VMotion or network file system (NFS) mount.

- You must configure control VLANs, packet VLANs, and management VLANs as regular VLANs and not as private VLANs.

Default Settings

Parameter	Default
Control VLAN (svs-domain)	VLAN 1
Packet VLAN (svs-domain)	VLAN 1
VMware port group name (port-profile)	The name of the port profile
SVS mode (svs-domain)	Layer 3
Switchport mode (port-profile)	Access
State (port-profile)	Disabled
State (VLAN)	Active
Shut state (VLAN)	No shutdown

Configuring the Domain

Creating a Domain

You can create a domain name for the Cisco Nexus 1000V that identifies the VSM and VEMs; and then add control and packet VLANs for communication and management. This process is part of the initial setup of the Cisco Nexus 1000V when installing the software. If you need to create a domain after initial setup, you can do so by using this procedure.

Note We recommend the following:

- Use one VLAN for control traffic and a different VLAN for packet traffic.
- Use a distinct VLAN for each instances of Cisco Nexus 1000V (different domains)

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in EXEC mode.

You must know the following information:

- If two or more VSMs share the same control and/or packet VLAN, the domain helps identify the VEMs managed by each VSM.
- A unique domain ID for this Cisco Nexus 1000V instance.
- Identity of the VLANs to be used for control and packet traffic.
- The **svs mode** command in the SVS Domain Configuration mode is not used and has no effect on a configuration.

Procedure

	Command or Action	Purpose
Step 1	switch# **config terminal**	Places you in global configuration mode.
Step 2	switch(config)# **svs-domain**	Places you in SVS domain configuration mode.
Step 3	switch(config-svs-domain)# **domain id** *number*	Creates the domain ID for this Cisco Nexus 1000V instance.
Step 4	switch(config-vlan)# **show svs domain**	(Optional) Displays the domain configuration.
Step 5	switch(config-vlan)# **exit**	Returns you to global configuration mode.
Step 6	switch(config)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

```
switch# config terminal
switch(config)# svs-domain
switch(config-svs-domain)# domain id 100

switch(config-vlan)# exit

switch(config)# show svs domain
SVS domain config:
Domain id: 211
Control vlan: NA
Packet vlan: NA
Control mode: L3
Switch guid: 20ccba13-3738-60db-b077-91a774b41eda
L3 control interface: mgmt0
Status: Config push to VC successful.
Control type multicast: No

Note: Control VLAN and Packet VLAN are not used in L3 mode
switch(config)#
switch(config)# copy run start
[########################################] 100%
switch(config)#
```

Changing to Layer 3 Transport

This procedure requires you to disable the control and packet VLANs. You cannot change to Layer 3 Control before disabling the control and packet VLANs.

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in EXEC mode.

You have already configured the Layer 3 interface (mgmt 0 or control 0) and assigned an IP address.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# **show svs domain**	Displays the existing domain configuration, including control and packet VLAN IDs.
Step 2	switch# **config t**	Places you in global configuration mode.
Step 3	switch(config)# **svs-domain**	Places you in SVS domain configuration mode.
Step 4	switch(config-svs-domain)# **no packet vlan**	Removes the packet VLAN configuration.
Step 5	switch(config-svs-domain)# **no control vlan**	Removes the control VLAN configuration.
Step 6	switch(config-svs-domain)# **show svs domain**	(Optional) Displays the domain configuration.
Step 7	switch(config-svs-domain)# **svs mode L3 interface** { **mgmt0** | **control0** }	Configures Layer 3 transport mode for the VSM domain. If configuring Layer 3 transport, then you must designate which interface to use; and the interface must already have an IP address configured.
Step 8	switch(config-vlan)# **show svs domain**	(Optional) Displays the new Layer 3 control mode configuration for this VSM domain.
Step 9	switch(config-svs-domain)# **[no] control type multicast**	Configures the control type multicast in Layer 3 mode on the VSM.
Step 10	switch(config-vlan)# **show svs domain**	(Optional) Displays the control type multicast status in Layer 3 mode on the VSM.
Step 11	switch(config)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

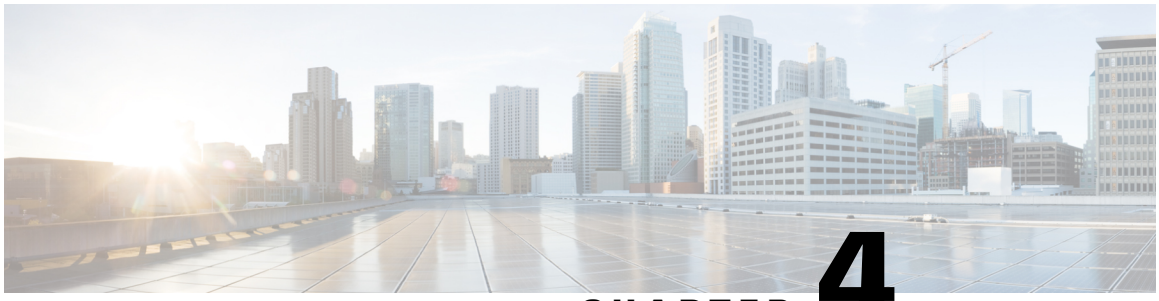
```
switch(config)# show svs domain
SVS domain config:
  Domain id:    100
  Control vlan: 100
  Packet vlan:  101
  L2/L3 Control mode: L2
  L3 control interface:  NA
  Status: Config push to VC successful.
switch# config t
```

```
switch(config)# svs-domain
switch(config-svs-domain)# no packet vlan
switch(config-svs-domain)# no control vlan
switch(config)# show svs domain
SVS domain config:
  Domain id:    100
  Control vlan: 1
  Packet vlan:  1
  L2/L3 Control mode: L2
  L2/L3 Control interface: NA
  Status: Config push to VC successful.
switch(config-svs-domain)# svs mode l3 interface mgmt0
SVS domain config:
  Domain id:    100
  Control vlan: 1
  Packet vlan:  1
  L2/L3 Control mode: L3
  L3 control interface: mgmt0
  Status: Config push to VC successful.
switch(config-svs-domain)# show svs domain

switch(config-svs-domain)# control type multicast
switch(config)# show svs domain
SVS domain config:
  Domain id:    343
  Control vlan:  NA
  Packet vlan:   NA
  L2/L3 Control mode: L3
  L3 control interface: mgmt0
  Status: Config push to VC successful.
  Control type multicast: Yes

switch(config-svs-domain)# no control type multicast
switch(config)# show svs domain
SVS domain config:
  Domain id:    343
  Control vlan:  NA
  Packet vlan:   NA
  L2/L3 Control mode: L3
  L3 control interface: mgmt0
  Status: Config push to VC in progress.
  Control type multicast: No
  Limitation : Control type multicast is configured. It is not applicable in svs L2 mode.

switch(config-svs-domain)# copy running-config startup-config
[########################################] 100%
switch(config-svs-domain)#
```

Feature History for the VSM Domain

This table only includes updates for those releases that have resulted in additions to the feature.

Feature Name	Releases	Feature Information
VSM Domain	Release 5.2(1)IC1(1.1)	This feature was introduced.



CHAPTER 4

Managing Server Connections

This chapter contains the following sections:

Information About Server Connections

In order to connect to vCenter Server or an ESX server, you must first define the connection in theCisco Nexus 1000V including the following:

- A connection name
- The protocol used
- The server IP address
- The server DNS name
- All communication with vCenter Server is secured by the Transport Layer Security (TLS) protocol.

Guidelines and Limitations

InterCloud Extender will fail to attach as a module on the VSM if its tunnel interface and the VSM management are on the same subnet.

Connecting to the vCenter Server

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in EXEC mode.

You must know the following:

- The datacenter name
- The vCenter Server IP address or hostname.

You must be sure the following is set up:

- The vCenter Server management station is installed and running.
- The ESX servers are installed and running.
- The Cisco Nexus 1000V appliance is installed.
- The management port is configured.
- The DNS is already configured if you are configuring a connection using a hostname.
- An extension with vCenter Server has been registered. The extension includes the extension key and public certificate for the VSM. vCenter Server uses the extension to verify the authenticity of the request it receives from the VSM. For instructions about adding and registering an extension, see the *Cisco Nexus 1000V Installation and Upgrade Guide*.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Places you in global configuration mode.
Step 2	switch(config)# **svs connection** *name*	Places you in connection configuration mode for adding this connection between the Cisco Nexus 1000V and either a particular ESX server or vCenter Server. By using a name, information for multiple connections can be stored in the configuration.
Step 3	switch(config-svs-conn)# **protocol vmware-vim** [**http**]	Use the **http** keyword to specify 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	Do one of the following:	• If you are configuring an IP address, go to Step 5. • If you are configuring a hostname, go to Step 6.
Step 5	switch(config-svs-conn)# **remote ip address** *ipaddress*	Specifies the IP address of the ESX server or vCenter Server for this connection. This command is stored locally. Go to step 7 to configure the datacenter name.

	Command or Action	Purpose
Step 6	switch(config-svs-conn)# **remote hostname** *hostname*	Specifies the DNS name of the ESX server or vCenter Server for this connection. This command is stored locally. **Note** DNS is already configured.
Step 7	switch(config-svs-conn)# **vmware dvs datacenter-name** *name*	Identifies the datacenter name in the vCenter Server where the 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 8	switch(config-svs-conn)# **connect**	Initiates the connection. If the username and password have not been configured for this connection, the you are prompted for a username and password. The default is no connect. There can be only one active connection at a time. If a previously defined connection is up, an error message appears and the command is rejected until you close the previous connection by entering no connect.

```
switch# config t
switch(config)# svs connection VC
switch(config-svs-conn)# protocol vmware-vim
switch(config-svs-conn)# remote ip address 192.168.0.1
switch(config-svs-conn)# vmware dvs datacenter-name Hamilton-DC
switch(config-svs-conn)# connect
switch# show svs connections
connection VC:
    ip address: 192.168.0.1
    protocol: vmware-vim https
    certificate: default
    datacenter name: Hamilton-DC
    DVS uuid: ac 36 07 50 42 88 e9 ab-03 fe 4f dd d1 30 cc 5c
    config status: Enabled
    operational status: Connected
switch#
```

Configuring Host Mapping

This section includes the following topics:

- Information about Host Mapping
- Removing Host Mapping from a Module
- Mapping to a New Host
- Viewing Host Mapping

Information about Host Server Connections

When a VSM detects a new VEM, it automatically assigns a free module number to the VEM and then maintains the mapping between the module number and the universally unique identifier (UUID) of a host server. This mapping is used to assign the same module number to a given host server.

Removing Host Mapping from a Module

Before You Begin

Before beginning this procedure, be sure you have done the following:

- Logged in to theCisco Nexus 1000V in EXEC mode.
- Removed the host from the Cisco Nexus 1000V DVS on vCenter

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Places you in global configuration mode.
Step 2	switch(config)# **no vem** *module-number*	Removes the specified module from software. **Note** If the module is still present in the slot, the command is rejected, as shown in this example.
Step 3	switch(config)# **show module vem mapping**	(Optional) Displays the mapping of modules to host servers.
Step 4	switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

```
switch# configure terminal
switch(config)# no vem 4
switch(config)# no vem 3
cannot modify slot 3: host module is inserted
switch(config)# show module vem mapping
Mod     Status          UUID                                    License Status
---     -----------     ------------------------------------    --------------
  3      powered-up     93312881-309e-11db-afa1-0015170f51a8    licensed
switch(config-vem-slot)# copy running-config startup-config
```

Mapping to a New Host

Before You Begin

Before beginning this procedure, be sure you have done the following:

- Logged in to the CLI in EXEC mode

- Removed the host from the Cisco Nexus 1000V DVS on vCenter

Note If you do not first remove the existing host server mapping, the new host server is assigned a different module number.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Places you in global configuration mode.
Step 2	switch(config)# **vem** *module number*	Places you in VEM slot configuration mode.
Step 3	switch(config-vem-slot)# **host vmware id** *server-bios-uuid*	Assigns a different host server UUID to the specified module.
Step 4	switch(config-vem-slot)# **show module vem mapping**	(Optional) Displays the mapping of modules to host servers.
Step 5	switch(config-vem-slot)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

```
switch# config t
switch(config)# vem 3
switch(config-vem-slot)# host vmware id 6dd6c3e3-7379-11db-abcd-000bab086eb6
switch(config-vem-slot)# show module vem mapping
Mod     Status          UUID                                    License Status
---     -----------     ------------------------------------    --------------
  3      powered-up     93312881-309e-11db-afa1-0015170f51a8    licensed
  4          absent     6dd6c3e3-7379-11db-abcd-000bab086eb6    licensed

switch(config-vem-slot)# copy running-config startup-config
```

Viewing Host Mapping

- Use this procedure in EXEC mode to view the mapping of modules to host servers.

Procedure

Display the mapping on modules to host servers by entering the following command: **show module vem mapping**

```
Mod Status      UUID                                    License Status
--- ----------- ------------------------------------ --------------
3   powered-up  93312881-309e-11db-afa1-0015170f51a8  licensed
n1000v(config)#
```

Verifying the Domain

Use the following command to verify the configured domain:

Command	Description
show svs domain	Displays the domain configured on the Cisco Nexus 1000V.

```
n1000v# show svs domain
SVS domain config:
Domain id: 98
Control vlan: 70
Packet vlan: 71
Sync state: -
n1000v#
```

Verifying the Configuration

Use one of the following commands to verify the configuration:

Command	Description
show running-config	Displays the current configuration. If the Cisco Nexus 1000V is not connected to a vCenter Server or ESX server, the output is limited to connection-related information.
show svs domain	Displays the domain configured on the Cisco Nexus 1000V.
show module	Displays module information.
show server_info	Displays server information.
show interface brief	Displays interface information, including the uplinks to vCenter Server.
show interface virtual	Displays virtual interface information.
show module vem mapping	Displays the mapping of modules to host servers.

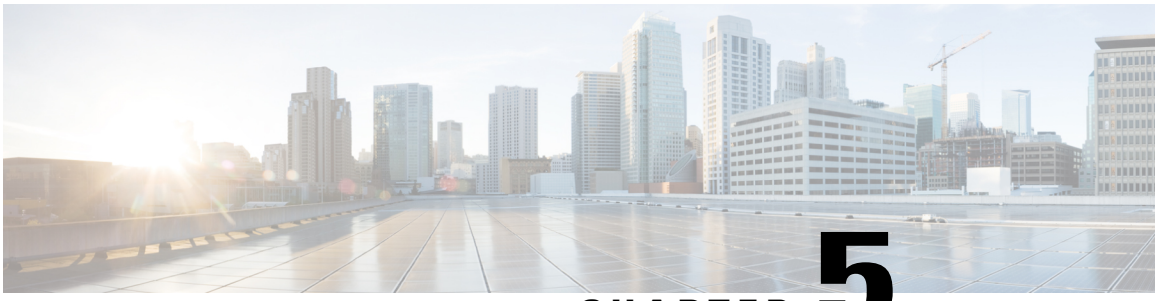
Verifying Module Information

Use one of the following commands to verify the configuration:

Command	Description
show module	Displays module information.
show server_info [*name*]	Displays server information.
show interface brief	Displays interface information, including the uplinks to vCenter Server.
show interface virtual	Displays virtual interface information.

Feature History for Server Connections

Feature Name	Releases	Feature Information
Server Connections	Release 5.2(1)IC1(1.1)	This feature was introduced.



CHAPTER 5

Managing the Configuration

This chapter contains the following sections:

Information About Configuration Management

The Cisco Nexus 1000V provides you with the capability to change the switch name, configure messages of the day, and display, save, and erase configuration files

Changing the Switch Name

Use this procedure to change the switch name or prompt from the default (switch#) to another character string.

If the VSM is connected to vCenter Server then this procedure also changes the Dynamic Vectoring and Streaming (DVS) engine that the VSM is managing. If you make an error when renaming the DVS, a syslog is generated and the DVS on vCenter Server continues to use the old DVS name.

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# **switchname**	Changes the switch prompt.

```
switch(config)# switchname metro
metro(config)# exit
metro#
```

Configuring a Message of the Day

Use this procedure to configure a message of the day (MOTD) to display before the login prompt on the terminal when a user logs in.

- The banner message can be up to 40 lines with up to 80 characters per line.
- Use the following guidelines when choosing your delimiting character:
  - Do not use the delimiting-character in the message string.
  - Do not use " and % as delimiters.
- The following tokens can be used in the the message of the day:
  - $(hostname) displays the host name for the switch.
  - $(line) displays the vty or tty line or name.

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# **banner motd** [*delimiting-character message delimiting-character*]	Configures a banner message of the day with the following features: • Up to 40 lines • Up to 80 characters per line • Enclosed in delimiting character, such as # • Can span multiple lines • Can use tokens
Step 2	switch(config)# **show banner motd**	Displays the configured banner message.

```
switch(config)# banner motd #April 16, 2011 Welcome to the svs#
switch(config)# show banner motd
April 16, 2011 Welcome to the Switch
```

Verifying the Configuration

Use this section to view the switch configuration. This section includes the following topics:

- Verifying the Software and Hardware Versions
- Verifying the Running Configuration
- Comparing the Startup and Running Configurations
- Verifying the Interface Configuration

Verifying the Software and Hardware Versions

Use this command to verify the versions of software and hardware on your system, for example, before and after an upgrade.

Command	Description
show version	Displays the versions of system software and hardware that are currently running on the switch,

Verifying the Running Configuration

Use this command to verify the configuration currently running on the system.

Command	Description
show running-config	Displays the versions of system software and hardware that are currently running on the switch.

Comparing the Startup and Running Configurations

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in any command mode.

Procedure

	Command or Action	Purpose
Step 1	swtich# **show running-config diff**	Displays the difference between the startup configuration and the running configuration currently on the switch.

Verifying the Interface Configuration in a Brief Version

Use the following command to verify the interface configuration in a brief version:

Command	Description
show interface {*type*} {*name*} **brief**	Displays a brief version of information about the specified interface configuration.

Verifying a Detailed Version of an Interface Configuration

Use the following command to verify the configured domain:

Command	Description
show interface {*type*} {*name*}	Displays details about the specified interface configuration.

Verifying a Brief Version of all Interfaces

Use the following command to verify a brief version all interfaces:

Command	Description
show interface brief	Displays a brief version of all interface configurations on your system.

Verifying the Running Configuration for all Interfaces

Use the following command to verify the running configuration for all interfaces on your system:

Command	Description
show running-config interface	Displays the running configuration for all interfaces on your system.

Saving a Configuration

Use this procedure to save the running configuration to the startup configuration so that your changes are retained in the configuration file the next time you start the system.

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in any command mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

```
switch# copy run start
[########################################] 100%
switch#
```

Erasing a Configuration

Use this procedure to erase a startup configuration.

Caution The **write erase** command erases the entire startup configuration with the exception of loader functions, the license configuration, and the certificate extension configuration

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in any command mode.

-

Procedure

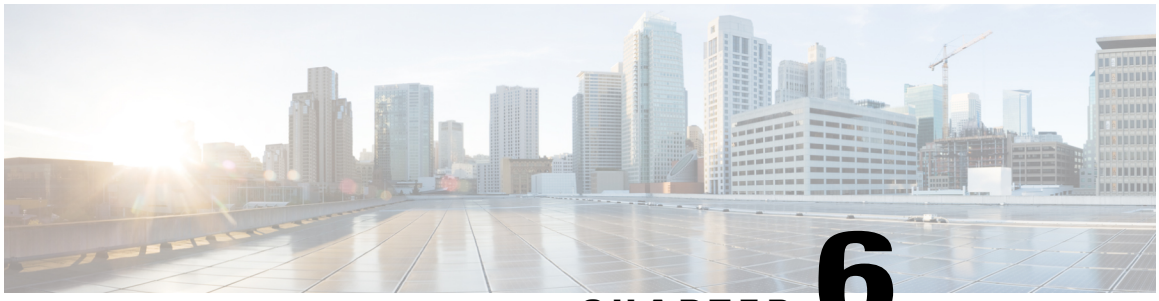
	Command or Action	Purpose
Step 1	switch# **write erase** [**boot** | **debug**]	The existing startup configuration is completely erased and all settings revert to their factory defaults. The running configuration is not affected. The following parameters are used with this command: • boot: Erases the boot variables and the mgmt0 IP configuration. • debug: Erases the debug configuration.

	Command or Action	Purpose

```
switch# write erase debug
```

Feature History for Configuration Management

Feature Name	Releases	Feature Information
Configuration Management	Release 5.2(1)IC1(1.1)	This feature was introduced.



CHAPTER 6

Working with Files

This chapter contains the following sections:

Information About Files

The Cisco Nexus 1000V file system provides a single interface to all the file systems that the Cisco Nexus 1000V switch uses, including:

- Flash memory file systems
- Network file systems (TFTP and FTP)
- Any other endpoint for reading or writing data (such as the running configuration)

Navigating the File System

This section describes how to navigate the file system and includes the following topics:

- Specifying File Systems
- Identifying the Directory You are Working From
- Changing Your Directory
- Listing the Files in a File System
- Identifying Available File Systems for Copying Files
- Using Tab Completion

Specifying File Systems

The syntax for specifying a file system is *<file system name>*:[//*server*/]. The following table describes file system syntax.

File System Name	Server	Description
bootflash	sup-active sup-local sup-1 module-1	Internal memory located on the active supervisor used for storing system images, configuration files, and other miscellaneous files. Cisco Nexus 1000V CLI defaults to the bootflash: file system
	sup-standby sup-remote sup-2 module-2	Internal memory located on the standby supervisor used for storing system images, configuration files, and other miscellaneous files.
volatile	—	Volatile random-access memory (VRAM) located on a supervisor module used for temporary or pending changes.

Identifying the Directory You are Working From

You can display the directory name of your current CLI location.

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in any command mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **pwd**	Displays the present working directory.

```
switch# pwd
bootflash:
```

Changing Your Directory

You can change your location in the CLI, from one directory or file system to another.

Cisco Nexus 1000V CLI defaults to the bootflash: file system.

Note Any file saved in the volatile: file system is erased when the switch reboots.

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in any command mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **pwd**	Displays the directory name of your current CLI location.
Step 2	switch# **cd directory name** • switch# **cd bootflash:** Changes your CLI location to the root directory on the bootflash: file system. • switch# **cd bootflash:mydir** Changes your CLI location to the mydir directory that resides in the bootflash: file system. • switch# **cd mystorage** Changes your CLI location to the mystorage directory that resides within the current directory. If the current directory is bootflash: mydir, this command changes the current directory to bootflash: mydir/mystorage.	Changes your CLI location to the root directory on the bootflash: file system.

```
switch# pwd
volatile:
switch# cd bootflash:

switch# pwd
volatile:
switch# cd bootflash:mydir
switch# pwd
volatile:
switch# cd mystorage
```

Listing the Files in a File System

Procedure

	Command or Action	Purpose
Step 1	switch# **dir** [*directory* | *filename*]	Displays the contents of a directory or file.

```
switch# dir lost+found/
      49241     Jul 01 09:30:00 2008  diagclient_log.2613
      12861     Jul 01 09:29:34 2008  diagmgr_log.2580
         31     Jul 01 09:28:47 2008  dmesg
       1811     Jul 01 09:28:58 2008  example_test.2633
         89     Jul 01 09:28:58 2008  libdiag.2633
      42136     Jul 01 16:34:34 2008  messages
         65     Jul 01 09:29:00 2008  otm.log
        741     Jul 01 09:29:07 2008  sal.log
         87     Jul 01 09:28:50 2008  startupdebug

Usage for log://sup-local
   51408896 bytes used
  158306304 bytes free
  209715200 bytes total
switch#
```

Identifying Available File Systems for Copying Files

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **copy ?**	Displays the source file systems available to the copy command.
Step 2	switch# **copy filename ?**	Displays the destination file systems available to the copy command for a specific file.

```
switch# copy ?
bootflash: Select source filesystem
core: Select source filesystem
debug: Select source filesystem
ftp: Select source filesystem
licenses Backup license files
log: Select source filesystem
nvram: Select source filesystem
running-config Copy running configuration to destination
scp: Select source filesystem
sftp: Select source filesystem
startup-config Copy startup configuration to destination
system: Select source filesystem
tftp: Select source filesystem
volatile: Select source filesystem
```

Using Tab Completion

You can have the CLI complete a partial file name in a command.

Procedure

	Command or Action	Purpose
Step 1	switch# **show file** *filesystem name: partial filename* <Tab>	Completes the filename when you type a partial filename and then press Tab and if the characters you typed are unique to a single file. If not, the CLI lists a selection of file names that match the characters that you typed. You can then retype enough characters to make the file name unique; and CLI completes the filename for you.
Step 2	switch# **show file bootflash:c** <Tab>	Completes the file name for you

```
n1000v# show file bootflash: nexus-1000v-
bootflash:nexus-1000v-dplug-mzg.4.0.4.SV1.0.42.bin
bootflash:nexus-1000v-mzg.4.0.4.SV1.0.42.bin
bootflash:nexus-1000v-kickstart-mzg.4.0.4.SV1.0.42.bin
n1000v# show file bootflash:c<Tab>
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDSq93BrlHcg3bX1jXDMY5c9+yZSST3VhuQBqogvCPDGeLecA+j
...
...
n1000v#
```

Copying and Backing Up Files

You can copy a file, such as a configuration file, to save it or reuse it at another location. If your internal file systems are corrupted, you could potentially lose your configuration. Save and back up your configuration files periodically. Also, before installing or migrating to a new software configuration, back up the existing configuration files.

Note Use the **dir** command to ensure that enough space is available in the destination file system. If enough space is not available, use the **delete** command to remove unneeded files.

Before You Begin

Before beginning this procedure, you must be of the following:

- You are logged in to the CLI through a Telnet, or SSH connection.
- Your device has a route to the destination if you are copying to a remote location. Your device and the remote destination must be in the same subnetwork if you do not have a router or default gateway to route traffic between subnets.
- Your device has connectivity to the destination. Use the **ping** command to be sure.
- The source configuration file is in the correct directory on the remote server.
- The permissions on the source file are set correctly. Permissions on the file should be set to world-read.

Procedure

	Command or Action	Purpose
Step 1	switch# **copy** [*source filesystem:*] *filename* [*destination filesystem*:] *filename* • switch# **copy system:running-config** *system* **run.cfg** Saves a copy of the running configuration to a remote switch. • switch# **copy bootflash:** *system_image* **bootflash:**//*sup-standby/system_image* Copies a file from bootflash in the active supervisor module to bootflash in the standby supervisor module. • switch# **copy system:running-config bootflash:***config* Copies a running configuration to the bootflash: file system. • switch# **copy scp:**[//[*username@*]*server*][/*path*]/*filename* Copies a source or destination URL for a network server that supports Secure Shell (SSH) and accepts copies of files using the secure copy protocol (scp). • switch# **copy sftp:**[//[*username@*]*server*][/*path*]/*filename*/// Copies a source or destination URL for an SSH FTP (SFTP) network server • switch# **copy system:running-config** *bootflash:my-config* Places a back up copy of the running configuration on the bootflash: file system (ASCII file). • switch# **copy bootflash:** *filename* **bootflash:***directory*/*filename* Copies the specified file from the root directory of the bootflash: file system to the specified directory. • switch# **copy** *filename directory*/*filename* Copies a file within the current file system.	Copies a file from the specified source location to the specified destination location.

	Command or Action	Purpose
	• switch# **copy tftp:**[*//server*[*:port*]][*/path*]*/filename* Copies the source file to the running configuration on the switch, and configures the switch as the file is parsed line by line.	

```
switch# copy system:running-config tftp://10.10.1.1/home/configs/switch3-run.cfg
switch# copy bootflash:system_image bootflash://sup-2/system_image
switch# copy system:running-config bootflash:my-config
switch# copy scp://user@10.1.7.2/system-image bootflash:system-image
switch# copy sftp://172.16.10.100/myscript.txt volatile:myscript.txt
switch# copy system:running-config bootflash:my-config
switch# copy bootflash:samplefile bootflash:mystorage/samplefile

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

Creating a Directory

Procedure

	Command or Action	Purpose
Step 1	switch# **mkdir** *directory name* • **mkdir** {**bootflash:** | **debug:** | **volatile:**} Specifies the directory name you choose: ◦ bootflash: ◦ debug: ◦ volatile: • switch# **mkdir bootflash:***directory name* Creates a directory that you name in the bootflash: directory.	Creates a directory at the current directory level.

```
switch# mkdir test
switch# mkdir bootflash:test
```

Removing an Existing Directory

This command is valid only on Flash file systems.

Before You Begin

Before beginning this procedure, be sure of the following:

- You are logged in to the CLI.
- The directory you want to remove is empty.

Procedure

	Command or Action	Purpose
Step 1	switch# **rmdir** [**filesystem:**[//**module**/]]*directory* • switch# **rmdir** *directory* Removes the specified directory at the current directory level. • switch# **rmdir** {**bootflash:** | **debug:** | **volatile:**} *directory* Removes a directory from the file system.	Removes a directory. The directory name is case sensitive.

```
switch# rmdir test
switch# rmdir bootflash:test
```

Moving Files

Caution If a file with the same name already exists in the destination directory, that file is overwritten by the moved file.

The move will not complete if there is not enough space in the destination directory.

Before You Begin

Before beginning this procedure, you must be logged in to the CLI.

Procedure

	Command or Action	Purpose
Step 1	switch# **move** {*source path and filename*} {*destination path and filename*} • switch# **move** *filename path*/*filename* Moves the file from one directory to another in the current file system.	Moves the file from one directory to another in the same file system (bootflash:).

```
switch# move bootflash:samplefile bootflash:mystorage/samplefile
switch# move samplefile mystorage/samplefile
```

Deleting Files or Directories

You can delete files or directories on a Flash Memory device.

Caution When deleting, if you specify a directory name instead of a file name, the entire directory and its contents are deleted.

Before You Begin

You must understand the following information:

- When you delete a file, the software erases the file.
- If you attempt to delete the configuration file or image specified by the CONFIG_FILE or BOOTLDR environment variable, the system prompts you to confirm the deletion.
- If you attempt to delete the last valid system image specified in the BOOT environment variable, the system prompts you to confirm the deletion.

Procedure

	Command or Action	Purpose
Step 1	switch# **delete** [**bootflash:** | **debug:** | **log:** | **volatile:**] *filename* or *directory name* • switch# **delete** *filename* Deletes the named file from the current working directory. • switch# **delete bootflash:***directory name* Deletes the named directory and its contents.	Deletes a specified file or directory.

```
switch# delete bootflash:dns_config.cfg
switch# delete dns_config.cfg
```

Compressing Files

Before You Begin

Before beginning this procedure, you must be logged in to the CLI.

Procedure

	Command or Action	Purpose
Step 1	switch# **show** *command* > [*path*] *filename*	Directs the **show** command output to a file.

	Command or Action	Purpose
Step 2	switch# **dir**	Displays the contents of the current directory, including the new file created in the first step.
Step 3	switch# **gzip** [*path*] *filename*	Compresses the specified file
Step 4	switch# **dir**	Displays the contents of the specified directory, including the newly-compressed file. Shows the difference in the file size of the newly-compressed file.

```
switch# show system internal l2fm event-history errors >errorsfile
switch# dir
       2687     Jul 01 18:17:20 2008  errorsfile
      16384     Jun 30 05:17:51 2008  lost+found/
       4096     Jun 30 05:18:29 2008  routing-sw/
         49     Jul 01 17:09:18 2008  sample_test.txt
    1322843     Jun 30 05:17:56 2008  nexus-1000v-dplug-mzg.4.0.4.SV1.0.42.bin
   21629952     Jun 30 05:18:02 2008  nexus-1000v-kickstart-mzg.4.0.4.SV1.0.42.bin
   39289400     Jun 30 05:18:14 2008  nexus-1000v-mzg.4.0.4.SV1.0.42.bin

Usage for bootflash://
  258408448 bytes used
 2939531264 bytes free
 3197939712 bytes total
switch# gzip bootflash:errorsfile
switch# dir
       1681     Jun 30 05:21:08 2008  cisco_svs_certificate.pem
        703     Jul 01 18:17:20 2008  errorsfile.gz
      16384     Jun 30 05:17:51 2008  lost+found/
       4096     Jun 30 05:18:29 2008  routing-sw/
         49     Jul 01 17:09:18 2008  sample_test.txt
    1322843     Jun 30 05:17:56 2008  nexus-1000v-dplug-mzg.4.0.4.SV1.0.42.bin
   21629952     Jun 30 05:18:02 2008  nexus-1000v-kickstart-mzg.4.0.4.SV1.0.42.bin
   39289400     Jun 30 05:18:14 2008  nexus-1000v-mzg.4.0.0.S1.0.34.bin

Usage for bootflash://
  258408448 bytes used
 2939531264 bytes free
 3197939712 bytes total
switch#
```

Uncompressing Files

You can uncompress (unzip) a specified file that is compressed using LZ77 coding.

Before You Begin

Before beginning this procedure, you must be logged in to the CLI.

Procedure

	Command or Action	Purpose
Step 1	switch# **gunzip** [*path*] *filename*	Uncompresses the specified file. The filename is case sensitive .

	Command or Action	Purpose
Step 2	switch# **dir**	Displays the contents of a directory, including the newly uncompressed file.

```
switch# gunzip bootflash:errorsfile.gz
switch# dir bootflash:
       2687     Jul 01 18:17:20 2008  errorsfile
      16384     Jun 30 05:17:51 2008  lost+found/
       4096     Jun 30 05:18:29 2008  routing-sw/
         49     Jul 01 17:09:18 2008  sample_test.txt
    1322843     Jun 30 05:17:56 2008  nexus-1000v-dplug-mzg.4.0.0.SV1.0.42.bin
   21629952     Jun 30 05:18:02 2008  nexus-1000v-kickstart-mzg.4.0.4.SV1.0.42.bin
   39289400     Jun 30 05:18:14 2008  nexus-1000v-mzg.4.0.0.SV1.0424.bin

Usage for bootflash://sup-local
  258408448 bytes used
 2939531264 bytes free
 3197939712 bytes total
DCOS-112-R5#
```

Directing Command Output to a File

Procedure

	Command or Action	Purpose
Step 1	switch# **show running-config >** [*path* | *filename*] • switch# **show running-config > volatile:***filename* Directs the output of the command, **show running-config**, to the specified filename on the volatile file system. • switch# **show running-config > bootflash:***filename* Directs the output of the command, **show running-config**, to the specified file in bootflash. • switch# **show running-config > tftp:**// *ipaddress*/*filename* Directs the output of the command, **show running-config**, to the specified file on a TFTP server. • switch# **show interface >** *filename* Directs the output of the command, **show interface**, to the specified file at the same directory level, for example, in bootflash.	Directs the output of the command, **show running-config**, to a path and filename.

```
switch# show running-config > volatile:switch1-run.cfg
switch# show running-config > bootflash:switch2-run.cfg
switch# show running-config > tftp://10.10.1.1/home/configs/switch3-run.cfg
switch# show interface > samplefile
```

Verifying a Configuration File before Loading

Use the following commands to verify the integrity of a system or kickstart image before loading it.

Command	Description
copy *source path* and *file* **system:running-config**	Copies the source file to the running configuration on the switch, and configures the switch as the file is parsed line by line.
show version image [**bootflash:** | **modflash:** |**volatile:**]	Validates the specified image. bootflash:—specifies bootflash as the directory name. volatile:—Specifies volatile as the directory name. modflash:—Specifies modflash as the directory name.

```
switch# copy tftp://10.10.1.1/home/configs/switch3-run.cfg system:running-config
 switch# show version image bootflash:isan.bin
  image name: nexus-1000v-mz.4.0.4.SV1.1.bin
  bios:       version unavailable
  system:     version 4.0(4)SV1(1)
  compiled:   4/2/2009 23:00:00 [04/23/2009 09:55:29]
```

Rolling Back to a Previous Configuration

You can recover your configuration from a previously saved version.

Note Each time you use a **copy running-config startup-config** command, a binary file is created and the ASCII file is updated. A valid binary configuration file reduces the overall boot time significantly. A binary file cannot be uploaded, but its contents can be used to overwrite the existing startup configuration. The **write erase** command clears the binary file.

Procedure

	Command or Action	Purpose
Step 1	switch# **copy running-config bootflash:** {*filename*}	Reverts to a snapshot copy of a previously saved running configuration (binary file).
Step 2	switch# **copy bootflash:** {*filename*} **startup-config**	Reverts to a configuration copy that was previously saved in the bootflash: file system (ASCII file).

```
switch# copy running-config bootflash:June03-Running
switch# copy bootflash:my-config startup-config
```

Displaying Files

This section describes how to display information about files and includes the following procedures:

- Displaying File Contents
- Displaying Directory Contents
- Displaying File Checksums
- Displaying the Last Lines in a File

Displaying File Contents

Before You Begin

Before beginning this procedure, you must be logged in to the CLI.

Procedure

	Command or Action	Purpose
Step 1	switch# **show file** [**bootflash:** | **debug**: | **volatile:**] *filename*	Displays the contents of the specified file.

```
switch# show file bootflash:sample_test.txt
config t
Int veth1/1
no shut
end
show int veth1/1

switch#
```

Displaying Directory Contents

You can display the contents of a directory or file system.

Before You Begin

Before beginning this procedure, you must be logged in to the CLI.

Procedure

	Command or Action	Purpose
Step 1	switch# **pwd**	Displays the present working directory.
Step 2	switch# **dir**	Displays the contents of the directory.

```
switch# pwd
bootflash:
switch# dir

Usage for volatile://
         0 bytes used
   20971520 bytes free
   20971520 bytes total
switch#
```

Displaying File Checksums

You can display checksums for checking file integrity.

Procedure

	Command or Action	Purpose
Step 1	switch# **show file** *filename* [**cksum** | **md5sum**]**show file** {**bootflash:** | **volatile:** | **debug:**} *filename* [**cksum** | **md5sum**]	Provides the checksum or MD5 checksum of the file for comparison with the original file. Provides the Message-Digest Algorithm 5 (MD5) checksum of the file. MD5 is an electronic fingerprint for the file.

```
switch# show file bootflash:cisco_svs_certificate.pem cksum
266988670
switch# show file bootflash:cisco_svs_certificate.pem md5sum
d3013f73aea3fda329f7ea5851ae81ff
```

Displaying the Last Lines in a File

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in EXEC mode.

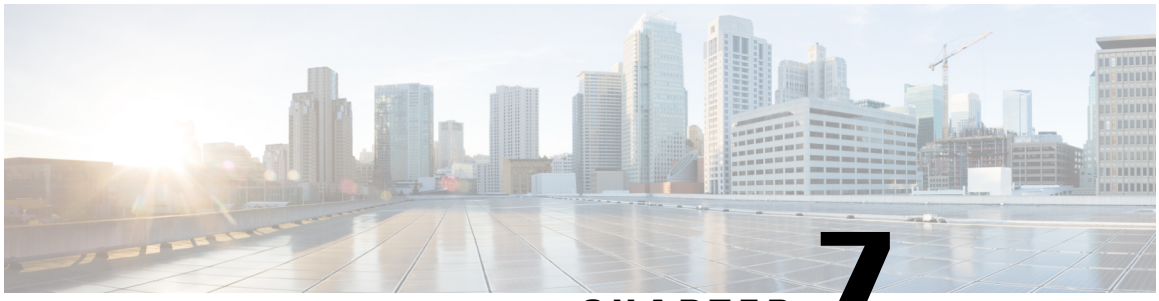
Procedure

	Command or Action	Purpose
Step 1	switch# **tail** {*path*}[*filename*] {*Number of lines*}	Displays the requested number of lines from the end of the specified file. The range for the number of lines is from 0 to 80.

```
switch# tail bootflash:errorsfile 5

20) Event:E_DEBUG, length:34, at 171590 usecs after Tue Jul  1 09:29:05 2008
    [102] main(326): stateless restart
```

Feature History for File Management

Feature Name	Releases	Feature Information
File Management	Release 5.2(1)IC1(1.1)	This feature was introduced.



CHAPTER 7

Managing Users

This chapter contains the following sections:

Information About User Management

You can identify the users currently connected to the device and send a message to either a single user or all users.

For information about creating user accounts and assigning user roles, see the *Cisco Nexus 1000V InterCloud Security Configuration Guide*.

Displaying Current User Access

You can display all users currently accessing the switch.

Before You Begin

Before beginning this procedure, you must be logged in to the CLI.

Procedure

	Command or Action	Purpose
Step 1	switch# **show users**	Displays a list of users who are currently accessing the system.

```
switch# show users
NAME     LINE         TIME         IDLE          PID COMMENT
```

```
admin    pts/0        Jul  1 04:40 03:29        2915 (::ffff:64.103.145.136)
admin    pts/2        Jul  1 10:06 03:37        6413 (::ffff:64.103.145.136)
admin    pts/3        Jul  1 13:49   .          8835 (171.71.55.196)*
switch#
```

Sending a Message to Users

You can send a message to all active CLI users currently using the system.

Before You Begin

Before beginning this procedure, you must be logged in to the CLI.

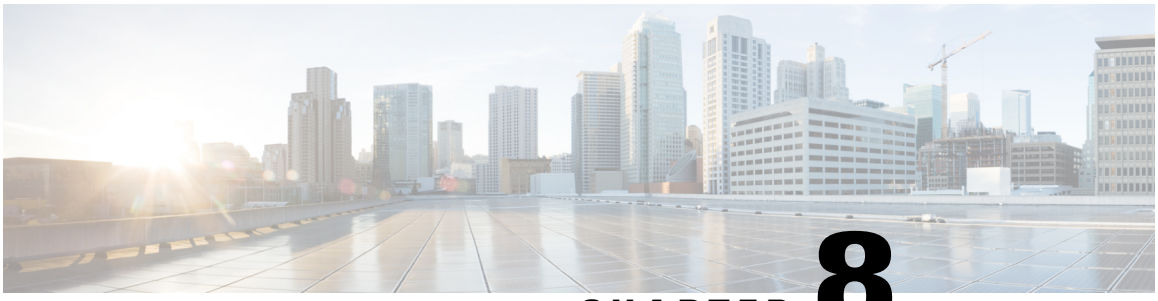
Procedure

	Command or Action	Purpose
Step 1	switch# **send** {*session device*} *line*	Sends a message to users currently logged in to the system. • The *session*argument sends the message to a specified pts/tty device type. • The *device* argument specifies the device type. • The *line* argument is a message of up to 80 alphanumeric characters in length.

```
switch# send Hello. Shutting down the system in 10 minutes.

Broadcast Message from admin@switch
        (/dev/pts/34) at 8:58 ...

Hello. Shutting down the system in 10 minutes.


switch#
```

Feature History for User Management

Feature Name	Releases	Feature Information
User Management	Release 5.2(1)IC1(1.1)	This feature was introduced.



CHAPTER 8

Configuring NTP

This chapter contains the following sections:

Information about NTP

The Network Time Protocol (NTP) synchronizes timekeeping among a set of distributed time servers and clients. This synchronization allows you to correlate events when you receive system logs and other time-specific events from multiple network devices.

NTP uses the User Datagram Protocol (UDP) as its transport protocol. All NTP communication uses the Universal Time Coordinated (UTC) standard. An NTP server usually receives its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of each other.

NTP uses a stratum to describe how many NTP hops away that a network device is from an authoritative time source. A stratum 1 time server has an authoritative time source (such as an atomic clock) directly attached to the server. A stratum 2 NTP server receives its time through NTP from a stratum 1 NTP server, which in turn connects to the authoritative time source.

NTP avoids synchronizing to a network device that may keep accurate time. NTP never synchronizes to a system that is not in turn synchronized itself. NTP compares the time reported by several network devices and does not synchronize to a network device that has a time that is significantly different than the others, even if its stratum is lower.

Cisco NX-OS cannot act as a stratum 1 server. You cannot connect to a radio or atomic clock. We recommend that the time service that you use for your network is derived from the public NTP servers available on the Internet.

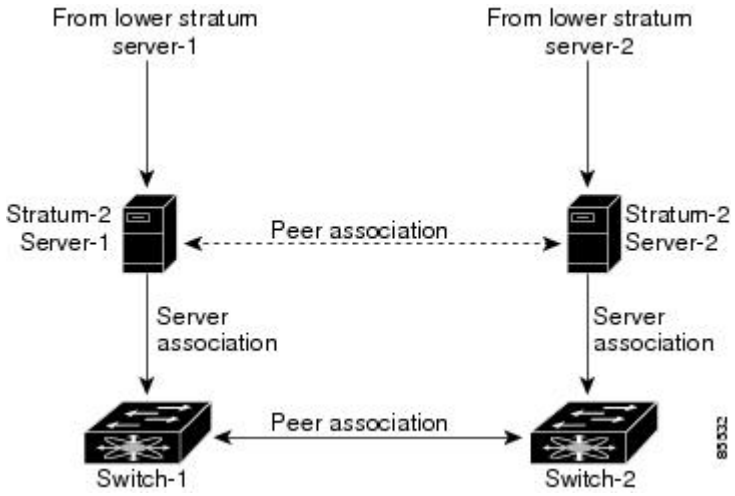
If the network is isolated from the Internet, Cisco NX-OS allows you to configure a network device so that the device acts as though it is synchronized through NTP, when in fact it has determined the time by using other means. Other network devices can then synchronize to that network device through NTP.

NTP Peers

NTP allows you to create a peer relationship between two networking devices. A peer can provide time on its own or connect to an NTP server. If both the local device and the remote peer point to different NTP servers, your NTP service is more reliable. The local device maintains the right time even if its NTP server fails by using the time from the peer.

The following diagram shows a network with two NTP stratum 2 servers and two switches.

Figure 2: NTP Peer and Server Association



In this configuration, switch 1 and switch 2 are NTP peers. switch 1 uses stratum-2 server 1, while switch 2 uses stratum-2 server 2. If stratum-2 server-1 fails, switch 1 maintains the correct time through its peer association with switch 2.

High Availability

Stateless restarts are supported for NTP. After a reboot or a supervisor switchover, the running configuration is applied.

You can configure NTP peers to provide redundancy in case an NTP server fails.

Prerequisites for NTP

You must have connectivity to at least one server that is running NTP.

Guidelines and Limitations for NTP

- You should have a peer association with another device only when you are sure that your clock is reliable (which means that you are a client of a reliable NTP server).
- A peer configured alone takes on the role of a server and should be used as a backup. If you have two servers, you can configure several devices to point to one server and the remaining devices point to the other server. You can then configure a peer association between these two servers to create a more reliable NTP configuration.
- If you only have one server, you should configure all the devices as clients to that server.
- You can configure up to 64 NTP entities (servers and peers).

Default Settings for NTP

Parameter	Default
NTP	Enabled

Configuring an NTP Server and Peer

You can configure NTP using IPv4 addresses or domain name server (DNS) names.

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Places you in global configuration mode.
Step 2	switch(config)# **ntp server** {*ip-address* | *dns-name*}	Forms an association with a server.
Step 3	switch(config)# **ntp peer** {*ip-address* | *dns-name*}	Forms an association with a peer. You can specify multiple peer associations.
Step 4	switch(config)# **show ntp peers**	(Optional) Displays the configured server and peers. **Note** A domain name is resolved only when you have a DNS server configured.

	Command or Action	Purpose
Step 5	switch(config)# **copy running-config startup-config**	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

```
switch# configure terminal
switch(config)# ntp server 192.0.2.10
switch(config# ntp peer 2001:0db8::4101
```

Clearing NTP Sessions

Command	Purpose
clear ntp session	Clears the NTP sessions.

Clearing NTP Statistics

Command	Purpose
clear ntp statistics	Clears the NTP sessions.

Verifying the NTP Configuration

Use one of the following commands to verify the configuration:

Command	Purpose
show ntp peer-status	Displays the status for all NTP servers and peers.
show ntp peers	Displays all the NTP peers.
show ntp statistics {**io** | **local** | **memory** | peer {*ip-address* | *dns-name*}	Displays the NTP statistics.

NTP Example Configuration

This example configures an NTP server:

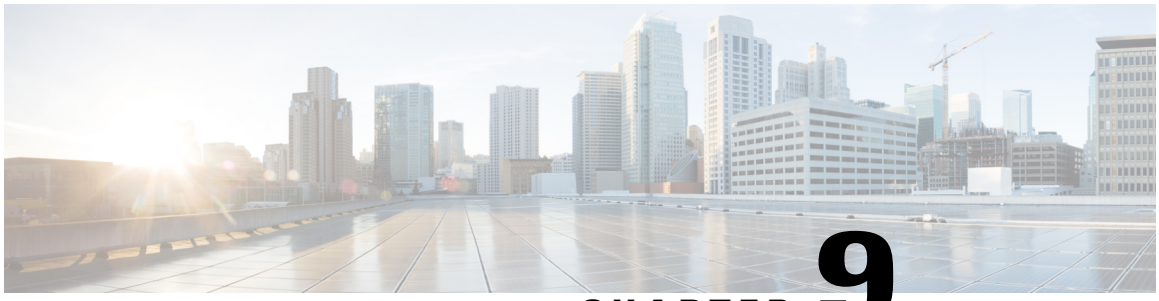
Procedure

Step 1 switch# **configure terminal**
Enters global configuration mode.

Step 2 **ntp server 192.0.2.10**
Configures an NTP server.

Feature History for NTP

Feature Name	Releases	Feature Information
NTP	Release 5.2(1)IC1(1.1)	This feature was introduced.



CHAPTER 9

Configuring SNMP

This chapter contains the following sections:

Information About SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

SNMP Functional Overview

The SNMP framework consists of three parts:

- An SNMP manager—The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent—The software component within the managed device that maintains the data for the device and reports these data, as needed, to managing systems. Cisco NX-OS supports the agent and MIB. To enable the SNMP agent, you must define the relationship between the manager and the agent.
- A managed information base (MIB)—The collection of managed objects on the SNMP agent.

SNMP is defined in RFCs 3411 to 3418.

Note SNMP Role Based Access Control (RBAC) is not supported.

Cisco NX-OS supports SNMPv1, SNMPv2c, and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security.

SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of a connection to a neighbor router, or other significant events.

Cisco NX-OS generates SNMP notifications as either traps or informs. A trap is an asynchronous, unacknowledged message sent from the agent to the SNMP managers listed in the host receiver table. Informs are asynchronous messages sent from the SNMP agent to the SNMP manager which the manager must acknowledge receipt of.

Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap. The Cisco NX-OS cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the Cisco NX-OS never receives a response, it can send the inform request again.

You can configure Cisco Nexus NX-OS to send notifications to multiple host receivers.

SNMPv3

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The security features provided in SNMPv3 are as follows:

- Message integrity—Ensures that a packet has not been tampered with while it was in-transit.
- Authentication—Determines the message is from a valid source.
- Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

Security Models and Levels for SNMPv1, v2, v3

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

- noAuthNoPriv—Security level that does not provide authentication or encryption.
- authNoPriv—Security level that provides authentication but does not provide encryption.

- authPriv—Security level that provides both authentication and encryption.

Three security models are available: SNMPv1, SNMPv2c, and SNMPv3. The security model combined with the security level determine the security mechanism applied when the SNMP message is processed.

The following table identifies what the combinations of security models and levels mean.

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash Algorithm (SHA).
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

User-Based Security Model

SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- Message integrity—Ensures that messages have not been altered or destroyed in an unauthorized manner and that data sequences have not been altered to an extent greater than can occur nonmaliciously.
- Message origin authentication—Ensures that the claimed identity of the user on whose behalf received data was originated is confirmed.
- Message confidentiality—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMPv3 authorizes management operations only by configured users and encrypts SNMP messages

Cisco NX-OS uses two authentication protocols for SNMPv3:

- HMAC-MD5-96 authentication protocol
- HMAC-SHA-96 authentication protocol

The Cisco NX-OS uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826.

The priv option offers a choice of DES or 128-bit AES encryption for SNMP security encryption. The priv option along with the aes-128 token indicates that this privacy password is for generating a 128-bit AES key.The AES priv password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 case-sensitive alphanumeric characters. If you use the localized key, you can specify a maximum of 130 characters.

Note For an SNMPv3 operation that uses the external AAA server, you must use AES for the privacy protocol in the user configuration on the external AAA server.

CLI and SNMP User Synchronization

SNMPv3 user management can be centralized at the Access Authentication and Accounting (AAA) server level. This centralized user management allows the SNMP agent in Cisco NX-OS to leverage the user authentication service of the AAA server. Once user authentication is verified, the SNMP PDUs are processed further. Additionally, the AAA server is also used to store user group names. SNMP uses the group names to apply the access/role policy that is locally available in the switch.

Any configuration changes made to the user group, role, or password results in database synchronization for both SNMP and AAA.

Cisco Nexus 1000V NX-OS synchronizes user configuration in the following ways:

- The authentication passphrase specified in the **snmp-server user** command becomes the password for the CLI user.
- The password specified in the **username** command becomes as the authentication and privacy passphrases for the SNMP user.
- If you delete a user using either SNMP or the CLI, the user is deleted for both SNMP and the CLI.
- User-role mapping changes are synchronized in SNMP and the CLI.
- Role changes (deletions or modifications) from the CLI are synchronized to SNMP.

Note When you configure passphrase/password in localized key/encrypted format, Cisco NX-OS does not synchronize the user information (password, roles, and so on).

Cisco NX-OS holds the synchronized user configuration for 60 minutes by default. See Modifying the AAA Synchronization Time, on page 60 for information on how to modify this default value.

Group-Based SNMP Access

Note Because group is a standard SNMP term used industry-wide, we refer to roles as groups in this SNMP section.

SNMP access rights are organized by groups. Each group in SNMP is similar to a role through the CLI. Each group is defined with read access or read-write access.

You can begin communicating with the agent once your username is created, your roles are set up by your administrator, and you are added to the roles.

High Availability

Stateless restarts for SNMP are supported. After a reboot or supervisor switchover, the running configuration is applied.

Guidelines and Limitations for SNMP

- Read-only access to some SNMP MIBs is supported. See the Cisco NX-OS MIB support list at the following URL for more information:

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

- SNMP Role Based Access Control (RBAC) is not supported.
- The SNMP set command is supported by the following Cisco MIBs:
  - CISCO-IMAGE-UPGRADE-MIB
  - CISCO-CONFIG-COPY-MIB
- The recommended SNMP polling interview time is 5 minutes.

Default Settings for SNMP

Parameters	Default
license notifications	enabled

Configuring SNMP

This section includes the following topics:

- Configuring SNMP
- Users Enforcing SNMP Message Encryption
- Creating SNMP Communities
- Configuring SNMP Notification Receivers
- Configuring the Notification Target User
- Enabling SNMP Notifications

- Disabling LinkUp/LinkDown Notifications on an Interface
- Enabling a One-time Authentication for SNMP over TCP
- Assigning the SNMP Switch Contact and Location Information
- Disabling SNMP
- Modifying the AAA Synchronization Time

Configuring SNMP Users

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Places you in global configuration mode.
Step 2	switch(config)# **snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] [**localizedkey**]]	Configures an SNMP user with authentication and privacy parameters. The *passphrase* can be any case-sensitive, alphanumeric string up to 64 characters. If you use the **localizekey** keyword, the *passphrase* can be any case-sensitive, alphanumeric string up to 130 characters. The *name* argument is the name of a user who can access the SNMP engine. The **auth** keyword enables one-time authentication for SNMP over a TCP session. It is optional. The **md5** keyword specifies HMAC MD5 algorithm for authentication. It is optional. The **sha** keyword specifies HMAC SHA algorithm for authentication. It is optional. The **priv** keyword specifies encryption parameters for the user. It is optional. The **aes-128** keyword specifies a 128-byte AES algorithm for privacy. It is optional. The **engineID** keyword specifies the engineID for configuring the notification target user (for V3 informs). It is optional. The *id* is a 12-digit colon-separated decimal number.
Step 3	switch(config-callhome)# **show snmp user**	(Optional) Displays information about one or more SNMP users.

	Command or Action	Purpose
Step 4	switch(config-callhome)# **copy running-config startup-config**	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh
```

Enforcing SNMP Message Encryption for All Users

Procedure

	Command or Action	Purpose
Step 1	switch(config)# **snmp-server globalEnforcePriv**	Enforces SNMP message encryption for all users.

```
switch(config)# snmp-server globalEnforcePriv
```

Creating SNMP Communities

You can create SNMP communities for SNMPv1 or SNMPv2c.

Before You Begin

You must be in global configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# **snmp-server community** *name* {**ro** | **rw**}	Creates an SNMP community string.

```
switch(config)# snmp-server community public ro
```

Configuring SNMP Notification Receivers

Configuring the Notification Target User

You must configure a notification target user on the device to send SNMPv3 inform notifications to a notification host receiver

TheCisco Nexus 1000V uses the credentials of the notification target user to encrypt the SNMPv3 inform notification messages to the configured notification host receiver.

Note For authenticating and decrypting the received INFORM PDU, the notification host receiver should have the same user credentials as configured in Cisco Nexus 1000V to authenticate and decrypt the inform s

Before You Begin

You must be in global configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# **snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*]	Configures the notification target user with the specified engine ID for notification host receiver. The *id* is a 12-digit colon-separated decimal number.

```
switch(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID
00:00:00:63:00:01:00:10:20:15:10:03
```

Enabling SNMP Notifications

You can enable or disable notifications. If you do not specify a notification name, Cisco Nexus 1000V enables all notifications.

The following table lists the commands that enable the notifications for Cisco Nexus 1000V MIBs.

Note The snmp-server enable traps command enables both traps and informs, depending on the configured notification host receivers.

MIB	Related Commands
All notifications	**snmp-server enable traps**
CISCO-AAA-SERVER-MIB	**snmp-server enable traps aaa**

MIB	Related Commands
ENITY-MIB	**snmp-server enable traps entity**
CISCO-ENTITY-FRU-CONTROL-MIB	**snmp-server enable traps entity fru**
CISCO-LICENSE-MGR-MIB	**snmp-server enable traps license**
IF-MIB	**snmp-server enable traps link**
CISCO-PSM-MIB	**snmp-server enable traps port-security**
SNMPv2-MIB	**snmp-server enable traps snmp** **snmp-server enable traps snmp authentication**

The license notifications are enabled by default. All other notifications are disabled by default.

Before You Begin

You must be in global configuration mode to enable the specified notification

Procedure

	Command or Action	Purpose
Step 1	switch(config)# **snmp-server enable traps**	Enables all SNMP notifications.
Step 2	switch(config)# **snmp-server enable traps aaa** [**server-state-change**]	Enables the AAA SNMP notifications.
Step 3	switch(config)# **snmp-server enable traps entity** [**fru**]	Enables the ENTITY-MIB SNMP notifications.
Step 4	switch(config)# **snmp-server enable traps license**	Enables the license SNMP notification.
Step 5	switch(config)# **snmp-server enable traps link**	Enables the link SNMP notifications.
Step 6	switch(config)# **snmp-server enable traps port-security**	Enables the port security SNMP notifications
Step 7	switch(config)# **snmp-server enable traps snmp** [**authentication**]	Enables the SNMP agent notifications.

Disabling LinkUp/LinkDown Notifications on an Interface

You can disable linkUp and linkDown notifications on an individual interface. You can use this limit notifications on flapping interface (an interface that transitions between up and down repeatedly).

Before You Begin

You must be in interface configuration mode to disable linkUp/linkDown notifications for the interface.

Procedure

	Command or Action	Purpose
Step 1	switch(config-if)# **no snmp trap link-status**	Disables SNMP link-state traps for the interface. This command is enabled by default.

```
switch(config-if)# no snmp trap link-status
```

Enabling a One-time Authentication for SNMP over TCP

Before You Begin

You must be in global configuration mode to enable one-time authentication for SNMP over TCP

Procedure

	Command or Action	Purpose
Step 1	switch(config)# **snmp-server tcp-session** [**auth**]	Enables a one-time authentication for SNMP over a TCP session. The default is disabled.

```
switch(config)# snmp-server tcp-session
```

Assigning the SNMP Switch Contact and Location Information

You can assign the switch contact information, which is limited to 32 characters (without spaces) and the switch location.

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **snmp-server contact** *name*	Configures sysContact, which is the SNMP contact name.

	Command or Action	Purpose
Step 3	switch(config)# **snmp-server location** *name*	Configures sysLocation, which is the SNMP location.
Step 4	switch(config)# **show snmp**	(Optional) Displays information about one or more destination profiles.
Step 5	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# snmp contact Admin
switch(config)# snmp location Lab-7
switch(config)# show snmp
switch(config)# copy running-config startup-config
```

Configuring a Host Receiver for SNMPv1 Traps

Before You Begin

You must be in global configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# **snmp-server host** *ip-address* **traps version 1** *community* [**udp_port** *number*]	Configures a host receiver for SNMPv1 traps. The community can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

```
switch(config)# snmp-server host 192.0.2.1 traps version 1 public
```

Disabling SNMP

Before You Begin

You must be in global configuration mode to disable the SNMP protocol on a device.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# **no snmp-server protocol enable**	Disables the SNMP protocol. This command is enabled by default.

```
switch(config)# no snmp-server protocol enable
```

Modifying the AAA Synchronization Time

You can modify how long Cisco NX-OS holds the synchronized user configuration.

Before You Begin

You must be in global configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# **snmp-server aaa-user cache-timeout** *seconds*	Configures how long the AAA synchronized user configuration stays in the local cache. The range is from 1 to 86400 seconds. The default is 3600.

```
switch(config)# snmp-server aaa-user cache-timeout 1200
```

Verifying the SNMP Configuration

Use one of the following commands to verify the configuration:

Command	Purpose
show running-config snmp [**all**]	Displays the SNMP running configuration.
show snmp	Displays the SNMP status.
show snmp community	Displays the SNMP community strings.
show snmp context	Displays the SNMP context mapping.
show snmp engineID	Displays the SNMP engineID.
show snmp group	Displays SNMP roles.
show snmp session	Displays SNMP sessions.

Command	Purpose
show snmp trap	Displays the SNMP notifications enabled or disabled.
show snmp user	Displays SNMPv3 users.

Configuration Example for SNMP

This example shows how to configure sending the Cisco linkUp/Down notifications to one notification host receiver using the Blue VRF and define two SNMP users, Admin and NMS

```
switch# configure terminal
 switch(config)# snmp-server contact Admin@company.com
 switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh
 switch(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID
00:00:00:63:00:01:00:22:32:15:10:03
 switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS
 switch(config)# snmp-server host 192.0.2.1 use-vrf Blue
 switch(config)# snmp-server enable traps link cisco
```

Related Documents for SNMP

Related Topic	Document Title
MIBs	http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

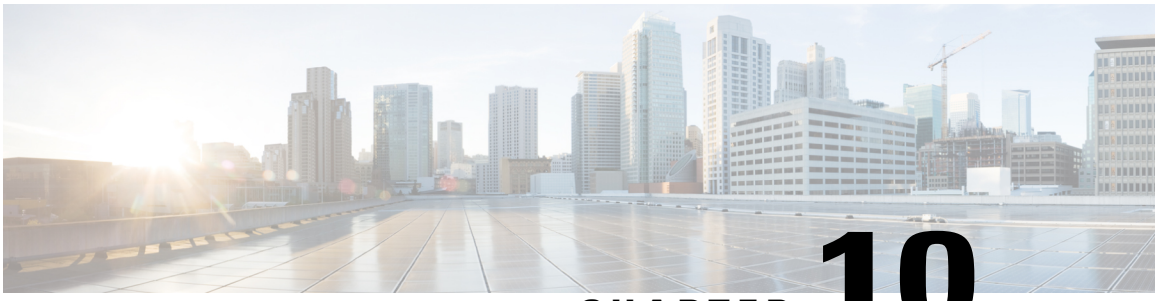
MIBs

• CISCO-TC • SNMPv2-MIB • SNMP-COMMUNITY-MIB • SNMP-FRAMEWORK-MIB • SNMP-NOTIFICATION-MIB • SNMP-TARGET-MIB • ENTITY-MIB • IF-MIB • CISCO-ENTITY-EXT-MIB • CISCO-ENTITY-FRU-CONTROL-MIB • CISCO-FLASH-MIB • CISCO-IMAGE-MIB • CISCO-VIRTUAL-NIC-MIB • CISCO-ENTITY-VENDORTYPE-OID-MIB • NOTIFICATION-LOG-MIB • IANA-ADDRESS-FAMILY-NUMBERS-MIB • IANAifType-MIB • IANAiprouteprotocol-MIB • HCNUM-TC	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

• CISCO-VLAN-MEMBERSHIP-MIB • CISCO-SYSTEM-MIB • CISCO-SYSTEM-EXT-MIB • CISCO-IMAGE-MIB • CISCO-IMAGE-UPGRADE-MIB • CISCO-BRIDGE-MIB • CISCO-CONFIG-COPY-MIB • CISCO-SYSLOG-EXT-MIB • CISCO-PROCESS-MIB • CISCO-AAA-SERVER-MIB • CISCO-AAA-SERVER-EXT-MIB • CISCO-COMMON-ROLES-MIB • CISCO-COMMON-MGMT-MIB	

Feature History for SNMP

Feature Name	Releases	Feature Information
SNMP	Release 5.2(1)IC1(1.1)	This feature was introduced.



CHAPTER 10

Configuring NetFlow

This chapter contains the following sections:

Information about NetFlow

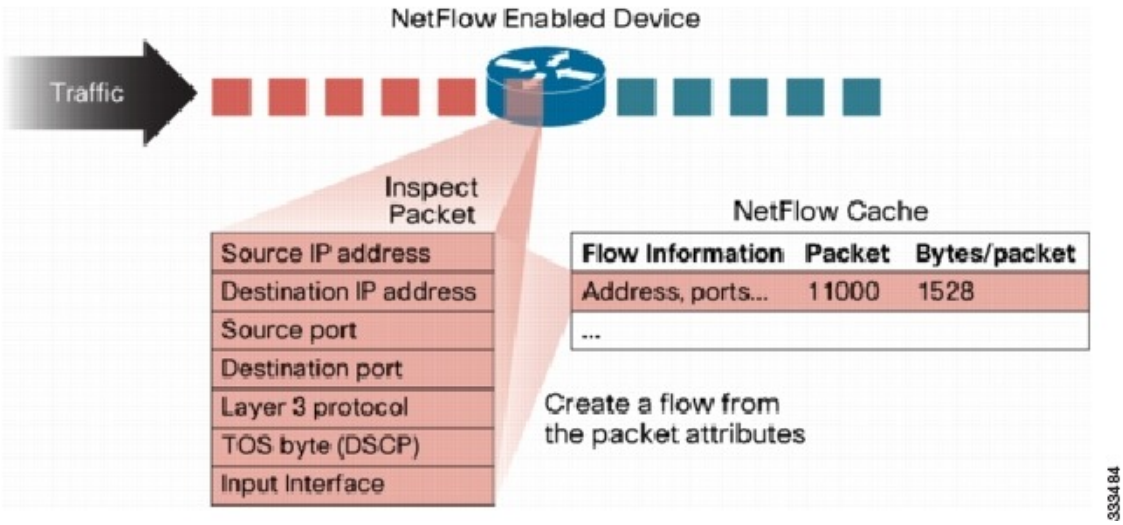
NetFlow lets you evaluate IP traffic and understand how and where it flows. NetFlow gives visibility into traffic transiting the virtual switch by characterizing IP traffic based on its source, destination, timing, and application information. This information is used to assess network availability and performance, assist in meeting regulatory requirements (compliance), and help with troubleshooting. NetFlow gathers data that can be used in accounting, network monitoring, and network planning.

What is a Flow

A flow is a one-directional stream of packets that arrives on a source interface (or subinterface), matching a set of criteria. All packets with the same source/destination IP address, source/destination ports, protocol

interface and class of service are grouped into a flow and then packets and bytes are tallied. This condenses a large amount of network information into a database called the NetFlow cache.

Figure 3: NetFlow Cache Example



You create a flow by defining the criteria it gathers. Flows are stored in the NetFlow cache. Flow information tells you the following:

- Source address tells you who is originating the traffic.
- Destination address tells who is receiving the traffic.
- Ports characterize the application using the traffic.
- Class of service examines the priority of the traffic.
- The device interface tells how traffic is being used by the network device.
- Tallied packets and bytes show the amount of traffic.

Flow Record Definition

A flow record defines the information that NetFlow gathers, such as packets in the flow and the types of counters gathered per flow. You can define new flow records or use the pre-defined Cisco Nexus 1000V flow record.

The following table describes the criteria defined in a flow record.

Table 2: Flow record criteria

Flow Record Criteria	Description
Match	Defines what information is matched for collection in the flow record. • ip: Data collected in the flow record matches one of the following IP options: ◦ protocol ◦ tos (type of service) • ipv4: Data collected in the flow record matches one of the following ipv4 address options: ◦ source address ◦ destination address • transport: Data collected in the flow record matches one of the following transport options: ◦ destination port ◦ source port
Collect	Defines how the flow record collects information. • counter: Collects Flow Record information in one of the following formats: ◦ bytes: collected in 32-bit counters unless the long 64-bit counter is specified. ◦ packets: collected in 32-bit counters unless the long 64-bit counter is specified. • timestamp sys-uptime: Collects the system up time for the first or last packet in the flow. • transport tcp flags: Collects the TCP transport layer flags for the packets in the flow.

Predefined Flow Records

Cisco Nexus 1000V Predefined Flow Record: Netflow-Original

```
switch# show flow record netflow-original
Flow record netflow-original:
    Description: Traditional IPv4 input NetFlow with origin ASs
    No. of users: 0
    Template ID: 0
    Fields:
        match ipv4 source address
        match ipv4 destination address
        match ip protocol
        match ip tos
        match transport source-port
```

```
        match transport destination-port
        match interface input
        match interface output
        match flow direction
        collect routing source as
        collect routing destination as
        collect routing next-hop address ipv4
        collect transport tcp flags
        collect counter bytes
        collect counter packets
        collect timestamp sys-uptime first
        collect timestamp sys-uptime last
switch#
```

Note Although the following lines appear in the output of the show flow record command, the commands they are based on are not currently supported in Cisco Nexus 1000V. The use of these commands has no affect on the configuration.

```
collect routing source as
collect routing destination as
collect routing next-hop address ipv4
```

Cisco Nexus 1000V Predefined Flow Record: Netflow IPv4 Original-Input

```
switch# show flow record netflow ipv4 original-input
Flow record ipv4 original-input:
    Description: Traditional IPv4 input NetFlow
    No. of users: 0
    Template ID: 0
    Fields:
        match ipv4 source address
        match ipv4 destination address
        match ip protocol
        match ip tos
        match transport source-port
        match transport destination-port
        match interface input
        match interface output
        match flow direction
        collect routing source as
        collect routing destination as
        collect routing next-hop address ipv4
        collect transport tcp flags
        collect counter bytes
        collect counter packets
        collect timestamp sys-uptime first
        collect timestamp sys-uptime last
switch#
```

Cisco Nexus 1000V Predefined Flow Record: Netflow IPv4 Original-Output

```
switch# show flow record netflow ipv4 original-output
Flow record ipv4 original-output:
    Description: Traditional IPv4 output NetFlow
    No. of users: 0
    Template ID: 0
    Fields:
        match ipv4 source address
        match ipv4 destination address
        match ip protocol
        match ip tos
        match transport source-port
        match transport destination-port
        match interface input
        match interface output
        match flow direction
        collect routing source as
        collect routing destination as
```

```
        collect routing next-hop address ipv4
        collect transport tcp flags
        collect counter bytes
        collect counter packets
        collect timestamp sys-uptime first
        collect timestamp sys-uptime last
switch#
```

Cisco Nexus 1000V Predefined Flow Record: Netflow Protocol-Port

```
switch# show flow record netflow protocol-port
Flow record ipv4 protocol-port:
    Description: Protocol and Ports aggregation scheme
    No. of users: 0
    Template ID: 0
    Fields:
        match ip protocol
        match transport source-port
        match transport destination-port
        match interface input
        match interface output
        match flow direction
        collect counter bytes
        collect counter packets
        collect timestamp sys-uptime first
        collect timestamp sys-uptime last
switch#
```

Accessing NetFlow Data

There are two primary methods used to access NetFlow data:

- Command Line Interface (CLI)
- NetFlow Collector

Command Line Interface for NetFlow

Use the Command Line Interface (CLI) to access NetFlow data, and to view what is happening in your network now.

The CLI uses the Flow Monitor and Flow Exporter to capture and export flow records to the Netflow Collector. Cisco Nexus 1000V supports the NetFlow Version 9 export format.

Note Cisco Nexus 1000V supports UDP as the transport protocol for exporting data to up to two exporters per monitor.

Flow Monitor

A flow monitor creates an association between the following NetFlow components:

- a flow record—consisting of matching and collection criteria
- a flow exporter—consisting of the export criteria

This flow monitor association enables a set, consisting of a record and an exporter, to be defined once and re-used many times. Multiple flow monitors can be created for different needs. A flow monitor is applied to a specific interface in a specific direction.

Flow Exporter

Use the flow exporter to define where the flow records are sent from the cache to the reporting server, called the NetFlow Collector. An exporter definition includes the following.

- Destination IP address
- Source interface
- UDP port number (where the collector is listening)
- Export format

NetFlow Collector

You can export NetFlow from the Cisco Nexus 1000V NetFlow cache to a reporting server called the NetFlow Collector. The NetFlow Collector assembles the exported flows and combines them to produce reports used for traffic and security analysis. NetFlow export, unlike SNMP polling, pushes information periodically to the NetFlow reporting collector. The NetFlow cache is constantly filling with flows. Cisco Nexus 1000V searches the cache for flows that have terminated or expired and exports them to the NetFlow collector server.

The following steps implement NetFlow data reporting:

- NetFlow records are configured to define the information that NetFlow gathers.
- Netflow monitor is configured to capture flow records to the NetFlow cache.
- NetFlow export is configured to send flows to the collector.
- Cisco Nexus 1000V searches the NetFlow cache for flows that have terminated and exports them to the NetFlow collector server.
- Flows are bundled together based on space availability in the UDP export packet or based on export timer.
- The NetFlow collector software creates real-time or historical reports from the data.

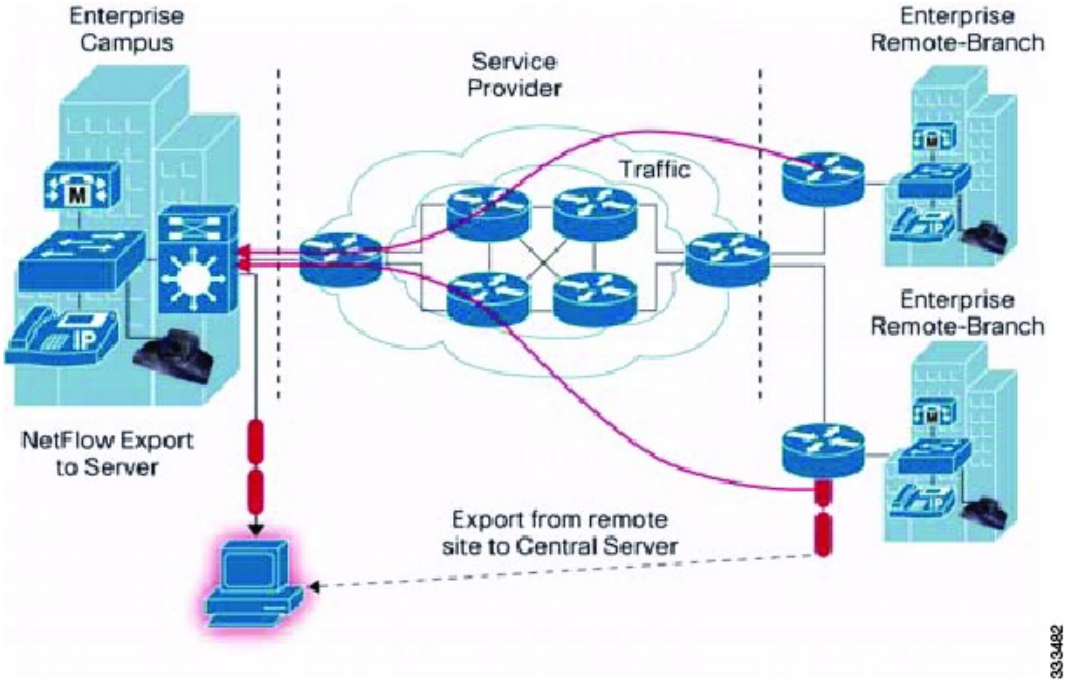
Exporting Flows to the NetFlow Collector Server

Timers determine when a flow is exported to the NetFlow Collector Server. A flow is ready for export when one of the following occurs:

- The flow is inactive for a certain time during which no new packets are received for the flow.
- The flow has lived longer than the active timer, for example, a long FTP download.

- The flow cache is full and some flows must be aged out to make room for new flows.

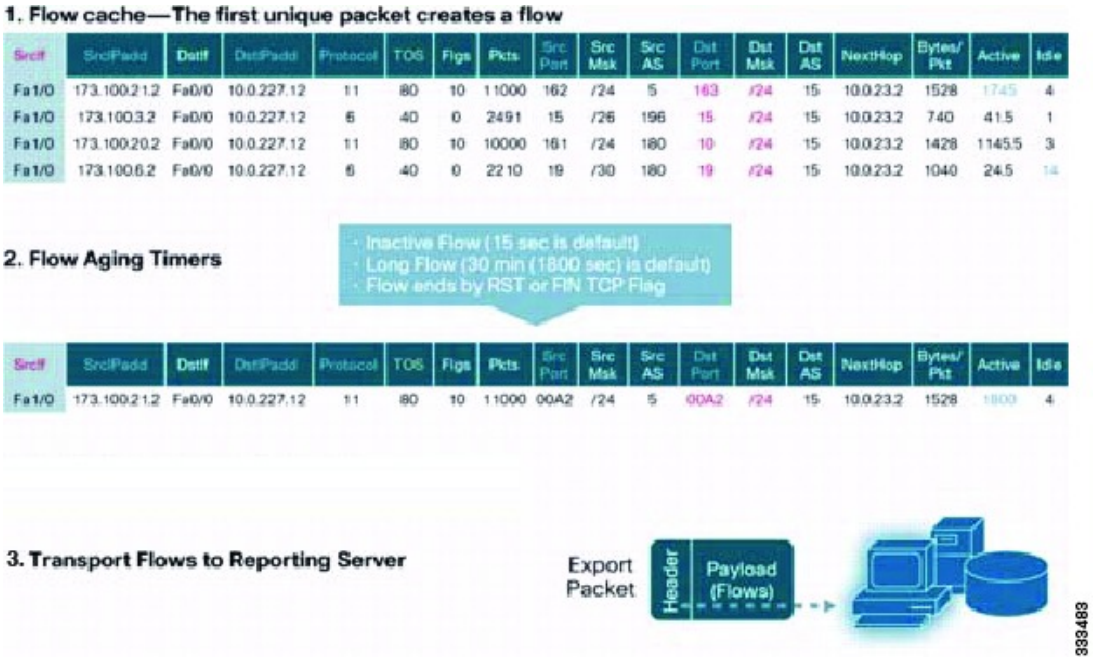
Figure 4: Exporting Flows to the NetFlow Collector Server



What NetFlow Data Looks Like

The following figure shows an example of NetFlow data.

Figure 5: NetFlow Cache Example



Network Analysis Module

You can also use the Cisco Network Analysis Module (NAM) to monitor NetFlow data sources. NAM enables traffic analysis views and reports such as hosts, applications, conversations, VLAN, and QoS.

High Availability for NetFlow

Cisco Nexus 1000V supports stateful restarts for NetFlow. After a reboot or supervisor switchover, Cisco Nexus 1000V applies the running configuration.

Prerequisites for NetFlow

- You must be aware of resource requirements since NetFlow consumes additional memory and CPU resources.
- Memory and CPU resources are provided by the VEM hosting the flow monitor interface. Resources are limited by the number of CPU cores present on the VEM.

Configuration Guidelines and Limitations for NetFlow

- In Cisco Nexus 1000V, Mgmt0 interface IP address is configured by default as the source IP address for an exporter. You can change the source IP address if needed.
- Cisco Nexus 1000V includes the following predefined flow records that can be used instead of configuring a new one.
  - netflow-original

    Cisco Nexus 1000V predefined traditional IPv4 input NetFlow with origin ASs

    Note The routing-related fields in this predefined flow record are ignored.

  - netflow ipv4 original-input

    Cisco Nexus 1000V predefined traditional IPv4 input NetFlow
  - netflow ipv4 original-output

    Cisco Nexus 1000V predefined traditional IPv4 output NetFlow
  - netflow protocol-port

    Cisco Nexus 1000V predefined protocol and ports aggregation scheme
- Cisco Nexus 1000V InterCloud supports a configuration of 32 monitors on 300 interfaces.

Default Settings for NetFlow

Parameters	Default
NetFlow version	9
source interface	mgmt0
match	direction and interface (incoming/outgoing)
flow monitor active timeout	1800
flow monitor inactive timeout	300
flow monitor cache size	65536
flow exporter UDP port transport udp command	9995
DSCP	default/best-effort (0)
VRF	default

Enabling the NetFlow Feature

Before You Begin

You are logged in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **feature netflow**	Enables the NetFlow feature.
Step 3	switch(config)# **show feature**	(Optional) Displays the available features and whether or not they are enabled.
Step 4	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to enable the NetFlow feature:

```
switch# configure terminal
switch(config)# feature netflow
switch(config)#
```

Configuring NetFlow

Defining a Flow Record

Before You Begin

- You know which of the options you want this flow record to match.
- You know which options you want this flow record to collect.

Note Although the following lines appear in the output of the show flow record command, the commands they are based on are not currently supported in Cisco Nexus 1000V. The use of these commands has no affect on the configuration.

```
collect routing source as
collect routing destination as
collect routing next-hop address ipv4
```

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **flow record** *name*	Creates a Flow Record by name, and places you in the CLI Flow Record Configuration mode for that specific record.
Step 3	switch(config#) **description** *string*	(Optional) Adds a description of up to 63 characters to the Flow Record and saves it to the running configuration.
Step 4	switch(config#) **match** {**ip** {**protocol** | **tos**} | **ipv4** {**destination address** | **source address**} | **transport** {**destination-port** | **source-port**}}	Defines the Flow Record to match one of the following and saves it in the running configuration. • ip: Matches one of the following IP options: ◦ protocol ◦ tos (type of service) • ipv4: Matches one of the following ipv4 address options: ◦ source address ◦ destination address • transport: Matches one of the following transport options: ◦ destination port ◦ source port
Step 5	switch(config)# **collect** {**counter** {**bytes** [**long**] | **packets** [**long**]} | **timestamp sys-uptime** | **transport tcp flags**}	Specifies a collection option to define the information to collect in the Flow Record and saves it in the running configuration. • counter: Collects Flow Record information in one of the following formats: ◦ bytes: collected in 32-bit counters unless the long 64-bit counter is specified. ◦ packets: collected in 32-bit counters unless the long 64-bit counter is specified. • timestamp sys-uptime: Collects the system up time for the first or last packet in the flow. • transport tcp flags: Collects the TCP transport layer flags for the packets in the flow.

	Command or Action	Purpose
Step 6	switch(config)# **show flow record** *name*	(Optional) Displays information about Flow Records.
Step 7	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to create a flow record:

```
switch# configure terminal
switch(config)# flow record RecordTest
switch(config-flow-record)# description Ipv4flow
switch(config-flow-record)# match ipv4 destination address
switch(config-flow-record)# collect counter packets
switch(config-flow-record)# show flow record RecordTest
Flow record RecordTest:
    Description: Ipv4flow
    No. of users: 0
    Template ID: 0
    Fields:
        match ipv4 destination address
        match interface input
        match interface output
        match flow direction
        collect counter packets
switch(config-flow-record)#
```

Defining a Flow Exporter

A Flow Exporter defines where and how Flow Records are exported to the NetFlow Collector Server.

- Export format version 9 is supported.
- A maximum of two flow exporters per monitor are permitted.

Before You Begin

- You know the destination IP address of the NetFlow Collector Server.
- You know the source interface that Flow Records are sent from.
- You know the transport UDP that the Collector is listening on.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)#**flow exporter** *name*	Creates a Flow Exporter, saves it in the running configuration, and then places you in CLI Flow Exporter Configuration mode.

	Command or Action	Purpose
Step 3	switch(config-flow-exporter)# **description** *string*	Adds a description of up to 63 characters to this Flow Exporter and saves it in the running configuration.
Step 4	switch(config-flow-exporter)# **destination** {*ipv4-address* | *ipv6-address*}	Specifies the IP address of the destination interface for this Flow Exporter and saves it in the running configuration.
Step 5	switch(config-flow-exporter)# **dscp** *value*	Specifies the differentiated services codepoint value for this Flow Exporter, between 0 and 63, and saves it in the running configuration.
Step 6	switch(config-flow-exporter)# **source mgmt** *lc-exp*	Specifies the line card, from which the Flow Records are sent to the NetFlow Collector Server, and saves it in the running configuration.
Step 7	switch(config-flow-exporter)# **transport udp** *port-number*	Specifies the destination UDP port, between 0 and 65535, used to reach the NetFlow collecton, and saves it in the running configuration.
Step 8	switch(config-flow-exporter)# **version** {**9**}	Specifies NetFlow export version 9, saves it in the running configuration, and places you into the export version 9 configuration mode.
Step 9	switch(config-flow-exporter-version-9)# **option** {**exporter-stats** | **interface-table** | **sampler-table**} **timeout** *value*	Specifies one of the following version 9 exporter resend timers and its value, between 1 and 86400 seconds, and saves it in the running configuration. • exporter-stats • interface-table • sampler-table
Step 10	switch(config-flow-exporter-version-9)# **template data timeout** *seconds*	Sets the template data resend timer and its value, between 1 and 86400 seconds, and saves it in the running configuration.
Step 11	switch(config-flow-exporter-version-9)# **show flow exporter** [*name*]	(Optional) Displays information about the Flow Exporter.
Step 12	switch(config-flow-exporter-version-9)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example displays the output of the command **show flow exporter** [*exp2-192*]:

```
switch(config-flow-exporter)# show flow exporter ExportTest
Flow exporter exp2-192:
Destination: 10.106.192.200
VRF: management (1)
Destination UDP Port 9012
Source IP Address 10.106.192.137/24
```

```
Export from Line Card
Export Version 9
Data template timeout 1800 seconds
Exporter Statistics
Number of Flow Records Exported 27060
Number of Templates Exported 175
Number of Export Packets Sent 10674
Number of Export Bytes Sent 595388
Number of Destination Unreachable Events 0
Number of No Buffer Events 0
Number of Packets Dropped (No Route to Host) 0
Number of Packets Dropped (other) 0
Number of Packets Dropped (LC to RP Error) 0
Number of Packets Dropped (Output Drops) 0
Time statistics were last cleared: Never
```

Defining a Flow Monitor

A Flow Monitor is associated with a Flow Record and a Flow Exporter.

A maximum of one flow monitor per interface per direction is permitted.

Before You Begin

- You know the name of an existing Flow Exporter to associate with this flow monitor.
- You know the name of an existing Flow Record to associate with this flow monitor. You can use either a flow record you previously created, or one of the following Cisco Nexus 1000V predefined flow records:
  - netflow-original
  - netflow ipv4 original-input
  - netflow ipv4 original-output
  - netflow protocol-port

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **flow monitor** *name*	Creates a flow monitor by name, saves it in the running configuration, and then places you in the CLI Flow Monitor Configuration mode.
Step 3	switch(config-flow-monitor)# **description** *string*	(Optional) For the specified flow monitor, adds a descriptive string of up to 63 alphanumeric characters, and saves it in the running configuration.
Step 4	switch(config-flow-monitor)# **exporter** *name*	For the specified flow monitor, adds an existing flow exporter and saves it in the running configuration.

	Command or Action	Purpose
Step 5	switch(config-flow-monitor)# **record** {*name* | **netflow** {**ipv4**}}	For the specified flow monitor, adds an existing flow record and saves it in the running configuration. • name: The name of a flow record you have previously created, or the name of a Cisco provided pre-defined flow record. • netflow: Traditional NetFlow collection schemes ipv4: Traditional IPv4 NetFlow collection schemes
Step 6	switch(config-flow-monitor)# **show flow monitor** [*name*]	(Optional) Displays information about existing flow monitors.
Step 7	switch(config-flow-monitor)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to create a flow monitor:

```
switch# configure terminal
switch(config)# flow monitor MonitorTest
switch(config-flow-monitor)# description Ipv4Monitor
switch(config-flow-monitor)# exporter ExportTest
switch(config-flow-monitor)# record RecordTest
switch(config-flow-monitor)# show flow monitor MonitorTest
Flow Monitor monitortest:
Description :Ipv4Monitor
Use count: 0
 Flow Record: RecordTest
    Flow Exporter: ExportTest

switch(config-flow-monitor)#
```

Assigning a Flow Monitor to an Interface

Before You Begin

- You know the name of the flow monitor you want to use for the interface.
- You know the interface type and its number.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *interface-type interface-number*	Places you in the CLI Interface Configuration mode for the specified interface.

	Command or Action	Purpose
Step 3	switch(config)# **ip flow monitor** *name* {**input** | **output**}	For the specified interface, assigns a flow monitor for input or output packets and saves it in the running configuration.
Step 4	switch(config)# **show flow** *interface-type interface-number*	(Optional) For the specified interface, displays the NetFlow configuration.
Step 5	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to assign a flow monitor to an interface:

```
switch# configure terminal
switch(config)# interface veth 2
switch(config-if)# ip flow monitor MonitorTest output
switch(config-if)# show flow interface veth 2
Interface veth 2:
    Monitor: MonitorTest
    Direction: Output
switch(config-if)#
```

Adding a Flow Monitor to a Port Profile

Before You Begin

- You are logged in to the CLI in EXEC mode.
- You have already created the flow monitor.
- If using an existing port profile, you have already created the port profile and you know its name.
- If creating a new port profile, you know the type, and you know the name you want to give it.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** [**type** vethernet}] *name*	Enters port profile configuration mode for the named port profile.
Step 3	switch(config-port-prof)# **ip flow monitor** *name* {**input** | **output**}	Applies a named flow monitor to the port profile for either incoming (input) or outgoing (output) traffic.
Step 4	switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]	(Optional) Displays the configuration for verification.

	Command or Action	Purpose
Step 5	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to add a flow monitor to a port profile:

```
switch# configure terminal
switch(config)# port-profile AccessProf
switch(config-port-prof)# ip flow monitor allacces4 output
switch(config-port-prof)# show port-profile name AccessProf
port-profile AccessProf
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    ip flow monitor allaccess4 output
  evaluated config attributes:
    ip flow monitor allaccess4 output
  assigned interfaces:
switch(config-port-prof)#
```

Verifying the NetFlow Configuration

Use one of the following commands to verify the configuration:

Command	Purpose
show flow exporter [*name*]	Displays information about NetFlow flow exporter maps.
show flow interface [*interface-type number*]	Displays information about NetFlow interfaces.
show flow monitor [*name* [**cache module** *number* | **statistics module** *number*]]	Displays information about NetFlow flow monitors. **Note** The **show flow monitor cache module** command differs from the **show flow monitor statistics module** command in that the cache command also displays cache entries . Since each processor has its own cache, all output of these commands is based on the number of processors on the server (also called module or host). When more than one processor is involved in processing packets for a single flow, then the same flow appears for each processor.

Command	Purpose
show flow record [*name*]	Displays information about NetFlow flow records.

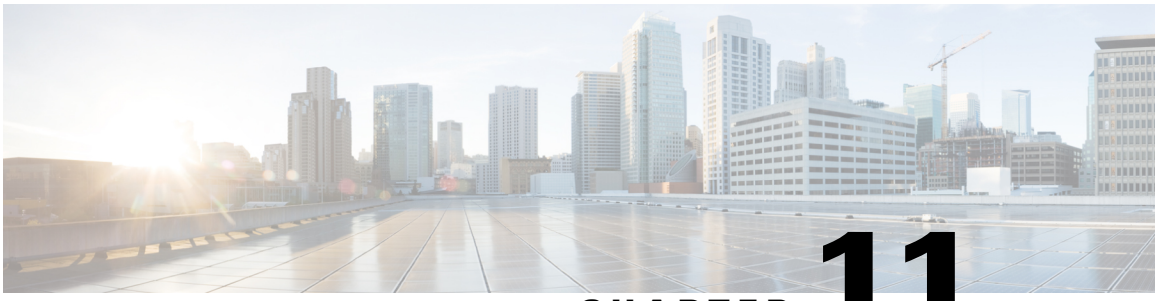
Related Documents for NetFlow

Related Topic	Document Title
Cisco NetFlow Overview	http://cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html

Feature History for NetFlow

This table includes only the updates for those releases that have resulted in additions or changes to the feature.

Feature Name	Releases	Feature Information
NetFlow	Release 5.2(1)IC1(1.2)	NetFlow was introduced.



CHAPTER 11

Configuring System Message Logging

This chapter contains the following sections:

Information about System Message Logging

You can use system message logging to control the destination and to filter the severity level of messages that system processes generate. You can configure logging to terminal sessions, a log file, and syslog servers on remote systems.

System message logging is based on RFC 3164. For more information about the system message format and the messages that the device generates, see the *Cisco NX-OS System Messages Reference*.

By default, the device outputs messages to terminal sessions.

The following table describes the severity levels used in system messages. When you configure the severity level, the system outputs messages at that level and lower.

Level	Description
0 – emergency	System unusable
1 – alert	Immediate action needed
2 – critical	Critical condition
3 – error	Error condition

Level	Description
4 – warning	Warning condition
5 – notification	Normal but significant condition
6 – informational	Informational message only
7 – debugging	Appears during debugging only

The device logs the most recent 100 messages of severity 0, 1, or 2.

You can configure which system messages should be logged based on the facility that generated the message and its severity level.

Syslog servers run on remote systems that are configured to log system messages based on the syslog protocol. You can configure up to three syslog servers.

Note When the device first initializes, messages are sent to syslog servers only after the network is initialized.

System Message Logging Facilities

The following table lists the facilities that you can use in system message logging configuration

Facility	Description
aaa	AAA manager
aclmgr	ACL manager
adjmgr	Adjacency Manager
all	Keyword that represents all facilities
arbiter	Arbiter manager
arp	ARP manager
auth	Authorization system
authpriv	Private authorization system
bootvar	Bootvar
callhome	Call home manager
capability	MIG utilities daemon

Facility	Description
cert-enroll	Certificate enroll daemon
cfs	CFS manager
clis	CLIS manager
cmpproxy	CMP proxy manager
copp	CoPP manager
core	Core daemon
cron	Cron and at scheduling service
daemon	System daemons
dhcp	DHCP manager
diagclient	GOLD diagnostic client manager
diagmgr	GOLD diagnostic manager
eltm	ELTM manager
evmc	EVMC manager
evms	EVMS manager
feature-mgr	Feature manager
fs-daemon	Fs daemon
ftp	File transfer system
glbp	GLBP manager
hsrp	HSRP manager
im	IM manager
ipconf	IP configuration manager
ipfib	IP FIB manager
kernel	OS kernel
l2fm	L2 FM manager

Facility	Description
l2nac	L2 NAC manager
l3vm	L3 VM manager
license	Licensing manager
local0	Local use daemon
local1	Local use daemon
local2	Local use daemon
local3	Local use daemon
local4	Local use daemon
local5	Local use daemon
local6	Local use daemon
local7	Local use daemon
lpr	Line printer system
m6rib	M6RIB manager
mail	Mail system
mfdm	MFDM manager
module	Module manager
mrib	MRIB manager
mvsh	MVSH manager
news	USENET news
nf	NF manager
ntp	NTP manag
otm	GLBP manager
pblr	PBLR manager
pfstat	PFSTAT manager

Facility	Description
pixm	PIXM manager
pixmc	PIXMC manager
pktmgr	Packet manager
platform	Platform manager
pltfm_config	PLTFM configuration manager
plugin	Plug-in manager
port_client	Port client manager
port_lb	Diagnostic port loopback test manager
qengine	Q engine manager
radius	RADIUS manager
res_mgr	Resource manager
rpm	RPM manager
security	Security manager
session	Session manager
spanning-tree	Spanning tree manager
syslog	Internal syslog manager
sysmgr	System manager
tcpudp	TCP and UDP manager
u2	U2 manager
u6rib	U6RIB manager
ufdm	UFDM manager
urib	URIB manager
user	User process
uucp	Unix-to-Unix copy system

Facility	Description
vdc_mgr	VDC manager
vlan_mgr	VLAN manager
vmm	VMM manager
vshd	VSHD manager
xbar	XBAR manager
xbar_client	XBAR client manager
xbar_driver	XBAR driver manager
xml	XML agent

Guidelines and Limitations for System Message Logging

System messages are logged to the console and the logfile by default.

Default System Message Logging Settings

Parameter	Default
Console logging	Enabled at severity level 2
Monitor logging	Enabled at severity level 5
Log file logging	Enabled to log messages at severity level 5
Module logging	Enabled at severity level 5
Facility logging	Enabled
Time-stamp units	Seconds
syslog server logging	Disabled
syslog server configuration distribution	Disabled

Configuring System Message Logging

This section includes the following topics:

- Configuring System Message Logging to Terminal Sessions
- Restoring System Message Logging Defaults for Terminal Sessions
- Configuring System Message Logging for Modules
- Restoring System Message Logging Defaults for Modules
- Configuring System Message Logging for Facilities
- Restoring System Message Logging Defaults for Facilities
- Configuring syslog Servers
- Restoring System Message Logging Defaults for Servers
- Using a UNIX or Linux System to Configure Logging
- Displaying Log Files

Configuring System Message Logging to Terminal Sessions

You can log messages by severity level to console, telnet, and SSH sessions. By default, logging is enabled for terminal sessions.

Procedure

	Command or Action	Purpose
Step 1	switch# **terminal monitor**	Enables the device to log messages to the console.
Step 2	switch# **configure terminal**	Enters global configuration mode.
Step 3	switch(config)# **logging console** [*severity-level*]	Configures the device to log messages to the console session based on a specified severity level or higher. The default severity level is 2.
Step 4	switch(config)# **show logging console**	(Optional) Displays the console logging configuration.
Step 5	switch(config)# **logging monitor** [*severity-level*]	Enables the device to log messages to the monitor based on a specified severity level or higher. The configuration applies to telnet and SSH sessions. The default severity level is 2.
Step 6	switch(config)# **show logging monitor**	(Optional) Displays the monitor logging configuration.

	Command or Action	Purpose
Step 7	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

```
switch# terminal monitor
switch# configure terminal
switch(config)# logging console 2
switch(config)# show logging console
Logging console:                enabled (Severity: critical)
switch(config)# logging monitor 3
switch(config)# show logging monitor
Logging monitor:                enabled (Severity: errors)
switch(config)# copy running-config startup-config
switch(config)#
```

Restoring System Message Logging Defaults for Terminal Sessions

You can use the following commands in the CLI Global Configuration mode to restore default settings for system message logging for terminal sessions.

Command	Description
no logging console [*severity-level*]	Disables the device from logging messages to the console.
no logging monitor [*severity-level*]	Disables logging messages to telnet and SSH sessions.

Configuring System Message Logging for Modules

You can configure the severity level and time-stamp units of messages logged by modules.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **logging module** [*severity-level*]	Enables module log messages that have the specified severity level or higher. If the severity level is not specified, the default of 5 is used.
Step 3	switch(config)# **show logging module**	
Step 4	switch(config)# **logging timestamp** {**microseconds** | **milliseconds** | **seconds**}	Sets the logging time-stamp units. The default unit is seconds.

	Command or Action	Purpose
Step 5	switch(config)# show logging timestamp	(Optional) Displays the logging time-stamp units configured.
Step 6	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to configure system message logging for modules.

```
switch# configure terminal
switch(config)# logging module 3
switch(config)# show logging module
Logging linecard:                enabled (Severity: errors)
switch(config)# logging timestamp microseconds
switch(config)# show logging timestamp
Logging timestamp:               Microseconds
switch(config)# copy running-config startup-config
switch(config)#
```

Restoring System Message Logging Defaults for Modules

You can use the following commands in the CLI Global Configuration mode to restore default settings for system message logging for modules.

Command	Description
no logging module [*severity-level*]	Restores the default severity level for logging module system messages.
no logging timestamp {**microseconds** | **milliseconds** | **seconds**}	Resets the logging time-stamp unit to the default (seconds).

Configuring System Message Logging for Facilities

Use this procedure to configure the severity level and time-stamp units of messages logged by facilities.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **logging module** [*severity-level*]	Enables module log messages that have the specified severity level or higher. If the severity level is not specified, the default of 5 is used.

	Command or Action	Purpose
Step 3	switch(config)# **show logging module**	(Optional) Displays the module logging configuration.
Step 4	switch(config)# **logging timestamp** {**microseconds** | **milliseconds** | **seconds**}	Sets the logging time-stamp units. The default unit is seconds.
Step 5	switch(config)# **show logging timestamp**	(Optional) Copies the running configuration to the startup configuration.
Step 6	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to configure system message logging for modules.

```
switch# configure terminal
switch(config)# logging module 3
switch(config)# show logging module
Logging linecard:                enabled (Severity: errors)
switch(config)# logging timestamp microseconds
switch(config)# show logging timestamp
Logging timestamp:               Microseconds
switch(config)# copy running-config startup-config
switch(config)#
```

Restoring System Message Logging Defaults for Facilities

You can use the following commands to restore system message logging defaults for facilities.

Command	Description
no logging level [*facility severity-level*]	Restores the default logging severity level for the specified facility. If you do not specify a facility and severity level, the device resets all facilities to their default levels.
no logging timestamp {**microseconds** | **milliseconds** | **seconds**}	Resets the logging time-stamp unit to the default (seconds).

Configuring syslog Servers

Use this procedure to configure syslog servers for system message logging.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **logging server** *host* [*severity-level* [**use-vrf** *vrf-name*]]	Configures a syslog server at the specified host name or IPv4 or IPv6 address. You can limit logging of messages to a particular VRF by using the use_vrf keyword. Severity levels range from 0 to 7. The default outgoing facility is local7.
Step 3	switch(config)# **show logging server**	(Optional) Displays the syslog server configuration.
Step 4	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to forward all messages on facility local7.

```
switch# configure terminal
switch(config)# logging server 10.10.2.2 7
switch(config)# show logging server
Logging server:                 enabled
{10.10.2.2}
        server severity:        debugging
        server facility:        local7
switch(config)# copy running-config startup-config
switch(config)#
```

Restoring System Message Logging Defaults for Servers

You can use the following command to restore server system message logging default.

Command	Description
no logging server *host*	Removes the logging server for the specified host.

Using a UNIX or Linux System to Configure Logging

Before You Begin

The following UNIX or Linux fields must be configured for syslog.

Field	Description
Facility	Creator of the message, which can be auth, authpriv, cron, daemon, kern, lpr, mail, mark, news, syslog, user, local0 through local7, or an asterisk (*) for all. These facility designators allow you to control the destination of messages based on their origin. **Note** Check your configuration before using a local facility.
Level	Minimum severity level at which messages are logged, which can be debug, info, notice, warning, err, crit, alert, emerg, or an asterisk (*) for all. You can use none to disable a facility.
Action	Destination for messages, which can be a filename, a host name preceded by the at sign (@), or a comma-separated list of users or an asterisk (*) for all logged-in users.

Procedure

Step 1 On the UNIX or Linux system, add the following line to the file, /var/log/myfile.log:
facility.level <five tab characters> action

Step 2 Create the log file by entering these commands at the shell prompt:
$ touch /var/log/myfile.log

$ chmod 666 /var/log/myfile.log

Step 3 Make sure the system message logging daemon reads the new changes by checking myfile.log after entering this command:
$ kill -HUP ~cat /etc/syslog.pid~

Displaying Log Files

Use this procedure to display messages in the log file.

Procedure

	Command or Action	Purpose
Step 1	**show logging last** *number-lines*	Displays the last number of lines in the logging file. You can specify from 1 to 9999 for the last number of lines.

The following example shows the last five lines in the logging file.

```
switch# show logging last 5
2008 Aug 31 09:37:04 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
2008 Aug 31 09:37:04 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
2008 Aug 31 09:37:05 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
2008 Aug 31 09:37:05 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
2008 Aug 31 09:37:05 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
switch#
```

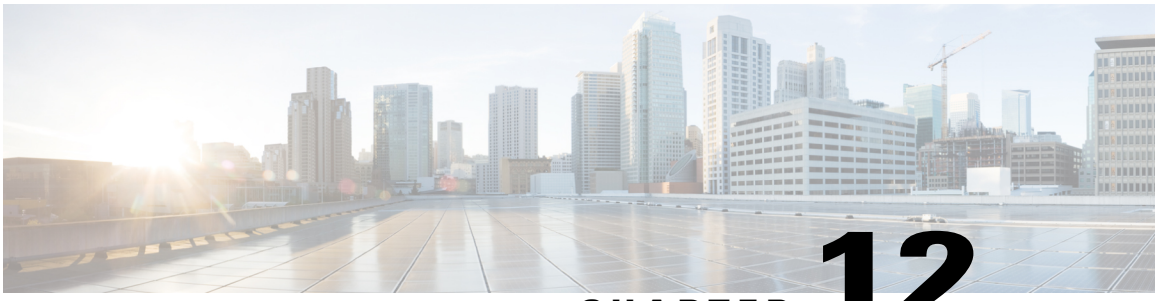
Verifying the System Message Logging Configuration

Use one of the following commands to verify the configuration:

Command	Purpose
show logging console	Displays the console logging configuration.
show logging info	Displays the logging configuration.
show logging last *number-lines*	Displays the last number of lines of the log file.
show logging level [*facility*]	show logging level [facility]
show logging module	Displays the module logging configuration.
show logging monitor	Displays the monitor logging configuration.
show logging server	Displays the syslog server configuration.
show logging session	Displays the logging session status.
show logging status	Displays the logging status.
show logging timestamp	Displays the logging time-stamp units configuration.

Feature History for System Message Logging

Feature Name	Releases	Feature Information
System Message Logging	Release 5.2(1)IC1(1.1)	This feature was introduced.



CHAPTER 12

Configuring VSM Backup and Recovery

This chapter contains the following sections:

Information About VSM Backup and Recovery

You can use the VSM backup and recovery procedure to create a template from which the VSMs can be re-created in the event that both VSMs fail in a high availability (HA) environment.

Note We recommend that you do periodic backups after the initial backup to ensure that you have the most current configuration. See the Performing a Periodic Backup section for more information.

Guidelines and Limitations

VSM backup and recovery has the following configuration guidelines and limitations:

- Backing up the VSM is a onetime task.
- Backing up the VSM requires coordination between the network administrator and the server administrator.
- These procedures are not for upgrades and downgrades.
- These procedures require that the restoration is done on the VSM with the same release as the one from which the backup was made.
- Configuration files do not have enough information to re-create a VSM.

Configuring VSM Backup and Recovery

This section includes the following topics:

- Performing a Backup of the VSM
- Performing a Periodic Backup
- Recovering the VSM

Note Be aware that Cisco NX-OS commands might differ from the Cisco IOS commands.

Backing Up the VSM

This section includes the following topics:

- Performing a Backup of the VSM
- Performing a Periodic Backup

Performing a Backup of the VSM

This section describes how to create a backup of the VSM.

-

Before You Begin

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

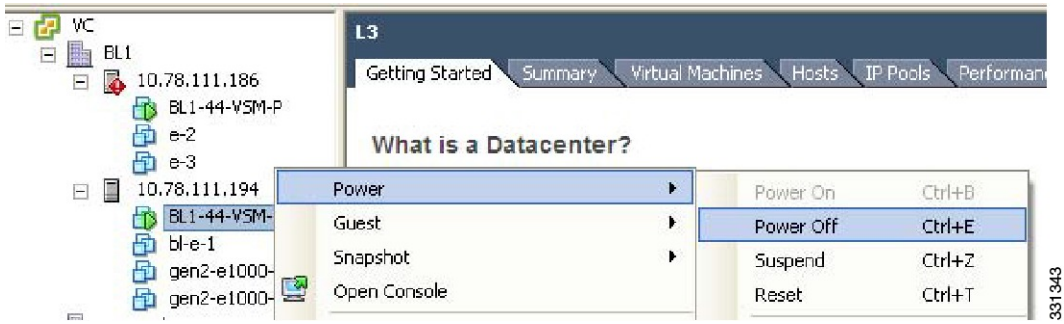
- If the VSM is on a Virtual Ethernet Module (VEM) host, you must configure the management VLAN as a system VLAN.
- Enter the **copy running-config startup-config** command at the VSM before beginning this procedure.

Procedure

Step 1 Open the vSphere Client.

The vSphere Client window opens as displayed in the following illustration.

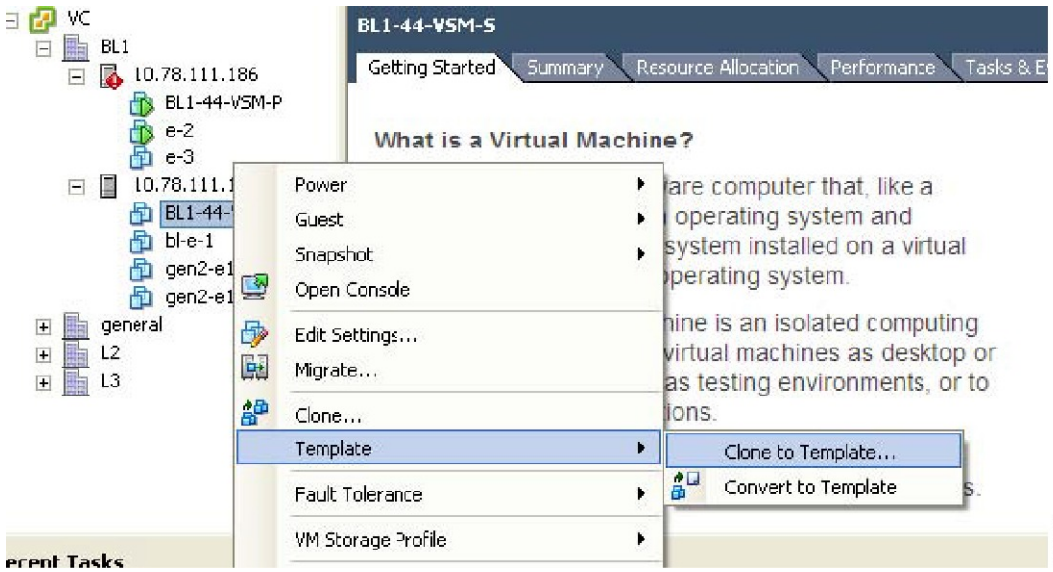
Figure 6: vSphere Client Window



Step 2 In the left navigation pane, right-click the standby VSM. A drop-down list is displayed.

Step 3 Choose **Power > Power Off**.
The action is displayed in the Clone to Template Window.

Figure 7: Clone to Template Window

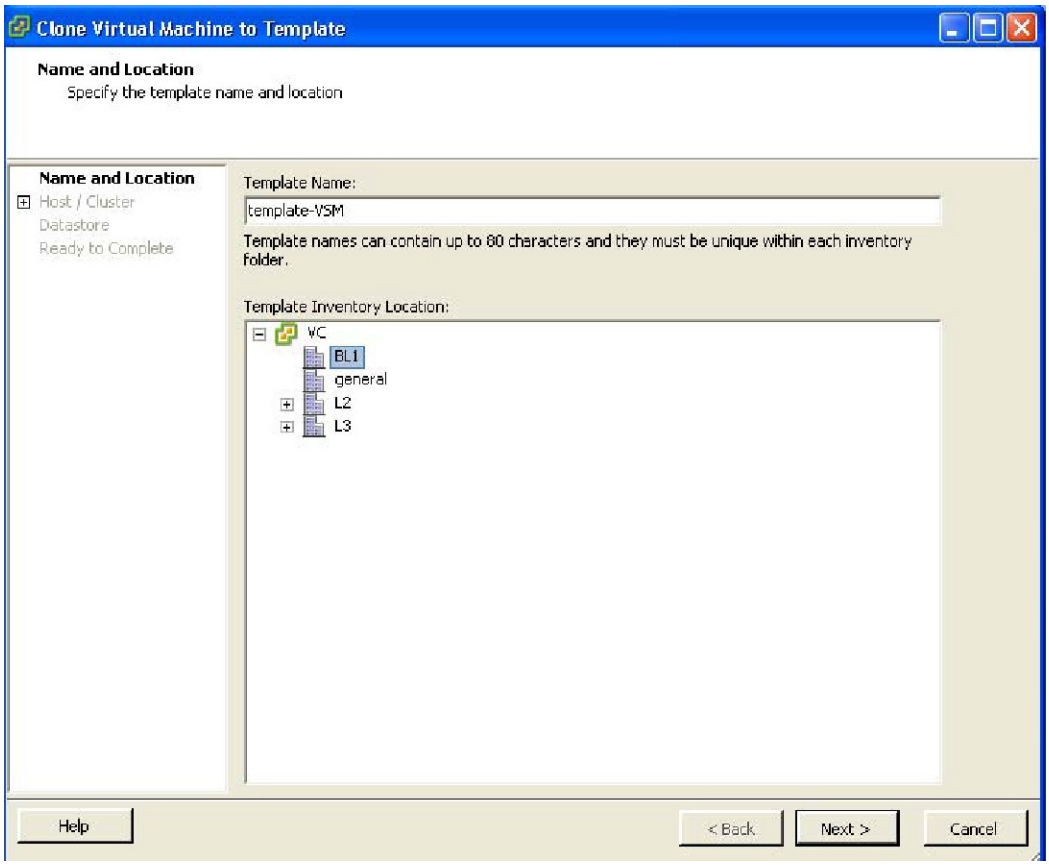


Step 4 In the left navigation pane, right-click the standby VSM.
A drop-down list is displayed.

Step 5 Choose **Template > Clone to Template**.

The Clone Virtual Machine to Template window opens.

Figure 8: Clone Virtual Machine to Template Window



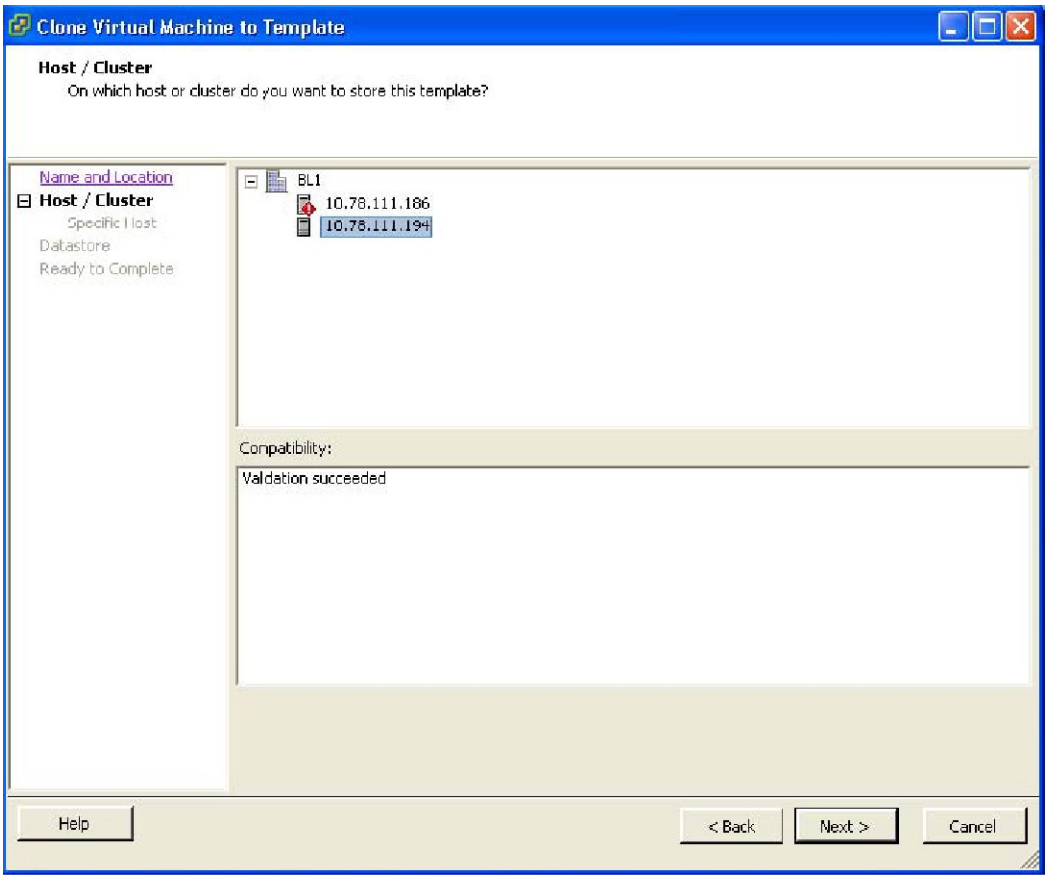
Step 6 In the Template Name field, enter a name.

Step 7 In the Template Inventory Location pane, choose a location for the template.

Step 8 Click Next.

The Choosing the Host Window opens.

Figure 9: Host Window

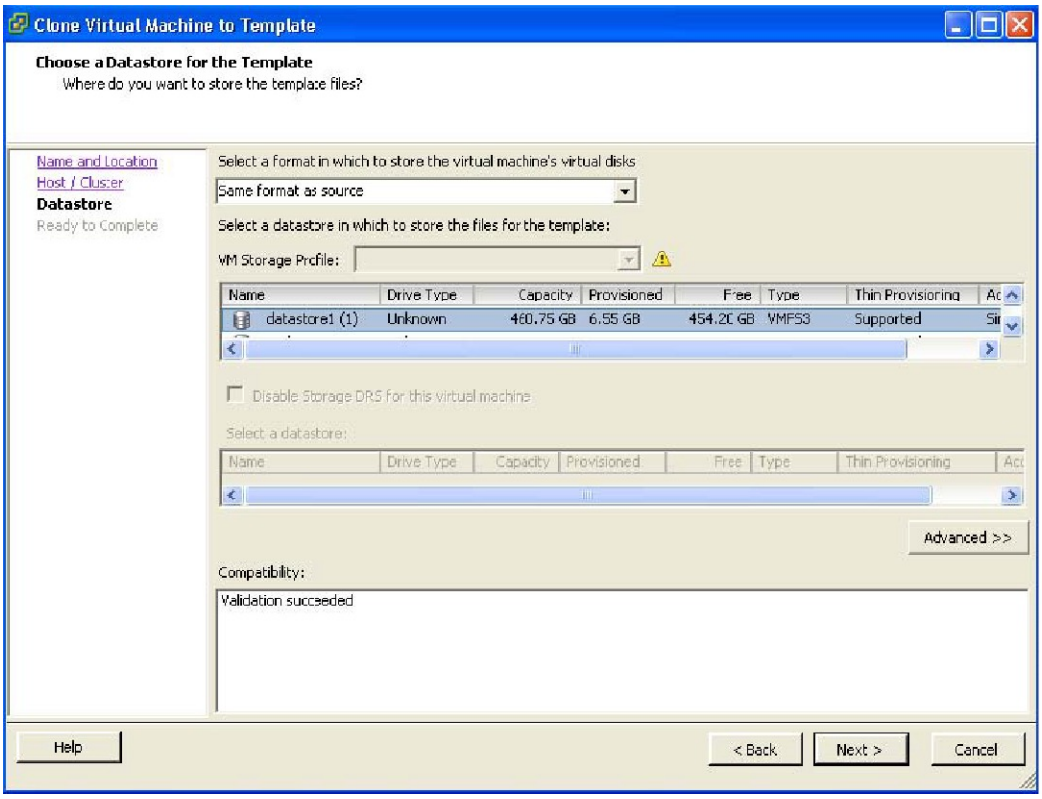


Step 9 Choose the host on which the template will be stored.

Step 10 Click Next.

The Choosing a Datastore window opens.

Figure 10: Choosing a Datastore Window



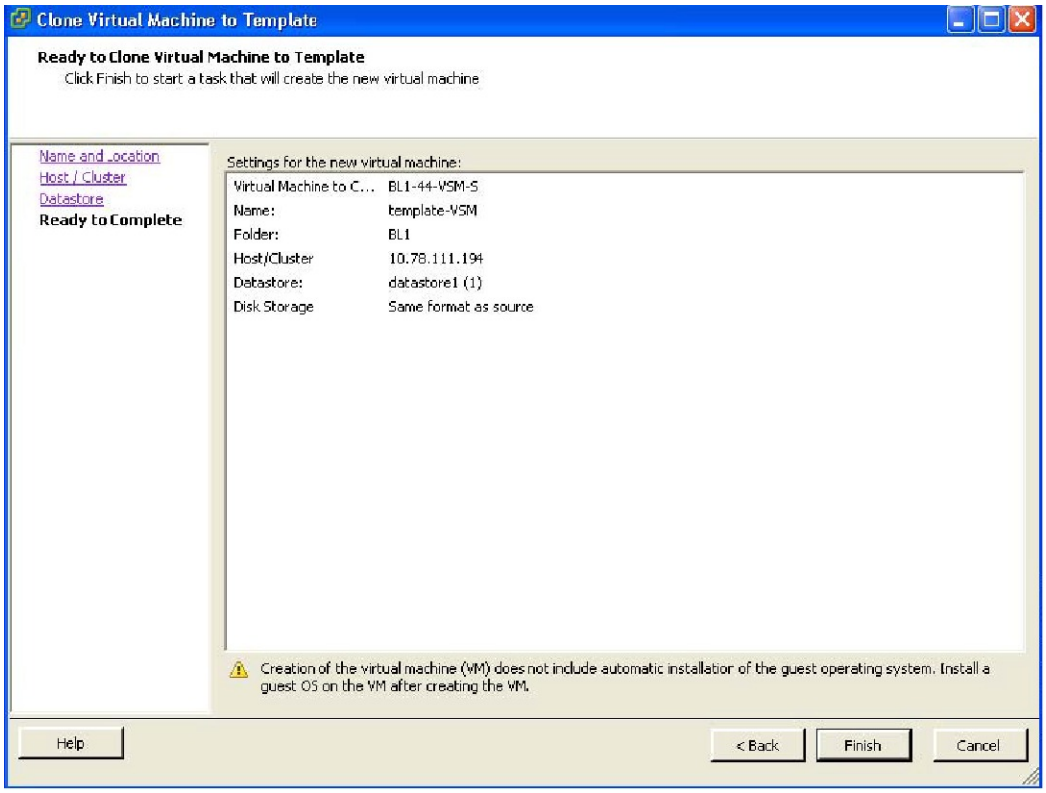
Step 11 In the Select a format in which to store the virtual machine's virtual disks drop-down list, choose Same format as source.

Step 12 Choose a datastore.

Step 13 Click Next.

The Confirming the Settings window opens.

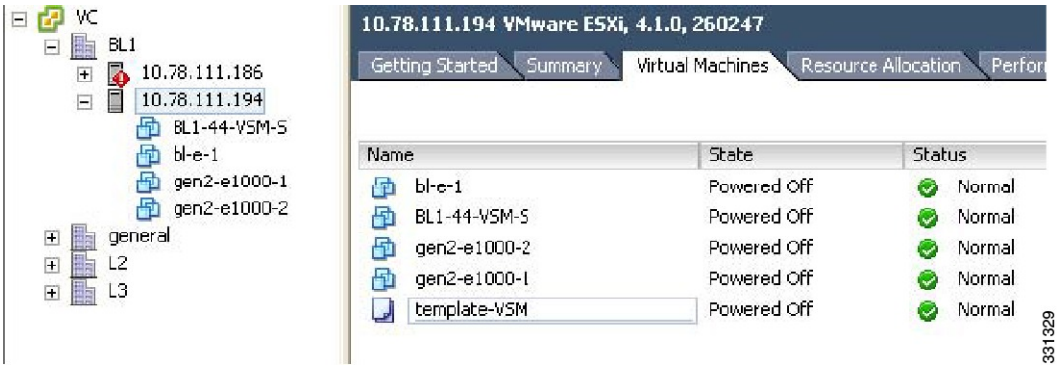
Figure 11: Confirming the Settings Window



Step 14 Confirm the settings for the new virtual machine and click Finish.
The backup template is created and appears under the Virtual Machines tab.

Step 15 The Template Virtual Machine window opens.
The template creation is complete.

Figure 12: Template Virtual Machine Window



Performing a Periodic Backup

This section describes how to back up the active VSM after the initial backup of the standby VSM has been performed.

Before You Begin

The following lists some instances when you should run this procedure:

- You have performed an upgrade.
- You have made a significant change to the configuration.

Procedure

Enter the command **copy running-config scp://root@10.78.19.15/tftpboot/config/** to back up the VSM.

Example:

```
switch# copy running-config scp://root@10.78.19.15/tftpboot/config/
Enter destination filename: [switch-running-config]
Enter vrf (If no input, current vrf 'default' is considered):
The authenticity of host '10.78.19.15 (10.78.19.15)' can't be established.
RSA key fingerprint is 29:bc:4c:26:e3:6f:53:91:d4:b9:fe:d8:68:4a:b4:a3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.78.19.15' (RSA) to the list of known hosts.
root@10.78.19.15's password:
switch-running-config 100% 6090 6.0KB/s 00:00
switch#
```

Recovering the VSM

This section describes how to deploy a VSM by using the backup template. This section includes the following topics:

- Deploying the Backup VSM VM
- Erasing the Old Configuration
- Restoring the Backup Configuration on the VSM

Deploying the Backup VSM VM

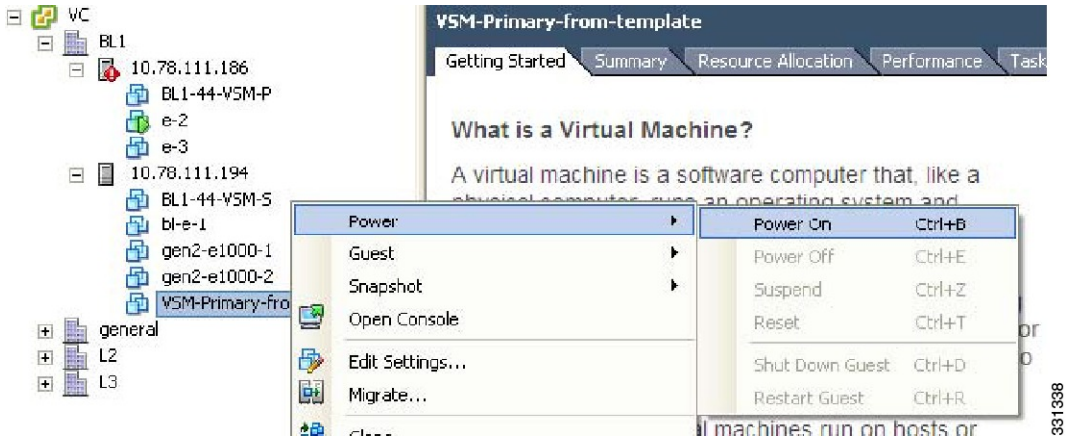
This section describes how to deploy the backup VSM VM when the primary and secondary VSMs are not present.

Note While deploying the VSM VM, do not power it on.

Procedure

Step 1 Open the vSphere Client.
The vSphere Client window opens as displayed in the following illustration.

Figure 13: vSphere Client Window



Step 2 In the left navigation pane, choose the host of the standby VSM.

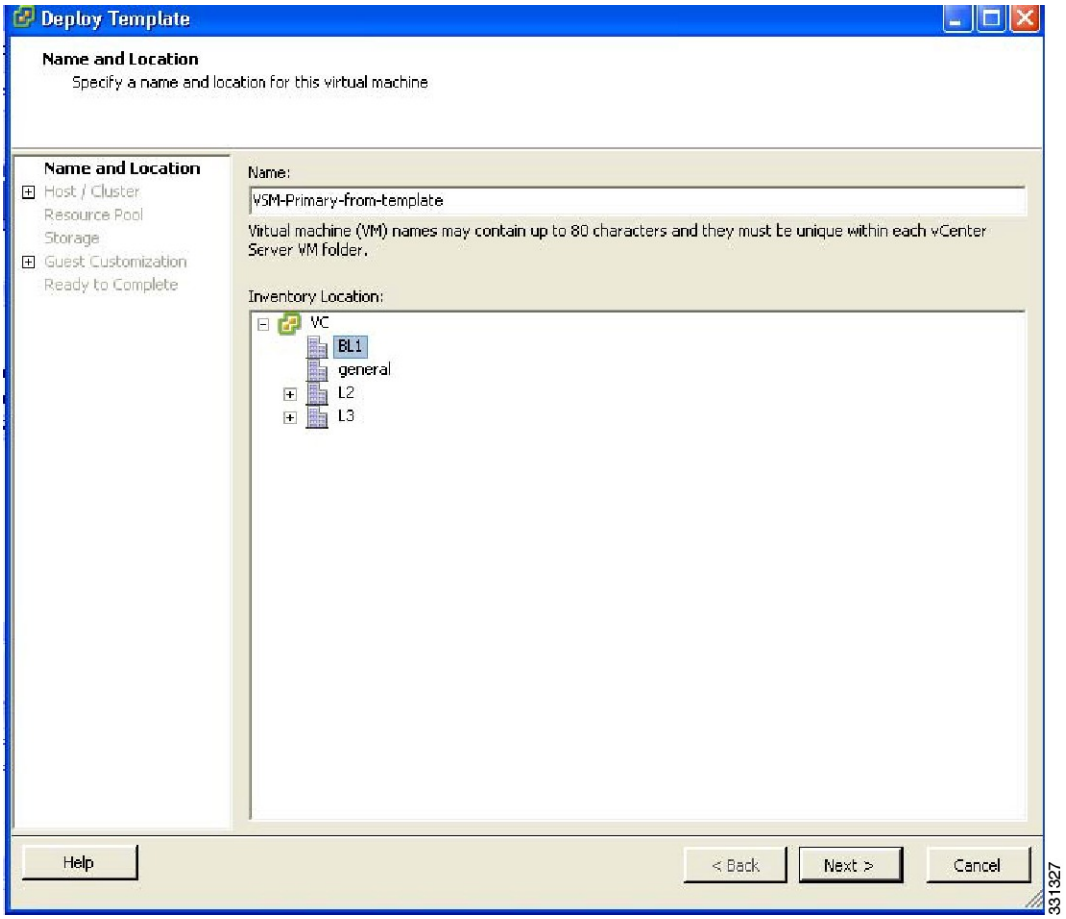
Step 3 Click the Virtual Machines tab.

Step 4 Right-click the template_VSM.

Step 5 Choose Deploy Virtual Machine from this Template.

The Deploy Template Wizard window opens.

Figure 14: Deploy Template Wizard Window



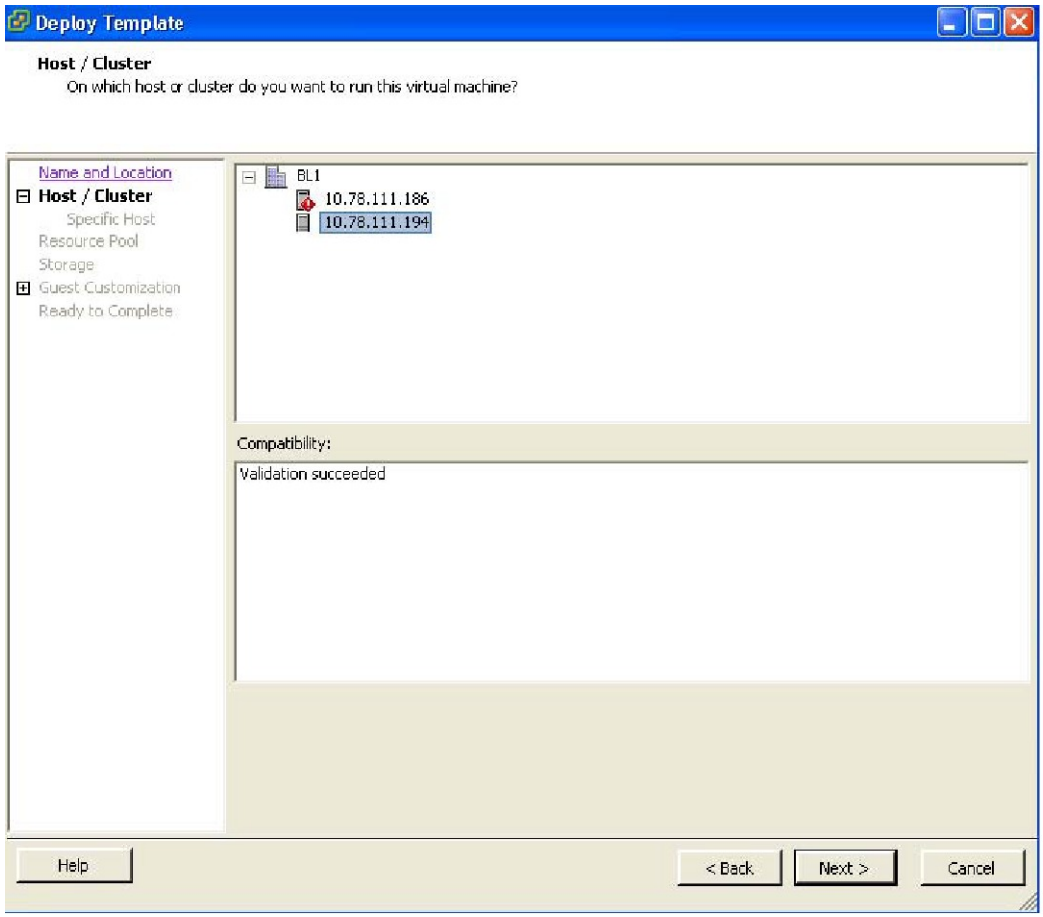
Step 6 In the Name field, enter a name for the VSM.

Step 7 In the Inventory Location pane, choose a cluster.

Step 8 Click Next.

The Choosing a Host Window opens.

Figure 15: Choosing a Host Window



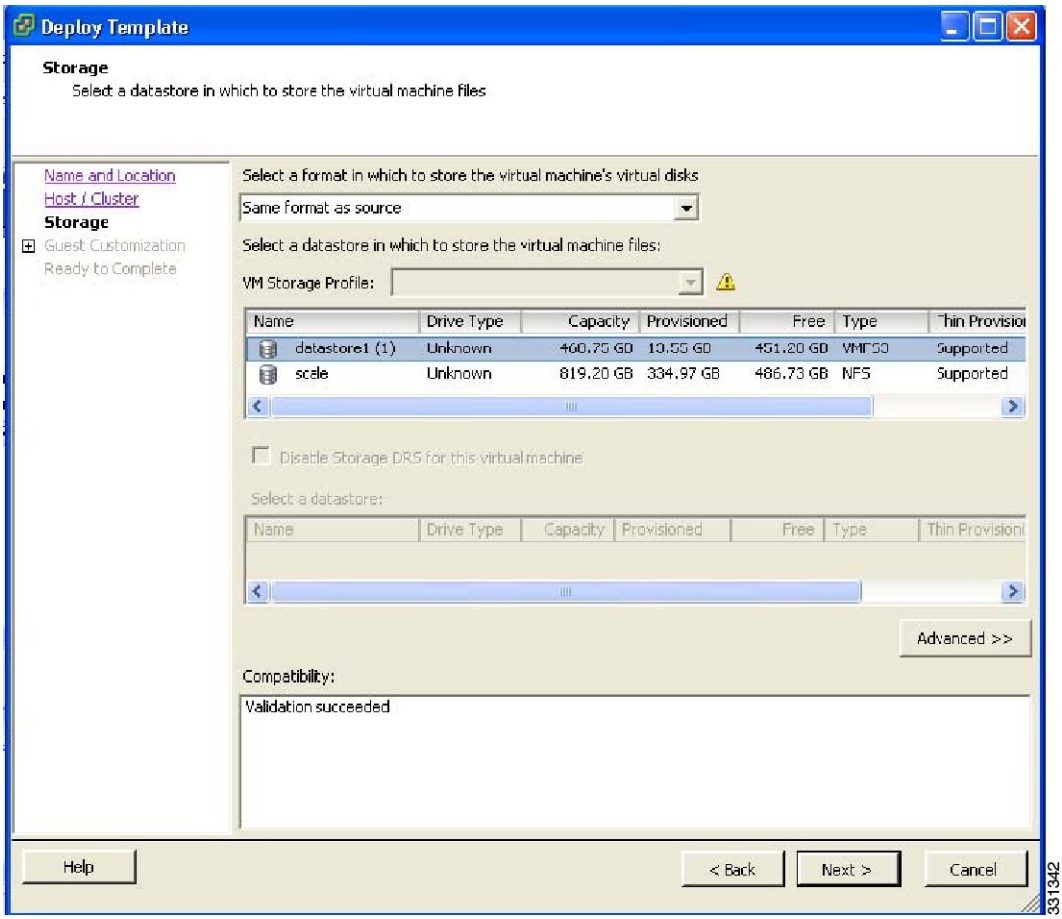
Step 9 Choose a host.

Step 10

Example:
Click Next.

The Choosing a Datastore window opens.

Figure 16: Choosing a Datastore Window



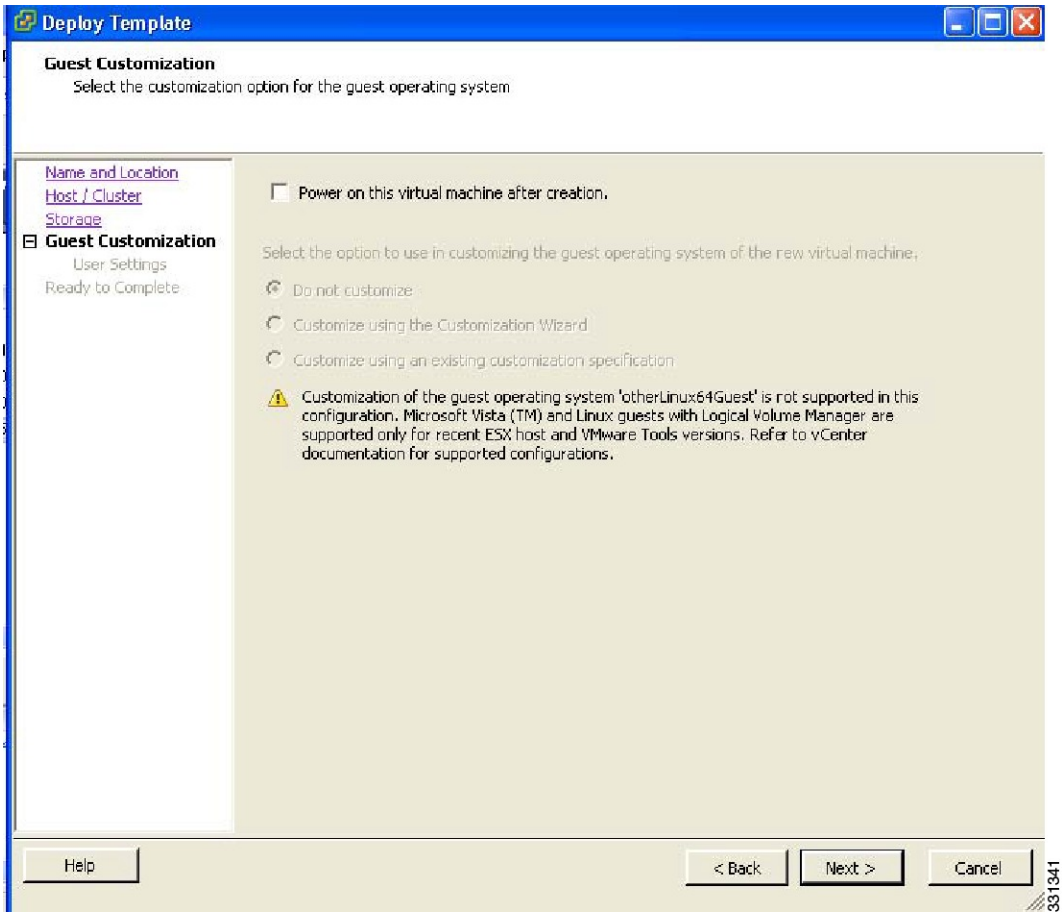
Step 11 In the Select a format in which to store the virtual machine's virtual disks drop-down list, choose Same format as source.

Step 12 Choose a datastore

Step 13 Click Next.

The Guest Customization window opens. Make sure that the Power on this virtual machine after creation check box is not checked.

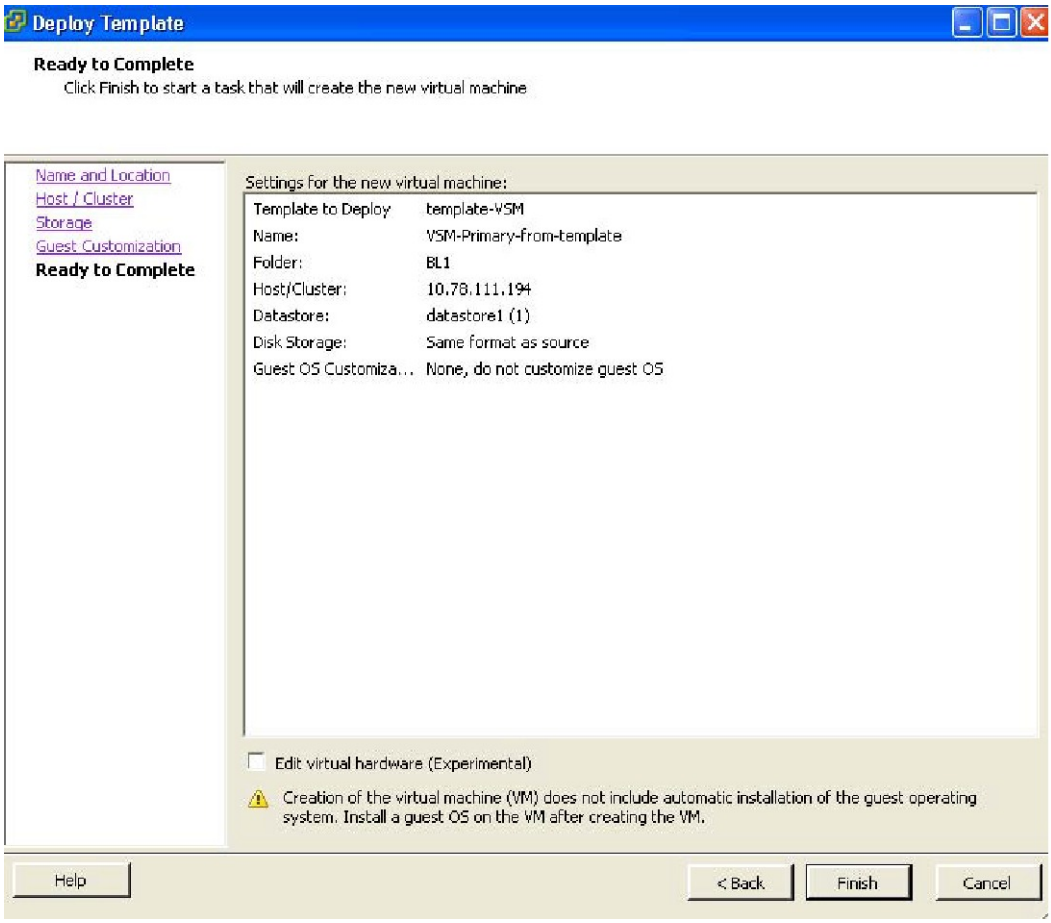
Figure 17: Guest Customization Window



Step 14 Click Next.

The Deploy Template - Ready to Complete window opens.

Figure 18: Guest Customization Window



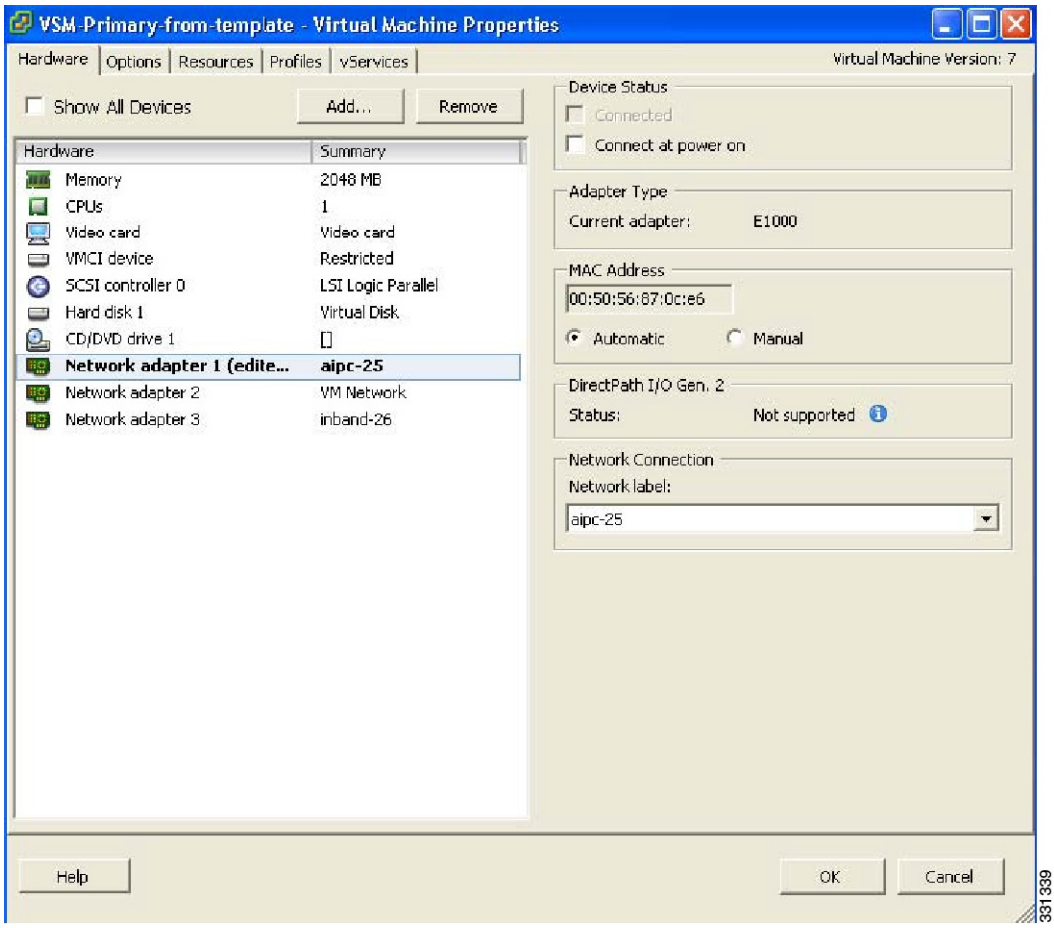
Step 15 Confirm the settings for the new virtual machine and click Finish. If the management VLAN is not available on the VEM, you must add the management interface to the vSwitch.

Step 16 Right-click the newly deployed VM.

Step 17 Choose Edit Settings.

The Virtual Machine Properties window opens.

Figure 19: Guest Customization Window



Step 18 In the Hardware / Summary pane, choose Network adapter 1.

Step 19 Uncheck the Connect at power on check box.

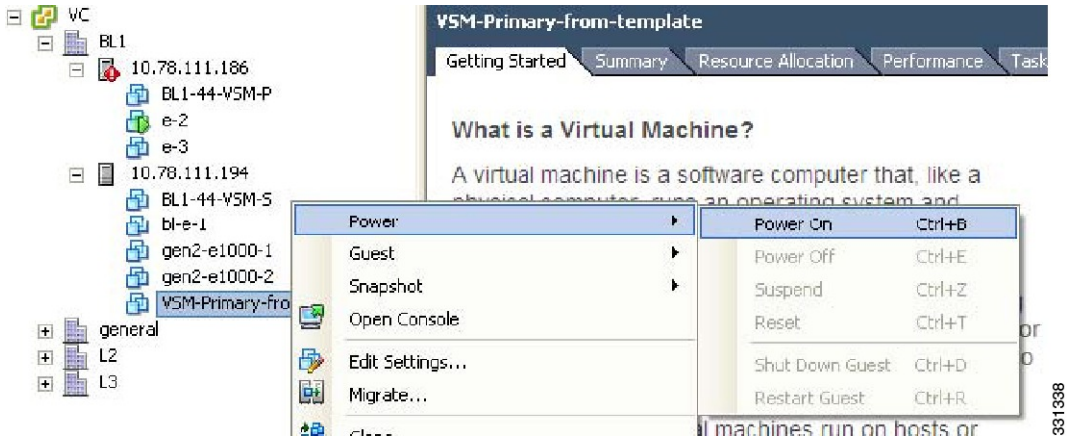
Step 20 Choose Network adapter 2.

Step 21 In the Device Status area, uncheck the Connect at power on check box.

Step 22 Click OK.

The Power On window opens.

Figure 20: Guest Customization Window



Step 23 Right-click the newly deployed VSM.
A drop-down list appears.

Step 24 Choose Power > Power On.
Deploying the backup VSM VM is complete.

Erasing the Old Configuration

This section describes how to erase the startup configuration of the newly deployed VSM.

Procedure

Step 1 Launch the virtual machine console of the newly deployed VSM.

Step 2 Set the redundancy role to primary by entering the following command:

Step 3 Copy the running configuration to the startup configuration by entering the following command:

Step 4 Erase the startup configuration by entering the following command:

Step 5 Reboot the primary and secondary VSMs by entering the following command:

This example describes how to erase the startup configuration of the newly deployed VSM

```
switch# system redundancy role primary
Setting will be activated on next reload
switch# copy running-config startup-config
scp:        sftp:           startup-config
[####################################] 100%
switch# write erase
Warning: The command will erase the startup-configurations.
Do you wish to proceed anyway? (y/n) [n] y
switch# reload
This command will reboot the system. (y/n)? [n] y
```

```
switch# reload
This command will reboot the system. (y/n)? [n] y
```

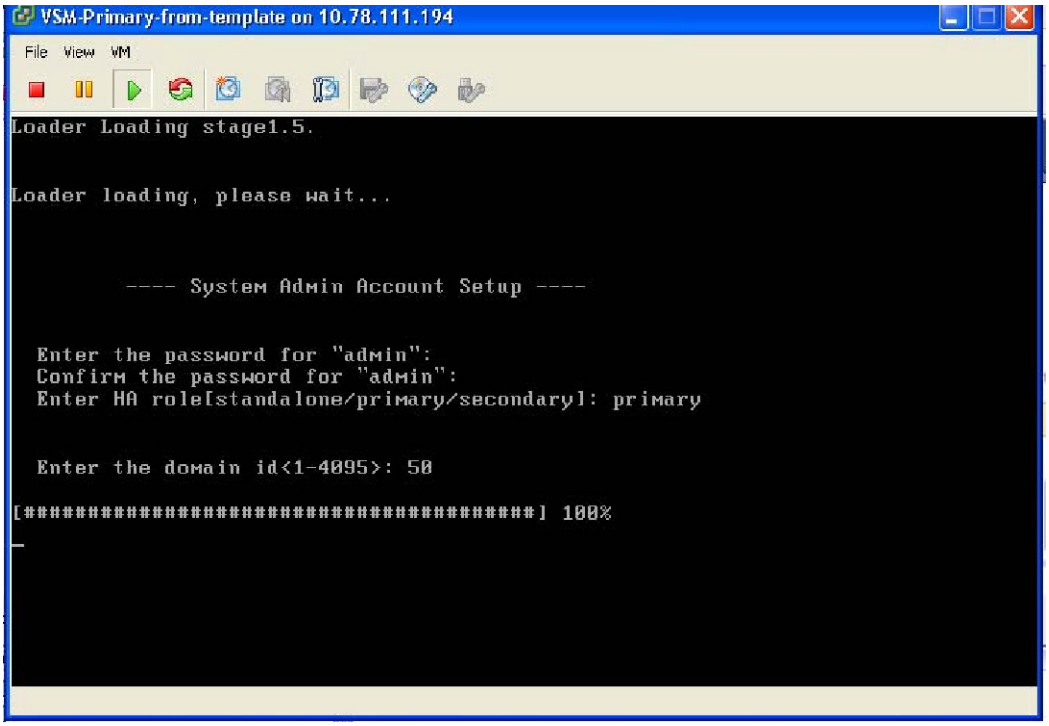
Restoring the Backup Configuration on the VSM

This section describes how to restore the backup configuration on the VSM.

Procedure

Step 1 When the VSM reboots, the System Admin Account Setup window opens.

Figure 21: System Admin Account Setup Window



Step 2 Enter and confirm the Administrator password.

Example:

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

Step 3 Enter the domain ID.

Example:

```
Enter the domain id<1-4095>: 50
```

Step 4 Enter the HA role. If you do not specify a role, standalone is assigned by default.

Example:
```
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.

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

Step 5 Enter yes when you are prompted to enter the basic configuration dialog.

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

Step 6 Enter no when asked to create another Login account.

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

Step 7 Enter no when asked to configure a read-only SNMP community string.

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

Step 8 Enter no when asked to configure a read-write SNMP community string.

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

Step 9 Enter a name for the switch.

Example:
```
Enter the switch name:
```

Step 10 Enter yes, when asked to configure out-of-band management 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 11 Enter no when asked to configure the default gateway.

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

    IPv4 address of the default gateway : 172.23.233.1
```

Step 12 Enter yes when asked to enable the Telnet service.

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

Step 13 Enter yes when asked to enable the SSH service, and then enter the key type and number of key bits. For more information, see the *Cisco Nexus 1000V InterCloud Security Configuration Guide*.

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 14 Enter yes when asked to enable the HTTP server.

Example:
```
Enable the http-server? (yes/no) yes
```

Step 15 Enter no when asked to configure the NTP server

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

Step 16 Enter no when asked to configure the VEM feature level.

Example:
```
Vem feature level will be set to 4.2(1)SV1(4a).
Do you want to reconfigure? (yes/no) [n] no
```
The system now summarizes the complete configuration and prompts you to edit it.

Example:
```
The following configuration will be applied:
 interface Mgmt0
ip address 172.28.15.152 255.255.255.0
no shutdown
vrf context management
ip route 0.0.0.0/0 10.78.111.11
  no telnet server enable
  ssh key rsa 1024 force
  ssh server enable
  feature http-server
  svs-domain
    svs mode L2
    control vlan 1
    packet vlan 1
    domain id 1
```

Step 17 Enter no when asked if you would like to edit the configuration.

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

Enter SVS Control mode (L2 / L3) : L2
Enter control vlan <1-3967, 4048-4093> : 100
Enter packet vlan <1-3967, 4048-4093> : 101
```

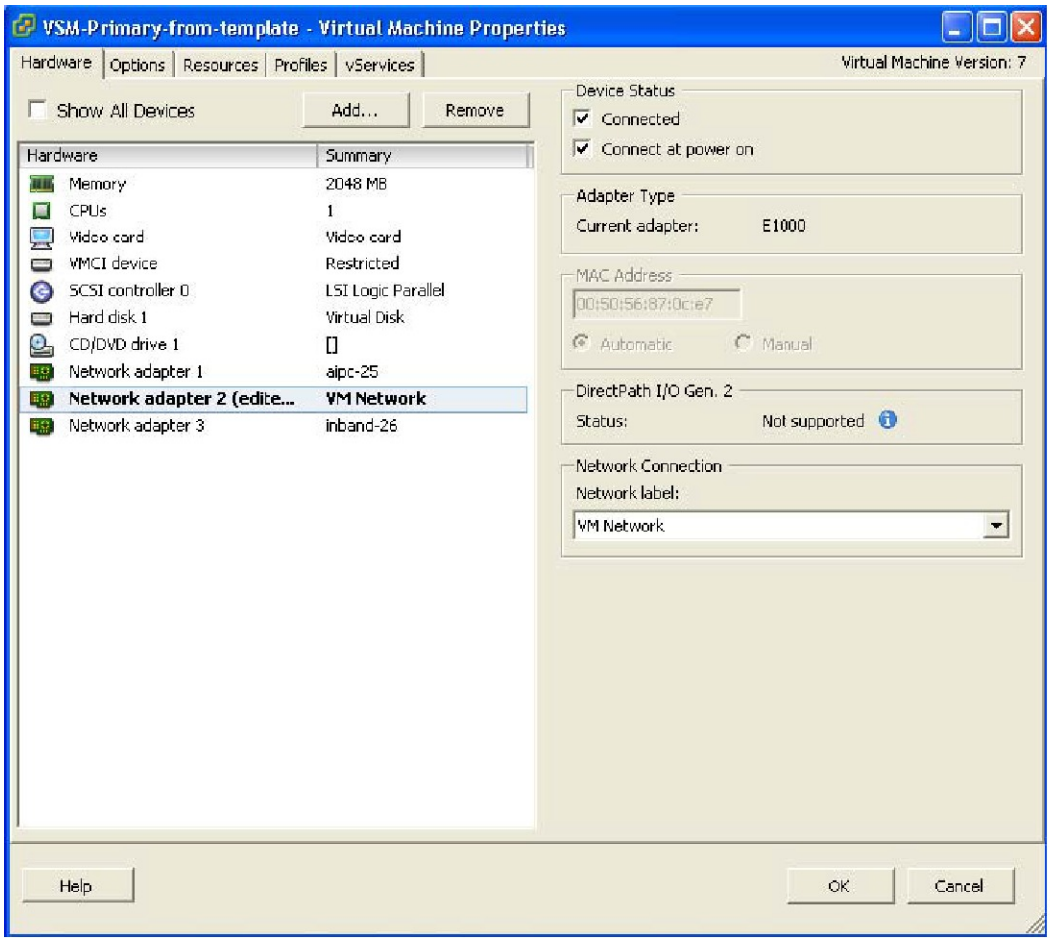
Step 18 Enter yes when asked to use and save this configuration.

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

Step 19 In the vSphere Client, right-click the VSM and choose Edit Settings.

The VSM Virtual Machine Properties window opens.

Figure 22: VSM Virtual Machine Properties Window



Step 20 In the Hardware/Summary pane, choose Network adapter 2.

Step 21 Check the Connect at power on check box.

Step 22 Log in to the VSM.

Step 23 Copy the backup configuration to the VSM bootflash by entering the following command:

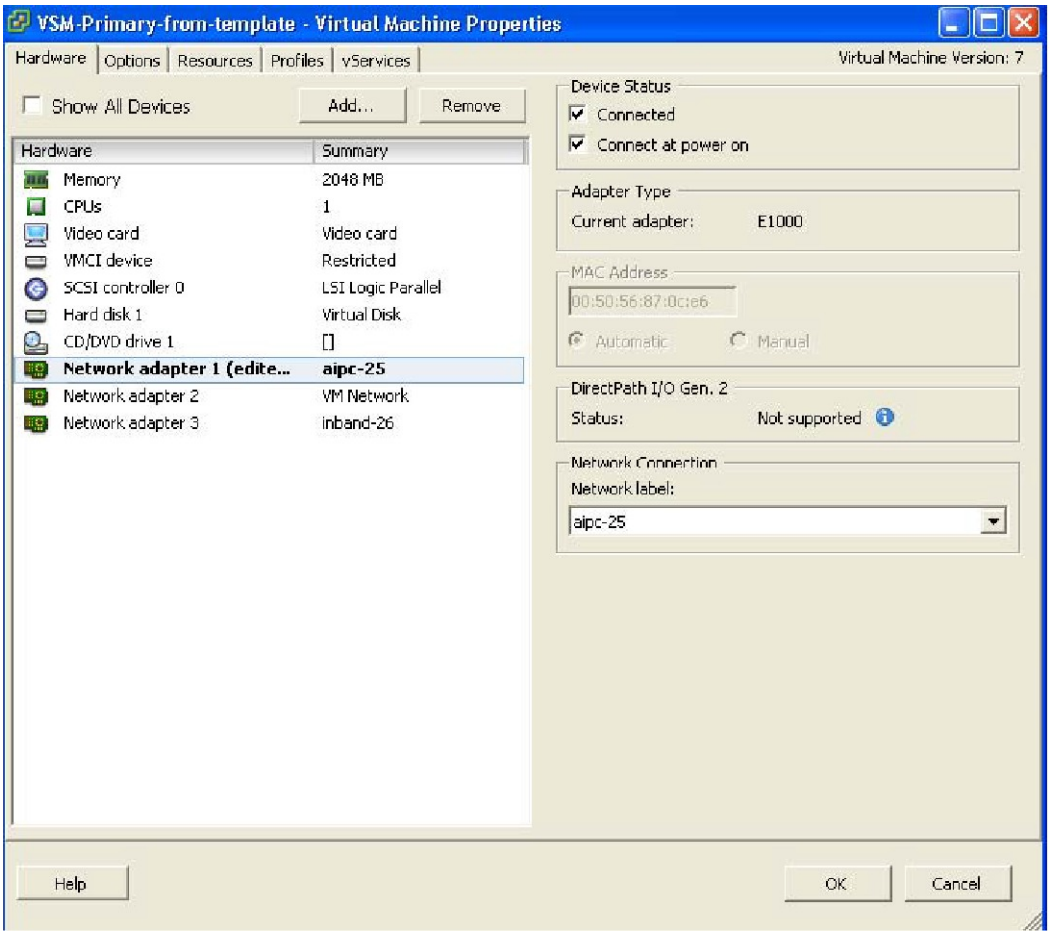
Example:

```
switch# copy scp://root@10.78.19.15/tftpboot/backup/VSM-Backup-running-config
bootflash:
Enter vrf (If no input, current vrf 'default' is considered):
The authenticity of host '10.78.19.15 (10.78.19.15)' can't be established.
RSA key fingerprint is 29:bc:4c:26:e3:6f:53:91:d4:b9:fe:d8:68:4a:b4:a3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.78.19.15' (RSA) to the list of known hosts.
root@10.78.19.15's password:
switch-running-config 100%
```

```
6090 6.0KB/s 00:00
switch#
```

Step 24 The Virtual Machine Properties window displays.

Figure 23: Virtual Machine Properties Window



Step 25 In the Hardware / Summary pane, choose Network adapter 1.

Step 26 In the Device Status area, check the Connect at power on check box.

Step 27 Confirm that the VEMs are attached to the VSM by entering the command **show module**

Step 28 Copy the backup configuration to the running configuration by entering the command **copy bootflash:VSM-Backup-running-config running-config**
This step is necessary for features like ERSPAN/NFM.

Step 29 Register the Cisco Nexus 1000V InterCloud VSM with Cisco Prime Network Services Controller. On the Cisco Nexus 1000V InterCloud VSM CLI, enter the following commands:

```
switch# configure terminal
switch(config)#  nsc-policy-agent
switch(config-nsc-policy-agent)#   no policy-agent-image
switch(config-nsc-policy-agent)#  no shared-secret
switch(config-nsc-policy-agent)#   shared-secret Example_Secret123
```

```
switch(config)#  policy-agent-image bootflash:///vsmcpa.3.0.1c.bin
switch(config)# exit
```

Step 30 Copy the running-configuration to the startup-configuration by entering the following command:

Example:

```
switch# copy running-config startup-config
[########################################] 100%
switch#
```

Step 31 Confirm that the VEMs are attached to the VSM by entering the command **show module**

Step 32 Create the standby VSM by using the OVA/OVF files to form an HA pair.

Feature History for VSM Backup and Recovery

This section provides the VSM backup and Recovery feature release history.

Feature Name	Releases	Feature Information
VSM Backup and Recovery	Release 5.2(1)IC1(1.1)	This feature was introduced.