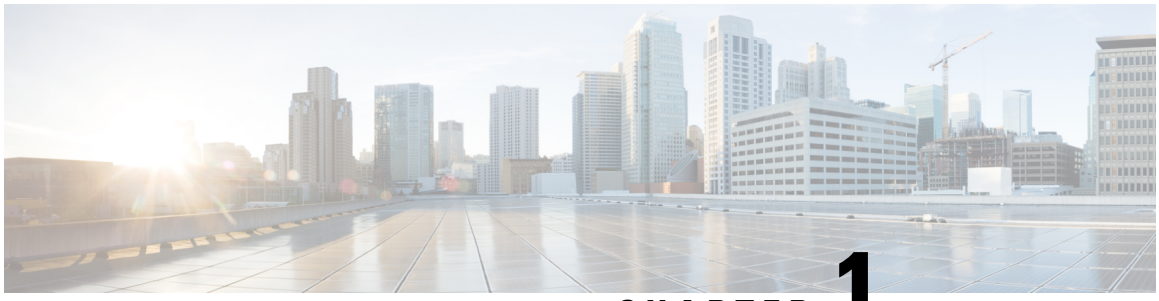
Cisco Nexus 1000VE for VMware vSphere System Management Configuration Guide, Release 5.2(1)SV5(1.1)

First Published: 2018-07-11

Last Modified: 2019-12-04

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

CONTENTS



CHAPTER 1

Overview

This chapter contains the following sections:

System Management Overview

This chapter describes the following system management features:

- Domains
- Server Connections
- Configuration Management
- File Management
- User Management
- NTP
- Local SPAN and ERSPAN
- SNMP System Messages
- System Messages
- Troubleshooting

Domains

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

You can establish Layer 3 Control in your VSM domain, which means 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 VMware vCenter Server, you must first define the connection in the Cisco Nexus 1000VE.

Configuration Management

The Cisco Nexus 1000VE enables you 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 who are 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.

Local SPAN and ERSPAN

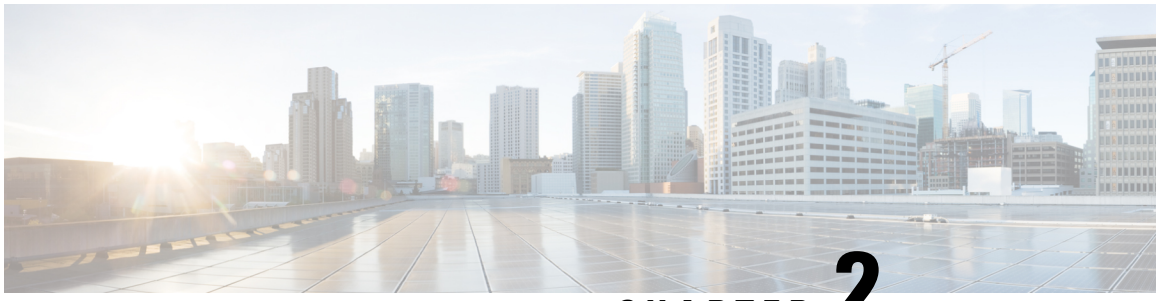
The Ethernet switched port analyzer (SPAN) enables you to monitor traffic in and out of your device and duplicate packets from source ports to destination ports. For information about configuring SPAN, see Configuring a Local SPAN Session, on page 74. You can also use the Cisco Network Analysis Module (NAM) to monitor ERSPAN data sources for application performance, traffic analysis, and packet header analysis.

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 that you can use to use to monitor and manage 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.



CHAPTER 2

Configuring the Domain

This chapter contains the following sections:

Information About Domains

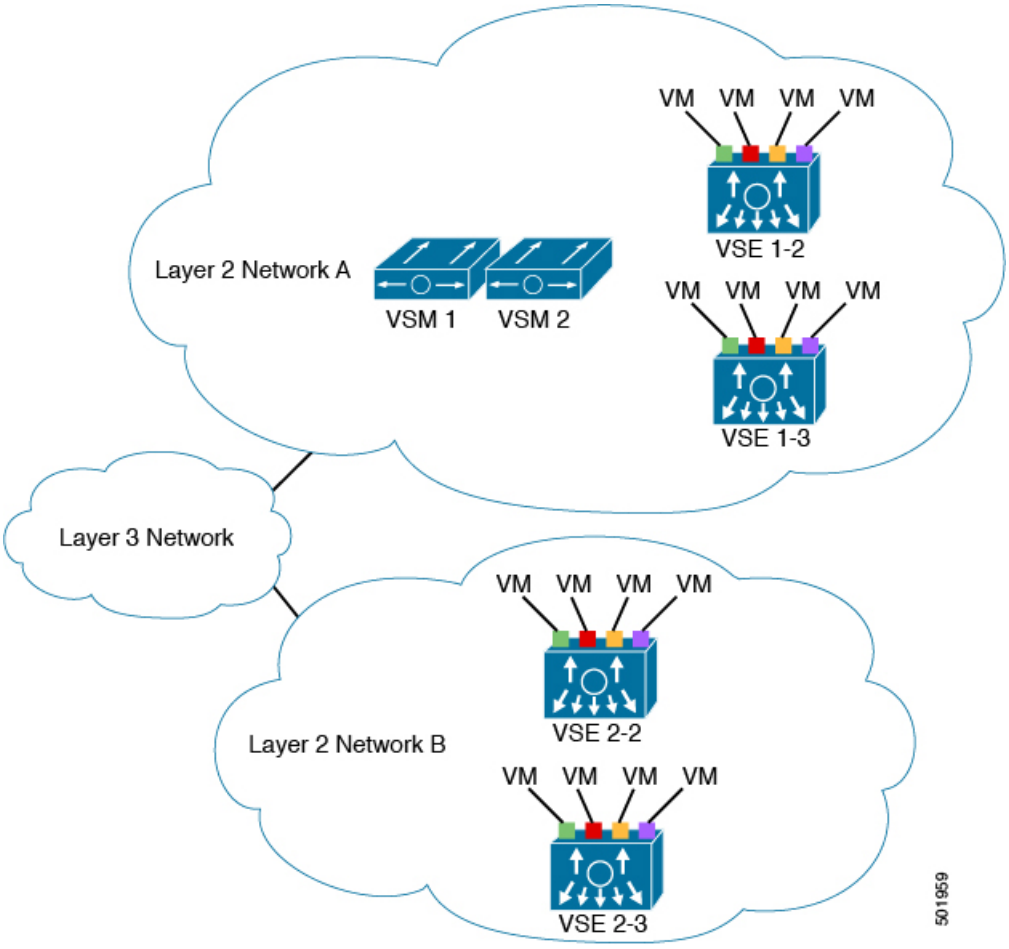
You must create a domain for the Cisco Nexus 1000VE. This process is part of the initial setup of the Cisco Nexus 1000VE when you install the software. If you need to create a domain later, you can do so by using the **svs-domain** command or the procedures described in this chapter.

Layer 3 Control

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

Figure 1: Example of Layer 3 Control IP Connectivity

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



Guidelines and Limitations

Follow these usage guidelines and limitations while configuring the domain:

Default Settings

Parameter	Default
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

Parameter	Default
State (VLAN)	Active
Shut state (VLAN)	No shutdown

Creating a Domain

You can create a domain for the Cisco Nexus 1000VE that identifies the VSM and VSEs. This process is part of the initial setup of the Cisco Nexus 1000VE when you install the software. If you need to create a domain after the initial setup, you can do so by using this procedure.

Note We recommend you to use a distinct VLAN for each instance of the Cisco Nexus 1000VE (different domains).

Before you begin

Log 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 VSEs managed by each VSM.
- A unique domain ID for this Cisco Nexus 1000VE instance.
- The **svs mode** command in the SVS domain configuration mode is not used and has no effect on a configuration.

Procedure

Step 1 switch# **configure terminal**

Enters global configuration mode.

Step 2 switch(config)# **svs-domain**

Enters SVS domain configuration mode.

Step 3 switch(config-svs-domain)# **domain id** *number*

Creates the domain ID for this Cisco Nexus 1000VE instance.

Step 4 switch(config-svs-domain)# **svs mode L3 interface mgmt0** | **control0**

Configures Layer 3 transport mode for the VSM domain.

If configuring Layer 3 transport, you must designate which interface to use. The interface must already have an IP address configured.

Note Layer 2 configuration mode is not supported.

Step 5 switch(config-svs-domain)# **[no] control type multicast**

Configures the control type multicast in Layer 3 mode on the VSM.

Step 6 (Optional) switch(config--svs-domain)# **show svs domain**

Displays the domain configuration.

Step 7 (Optional) switch(config)# **copy running-config startup-config**

Copies the running configuration to the startup configuration.

Example

This example shows how to create a domain:

```
switch# configure terminal
switch(config)# svs-domain
switch(config-svs-domain)# domain id 100
switch(config-svs-domain)# svs mode l3 interface mgmt0
switch(config-svs-domain)# show svs domain
SVS domain config:
  Domain id:    100
  Control vlan: NA
  Packet vlan:  NA
  L2/L3 Control mode: L3
  L3 control interface: mgmt0
  Status: Config push to VC successful
  Control type multicast: No
  L3Sec Status: Enabled
switch(config-svs-domain)# control type multicast
switch(config)# show svs domain
SVS domain config:
  Domain id:    100
  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
  L3Sec Status: Enabled
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

Managing Domain ID or Management IP Address

We recommend that you do not change the management IP address and the domain ID after the SVS connection is established. During an inevitable instance, if you have to change the management IP address or the domain ID, use this procedure to change it.

Before you begin

Log in to the CLI in EXEC mode.

Procedure

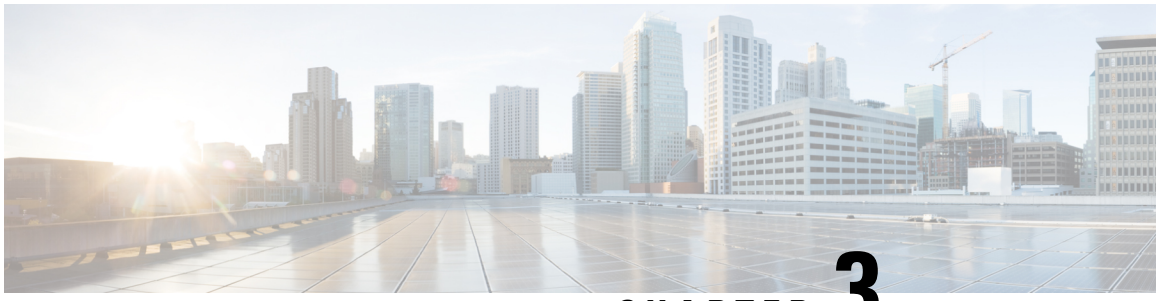
Step 1 Change the management IP address or the domain ID in the VSM. For more information, you can see the example in the Creating a Domain section. One changed, the VSE modules are in an offline state.

Step 2 SSH to the VSE with the administrator credentials and open the configuration file named `/etc/n1kv/n1kv.conf`.

Step 3 To change the domain ID, enter the correct value of the domain ID in the **switch-domain** field.

Step 4 To change the management IP address, enter the new management IP address in the **l3control-ipaddr** field.

Step 5 Restart the Cisco Nexus 1000v services using the **service nexus1000v restart** command and verify that the module is online in the VSM.



CHAPTER 3

Managing Server Connections

This chapter contains the following sections:

Information About Server Connections

- A connection name
- The protocol used
- The server IP address
- The server DNS name
- Transport mode: IPv4
- All communication with vCenter Server is secured by the Transport Layer Security (TLS) protocol.

Guidelines and Limitations

Follow these guidelines and limitations while configuring server connections:

- A single Virtual Supervisor Module (VSM) can only connect to one vCenter Server at a time.

- A single VSM cannot connect to multiple vCenter Server at once.
- When the SVS connection is in connected state, you can not reconfigure the IP address of the vCenter Server. To the change the IP address, you need to disconnect the SVS connection and change the IP address.

Connecting to the vCenter Server

Before you begin

- Log in to the CLI in EXEC mode.
- You must know the following:
  - The datacenter name.
  - The vCenter Server IP address (IPv4) 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 1000VE appliance is installed.
  - The management port is configured.
  - The DNS is already configured if you are configuring a connection using a hostname.

Procedure

Step 1 switch# **configure terminal**

Enters global configuration mode.

Step 2 switch(config)# **svs connection** *name*

Enters connection configuration mode for adding this connection between the Cisco Nexus 1000VE and a 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**

Use this command to specify that this connection uses the VIM protocol.

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* [vrf {*vrf-name* | `default|management`}

Specifies the IP address of the ESX server or vCenter Server for this connection. This command is stored locally. *vrf-name* is case sensitive and can be a maximum of 32 characters. If a VRF option is not specified, the management VRF is taken by default.

Go to Step 8 to configure the datacenter name.

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)# **remote port** *port number*

Specifies the HTTP port number of vCenter for this connection. The default port number is 80. Though the communication is HTTPS, vCenter receives the packets on its HTTP port.

Step 8 switch(config-svs-conn)# **vmware dvs datacenter-name** [*folder/*] *name*

Identifies the datacenter name in the vCenter Server where the Cisco Nexus 1000VE is to be created as a distributed virtual switch (DVS). The datacenter name is stored locally.

Note The Cisco Nexus 1000VE folder name must be the same in the vCenter Server and in the VSM. If the Cisco Nexus 1000VE folder is renamed in the vCenter Server, you must manually rename the folder name in the VSM. The names are not automatically synchronized, and if they are not the same, the DVS connection between the VSM and vCenter Server is broken.

Step 9 Do one of the following:

- To use login and password to connect to the vCenter, go to Step 10.
- To register VSM's extension key to connect to the vCenter, go to Step 11

Step 10 switch(config-svs-conn)# **remote username** *user_name* **password** *pwd*

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 11 switch(config-svs-conn)# **register-plugin remote username** *user_name* **password** *pwd*

CLI to register the VSM's extension key with the VMware vCenter.

Step 12 switch(config-svs-conn)# **connect**

Initiates the connection. If the username and password is not configured or the plugin is not registered, then connect will fail indicating the same.

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.

Note The **connect** command may return the following message, `SVS connection service is busy. Please try again later`.

Example

This example shows how to connect to the vCenter server using IPv4 address:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)#
switch(config)# svs connection vc
switch(config-svs-conn)#
switch(config-svs-conn)# protocol vmware-vim
switch(config-svs-conn)# remote ip address 110.23.43.170
switch(config-svs-conn)# vmware dvs datacenter-name dataCTR

switch(config-svs-conn)# remote username administrator password pwd
switch(config-svs-conn)#
switch(config-svs-conn)# connect



switch#
```

Validating vCenter Server Certificates

The VSM can validate the certificate presented by vCenter Server to authenticate it. The certificate may be self-signed or signed by a Certificate Authority (CA). The validation is done every time the VSM connects to the vCenter Server. If the certificate authentication fails, a warning is generated but the connection is not impaired.

Installing Certificates

Before you begin

Check if a vCenter Server certificate can be received:

1. Enter the following command and store the output of this command in a file, for example, `sconnect_out`.

   ```
   openssl s_client -connect vCenterServer_IPaddress:443 -showcerts
   ```

2. Add information about the certificates in a file named `cacerts.pem`.
3. Verify that a certificate is received from vCenter Server:

   ```
   openssl verify -CAfile cacerts.pem sconnect_out
   ```

For more information about the OpenSSL commands, go to www.openssl.org.

Procedure

Step 1 Create a file named `cacerts.pem` in `bootflash:`.

Step 2 Add a list of trusted certificates in the `cacerts.pem` file.

You can add the self-signed certificate of vCenter Server or the list of root certificate authorities that your security policy allows. The information about each certificate must be included within the following lines:

```
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
```

Verifying vCenter Server Certificates

You can verify the authentication of the vCenter certificates.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

Step 2	switch#(config) **show svs connections**	Verifies the vCenter server certificate.
		If the authentication fails or the `bootflash:/cacerts.pem` file is not present, the following message is displayed:
		`ssl-cert: self-signed or not authenticated`
		In addition, the following warning message is displayed five times or less after every 3 minutes:
		`VMS-1-CONN_SSL_NOAUTH: SSL AUTHENTICATION failure`

Step 3	(Optional) switch#(config) **vmware cert warning disable**	Disables the display of the warning messages. **Note** Although this command is hidden in the CLI, the command is available for use.

Example

This example shows how to verify the vCenter server certificate and how to disable the display of warning messages, if the authentication fails.

```
switch# configure terminal
switch#(config) show svs connections
```

```
connection vc:
    ip address: 110.23.43.170
    remote port: 80
    protocol: vmware-vim https
    certificate: default
    ssl-cert: ssl-cert: self-signed or not authenticated
VMS-1-CONN_SSL_NOAUTH: SSL AUTHENTICATION failure
VMS-1-CONN_SSL_NOAUTH: SSL AUTHENTICATION failure
VMS-1-CONN_SSL_NOAUTH: SSL AUTHENTICATION failure
VMS-1-CONN_SSL_NOAUTH: SSL AUTHENTICATION failure
VMS-1-CONN_SSL_NOAUTH: SSL AUTHENTICATION failure
switch#(config) vmware cert warning disable
switch#(config)

. . .
```

Disconnecting From the vCenter Server

You can disconnect from vCenter Server, for example, after correcting a vCenter Server configuration.

Before you begin

- Log in to the Cisco Nexus 1000VE in EXEC mode.
- Configure a Cisco Nexus 1000VE connection.
- Connect the Cisco Nexus 1000VE to vCenter Server/ESX.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **svs connection** *name*	Enters global configuration submode for the connection to vCenter Server.
Step 3	switch(config-svs-conn)# **no connect**	Closes the connection.

Example

This example shows how to disconnect from vCenter Server:

```
switch# configure terminal
switch# (config#) svs connection vcWest
switch# (config-svs-conn)# no connect
```

Removing the DVS from the vCenter Server

You can use remove the Distributed Virtual Switch (DVS) from the vCenter Server.

Before you begin

- Log in to the Cisco Nexus 1000VE in EXEC mode.
- Configure a connection to the vCenter Server.
- Connect the Cisco Nexus 1000VE to the vCenter Server/ESX.
- Check that the server administrator has removed all of the hosts that are connected to the Cisco Nexus 1000VE from the VM client. For more information, see the VMware documentation.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **svs connection** *name*	Enters global configuration submode for the connection to the vCenter Server.
Step 3	switch(config-svs-conn)# **no vmware dvs**	Removes the DVS associated with the specified connection from the vCenter Server.

Example

```
switch# configure terminal
switch(config)# svs connection vcWest
switch(config-svs-conn)# no vmware dvs
```

Removing the DVS from the vCenter Server when the VSM Is Not Connected

You can configure whether or not you will allow administrators to delete a DVS when the VSM is not connected to the vCenter Server.

Procedure

Step 1 Configure the admin user or group. See Configuring the Admin User or Admin Group, on page 18.

Step 2 Remove the DVS from the vCenter Server. See Removing the DVS from the vCenter Server, on page 16.

Configuring the Admin User or Admin Group

Before you begin

- Ensure that the system administrator has created an admin user or admin group on vCenter Server to manage and delete the DVS. This user should not be given any other permissions such as deploying VMs or hosts, and so on.
- The admin user name configured on the VSM is the same as the username on vCenter Server.

Procedure

Step 1 Determine the name of the DVS.

Step 2 Configure the admin user in vCenter Server.

Note You can also configure an admin group by entering the **admin group** *groupname* command.

Step 3 Verify that the admin user has been created.

Example

This example shows how to configure the admin user or an admin group on vCenter Server.

```
switch# show svs connections

connection VC:
    ipaddress: 10.104.63.16
    remote port: 80
    protocol: VMware-vim https
    certificate: default
    datacenter name: N1K-DC
    admin:
    DVS uuid: a2 …
    dvs version: 5.0
    config status: Enabled
    operational status: Connected
    sync status: Complete
    version: VMware vCenter Server 4.1.0 build 258902

switch# configure terminal
switch(config)# svs connection VC
switch(config-svs-conn) # admin user NAuser
switch(config-svs-conn) #show svs connections

connection VC:
    ipaddress: 10.104.63.16
    remote port: 80
    protocol: VMware-vim https
    certificate: default
    datacenter name: N1K-DC
    admin: NAuser(user)
    DVS uuid: a2 …
    dvs version: 5.0
    config status: Enabled
```

```
operational status: Connected
sync status: Complete
version: VMware vCenter Server 4.1.0 build 258902
```

Removing the DVS from the vCenter Server Using the Graphical User Interface

Procedure

Step 1 Log in to vCenter Server through the VMware vSphere Client with the admin user account.

Step 2 In the **vSphere Client** left pane, choose the data center.

Step 3 Choose **Hosts and Clusters** > **Networking**.

Step 4 Right-click the **DVS** and choose **Remove**.

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 Virtual Service Engine (VSE), it automatically assigns a free module number to the VSE and then maintains the mapping between the module number and the universally unique identifier (UUID) of a VSE. This mapping is used to assign the same module number to a given VSE.

Removing Host Mapping from a Module

Before you begin

- Log in to the Cisco Nexus 1000VE in EXEC mode.
- Remove the host from the Cisco Nexus 1000VE DVS on the vCenter.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# **no vse** *module-number*	Removes the specified module from the software. **Note** If the module is still present in the slot, the command is rejected, as shown in this example.
Step 3	(Optional) switch(config)# **show module vse mapping**	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.

Example

This example shows how to remove a host mapping from a specified VSE module:

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

Mapping to a New Host

Before you begin

- Log in to the CLI in EXEC mode.
- Remove the host from the Cisco Nexus 1000VE DVS on the 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**	Enters global configuration mode.
Step 2	switch(config)# **vse** *module number*	Enters VSE slot configuration mode.
Step 3	switch(config-vse-slot)# **host vmware id** *vse-uuid*	Assigns a different VSE UUID to the specified module.

	Command or Action	Purpose
Step 4	(Optional) switch(config-vse-slot)# **show module vse mapping**	Displays the mapping of modules to host servers.
Step 5	switch(config-vse-slot)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to map a host server to a module:

```
switch# configure terminal
switch(config)# vse 3
switch(config-vse-slot)# host vmware id 6dd6c3e3-7379-11db-abcd-000bab086eb6
switch(config-vse-slot)# show module vse 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-vse-slot)# copy running-config startup-config
```

Viewing Host Mapping

You can view the mapping of modules to host servers.

Command	Description
show module vse mapping	Displays the mapping on modules to host servers.

This example shows how to view the mapping of a module:

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

Verifying Connections

You can view and verify connections.

Commands	Description

show svs connections [*name*]	Displays the current connections to the Cisco Nexus 1000VE. **Note** Network connectivity issues may shut down your connection to the vCenter Server. When network connectivity is restored, the Cisco Nexus 1000VE will not automatically restore the connection. In this case, you must restore the connection manually using the following command sequence: **no connect** **connect**

Before you begin

- Log in to the CLI in any command mode.
- Configure the connection using the Connecting to the vCenter Server, on page 12 procedure.
- Know that the Cisco Nexus 1000VE is connected to vCenter Server.

Procedure

	Command or Action	Purpose
Step 1		

Example

This example shows how to verify a connection:

```
switch# show svs connections VC
Connection vc:
IP address: 172.28.15.206
Protocol: vmware-vim https
datacenter name: HamiltonDC
admin: NAuser(user)
DVS uuid: a2 …
dvs version: 5.0
config status: Enabled
operational status: Connected

n1000v#
```

Verifying the Domain

You can view and verify the configured domain.

Commands	Description
show svs domain	Display the domain configured on the Cisco Nexus 1000V.

Before you begin

- Log in to the CLI in any command mode.
- Configure a domain using the Creating a Domain procedure.

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 1000VE is not connected to a vCenter Server or ESX server, the output is limited to connection-related information.
show svs connections [*name*]	Displays the current connections to the Cisco Nexus 1000VE. **Note** Network connectivity issues might shut down your connection to the vCenter Server. When network connectivity is restored, the Cisco Nexus 1000VE will not automatically restore the connection. In this case, you must restore the connection manually using the **no connect** command followed by the **connect** command.
show svs domain	Displays the domain configured on the Cisco Nexus 1000VE.
show module	Displays module information.
show interface brief	Displays interface information.
show interface virtual	Displays virtual interface information.
show module vse mapping	Displays the mapping of modules to host servers.

Verifying the Module Information

You can display and verify module information, including a view of the DVS from the Cisco Nexus 1000VE.

Before you begin

- Log in to the CLI in any command mode.
- Configure the Cisco Nexus 1000VE connection using the Connecting to the vCenter Server procedure.
- Know that the Cisco Nexus 1000VE is connected to the vCenter Server.
- Know that the server administrator has already added the host running the Cisco Nexus 1000VE to the DVS in the vCenter Server.

Procedure

Step 1 **show module**

Example:

```
n1kve# show module
Mod  Ports  Module-Type                       Model               Status
---  -----  --------------------------------  ------------------  ------------
1    0      Virtual Supervisor Module         Nexus1000V          active *
3    1022   Virtual Service Engine            NA                  ok
4    1022   Virtual Service Engine            NA                  ok
5    1022   Virtual Service Engine            NA                  ok

Mod  Sw                Hw
---  ----------------  ------------------------------------------------
1    5.2(1)SV5(1.1)    0.0
3    5.2(1)SV5(1.1)    NA
4    5.2(1)SV5(1.1)    NA
5    5.2(1)SV5(1.1)    NA

Mod  Server-IP        Server-UUID                          Server-Name
---  ---------------  -----------------------------------  --------------------
1    10.197.128.101   NA                                   NA
3    10.197.128.122   4213D2CA-1D9A-FE4E-6368-9E4B4F74B3AE  localhost.localdomai
n
4    10.197.128.123   42136761-CB7A-7AE8-B81B-7504E7309AF8  localhost.localdomai
n
5    10.197.128.124   4213B1A8-6CCB-5C5B-ACF0-064C7900F3C5  localhost.localdomai
n

Mod  VSE-IP           Host-IP
---  ---------------  -----------------------------------
3    10.197.128.122   10.197.128.89
4    10.197.128.123   10.197.128.93
5    10.197.128.124   10.197.128.90

* this terminal session
================================================================================
```

Displays module information.

Step 2 show interface brief

Example:

```
n1kve# show interface brief
--------------------------------------------------------------------------------
Port     VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0    --           up     16.1.0.103                              1000     1500

--------------------------------------------------------------------------------
Ethernet     VLAN    Type Mode    Status  Reason                     Speed    Port
Interface                                                                    Ch #
--------------------------------------------------------------------------------
Eth3/1       1       eth  trunk   up      none                       10G
Eth4/1       1       eth  trunk   up      none                       10G
Eth5/1       1       eth  trunk   up      none                       10G

--------------------------------------------------------------------------------
Vethernet    VLAN/    Type Mode    Status  Reason                      MTU  Module
             Segment
```

```
--------------------------------------------------------------------------------
Veth1         1602     virt access  up      none                    1500 4
Veth2         1602     virt access  up      none                    1500 4
Veth3         1602     virt access  up      none                    1500 5
Veth4         1602     virt access  up      none                    1500 5

--------------------------------------------------------------------------------
Port     VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
control0 --           up     --                                      1000     1500

NOTE : * Denotes ports on modules which are currently offline on VSM
```

Displays interface information, including the uplinks to the vCenter Server.

Step 3 **show interface virtual**

Example:

```
n1kve# show interface virtual
-------------------------------------------------------------------------------
Port        Adapter        Owner                    Mod Host
-------------------------------------------------------------------------------
Veth1       Net Adapter 1  vm14                     4   localhost.localdomain
Veth2       Net Adapter 1  vm12                     4   localhost.localdomain
Veth3       Net Adapter 1  vm13                     5   localhost.localdomain
Veth4       Net Adapter 1  vm11                     5   localhost.localdomain
n1kve#
```

Displays virtual interface information.

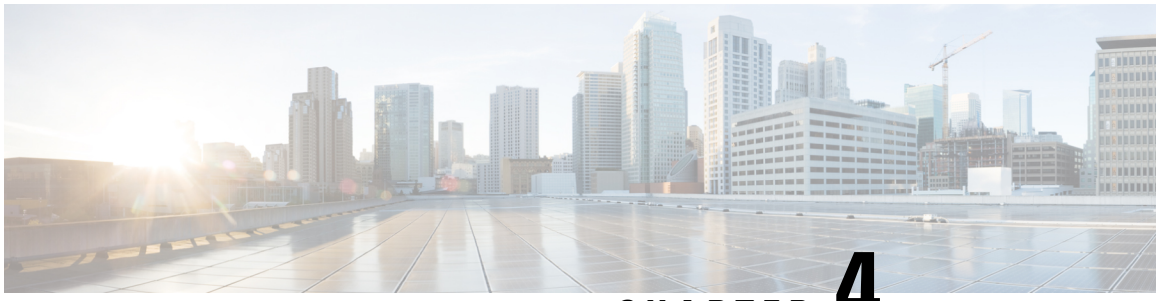
Verifying the Module Information Using the vCenter Server

You can display and verify module information using the vCenter Server. The following alarms are raised in the vCenter Server based on the condition.

All alarms are cleared when the VSM disconnects from the vCenter Server.

Alarm	Description
<*Host-Ref_Name*> Online	This alarm is raised as a warning on the host object. It indicates that the VSE is online in the VSM. This alarm persists as long as the VSE is communicating with the VSM and the VSE is online.
<*Host-Ref_Name*> Offline	This alarm is raised as an alert on the host object. It indicates that the VSE is offline in the VSM. This alarm is cleared when the VSE comes online.
<*Host-Ref_Name*> Deleted from VSM	This alarm is raised as a warning on the host object. It indicates that the VSE is being removed from the VSM but it is not removed from the DVS. This alarm is cleared when the VSE is detected as a module in the VSM.

Alarm	Description
<*Host-Ref_Name*> Update failed in VSM	This alarm is raised as an alert on the host object. It indicates that the VSE has already been removed from the VSM but updates are still being received from the vCenter Server. There can be connectivity issues between the VSM and the VSE. This alarm can coexist with the <*Host-Ref_Name*> Deleted from VSM alarm. This alarm is cleared when the VSE is detected as a module in the VSM.



CHAPTER 4

Managing the Configuration

This chapter contains the following sections:

Information About Configuration Management

The Cisco Nexus 1000VE enables you to change the switch name, configure messages of the day, and display, save, and erase configuration files.

Changing the Switch Name or Prompt

You can change the switch name or prompt from the default (switch#) to another character string.

Before you begin

Log in to the CLI in global configuration mode.

Procedure

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

Example

This example shows how to change the switch name:

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

Configuring a Message of the Day

You can 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.
- You can use the following tokens the message of the day:
  - $(hostname) displays the hostname for the switch.
  - $(line) displays the vty or tty line or name.

Before you begin

Log in to the CLI in global 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.

Example

This example shows how to configure a message of a day:

```
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

You can view the versions of software and hardware on your system, for example, to verify the version before and after an upgrade.

Before you begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **show version**	Displays the versions of system software and hardware that are currently running on the switch.

Example

This example shows how to verify the software and hardware versions on your system:

```
switch# show version
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2018, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
kickstart: version 5.2(1)SV5(1.1)
system: version 5.2(1)SV5(1.1)
kickstart image file is: bootflash:///n1000v-dk9-kickstart.5.2.1.SV5.1.1.bin
kickstart compile time: 7/5/2018 0:00:00 [07/05/2018 07:54:21]
system image file is: bootflash:///n1000v-dk9.5.2.1.SV5.1.1.bin
system compile time: 7/5/2018 0:00:00 [07/05/2018 08:23:05]


Hardware
```

```
cisco Nexus 1000V Chassis ("Virtual Supervisor Module")
Intel(R) Xeon(R) CPU E5-2620 with 4126584 kB of memory.
Processor Board ID T505698E126

Device name: switch
bootflash: 2332296 kB

System uptime is 2 days, 19 hours, 18 minutes, 12 seconds

Kernel uptime is 2 day(s), 19 hour(s), 18 minute(s), 45 second(s)


plugin
Core Plugin, Ethernet Plugin, Virtualization Plugin


Reset reason
1) Time: Fri Jul 6 08:25:12 2018
Reason: Reset Requested by CLI command reload

switch#
================================================================================
```

Verifying the Running Configuration

You can view the configuration that is currently running on the system.

Before you begin

Log in to the CLI in any command mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **show running-config**	Displays the versions of system software and hardware that are currently running on the switch.

Example

This example shows how to verify the software and hardware versions running on a switch:

```
switch# show running-config
version 5.2(1)SV5(1.1)
hostname <VSM-NAME>

ip domain-lookup
ip host <VSM-NAME> <VSM-IP>
radius-server host <RADIUS-SERVER-IP> key 7 "<PASSWORD>" pac authentication accounting
errdisable recovery cause failed-port-state
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
snmp-server context mib2
```

```
snmp-server context system
snmp-server community <removed> group network-operator
snmp-server mib community-map <removed> context system
no ntp passive
aaa authentication login error-enable

vrf context management
  ip route 0.0.0.0/0 <GATEWAY-IP>
vlan 2-1000

port-channel load-balance ethernet source-mac
port-profile default max-ports 32
port-profile default port-binding static
port-profile type ethernet Unused_Or_Quarantine_Uplink
  shutdown
  description Port-group created for Nexus 1000VE internal usage. Do not use.
  state enabled
  vmware port-group
port-profile type vethernet Unused_Or_Quarantine_Veth
  shutdown
  description Port-group created for Nexus 1000VE internal usage. Do not use.
  state enabled
  vmware port-group
port-profile type ethernet outside-trunk
  switchport mode trunk
  switchport trunk allowed vlan 1-3967,4048-4093
  no shutdown
  description Port-group created for Nexus 1000VE internal usage. Do not use.
  state enabled
  vmware port-group
port-profile type vethernet inside-trunk1
  switchport mode trunk
  switchport trunk allowed vlan 1-50
  no shutdown
  description Port-group created for Nexus 1000VE internal usage. Do not use.
  state enabled
  vmware port-group
port-profile type vethernet inside-trunk2
  switchport mode trunk
  switchport trunk allowed vlan 2047-2097
  no shutdown
  description Port-group created for Nexus 1000VE internal usage. Do not use.
  state enabled
  vmware port-group

system storage-loss log time 60
system inter-sup-heartbeat time 15


interface mgmt0
  ip address <Mgmt-IP>/<MASK>
line console
  exec-timeout 0
line vty
  exec-timeout 0

boot kickstart bootflash:/kick.bin
boot system bootflash:/sys.bin
boot kickstart bootflash:/kick.bin
boot system bootflash:/sys.bin

svs-domain
  domain id 100
  control vlan 1
```

```
  packet vlan 1
  svs mode L3 interface mgmt0
  switch-guid <Switch-GUID>
  enable l3sec
vse-dvs
  outside-trunk vlan 1-4094
  inside-trunk 1 tag  1-50
  inside-trunk 2 tag  2047-2097
svs connection vc
  protocol vmware-vim
  remote ip address <VCenter-IP> port 80 vrf management
  transport type ipv4
  vmware dvs uuid "<DVS-UUID>" datacenter-name <DataCenter Name>
  max-ports 12000
  vmware dvs-version 5.0.0
  connect
vservice global type vsg
  no tcp state-checks invalid-ack
  no tcp state-checks seq-past-window
  no tcp state-checks window-variation
  no bypass asa-traffic
  no l3-frag
vservice global
  idle-timeout
    tcp 30
    udp 4
    icmp 4
    layer-3 4
    layer-2 2
nsc-policy-agent
  registration-ip 0.0.0.0
  shared-secret **********
  log-level
no logging logfile
logging monitor 7


switch#
```

Comparing the Startup and Running Configurations

Before you begin

Log in to the CLI in any command mode.

Procedure

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

Example

This example shows how to compare the startup and running configurations:

```
switch# show running-config diff*** Startup-config
--- Running-config
***************
*** 261,276 ****
    inherit port-profile VSG_Secured_1161
    description HPING-1161_24, Net Adapter 1
    vmware dvport 0 dvswitch uuid "50 13 3b cc 83 4a 88 c8-21 c6 c4 e8 c9 34 e8 bd"
    vmware vm mac 0050.5693.288B

- interface Vethernet15
-   inherit port-profile VSG_Data_1163
-   description VMware VMkernel, vmk1
-   vmware dvport 0 dvswitch uuid "50 13 3b cc 83 4a 88 c8-21 c6 c4 e8 c9 34 e8 bd"
-   vmware vm mac 0050.566C.1B76
-
  interface Vethernet16
    inherit port-profile vlan-1057
    description VMware VMkernel, vmk2
    vmware dvport 0 dvswitch uuid "50 13 3b cc 83 4a 88 c8-21 c6 c4 e8 c9 34 e8 bd"
    vmware vm mac 0050.566D.815A
--- 260,269 --


================================================================================
```

Verifying the Interface Configuration

This section includes the following procedures:

- Verifying a Brief Version of an Interface Configuration
- Verifying a Detailed Version of an Interface Configuration
- Verifying a Brief Version of all Interfaces
- Verifying the Running Configuration for all Interfaces

Verifying the Interface Configuration in a Brief Version

Before you begin

Log in to the CLI in any command mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **show interface** {*type*} {*name*} **brief**	Displays a brief version of information about the specified interface configuration.

Example

```
switch# show interface mgmt 0 brief

--------------------------------------------------------------------------------
Port   VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --           up     10.78.1.63                              1000     1500
```

Verifying an Interface Configuration in a Detailed Version

Before you begin

Log in to the CLI in any command mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **show interface** {*type*} {*name*}	Displays details about the specified interface configuration.

Example

This example shows how to verify configuration details of an interface:

```
switch# show interface mgmt 0
mgmt0 is up
  Hardware: Ethernet, address: 0050.5689.3321 (bia 0050.5689.3321)
  Internet Address is 172.23.232.141/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  full-duplex, 1000 Mb/s
  Auto-Negotiation is turned on
    4961 packets input, 511995 bytes
    0 multicast frames, 0 compressed
    0 input errors, 0 frame, 0 overrun, 0 fifo
    245 packets output, 35853 bytes
    0 underrun, 0 output errors, 0 collisions
    0 fifo, 0 carrier errors
```

Verifying All Interfaces in a Brief Version

Before you begin

Log in to the CLI in any command mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **show interface brief**	Displays a brief version of all interface configurations on your system.

Example

This example show how to verify the configuration of all available interfaces:

```
switch# show interface brief

--------------------------------------------------------------------------------
Port     VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0    --           up     10.197.128.101                          1000     1500

--------------------------------------------------------------------------------
Ethernet     VLAN    Type Mode    Status  Reason                     Speed    Port
Interface                                                                    Ch #
--------------------------------------------------------------------------------
Eth3/1       1       eth  trunk   up      none                       10G
Eth4/1       1       eth  trunk   up      none                       10G
Eth5/1       1       eth  trunk   up      none                       10G

--------------------------------------------------------------------------------
Vethernet    VLAN/    Type Mode    Status  Reason                      MTU  Module
             Segment
--------------------------------------------------------------------------------
Veth1        1161     virt access  up      none                        1500 3
Veth2        1161     virt access  up      none                        1500 3
Veth3        1161     virt access  up      none                        1500 3
Veth4        1163     virt access  up      none                        1500 3


================================================================================
```

Verifying the Running Configuration for All Interfaces

The output for the **show running-config interface** command differs from the output of the **show interface** command.

Before you begin

Log in to the CLI in any command mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **show running-config interface**	Displays the running configuration for all interfaces on your system.

Example

This example shows how to view the running configuration for all interfaces on a system:

```
switch# show running-config interface
!Command: show running-config interface
!Time: Tue Jul  3 07:02:44 2018

version 5.2(1)SV5(1.1)

interface mgmt0
  ip address 10.197.128.101/27

interface Vethernet1
  inherit port-profile VSG_Secured_1161
  description HPING-1161_8, Net Adapter 1
  vmware dvport 0 dvswitch uuid "50 13 3b cc 83 4a 88 c8-21 c6 c4 e8 c9 34 e8 bd"
  vmware vm mac 0050.5693.9437

interface Vethernet2
  inherit port-profile VSG_Secured_1161
  description HPING-1161_7, Net Adapter 1
  vmware dvport 0 dvswitch uuid "50 13 3b cc 83 4a 88 c8-21 c6 c4 e8 c9 34 e8 bd"
  vmware vm mac 0050.5693.3F26

interface Vethernet3
  inherit port-profile VSG_Secured_1161
  description HPING-1161_6, Net Adapter 1
  vmware dvport 0 dvswitch uuid "50 13 3b cc 83 4a 88 c8-21 c6 c4 e8 c9 34 e8 bd"
  vmware vm mac 0050.5693.0FDB

interface Vethernet4
  inherit port-profile VSG_Data_1163
  description VMware VMkernel, vmk1
  vmware dvport 0 dvswitch uuid "50 13 3b cc 83 4a 88 c8-21 c6 c4 e8 c9 34 e8 bd"
  vmware vm mac 0050.566D.BAF9
```

Saving a Configuration

You can 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

Log in to the CLI in any command mode.

Procedure

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

Example

This example shows how to save a running configuration:

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

Erasing a Configuration

You can use this procedure to erase a startup configuration.

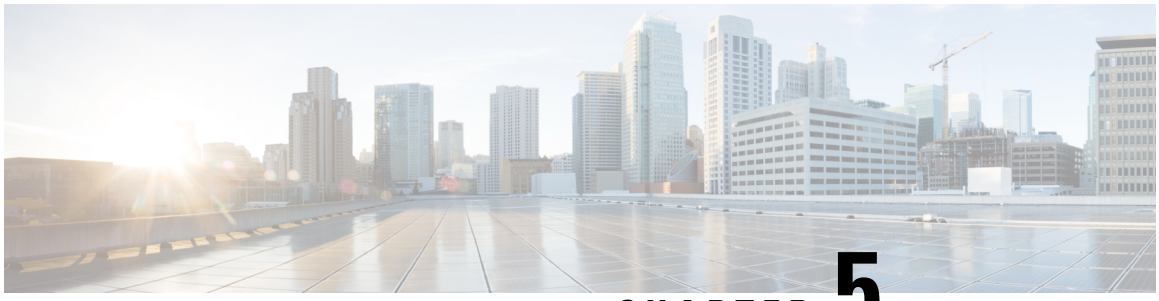
Caution The **write erase** command erases the entire startup configuration with the exception of loader functions, the license configuration, and the certificate extension configuration

Before you begin

Log 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.



CHAPTER 5

Working with Files

This chapter contains the following sections:

Information About Files

The Cisco Nexus 1000VE file system provides a single interface to all the file systems that the Cisco Nexus 1000VE 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. The Cisco Nexus 1000VE 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 of Your Current Location

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

Before you begin

Log in to the CLI in any command mode.

Procedure

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

Changing Your Directory

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

The Cisco Nexus 1000VE 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

Log 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.

Example

This example shows how to change the directory:

```
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

You can use this procedure to list the files in a file system.

Before you begin

Log in to the CLI in any command mode.

Procedure

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

Example

This example shows how to list files within a file system:

```
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

Log 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.

Example

This example shows how to identify available file systems:

```
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 filename 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 filenames 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 filename for you

Example

This example shows how to complete a partial filename:

```
switch# show file bootflash: nexus-1000ve-
bootflash:nexus-1000ve-dplug-mzg.5.2.1.SV5.1.1.bin
bootflash:nexus-1000ve-mzg.5.2.1.SV5.1.1.bin
bootflash:nexus-1000ve-kickstart-mzg.5.2.1.SV5.1.1.bin
n1000v# show file bootflash:c<Tab>
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDSq93BrlHcg3bX1jXDMY5c9+yZSST3VhuQBqogvCPDGeLecA+j
...
...
switch#
```

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

- Log in to the CLI through a Telnet or Secure Shell (SSH) connection.
- Know that 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.
- Know that your device has connectivity to the destination. Use the **ping** command to be sure.
- Know that the source configuration file is in the correct directory on the remote server.
- Know that 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.	Copies a file from the specified source location to the specified destination location.

	Command or Action	Purpose
	• 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. • 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.	

Example

```
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.

Example

This example shows how to create a directory:

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

Removing an Existing Directory

This command is valid only on Flash file systems.

Before you begin

- Make sure that 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 a directory. The directory name is case sensitive.

	Command or Action	Purpose
	Removes the specified directory at the current directory level. • switch# **rmdir** {**bootflash:** | **debug:** | **volatile:**} *directory* Removes a directory from the file system.	

Example

This example shows how to remove a directory:

```
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 is not completed if there is not enough space in the destination directory.

Before you begin

Log 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:).

Example

This example shows how to move the file from one directory to another directory:

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

Example

This example shows how to delete files and directories:

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

Compressing Files

Before you begin

Log in to the CLI.

Procedure

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

Example

This example shows how to compress a 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

Log in to the CLI.

Procedure

	Command or Action	Purpose
Step 1	switch# **gunzip** [*path*] *filename*	Uncompresses the specified file. The filename is case sensitive.
Step 2	switch# **dir**	Displays the contents of a directory, including the newly uncompressed file.

Example

This example shows how to uncompress a 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 **show running-config**command to a path and filename.

	Command or Action	Purpose
	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.	

Example

These examples show how to direct a command output to a file:

```
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

You can verify the integrity of an image before loading it. This command can be used for both the system and kickstart images.

Procedure

	Command or Action	Purpose
Step 1	switch# **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.
Step 2	switch# **show version image** [**bootflash:** | **modflash:** |**volatile:**]	Validates the specified image.

	Command or Action	Purpose
		bootflash—specifies bootflash as the directory name. volatile—Specifies volatile as the directory name. modflash—Specifies modflash as the directory name.

Example

This example shows how to verify an image before loading it:

```
switch# copy tftp://10.10.1.1/home/configs/switch3-run.cfg system:running-config
switch# show version image bootflash:isan.bin
  MD5 Verification Passed
  image name: n1000v-dk9-kickstart.5.2.1.SV5.1.0.228.bin
  kickstart:  version 5.2(1)SV5(1.1) [build 5.2(1)SV5(1.0.228)]
  compiled:   7/2/2018 16:00:00 [07/02/2018 23:33:55]
```

Rolling Back to a Previous Configuration

You can recover your configuration from a previously saved version.

Note Each time that 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).

Example

This example shows how to recover the previous configuration:

```
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

Log 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.

Example

This example shows how to display the file contents:

```
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

Log in to the CLI.

Procedure

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

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

Example

This example shows how to display contents of a 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 the file integrity.

Procedure

	Command or Action	Purpose
Step 1	switch# **show file** *filename* [**cksum** | **md5sum**]	Provides the checksum or MD5 checksum of the file for comparison with the original file.
Step 2	switch# **show file** {**bootflash:** | **volatile:** | **debug:**} *filename* [**cksum** | **md5sum**]	Provides the Message-Digest Algorithm 5 (MD5) checksum of the file. MD5 is an electronic fingerprint for the file.

Example

These examples show how to display checksums:

```
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

Log in to the CLI in EXEC mode.

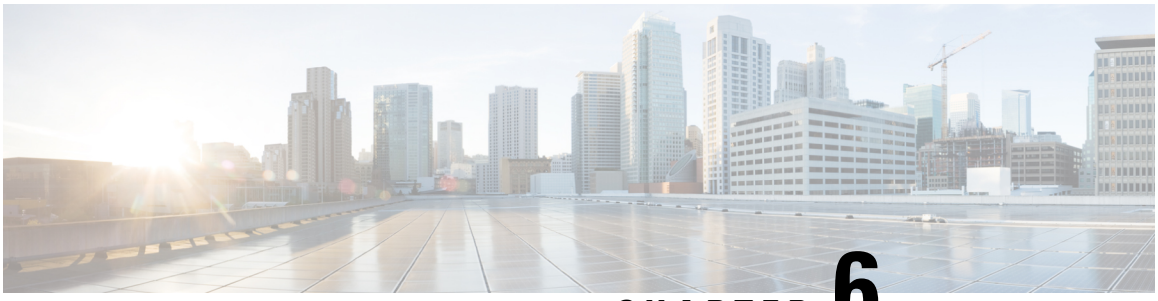
Procedure

	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.

Example

This example shows how to display the requested number of last lines from a specified file:

```
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
```



CHAPTER 6

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 .

Displaying Current User Access

You can display all users currently accessing the switch.

Before you begin

Log 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.

Example

This example shows how to display current user access:

```
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 who are currently using the system.

Before you begin

Log in to the CLI.

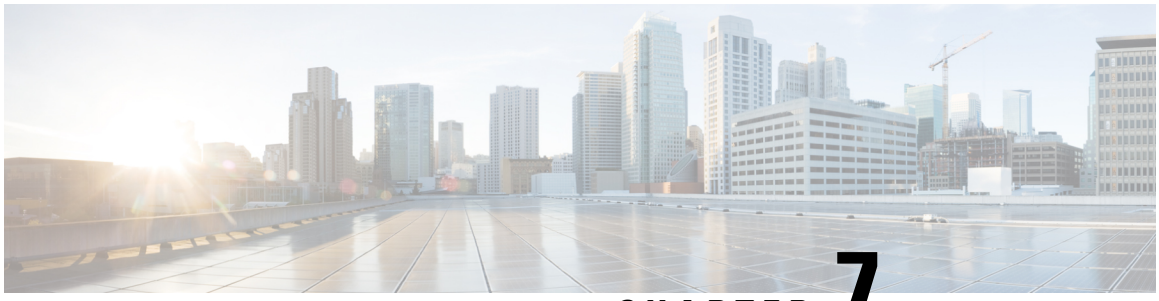
Procedure

	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.

Example

This example shows up to send a message to users:

```
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#
```



CHAPTER 7

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 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 it has determined the time by using other means. Other network devices can then synchronize to that network device through NTP.

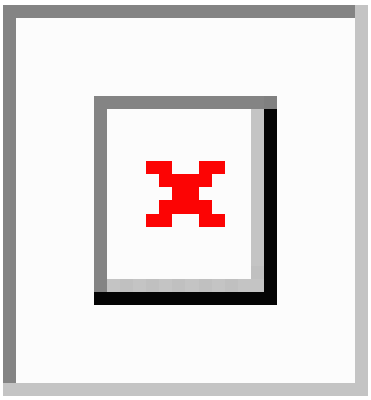
Note NTP supports IPv4 addresses.

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 figure 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

Log 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)# **ntp server** {*ipv4-address* | *ipv6-address* | *dns-name*}	Forms an association with a server.
Step 3	switch(config)# **ntp peer** {*ipv4-address* | *dns-name*}	Forms an association with a peer. You can specify multiple peer associations.
Step 4	(Optional) switch(config)# **show ntp peers**	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	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Example

This example shows how to configure an NTP server with an IPv4 address and an NTP peer with an IPv6 address:

```
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 {*ipv4-address* | *ipv6-address* | *dns-name*}	Displays the NTP statistics.

NTP Example Configuration

Procedure

Step 1 switch# **configure terminal**

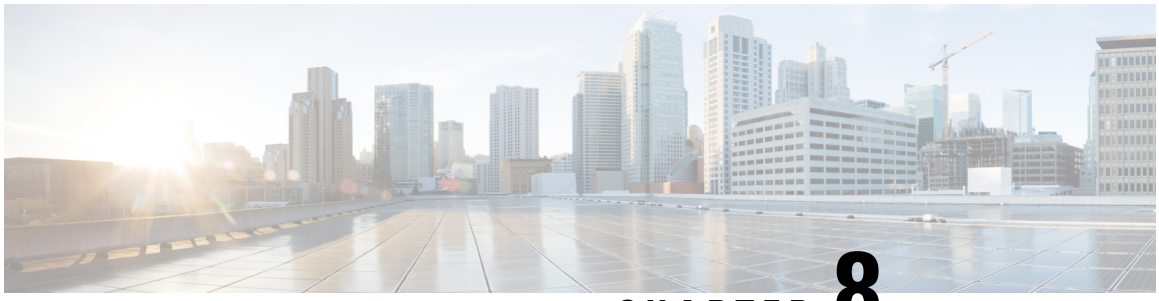
Enters global configuration mode.

Step 2 **ntp server 192.0.2.10**

Configures an NTP server.

Feature History for NTP

Feature Name	Releases	Feature Information
IPv6	5.2(1)SV3(1.1)	IPv6 was introduced.
NTP	4.0(4)SV1(1)	This feature was introduced.



CHAPTER 8

Configuring the HTTP Server

This chapter contains the following sections:

Information About the HTTP Server

An HTTP server, which can be turned off from the CLI to address security concerns, is embedded in the Virtual Supervisor Module (VSM).

Guidelines and Limitations for the HTTP Server

- The HTTP server is enabled by default.
- The HTTP server must be enabled in order to get the Cisco Nexus 1000VE XML plugin from the VSM.

Disabling HTTPS

Before you begin

- Ensure that feature http-server is enabled.
- Ensure that vnm-pa is uninstalled and nsmgr is disabled.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch# **http-server no https**	Disables the HTTPS service.
Step 3	(Optional) switch(config)# **show http-server**	Displays the HTTP server configuration.
Step 4	(Optional) switch(config)# **Show feature**	Displays the state (enabled or disabled) of each available feature.

Example

```
switch# configure terminal
switch(config)# http-server no https
httpd: no process killed
switch(config)# show http-server
http-server enabled
 http protocol enabled
 https protocol disabled
switch(config)# show feature
Feature Name                  Instance  State
----------------------------  --------  --------
http-server                   1         enabled
.
.
.
switch(config)#
```

Disabling HTTP

Before you begin

- Ensure that feature http-server is enabled.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch# **http-server no http**	Disables the HTTP service.
Step 3	(Optional) switch(config)# **show http-server**	Displays the HTTP server configuration.
Step 4	(Optional) switch(config)# **Show feature**	Displays the state (enabled or disabled) of each available feature.

Example

```
switch# configure terminal
switch(config)# http-server no http
httpd: no process killed
switch(config)# show http-server
```

```
http-server enabled
 http protocol disabled
 https protocol enabled


switch(config)# show feature
Feature Name                  Instance  State
----------------------------  --------  --------
http-server                   1         enabled
.
.
.
switch(config)#
```

Installing Certificates

Certificates are sent to the browser or server and contain public keys needed to begin a secure session.

Installing the HTTP-Server Certificate

To install an HTTP-server certificate, use the **install http-certificate** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch# **install http-certificate** {bootflash: [*// server/*] | default}	Installs the certificate where {bootflash: [*// server/*] specifies the source or destination URL for boot flash memory. To regenerate an expired default certificate, use the **install http-certificate default** command. **Note** File extensions with .crt and .pem are supported.

Example

This example shows how to install an HTTP certificate to the boot flash memory:

```
switch# configure terminal
switch(config-svs-conn)# install http-certificate bootflash:new.crt
```

Installing the SVS-Connection Certificate

To install a certificate for SVS-connection, use the **install certificate** command.

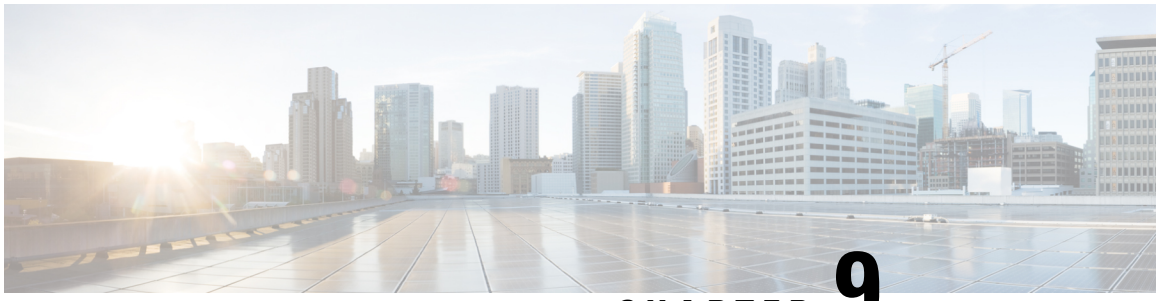
Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **svs connection vcenter**	Establishes vCenter connection.
Step 3	switch(config-svs-conn)# **install certificate** {bootflash: [*// server/*] | default}	Installs the certificate where {bootflash: [*// server/*] specifies the source or destination URL for boot flash memory. **Note** File extensions with .crt and .pem are supported.

Example

This example shows how to install a certificate to the boot flash memory:

```
switch# configure terminal
switch(config)# svs connection vcenter
switch(config-svs-conn)# install certificate bootflash:new.crt
```



CHAPTER 9

Configuring Local SPAN and ERSPAN

This chapter contains the following sections:

Information About SPAN and ERSPAN

The Switched Port Analyzer (SPAN) feature (sometimes called port mirroring or port monitoring) allows network traffic to be analyzed by a network analyzer such as a Cisco SwitchProbe or other Remote Monitoring (RMON) probes.

SPAN allows you to monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports where the network analyzer is attached.

SPAN Sources

The interfaces from which traffic can be monitored are called SPAN sources. These sources include Ethernet, virtual Ethernet, port-channel, port profile, and VLAN. When a VLAN is specified as a SPAN source, all supported interfaces in the VLAN are SPAN sources. When a port profile is specified as a SPAN source, all ports that inherit the port profile are SPAN sources. Traffic can be monitored in the receive direction, the transmit direction, or both directions for Ethernet and virtual Ethernet source interfaces as described by the following:

- Receive source (Rx)—Traffic that enters the switch through this source port is copied to the SPAN destination port.
- Transmit source (Tx)—Traffic that exits the switch through this source port is copied to the SPAN destination port

Characteristics of SPAN Sources

A local SPAN source has these characteristics:

- Can be port type Ethernet, virtual Ethernet, port profile, or VLAN.
- Cannot be a destination port or port profile
- Can be configured to monitor the direction of traffic — receive, transmit, or both.
- Can be in the same or different VLANs.
- For VLAN SPAN sources, all active ports in the source VLAN are included as source ports.
- Must be on the same host Virtual Service Engine (VSE) as the destination port.
- For port profile sources, all active interfaces attached to the port profile are included as source ports.

SPAN Destinations

SPAN destinations refer to the interfaces that monitor source ports.

Characteristics of Local SPAN Destinations

Each local SPAN session must have at least one destination port (also called a monitoring port) that receives a copy of traffic from the source ports or VLANs. A destination port has these characteristics:

- Can be any physical, virtual Ethernet port, or a port profile.
- Cannot be a source port or port profile.
- Is excluded from the source list and is not monitored if it belongs to a source VLAN of any SPAN session or a source port profile.
- Receives copies of transmitted and received traffic for all monitored source ports in the same VSE. If a destination port is oversubscribed, it can become congested. This congestion can affect traffic forwarding on one or more of the source ports.
- Must not be private VLAN mode.
- Can only monitor sources on the same host (VSE)
- In access mode, can receive monitored traffic on all the VLANs.
- In trunk mode, can receive monitored traffic only on the allowed VLANs in the trunk configuration.

Characteristics of ERSPAN Destinations

- An ERSPAN destination is specified by an IP address.
- In ERSPAN, the source SPAN interface and destination SPAN interface may be on different devices interconnected by an IP network. ERSPAN traffic is Generic Routing Encapsulation (GRE-encapsulated).

Local SPAN

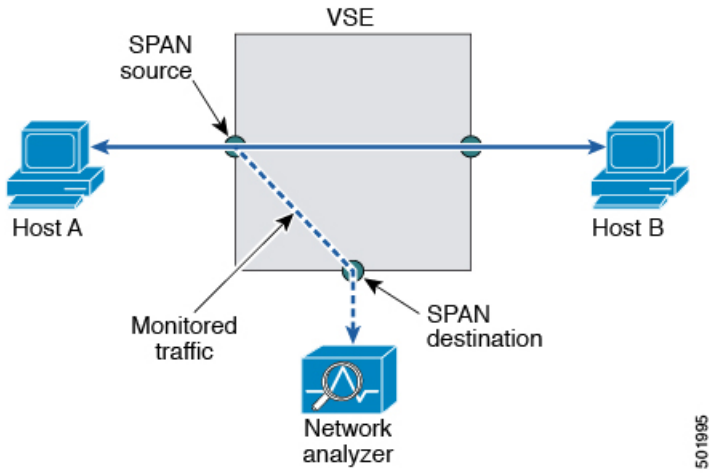
In Local SPAN, the source interface and destination interface are on the same VSE. The network analyzer is attached directly to the SPAN destination port. The SPAN source can be a port, a VLAN interface, or a port profile.The destination can be a port or port profile.

The diagram shows that traffic transmitted by host A is received on the SPAN source interface. Traffic (ACLs, QoS, and so forth) is processed as usual. Traffic is then replicated. The original packet is forwarded on toward host B. The replicated packet is then sent to the destination SPAN interface where the monitor is attached.

Local SPAN can replicate to one or more destination ports. Traffic can be filtered so that only traffic of interest is sent out the destination SPAN interface.

Local SPAN can monitor all traffic received on the source interface including Bridge Protocol Data Unit (BPDU).

Figure 3: Local SPAN

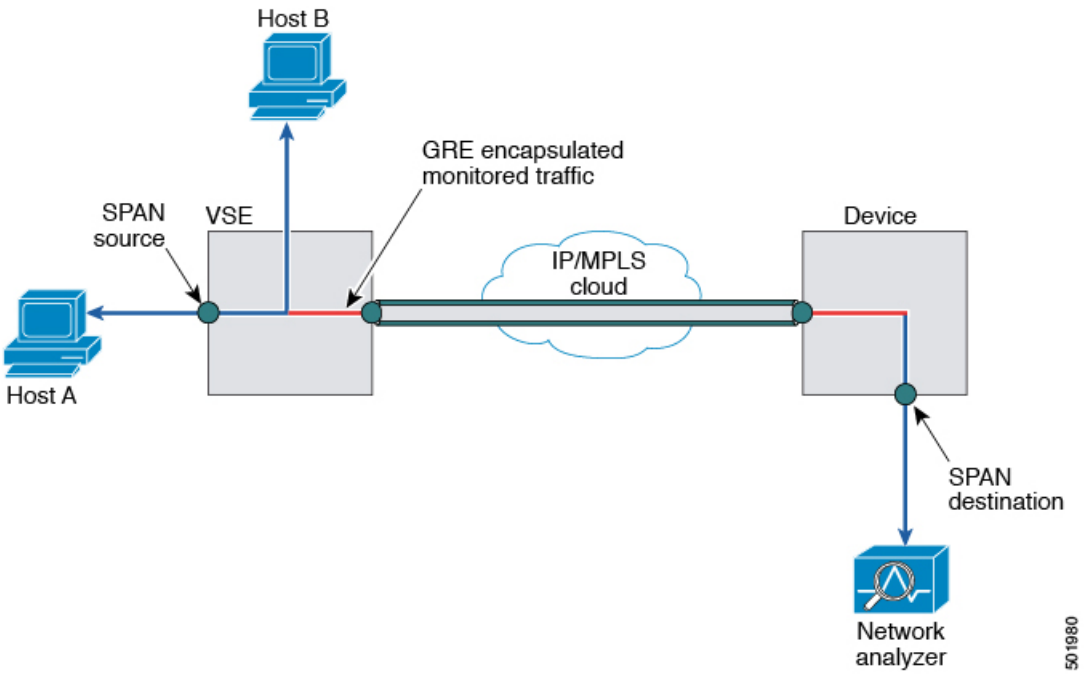


Encapsulated Remote SPAN

Encapsulated remote SPAN (ERSPAN) monitors traffic in multiple network devices across an IP network and sends that traffic in an encapsulated envelope to destination analyzers. In contrast, Local SPAN cannot forward traffic through the IP network. ERSPAN can be used to monitor traffic remotely. ERSPAN sources can be ports, VLANs, or port profiles.

In the following figure, the ingress and egress traffic for Host A are monitored using ERSPAN. Encapsulated ERSPAN packets are routed from Host A through the routed network to the destination device where they are decapsulated and forwarded to the attached network analyzer. The destination may also be on the same Layer 2 network as the source.

Figure 4: ERSPAN Example



Network Analysis Module

You can also use the Cisco Network Analysis Module (NAM) to monitor ERSPAN data sources for application performance, traffic analysis, and packet header analysis.

SPAN Sessions

You can create up to 64 total SPAN sessions (Local SPAN plus ERSPAN) on the VSE.

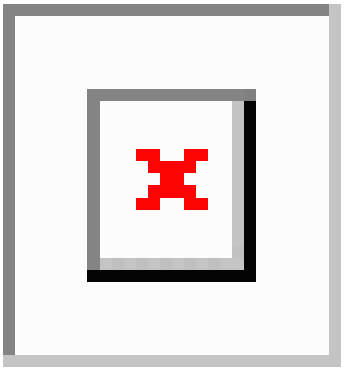
You must configure an ERSPAN session ID that is added to the ERSPAN header of the encapsulated frame to differentiate between ERSPAN streams of traffic at the termination box. You can also configure the range of flow ID numbers.

When trunk ports are configured as SPAN sources and destinations, you can filter VLANs to send to the destination ports from among those allowed. Both sources and destinations must be configured to allow the VLANs.

The following figure shows one example of a VLAN-based SPAN configuration in which traffic is copied from three VLANs to three specified destination ports. You can choose which VLANs to allow on each destination port to limit the traffic transmitted. In the figure, the device transmits packets from one VLAN at each destination port. The destinations in this example are trunks on which allowed VLANs are configured.

Note VLAN-based SPAN sessions cause all source packets to be copied to all destinations, whether the packets are required at the destination or not. VLAN traffic filtering occurs at transmit destination ports.

Figure 5: VLAN-based SPAN Configuration Example



Guidelines and Limitations for SPAN

- A maximum of 64 SPAN sessions (Local SPAN plus ERSPAN) can be configured on the Virtual Supervisor Module (VSM).
- A maximum of 32 source VLANs are allowed in a session.
- A maximum of 32 destination interfaces are allowed for a Local SPAN session.
- A maximum of 8 destination port-profiles are allowed for a Local SPAN session.
- A maximum of 16 source port-profiles are allowed in a session.
- A maximum of 128 source interfaces are allowed in a session.

⚠

Caution Overload Potential

To avoid an overload on uplink ports, use caution when configuring ERSPAN, especially when sourcing VLANs. The uplink that the VM kernel uses might get overloaded due to ERSPAN traffic. VSM-VSE communication might also be impacted. For example, when the Nexus 1000VE is configured for Layer 3 connectivity, both AIPC traffic and ERSPAN traffic use the same VM kernel NIC.

- A port can be configured in a maximum of four SPAN sessions.
- A port can be a source in a maximum of four SPAN sessions.
- The destination port used in one SPAN session cannot also be used as the destination port for another SPAN session.
- You cannot configure a port as both a source and destination port.
- In a SPAN session, packets that source ports receive may be replicated even though they are not transmitted on the ports. The following are examples of this behavior:
  - Traffic that results from flooding
  - Broadcast and multicast traffic

- For VLAN SPAN sessions switched on the same VLAN with both receive and transmit configured, two packets (one from receive and one from transmit) are forwarded from the destination port.

Default Settings for SPAN

Parameters	Default
State	SPAN sessions are created in the shut state.
Description	blank
Traffic direction for source interface or port profile	both
Traffic direction for source VLAN	receive (ingress or RX)

Configuring SPAN

This section describes how to configure SPAN and includes the following procedures:

- Configuring a Local SPAN Session
- Configuring an ERSPAN Port Profile
- Configuring an ERSPAN Session
- Shutting Down a SPAN Session
- Resuming a SPAN Session
- Verifying the SPAN Configuration

Configuring a Local SPAN Session

This procedure involves creating the SPAN session in monitor configuration mode, and then, optionally, configuring allowed VLANs in interface configuration mode.

It is important to know the following information about SPAN:

- SPAN sessions are created in the shut state by default.
- When you create a SPAN session that already exists, any additional configuration is added to that session. To make sure that the session is cleared of any previous configuration, you can delete the session first. This procedure includes how to do this.
- The source and destination ports are already configured in either access or trunk mode. For more information, see the *Cisco Nexus 1000VE Interface Configuration Guide*.

Before you begin

- Log in to the CLI in EXEC mode.

- Know that number of the SPAN session that you are going to configure.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **no monitor session** *session-number*	Clears the specified session.
Step 3	switch(config)# **monitor session** *session-number*	Creates a session with the given session number and places you in monitor configuration mode to further configure the session.
Step 4	switch(config-monitor)# **description** *description*	Adds a description for the specified SPAN session. The *description* can be up to 32 alphanumeric characters. The default is blank (no description)

Step 5	switch(config-monitor)# **source** {**interface** {*type*} {*id*} | **vlan** {*id* | *range*} | **port-profile** {*name*}} [**rx** | **tx** | **both**]	For the specified session, configures the sources and the direction of traffic to monitor.
		• For the *type* argument, specify the interface type—Ethernet or vEthernet.
		• For the *id* argument, specify the vEthernet number, the Ethernet slot/port, or the VLAN ID to monitor.
		• For the *range* argument, specify the VLAN range to monitor.
		• For the *name* argument, specify the name of the existing port profile. This port profile is different from the port profile created to carry ERSPAN packets through the IP network as defined in the Configuring an ERSPAN Port Profile, on page 77.
		• For the **traffic direction** keywords, specify as follows:
		  • **rx** is the VLAN default indicates receive.
		  • **tx** indicates transmit.
		  • **both** is the default keyword.

	Command or Action	Purpose
Step 6	(Optional) Repeat Step 5 to configure additional SPAN sources.	
Step 7	(Optional) switch(config-monitor)# **filter vlan** {*id* | *range*}	For the specified SPAN session, configures the filter from among the source VLANs.
Step 8	(Optional) Repeat Step 7 to configure all source VLANs to filter.	
Step 9	switch(config-monitor)# **destination** {**interface** {*type*} {*id* | *range*} | **port-profile** {*name*}}	For the specified SPAN session, configures the destination(s) for copied source packets. • For the *type* argument, specify the interface type—Ethernet or vEthernet. • For the *id* argument, specify the vEthernet number or the Ethernet slot/port to monitor. • For the *name* argument specify the name of the port profile to monitor.
Step 10	(Optional) Repeat Step 9 to configure all SPAN destination ports.	
Step 11	switch(config-monitor)# **no shut**	Enables the SPAN session. By default, the session is created in the shut state.
Step 12	(Optional) switch(config-monitor)# **exit**	Exits monitor configuration mode and enters interface configuration mode.
Step 13	(Optional) switch(config-if)# **show monitor session** *session-number*	Displays the configured monitor session.
Step 14	switch(config-if)# **show interface** {*type*} {*id*} **switchport**	Displays the configured port including allowed VLANs. • For the *type* argument, specify the interface type—Ethernet or vEthernet. • For the *id* argument, specify the vEthernet number or the Ethernet slot/port to monitor.
Step 15	(Optional) switch(config-if)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to configure a local SPAN session:

```
switch# configure terminal
switch(config)# no monitor session 3
switch(config)# monitor session 3
switch(config-monitor)# description my_span_session_3
switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-monitor)# filter vlan 3-5, 7
switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config-if)# show monitor session 3
switch(config-if)# show interface ethernet 2/5 switchport
switch(config-if)# copy running-config startup-config
```

Configuring an ERSPAN Port Profile

You can configure a port profile on the VSM to carry ERSPAN packets through the IP network to a remote destination analyzer.

You must complete this configuration for all hosts in vCenter Server.

The ERSPAN configuration requires a Layer 3 capable port profile. To configure this feature in a Layer 2 mode, you must configure the Layer 3 capable port profile as described in this section. However, if you configure this feature in a Layer 3 mode, you must use the existing Layer 3 capable port profile.

This procedure includes steps to configure the port profile for the following requirements:

- ERSPAN for Layer 3 control.
- An access port profile. It cannot be a trunk port profile.

Only one vMKNIC can be assigned to this Layer 3 control port profile per host as follows:

- If more than one vMKNIC is assigned to a host, the first one assigned takes effect. The second one is not considered a Layer 3 control vMKNIC.
- If more than one vMKNIC is assigned to a host, and you remove the second assigned one, the VSE does not use the first assigned one. Instead, you must remove both vMKNICs and then add one back.

Note Ensure that the IP subnet assigned to a vMKNIC does not interfere with the existing connectivity between the host and the vCenter.

Before you begin

- Log in to the CLI in EXEC mode
- Establish the name to be used for this port profile

Note The port profile name is used to configure the VM Kernal NIC (vMKNIC). A vMKNIC is required on each ESX host to send ERSPAN-encapsulated IP packets. It must have IP connectivity to the ERSPAN destination IP address.

- Establish the name of the VMware port group to which this profile maps.
- Create the system VLAN that sends IP traffic to the ERSPAN destination; and you know the VLAN ID that will be used in this configuration.
- Obtain the VMware documentation for adding a new virtual adapter.

Note To ensure that VSM-VSE control communication messages are not dropped, we recommend that you configure the Quality of Service (QoS) queuing feature on the uplink interface to which the vMKNIC with capability Layer 3 capable control is mapped.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** *port_profile_name*	Creates the port profile and enters global configuration mode for the specified port profile. This command saves the port profile in the running configuration. The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000VE.
Step 3	switch(config-prot-prof)# **capability l3control**	Configures the port profile to carry ERSPAN traffic and saves the port profile in the running configuration.
Step 4	switch(config-prot-prof)# **vmware port-group** *name*	Designates the port profile as a VMware port group and adds the name of the VMware port group to which this profile maps. This command saves the settings in the running configuration. The port profile is mapped to a VMware port group of the same name. When a vCenter Server connection is established, the port group created in the Cisco Nexus 1000VE is then distributed to the virtual switch on the vCenter Server. The *name* argument is the same as the port profile name if you do not specify a port group name. If you want to map the port profile to a different port group name, use the name option followed by the alternate name.
Step 5	switch(config-prot-prof)# **switchport mode access**	Designates the interfaces as switch access ports (the default).

	Command or Action	Purpose
Step 6	switch(config-prot-prof)# **switchport access vlan** *id*	Assigns a VLAN ID to the access port for this port profile and saves the setting in the running configuration. This VLAN is used to send IP traffic to the ERSPAN destination.
Step 7	switch(config-prot-prof)# **no shutdown**	Enables the interface in the running configuration.
Step 8	switch(config-prot-prof)# **system vlan** *id*	Associates the system VLAN ID with the port profile and saves it in the running configuration. The ID must match the VLAN ID that is assigned to the access port. If it does not match, the following error message is generated: `ERROR: System vlan being set does not match the switchport access vlan 2`
Step 9	switch(config-prot-prof)# **state enabled**	Enables the port profile in the running configuration. This port profile is now ready to send out ERSPAN packets on all ESX hosts with ERSPAN sources.
Step 10	(Optional) switch(config-prot-prof)# **show port-profile name** *port_profile_name*	Displays the configuration for the specified port profile as it exists in the running configuration.
Step 11	(Optional) switch(config-port-prof)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.
Step 12	Using the VMware documentation, go to vSphere Client and configure a vMKNIC on each ESX host for sending ERSPAN-encapsulated packets. Make sure that the vMKNIC points to this port profile as a new virtual adapter. This vMKNIC must have IP connectivity to the ERSPAN destination IP address.	—

Example

This example show how to configure a port profile on the VSM:

```
switch# configure terminal
switch(config)# port-profile erspan_profile
switch(config-port-prof)# capability l3control
```

```
switch(config-port-prof)# vmware port-group erspan
switch(config-port-prof)# switchport mode access
switch(config-port-prof)# switchport access vlan 2
switch(config-port-prof)# no shutdown
switch(config-port-prof)# system vlan 2
switch(config-port-prof)# state enabled
switch(config-port-prof)# show port-profile name erspan
port-profile erspan
  description:
  status: enabled
  capability uplink: no
  capability l3control: yes
  system vlans: 2
  port-group: access
  max-ports: 32
  inherit:
  config attributes:
    switchport access vlan 2
    no shutdown
  evaluated config attributes:
    switchport access vlan 2
    no shutdown
  assigned interfaces:
n1000v(config-port-prof)# copy running-config startup-config
```

Configuring an ERSPAN Session

This procedure involves creating the SPAN session in ERSPAN source configuration mode (config-erspan-source).

SPAN sessions are created in the shut state by default.

When you create a SPAN session that already exists, any additional configuration is added to that session. To make sure the session is cleared of any previous configuration, you can delete the session first.

Before you begin

- Log in to the CLI in EXEC mode
- Obtain the number of the SPAN session that you are going to configure
- Configure an ERSPAN-capable port profile on the VSM
- Using the VMware documentation for adding a new virtual adapter, configure the required vMKNIC on each ESX host. The vMKNIC must have IP connectivity to the ERSPAN destination IP address for sending ERSPAN-encapsulated packets.
- ERSPAN traffic uses GRE encapsulation. If there are firewalls between the ERSPAN source and destinations, we recommend that you set a rule to allow GRE traffic. This traffic could be identified by IP protocol number 47.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# **no monitor session** *session-number*	Clears the specified session.
Step 3	switch(config)# **monitor session** *session-number* **type erspan-source**	Creates a session with the given session number and places you in ERSPAN source configuration mode. This configuration is saved in the running configuration.
Step 4	switch(config-erspan-src)# **description** *description*	For the specified ERSPAN session, adds a description and saves it in the running configuration. The *description* can be up to 32 alphanumeric characters The default is blank (no description)
Step 5	switch(config-erspan-src)# **source** {**interface** *type* {*number*| *range*} | **vlan** {*number* | *range*} | **port-profile** {*name*}} [**rx** | **tx** | **both**]	For the specified session, configures the sources and the direction of traffic to monitor and saves them in the running configuration. • For the *type* argument, specify the interface type—ethernet, port-channel, vethernet. • For the *number* argument, specify the interface slot/port or range, or the VLAN number or range to monitor. • For the *name* argument, specify the name of the existing port profile. • For the traffic direction keywords, specify as follows: • **rx**— is the VLAN default that indicates receive. • **tx**— indicates transmit. • **both**—is the default keyword.
Step 6	(Optional) Repeat Step 5 to configure additional ERSPAN sources.	
Step 7	(Optional) switch(config-erspan-src)# **filter vlan** {*number* | *range*}	For the specified ERSPAN session, configures the VLANs, VLAN lists, or VLAN ranges to be monitored; and saves the VLAN arguments to the running configuration. On the monitor port, only the traffic from the VLANs that match the VLAN filter list are replicated to the destination.

	Command or Action	Purpose
Step 8	(Optional) Repeat Step 7 to configure all source VLANs to filter.	
Step 9	switch(config-erspan-src)# **destination ip** *ip_address*	Configures the IP address of the host to which the encapsulated traffic is sent in this monitor session and saves it in the running configuration.
Step 10	(Optional) switch(config-erspan-src)# **ip ttl** *ttl_value*	Specifies the IP time-to-live value, from 1 to 255, for ERSPAN packets in this monitor session and saves it in the running configuration.
Step 11	(Optional) switch(config-erspan-src)# **ip prec** *precedence_value*	Specifies the IP precedence value, from 0 to 7, for the ERSPAN packets in this monitor session and saves it in the running configuration. The default value is 0.
Step 12	(Optional) switch(config-erspan-src)# **ip dscp** *dscp_value*	Specifies the IP DSCP value, from 0 to 63. for the ERSPAN packets in this monitor session and saves it in the running configuration. The default is 0.
Step 13	(Optional) switch(config-erspan-src)# **mtu** *mtu_value*	Specifies an MTU size (from 50 to 9000) for ERSPAN packets in this monitor session and saves it in the running configuration. The 1500 MTU size limit includes a 50 byte overhead added to monitored packets by ERSPAN. Packets larger than this size are truncated. The default is 1500. **Note** If the ERSPAN destination is a Cisco 6500 Series switch, truncated ERSPAN packets are dropped unless the **no mls verify ip length consistent** command is configured on the Switch.
Step 14	switch(config-erspan-src)# **header-type** *value*	Specifies the ERSPAN header type (2 or 3) used for ERSPAN encapsulation for this monitor session as follows: • 2 is the ERPSPANv2 header type (the default) • 3 is the ERSPANv3 header type (used with NAM setups. Any other type of destination works only with the default v2 headers.)

	Command or Action	Purpose
Step 15	switch(config-erspan-src)# **erspan-id** *flow_id*	Adds an ERSPAN ID from 1 to 1023) to the session configuration and saves it in the running configuration. The session ERSPAN ID is added to the ERSPAN header of the encapsulated frame and can be used at the termination box to differentiate between various ERSPAN streams of traffic.
Step 16	switch(config-erspan-src)# **no shut**	Enables the ERSPAN session and saves it in the running configuration. By default, the session is created in the shut state.
Step 17	(Optional) switch(config-erspan-src)# **show monitor session** *session_id*	Displays the ERSPAN session configuration as it exists in the running configuration.
Step 18	(Optional) switch(config-erspan-src)# **copy running-config startup-config**	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Example

This example shows how to configure a SPAN session:

```
switch# configure terminal
switch(config)# no monitor session 3
switch(config)# monitor session 3 type erspan
switch(config-erspan-src)# description my_erspan_session_3
switch(config-erspan-src)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-erspan-src)# filter vlan 3-5, 7
switch(config-erspan-src)# destination ip 10.54.54.1
switch(config-erspan-src)# ip ttl 64
switch(config-erspan-src)# ip prec 1
switch(config-erspan-src)# ip dscp 24
switch(config-erspan-src)# mtu 1000
switch(config-erspan-src)# header-type 2
switch(config-erspan-src)# erspan-id 51
switch(config-erspan-src)# no shut
switch(config-erspan-src)# show monitor session 3
switch(config-erspan-src)# copy running-config startup-config
```

Shutting Down a SPAN Session from Global Configuration Mode

Before you begin

- Log in to the CLI in EXEC mode.
- Determine which session you want to shut down.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **monitor session** {*session-number* | *session-range* | **all**} **shut**	Shuts down the specified SPAN monitor session(s) from global configuration mode. • The *session-number* argument specifies a particular SPAN session number. • The *session-range* argument specifies a range of SPAN sessions from 1 to 64. • The **all** keyword specifies all SPAN monitor sessions.
Step 3	(Optional) switch(config)# **show monitor**	Displays the status of the SPAN sessions.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Example

This example shows how to shut down a SPAN session:

```
switch# configure terminal
switch(config)# monitor session 3 shut
switch(config)# show monitor
switch(config)# copy running-config startup-config
```

Shutting Down a SPAN Session from Monitor Configuration Mode

Before you begin

- Log in to the CLI in EXEC mode.
- Determine which session you want to shut down.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **monitor session** {*session-number* | *session-range* | **all**} **[type erspan-source]**	Specifies the SPAN monitor session(s)) you want to shut down from monitor-configuration mode. • The *session-number* argument specifies a particular SPAN session number.

	Command or Action	Purpose
		• The *session-range* argument specifies a range of SPAN sessions from 1 to 64. • The **all** keyword specifies all SPAN monitor sessions.
Step 3	switch(config)# **shut**	Shuts down the specified SPAN monitor session(s) from monitor configuration mode.
Step 4	(Optional) switch(config-monitor)# **show monitor**	Displays the status of the SPAN sessions.
Step 5	(Optional) switch(config-monitor)# **copy running-config startup-config**	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Example

This example shows how to shut down a SPAN session:

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# shut
switch(config-monitor)# show monitor
switch(config-monitor)# copy running-config startup-config
```

Resuming a SPAN Session from Global Configuration Mode

You can discontinue copying packets from one source and destination and then resume from another source and destination in global configuration mode.

Before you begin

- Log in to the CLI in EXEC mode.
- Determine which SPAN session that you want to configure.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# [**no**] **monitor session** {*session-number* | *session-range* | **all**} **shut**	Shuts down the specified SPAN monitor session(s) from global configuration mode. • The *session-number* argument specifies a particular SPAN session number. • The *session-range* argument specifies a range of SPAN sessions from 1 to 64.

	Command or Action	Purpose
		• The **all** keyword specifies all SPAN monitor sessions.
Step 3	(Optional) switch(config)# **show monitor**	Displays the status of the SPAN sessions.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Example

This example shows how to resume a SPAN configuration using the global configuration mode:

```
switch# configure terminal
switch(config)# no monitor session 3 shut
switch(config)# show monitor
switch(config)# copy running-config startup-config
```

Resuming a SPAN Session from Monitor Configuration Mode

You can discontinue copying packets from one source and destination and then resume from another source and destination in monitor configuration mode.

Before you begin

- Log in to the CLI in EXEC mode.
- Determine which SPAN session that you want to configure.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# [**no**] **monitor session** {*session-number* | *session-range* | **all**} **shut**	Shuts down the specified SPAN monitor session(s) from monitor configuration mode. • The *session-number* argument specifies a particular SPAN session number. • The *session-range* argument specifies a range of SPAN sessions from 1 to 64. • The **all** keyword specifies all SPAN monitor sessions.
Step 3	(Optional) switch(config-monitor)# **show monitor**	Displays the status of the SPAN sessions.

	Command or Action	Purpose
Step 4	(Optional) switch(config-monitor)# **show monitor session** *session-id*	Displays the detailed configuration and status of a specific SPAN session for verification.
Step 5	(Optional) switch(config-monitor)# **copy running-config startup-config**	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Example

This example shows how to resume a SPAN configuration using the monitor configuration mode:

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# no shut
switch(config-monitor)# show monitor
switch(config-monitor)# show monitor session 3
switch(config-monitor)# copy running-config startup-config
```

Configuring the Allowable ERSPAN Flow IDs

Restrict the allowable range of available flow IDs that can be assigned to ERSPAN sessions

The available ERSPAN flow IDs are from 1 to 1023.

Before you begin

- Log in to the CLI in EXEC mode.
- Determine the restricted range of ERSPAN flow IDs that you want to designate.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# [**no**] **limit-resource erspan-flow-id minimum** *min_val* **maximum** *max_va*l	Restricts the allowable range of ERSPAN flow IDs that can be assigned. The allowable range is from 1 to 1023. The defaults are as follows: The minimum value is 1 The maximum value is 1023 The **no** form of this command removes any configured values and restores default values.
Step 3	(Optional) switch(config)# **show running monitor**	Displays changes to the default limit-resource erspan-flow-id values for verification

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

Example

This example shows how to configure a designated ERSPAN flow ID:

```
switch# configure terminal
switch(config)# limit-resource erspan-flow-id minimum 20 maximum 40
switch(config)# show monitor
switch(config)# show running monitor
switch(config)# copy running-config startup-config
```

Verifying the SPAN Configuration

Use one of the following commands to verify the configuration:

Command	Purpose
show monitor session {**all** | *session-number* | **range** *session-range*} [**brief**]	Displays the SPAN session configuration.
show monitor	Displays Ethernet SPAN information.
module vse *module-number* **execute vemcmd show span**	Displays the configured SPAN sessions on a VSE module.
show port-profile name *port_profile_name*	Displays a port profile.

Configuration Example for an ERSPAN Session

This example shows how to create an ERSPAN session for a source Ethernet interface and destination IP address on the Cisco Nexus 1000VE. Packets arriving at the destination IP are identified by the ID 999 in their header.

```
switch# monitor session 2 type erspan-source
switch(config-erspan-src)# source interface ethernet eth3/1
switch(config-erspan-src)# source port-profile my_profile_src
switch(config-erspan-src)# destination ip 10.54.54.1
switch(config-erspan-src)# erspan-id 999
switch(config-erspan-src)# mtu 1000
switch(config-erspan-src)# no shut

switch(config-erspan-src)# show monitor session 2
   session 2
---------------
type              : erspan-source
state             : up
source intf       :
```

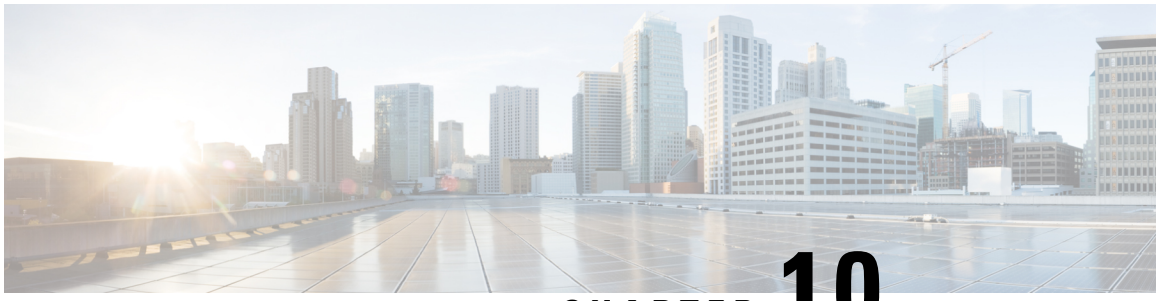
```
    rx            : Eth3/3
    tx            : Eth3/3
    both          : Eth3/3
source VLANs      :
    rx            :
    tx            :
    both          :
source port-profile :
    rx            : my_profile_src
    tx            : my_profile_src
    both          : my_profile_src
filter VLANs      : filter not specified
destination IP    : 10.54.54.1
ERSPAN ID         : 999
ERSPAN TTL        : 64
ERSPAN IP Prec.   : 0
ERSPAN DSCP       : 0
ERSPAN MTU        : 1000
ERSPAN Header Type: 2

switch(config-erspan-src)# module vse 3 execute vemcmd show span

VSE SOURCE IP: 10.54.54.10

HW SSN ID   ERSPAN ID   HDR VER   DST LTL/IP
        1                 local   49,51,52,55,56
        2         999         2   10.54.54.1
```

Example of Configuring a SPAN Session

This example shows how to create a SPAN session for a source ethernet interface and destination IP address on the Cisco Nexus 1000VE:

```
 switch(config)# no monitor session 1
switch(config)# monitor session 1
  switch(config-monitor)# source interface ethernet 2/1-3
  switch(config-monitor)# source interface eth2/1
  switch(config-monitor)# source port-profile my_profile_src
  switch(config-monitor)# source vlan 3, 6-8 tx
  switch(config-monitor)# filter vlan 3-5, 7
  switch(config-monitor)# destination interface ethernet 2/5
  switch(config-monitor)# destination port-profile my_profile_dst
  switch(config-monitor)# no shut
  switch(config-monitor)# exit
switch(config)# show monitor session 1
switch(config)# copy running-config startup-config

switch(config)# show monitor session 1
   session 1
---------------
type              : local
state             : up
source intf       :
    rx            : Eth2/1
    tx            : Eth2/1
    both          : Eth2/1
source VLANs      :
    rx            :
    tx            : 3,6,7,8
    both          :
source port-profile :
```

```
    rx            : my_profile_src
    tx            : my_profile_src
    both          : my_profile_src
filter VLANs      : 3,4,5,7
destination ports : Eth3/1
destination port-profile : my_profile_dst

switch# module vse 3 execute vemcmd show span

VSE SOURCE IP NOT CONFIGURED.

HW SSN ID   ERSPAN ID   HDR VER   DST LTL/IP
        1                 local   49,51,52,55,56
```



CHAPTER 10

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 supports IPv4 addresses.

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.

Note noAuthnoPriv is not supported in SNMPv3.

The following table lists identifies the combinations of security models and level information.

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	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 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 cleartext, 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. After user authentication is verified, the SNMP PDUs are processed. 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 NX-OS synchronizes a 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 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. For information about how to modify this default value, see Modifying the AAA Synchronization Time, on page 106.

Group-Based SNMP Access

Note Because group is a standard SNMP term used industry-wide, roles are referred 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 interval 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

Log 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 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 the HMAC MD5 algorithm for authentication. It is optional. The **sha** keyword specifies the 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 the 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	(Optional) switch(config-callhome)# **show snmp user**	Displays information about one or more SNMP users.
Step 4	(Optional) switch(config-callhome)# **copy running-config startup-config**	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Example

This example shows how to configure a SNMP user:

```
switch(config)# configure terminal
switch(config)# snmp-server user Admin auth sha Axlm1234# priv Axlm1234#
switch(config)# show snmp user
_____________________________________________________________________
SNMP USERS
_____________________________________________________________________
User Auth Priv(enforce) Groups
____ ____ _____________ ______
Admin sha des(no) network-operator
admin md5 des(no) network-admin
_____________________________________________________________________
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
_____________________________________________________________________
User Auth Priv
____ ____ ____
switch(config)#
```

Enforcing SNMP Message Encryption for All Users

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **snmp-server globalEnforcePriv**	Enforces SNMP message encryption for all users.

Example

This example shows how to enforce the SNMP message encryption:

```
switch# configure terminal
switch(config)# snmp-server galobalEnforcePriv
switch(config)# show snmp user
_____________________________________________________________________
SNMP USERS [global privacy flag enabled]
_____________________________________________________________________

User                          Auth  Priv(enforce) Groups
____                          ____  _____________ ______
Admin                         sha   des(no)       network-operator

admin                         md5   des(no)       network-admin

_____________________________________________________________________
 NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________________

User                          Auth  Priv
____                          ____  ____
switch(config)#
```

Creating SNMP Communities

You can create SNMP communities for SNMPv1 or SNMPv2c.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **snmp-server community** *name* {**ro** | **rw**}	Creates an SNMP community string.

Example

This example shows how to create an SNMP community:

```
switch# configure terminal
switch(config)# snmp-server community public ro
switch(config)# show snmp community
Community Group / Access context acl_filter
------------------------------ -------------- ------- ----------
public network-operator
switch(config)#
```

Filtering SNMP Requests

You can assign an access list (ACL) to a community to filter incoming SNMP requests. If the assigned ACL allows the incoming request packet, SNMP processes the request. If the ACL denies the request, SNMP drops the request and sends a system message. The ACL applies to IPv4 and IPv6 over UDP and TCP. After creating the ACL, assign the ACL to the SNMP community. For more information on creating ACLs, see the *Cisco Nexus 1000VE for VMware Security Configuration Guide*.

Before you begin

Create an ACL to assign to the SNMP community. Assign the ACL to the SNMP community. Create the ACL with the following parameters:

- Source IP address
- Destination IP address
- Source Port
- Destination Port
- Protocol (UDP or TCP)

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch(config-callhome)# **snmp-server community** *community-name* **use-acl** *acl-name*	Assigns an ACL to an SNMP community to filter SNMP requests.
Step 3	switch(config-callhome)# {**ip** | **ipv6**} **access-list acl_for_community**	Configures an IP ACL.
Step 4	switch(config-callhome)# **statistics per-entry**	Configures statistics.
Step 5	switch(config-callhome)# **permit udp any any**	Permits UDP protocol.
Step 6	(Optional) switch(config-callhome)# **show** {**ip** | **ipv6**} **access-lists**	Displays **show** command output.
Step 7	switch(config-callhome)# **snmp-server community public use-acl acl_for_community**	Configures SNMP community.
Step 8	(Optional) switch(config-callhome)# **showsnmp community**	Displays **show** command output.

Example

This example shows how to filter SNMP requests:

```
switch# configure terminal
switch(config)# show ip access-lists
IPV4 ACL acl_for_community
statistics per-entry
10 permit udp any any
switch(config)# show snmp community
Community Group / Access context acl_filter
------------------------------ -------------- ------- ----------
public network-operator acl_for_community
```

Configuring SNMP Notification Receivers

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. You can specify an IPv4 or IPv6 address. The community can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

Example

```
switch(config)# snmp-server host 192.0.2.1 traps version 1 public
switch(config)# show snmp host
-------------------------------------------------------------------
Host                            Port Version  Level  Type   SecName

-------------------------------------------------------------------
192.0.2.1                       162  v1       noauth trap   public

-------------------------------------------------------------------
switch(config)#
```

Configuring a Host Receiver for SNMPv2c Traps or Informs

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **snmp-server host** *ip-address* {**traps** | **informs**} **version 2c** *community* [**udp_port** *number*]	Configures a host receiver for SNMPv2c traps or informs. You can specify an IPv4 or IPv6 address. The community can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

Example

```
switch# configure terminal
switch(config)# snmp-server host 192.0.2.1 informs version 2c public
switch(config)# show snmp host
-------------------------------------------------------------------
Host                            Port Version  Level  Type   SecName

-------------------------------------------------------------------
192.0.2.1                       162  v2c      noauth inform public

-------------------------------------------------------------------
switch(config)#
```

Configuring a Host Receiver for SNMPv3 Traps or Informs

Note The SNMP manager must know the user credentials (authKey/PrivKey) based on the SNMP engine ID of the Cisco Nexus 1000VE device to authenticate and decrypt the SNMPv3 messages

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **snmp-server host** *ip-address* {**traps** | **informs**} **version 3** {**auth** | **noauth** | **priv**} *username* [**udp_port** *number*]	Configures a host receiver for SNMPv2c traps or informs. You can specify an IPv4 or IPv6 address. The username can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

Example

This example shows how to configure a host receiver:

```
switch# configure terminal
switch# configure terminal
switch(config)# snmp-server host 192.0.2.1 informs version 3 auth Admin
switch(config)# show snmp host
-------------------------------------------------------------------
Host Port Version Level Type SecName
-------------------------------------------------------------------
192.0.2.1 162 v3 auth inform Admin
-------------------------------------------------------------------
switch(config)#
```

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

The Cisco NX-OS 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 NX-OS to authenticate and decrypt the informs.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	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.

Example

This example shows how to configure a notification target user:

```
switch# configure terminal
switch(config)# snmp-server user Admin auth sha Axlm1234# priv Axlm1234#
engineID 00:00:00:63:00:01:00:10:20:15:10:03
switch(config)# show snmp user
_____________________________________________________________________
SNMP USERS [global privacy flag enabled]
_____________________________________________________________________
User Auth Priv(enforce) Groups
____ ____ _____________ ______
admin md5 des(no) network-admin
_____________________________________________________________________
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
_____________________________________________________________________
User Auth Priv
____ ____ ____
Admin sha des
(EngineID 0:0:0:63:0:1:0:10:20:15:10:3)
switch(config)#
```

Enabling SNMP Notifications

You can enable or disable notifications. If you do not specify a notification name, Cisco NX-OS enables all notifications.

The following table lists the commands that enable the notifications for Cisco NX-OS 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**
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**
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.

Procedure

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

Example

This example displays how to enable SNMP notifications:

```
switch# configure terminal
switch(config)# snmp-server enable traps
switch(config)# snmp-server enable traps aaa
switch(config)# snmp-server enable traps entity
switch(config)# snmp-server enable traps license
switch(config)# snmp-server enable traps link
switch(config)# snmp-server enable traps snmp
```

Disabling LinkUp/LinkDown Notifications on an Interface

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config-if)# **no snmp trap link-status**	Disables SNMP link-state traps for the interface. This command is enabled by default.

Example

```
switch# show running-config interface vethernet 1
interface Vethernet1
inherit port-profile
dynpp_d50369db-2fed-405d-ad84-a6bf89718d2c_f006e797-da04-4f29-9a0f-901294bc8b8f
```

```
description TEST, Network Adapter
dvport uuid "70D66D72-CDD9-4B68-9596-27E8F8E06F6D--0"
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface vethernet 1
switch(config-if)# no snmp trap link-status
switch(config-if)# show running-config interface vethernet 1
interface Vethernet1
inherit port-profile
dynpp_d50369db-2fed-405d-ad84-a6bf89718d2c_f006e797-da04-4f29-9a0f-901294bc8b8f
description TEST, Network Adapter
dvport uuid "70D66D72-CDD9-4B68-9596-27E8F8E06F6D--0"
no snmp trap link-status
```

Enabling a One-time Authentication for SNMP over TCP

Before you begin

You must be in global configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **snmp-server tcp-session** [**auth**]	Enables a one-time authentication for SNMP over a TCP session. The default is disabled.

Example

This example shows how to enable a one -time authentication:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server tcp-session
switch(config)# show snmp | grep "Tcp"
SNMP Tcp Authentication Flag : Enabled.
switch(config)#
```

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

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

Example

This example show how to assign information on the SNMP switch contact and location:

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

Disabling SNMP

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **no snmp-server protocol enable**	Disables the SNMP protocol. This command is enabled by default.

Example

This example shows how to disable the SNMP protocol:

```
switch# configure terminal
switch(config)# no snmp-server protocol enable
switch(config)# show snmp | grep protocol
SNMP protocol : Disabled
switch(config)#
```

Modifying the AAA Synchronization Time

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	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.

Example

This example shows how to modify the AAA synchronization time:

```
switch# configure terminal
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 interface snmp-ifindex	Displays the SNMP ifIndex value for all interfaces (from IF-MIB).
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.
show snmp trap	Displays the SNMP notifications that are enabled or disabled.
show snmp user	Displays SNMPv3 users.
show snmp host	Displays information about configured SNMP hosts.

Configuration Example for SNMP

This example shows how to configure Cisco NX-OS to send linkUp/Down notifications to one notification host receiver.

```
switch(config)# snmp-server user Admin auth sha Axlm1234# priv Axlm1234#
switch(config)# snmp-server host 192.0.2.1 traps version 3 priv Admin
switch(config)# snmp-server enable traps link
switch(config)# show snmp user

_______________________________________________________________________
SNMP USERS [global privacy flag enabled]

_______________________________________________________________________
User Auth Priv(enforce) Groups

____ ____ _____________ ______
Admin sha des(no) network-operator
admin md5 des(no) network-admin

_______________________________________________________________________
NOTIFICATION TARGET USERS (configured for sending V3 Inform)

_______________________________________________________________________
User Auth Priv

____ ____ ____
switch(config)# show snmp host
-------------------------------------------------------------------
Host Port Version Level Type SecName
-------------------------------------------------------------------
192.0.2.1 162 v3 priv trap Admin
-------------------------------------------------------------------
switch(config)# show snmp trap | grep link
link : linkDown Yes
link : linkUp Yes
link : extended-linkDown Yes
link : extended-linkUp Yes
link : cieLinkDown Yes
link : cieLinkUp Yes
link : cisco-xcvr-mon-status-chg Yes
switch(config)#
```

MIBs

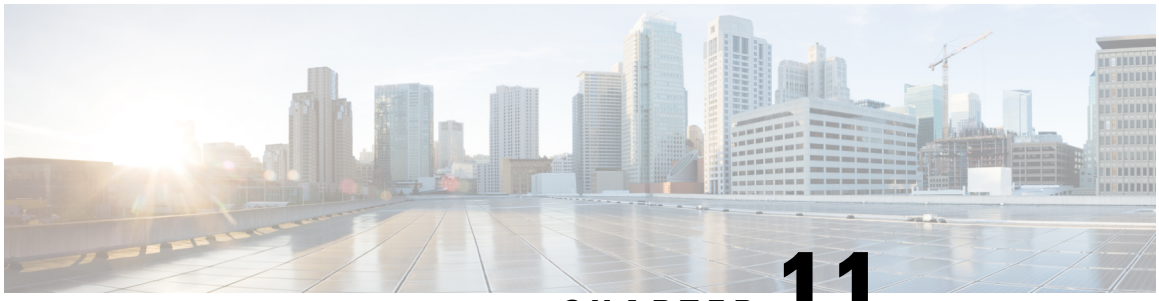
The supported SNMP MIBs are listed in this section.

To locate and download the MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

- IF-MIB
- ENTITY-MIB
- CISCO-ENTITY-EXT-MIB-V1SMI
- CISCO-ENTITY-FRU-CONTROL-MIB
- BRIDGE-MIB
- CISCO-FLASH-MIB
- CISCO-SYSTEM-MIB

- CISCO-SYSTEM-EXT-MIB
- CISCO-FEATURE-CONTROL-MIB
- CISCO-CDP-MIB
- CISCO-VIRTUAL-NIC-MIB
- CISCO-PROCESS-MIB
- CISCO-SYSLOG-EXT-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- TCP-MIB
- UDP-MIB
- CISCO-PRIVATE-VLAN-MIB
- CISCO-SECURE-SHELL-MIB
- CISCO-IMAGE-UPGRADE-MIB
- CISCO-LICENSE-MGR-MIB
- RMON2-MIB
- CISCO-AAA-SERVER-MIB
- CISCO-AAA-SERVER-EXT-MIB
- CISCO-COMMON-MGMT-MIB
- CISCO-COMMON-ROLES-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-FTP-CLIENT-MIB
- CISCO-IMAGE-MIB
- CISCO-LAG-MIB
- CISCO-NOTIFICATION-CONTROL-MIB
- CISCO-NTP-MIB
- CISCO-RF-MIB
- CISCO-RMON-CONFIG-MIB
- CISCO-SMI
- CISCO-SNMP-TARGET-EXT-MIB
- NOTIFICATION-LOG-MIB
- IP-MIB
- SNMP-COMMUNITY-MIB
- SNMP-FRAMEWORK-MIB

- SNMP-MPD-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-TARGET-MIB
- SNMP-USM-MIB
- SNMPv2-MIB



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 supports IPv4 and IPv6 addresses.

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
4 – warning	Warning condition
5 – notification	Normal but significant condition

Level	Description
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 the 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
cdp	CDP manager
cert-enroll	Certificate enroll daemon
cfs	CFS manager
clis	CLIS manager
cmpproxy	CMP proxy manager

Facility	Description
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
ethpm	Ethernet PM 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
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

Facility	Description
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
monitor	Ethernet SPAN 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
pixm	PIXM manager
pixmc	PIXMC manager
pktmgr	Packet manager
platform	Platform manager
pltfm_config	PLTFM configuration manager
plugin	Plug-in manager
port-channel	Port channel manager
port_client	Port client manager
port_lb	Diagnostic port loopback test manager
qengine	Q engine manager

Facility	Description
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
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 Secure Shell (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.
Step 7	(Optional) switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to configure system messages:

```
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 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**}	(Optional) Sets the logging time-stamp units. The default unit is seconds.
Step 5	switch(config)# show logging timestamp	(Optional) Displays the logging time-stamp units configured.
Step 6	(Optional) switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This 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 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

You can 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.
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	(Optional) switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This 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.

Command	Description
no logging timestamp {**microseconds** | **milliseconds** | **seconds**}	Resets the logging time-stamp unit to the default (seconds).

Configuring syslog Servers

You can 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 hostname or IPv4 or IPv6 address. You can limit logging of messages to a particular Virtual routing and forwarding (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	(Optional) switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This 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 hostname 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 that 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

You can 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.

Example

This example shows how to display 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*]	Displays the logging level
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.

This example shows how to display the console logging configuration:

```
switch# show logging console
Logging console:                disabled
switch#
```

This example shows how to display the logging configuration:

```
switch# show logging info
Logging console:                enabled (Severity: critical)
Logging monitor:                enabled (Severity: notifications)
Logging linecard:               enabled (Severity: notifications)
Logging timestamp:              Seconds
Logging server:                 disabled
Logging logfile:                enabled
        Name - g/external/messages: Severity - notifications Size - 4194304

Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     2                       2
auth                    0                       0
authpriv                3                       3
bootvar                 5                       5
callhome                2                       2
cdp                     2                       2
cert_enroll             2                       2
cfs                     3                       3
confcheck               2                       2
cron                    3                       3
daemon                  3                       3
diagclient              2                       2
diagmgr                 2                       2
eth_port_channel        5                       5
ethpm                   5                       5
evmc                    5                       5
evms                    2                       2
feature-mgr             2                       2
ftp                     3                       3
ifmgr                   5                       5
igmp_1                  3                       3
ip                      2                       2
ipv6                    2                       2
kern                    6                       6
l2fm                    2                       2
licmgr                  6                       6
local0                  3                       3
local1                  3                       3
local2                  3                       3
local3                  3                       3
local4                  3                       3
local5                  3                       3
local6                  3                       3
local7                  3                       3
lpr                     3                       3
mail                    3                       3
mfdm                    2                       2
module                  5                       5
monitor                 7                       7
msp                     2                       2
mvsh                    2                       2
news                    3                       3
ntp                     2                       2
otm                     3                       3
pblr                    2                       2
pixm                    2                       2
pixmc                   2                       2
platform                5                       5
```

```
portprofile             5                       5
private-vlan            3                       3
radius                  2                       2
res_mgr                 2                       2
rpm                     2                       2
sal                     2                       2
securityd               2                       2
sksd                    3                       3
stp                     3                       3
syslog                  3                       3
sysmgr                  3                       3
ufdm                    2                       2
urib                    3                       3
user                    3                       3
uucp                    3                       3
vdc_mgr                 6                       6
vim                     5                       5
vlan_mgr                2                       2
vms                     5                       5
vshd                    5                       5
xmlma                   3                       3

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
switch#
```

This example shows how to display the last number of lines of the log file:

```
switch# show logging last 5
2008 Jul 29 17:52:42 S22-DCOS %ETHPORT-5-IF_UP: Interface Ethernet2/5 is up in mode access
2008 Jul 29 17:52:43 S22-DCOS %ETHPORT-5-IF_UP: Interface Ethernet2/2 is up in mode trunk
2008 Jul 29 17:52:43 S22-DCOS %ETHPORT-5-IF_UP: Interface Ethernet2/4 is up in mode access
2008 Jul 29 17:53:04 S22-DCOS %SYSMGR-3-BASIC_TRACE: process_cfg_write: PID 1858 with message
 rcvd cfg_action from
sap 0x545 for vdc 1 at time 1217353984 .
2008 Jul 29 17:53:04 S22-DCOS clis[2558]: CLI-3-NVDB: Batched send failed for component:
clic
switch#
```

This example shows how to display the logging levels:

```
switch# show logging level aaa
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     2                       2

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
switch#
```

This example shows how to display the module logging configuration:

```
switch# show logging module
Logging linecard:               enabled (Severity: notifications)
switch#
```

This example shows how to display the monitor logging configuration:

```
switch# show logging monitor
Logging monitor:                enabled (Severity: errors)
switch#
```

This example shows how to display the syslog server configuration:

```
switch# show logging server
Logging server:                 enabled
{10.10.2.2}
        server severity:        debugging
        server facility:        local7
switch#
```

This example shows how to display the logging session status:

```
switch# show logging session status
Last Action Time Stamp     : Fri Nov 18 11:28:55 1910
Last Action                : Distribution Enable
Last Action Result         : Success
Last Action Failure Reason : none
switch#
```

This example shows how to display the logging status:

```
switch# show logging status
Fabric Distribute     : Enabled
Session State         : IDLE
switch#
```

This example shows how to display the logging session status:

```
switch# show logging timestamp
Logging timestamp:              Seconds
switch#
```

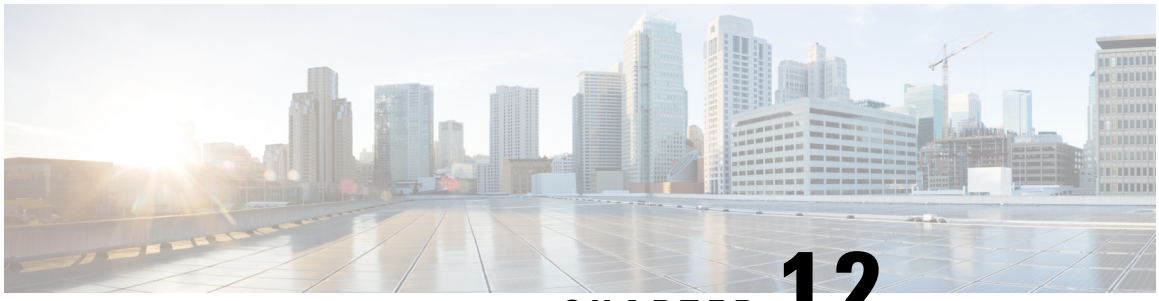
System MEssage Logging Example Configuration

The following example shows how to configure system message logging:

```
switch# configure terminal
switch(config)# logging console 3
switch(config)# logging monitor 3
switch(config)# logging logfile my_log 6
switch(config)# logging module 3
switch(config)# logging level aaa 2
switch(config)# logging timestamp milliseconds
switch(config)# logging distribute
switch(config)# logging server 172.28.254.253
switch(config)# logging server 172.28.254.254 5 local3
switch(config)# logging commit
switch(config)# copy running-config startup-config
switch(config)#
```

Feature History for System Message Logging

Feature Name	Releases	Feature Information
System Message Logging	4.0(4)SV1(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 VM is a onetime task.
- Backing up the VSM VM 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.
- It is not recommended to take VSM snapshots as this could cause unpredictable behavior in the system.

Configuring VSM Backup and Recovery

This section provides information on how to create a backup of the VSM and recover it.

Before you begin

The VSMs must be in a HA pair.

Procedure

Step 1 Open the vSphere Client.

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

Step 3 Click the **Virtual Machines** tab.

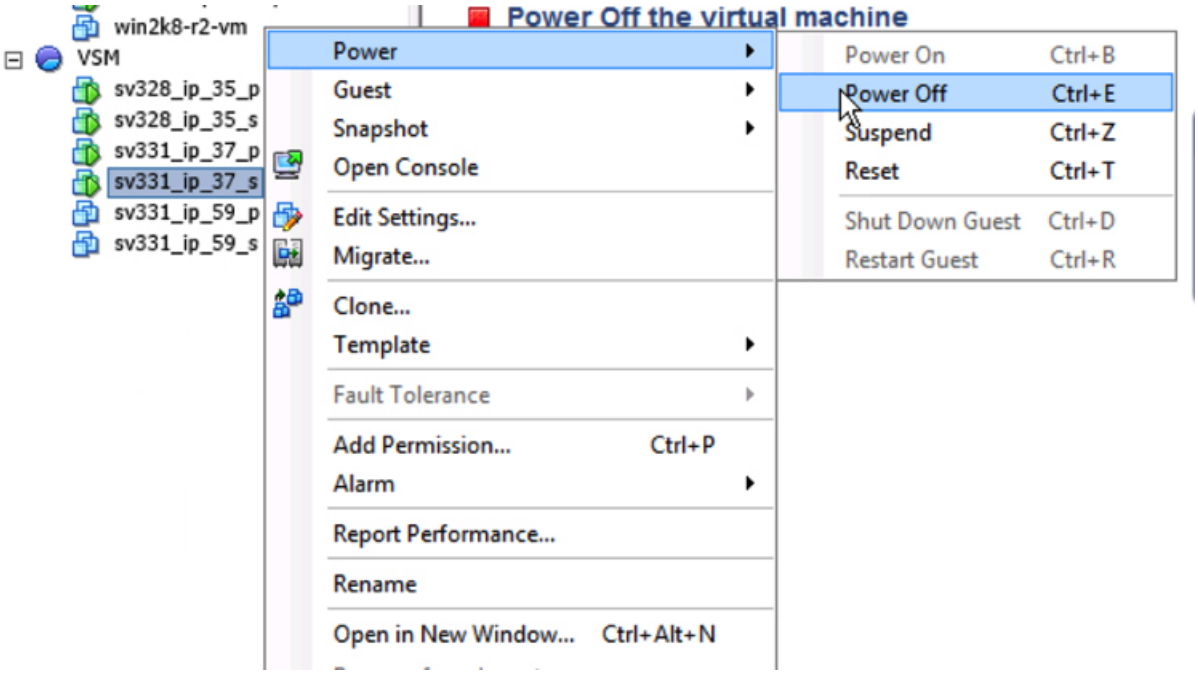
Step 4 Right-click the standby VSM and choose Edit Settings.

Step 5 In the Device Status area, uncheck the Connect at power on check box.

Step 6 Click **OK**.

The Power Off window opens.

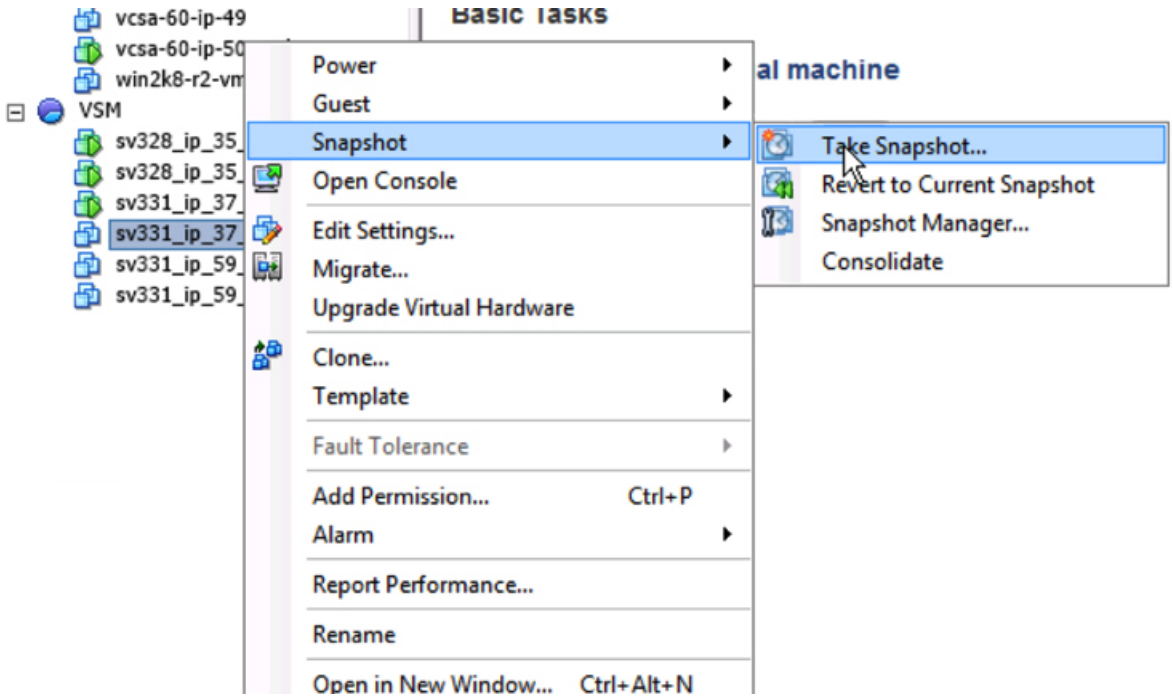
Figure 6: Guest Customization Window - Power off the Virtual Machine



Step 7 Take Snapshot of the Standby VSM.

We recommend that you do periodic backups (in the form of a snapshot after the initial backup to ensure that you have the most current configuration.

Figure 7: Guest Customization Window - Snapshot of the VSM



Step 8 Restore the VSM from the snapshot taken earlier.

Figure 8: Guest Customization Window - Restore the VSM

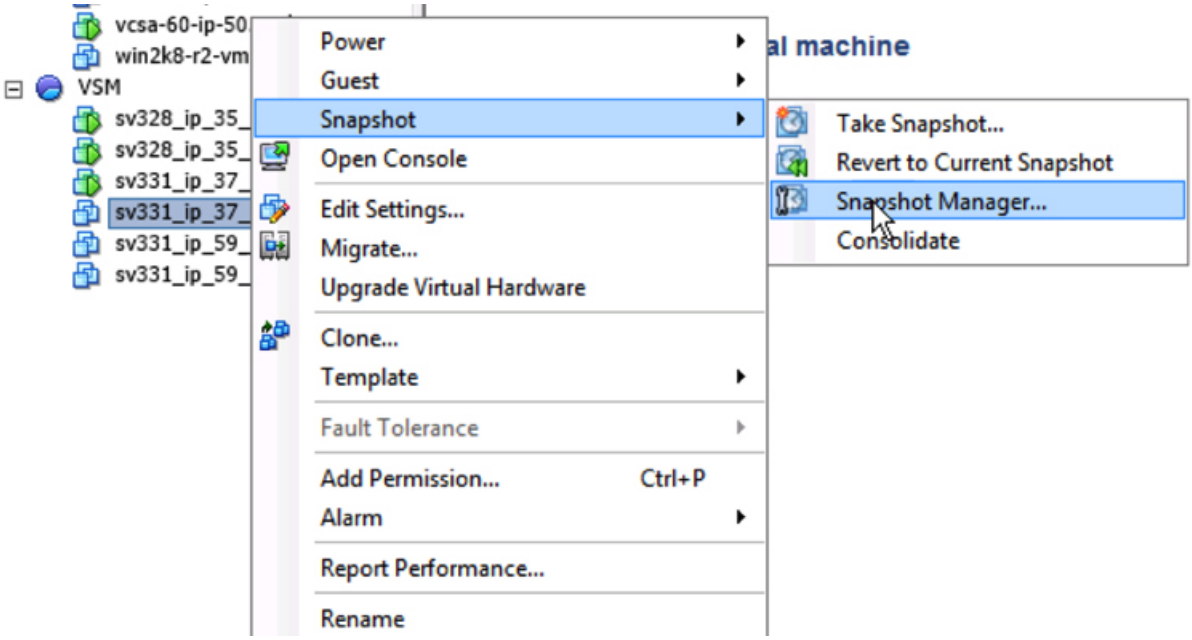
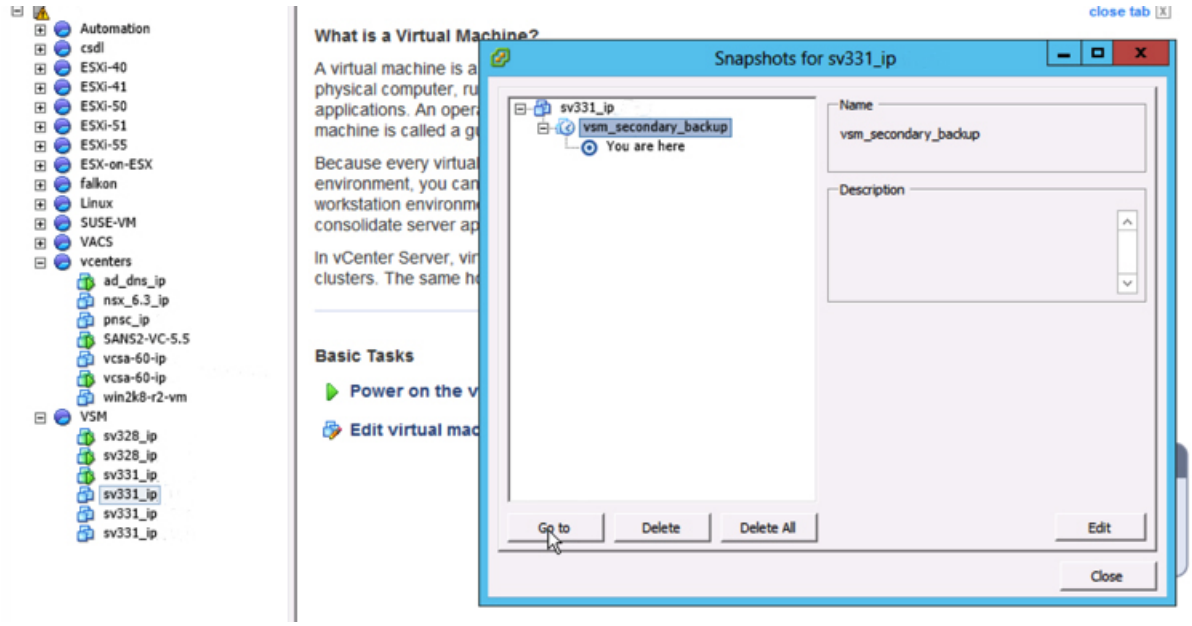
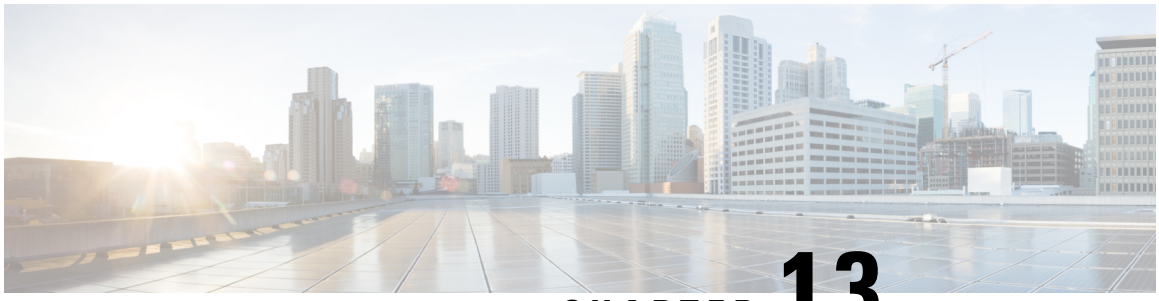


Figure 9: Guest Customization Window - Snapshot of the VSM



Step 9 Power on the newly deployed VSM.



CHAPTER 13

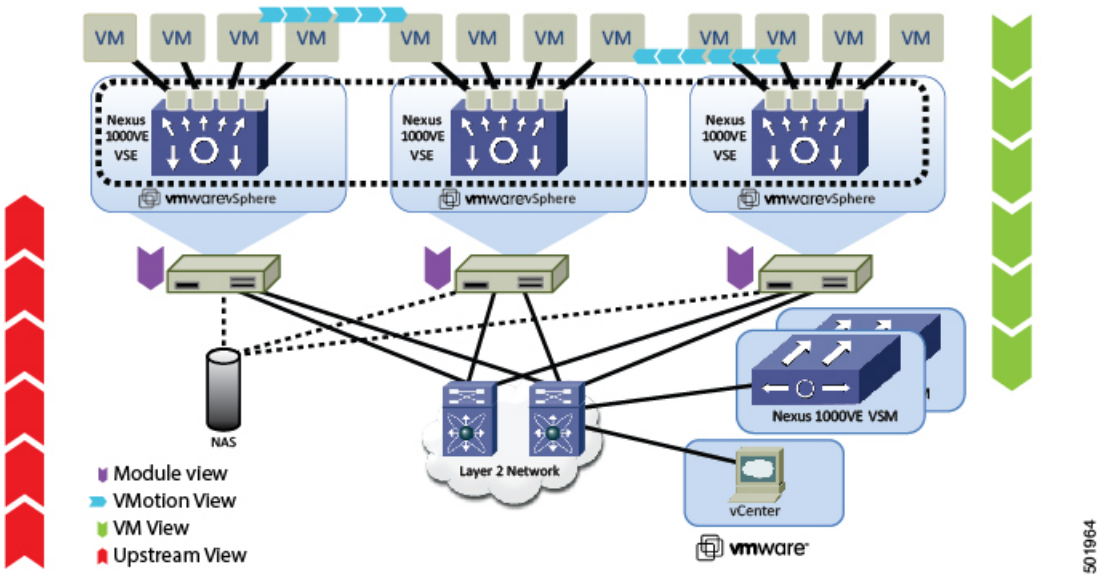
Enabling vTracker

This chapter contains the following sections:

Information About vTracker

The following illustration displays the vTracker setup diagram:

Figure 10: vTracker Setup Diagram in the Cisco Nexus 1000VE Environment



The vTracker feature on the Cisco Nexus 1000VE switch provides information about the virtual network environment. Once you enable vTracker, it becomes aware of all the modules and interfaces that are connected with the switch. vTracker provides various views that are based on the data sourced from the vCenter, the Cisco Discovery Protocol (CDP), and other related systems connected with the virtual switch. You can use vTracker to troubleshoot, monitor, and maintain the systems. Using vTracker show commands, you can access consolidated network information across the following views:

- Upstream View—Provides information on all the virtual ports connected to an upstream physical switch. The view is from top of the network to the bottom.
- VM View—Supports two sets of data:
  - VM vNIC View—Provides information about the virtual machines (VMs) that are managed by the Cisco Nexus 1000VE switch. The vNIC view is from the bottom to the top of the network.
  - VM Info View—VM Info View—Provides information about all the VMs that run on each server module.
- Module pNIC View—Provides information about the physical network interface cards (pNIC) that are connected to each Virtual Service Engine (VSE).
- VLAN View—Provides information about all the VMs that are connected to specific VLANs.
- vMotion View—Provides information about all the ongoing and previous VM migration events.

Note vTracker is available with both Essential and Advanced edition of Cisco Nexus 1000VE.

Guidelines and Limitations

vTracker has the following configuration guidelines and limitations:

- For VM and VMotion views, you should connect the Virtual Supervisor Module (VSM) with the OpenStack for the vTracker **show** commands to work.
- vTracker is disabled by default.
- While the Cisco Nexus 1000VE switch information is validated, the information sourced by vTracker from the OpenStack is not verifiable.
- All vTracker views are valid for a given time only, because the virtual environment is dynamic and constantly changing.
- In a scaled-up environment, vTracker can experience delays in retrieving real-time information, which is distributed across VSEs and OpenStack, among other components.

Default Settings for vTracker Parameters

Parameters	Default
feature vtracker	Disabled globally

Enabling vTracker Globally

- vTracker can be configured only globally, not on individual interfaces.
- By default, vTracker is disabled.

Before you begin

- You are logged in to the VSM CLI in EXEC mode or the configuration mode of any node.
- vTracker does not change any VSM configuration settings or behavior. Rather, it only tracks and displays the current configuration views.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **[no] feature vtracker**	Enables the vTracker feature. Use the **no** form of this command to disable this feature.
Step 3	(Optional) switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

The following example enables vTracker:

```
switch# configure terminal
switch(config)# feature vtracker
switch(config)# copy running-config startup-config
```

Virtual Machine (VM) View

Virtual Machine (VM) View Overview

The VM view provides you with comprehensive information about the VMs that are connected with the Cisco Nexus 1000VE switch.

- VM vNIC View—Provides information about all the vNICs (virtual network interface cards) adapters that are managed by the Cisco Nexus 1000VE switch.

Note The VSM must be connected with the vCenter in order to generate the required VM view output. You can enter the **show svs connections** command on the VSM to verify the connection.

Displaying the VM vNIC View

To display the VM vNIC view, follow the given step.

Procedure

show vtracker vm-view vnic [**module** *number* | **vm** *name*]

Note The timeout for this command is 180 seconds.

The following examples show the vTracker VM vNIC view in a VSM:

Example:

```
switch(config)# show vtracker vm-view vnic
* Network: For Access interface - Access vlan, Trunk interface - Native vlan,
           VXLAN interface - Segment Id.
--------------------------------------------------------------------------------
Mod VM-Name         VethPort    Drv Type  Mac-Addr        State Network Pinning
    HypvPort        Adapter     Mode      IP-Addr
--------------------------------------------------------------------------------
3   gentoo-2        Veth3       Vmxnet3   0050.56b5.37de  up    339     Eth3/8
    1025            Adapter 3   access    n/a

3   gentoo-2        Veth4       E1000     0050.56b5.37df  up    339     Eth3/8
    1026            Adapter 4   access    n/a

3   gentoo-2        Veth5       Vmxnet2   0050.56b5.37dd  up    339     Eth3/8
    1024            Adapter 2   access    n/a

4   Fedora-VM1      Veth7       E1000     0050.56bb.4fc1  up    406     Eth4/3
    4258            Adapter 2   pvlan     10.104.249.49

5   Fedora-VM2      Veth1       E1000     0050.56b5.098b  up    1       Po9
    100             Adapter 1   trunk     n/a

5   Fedora-VM2      Veth2       E1000     0050.56b5.098d  up    405     Po9
    3232            Adapter 3   pvlan     10.104.249.60
--------------------------------------------------------------------------------
```

Example:

```
switch(config)# show vtracker vm-view vnic module 4
* Network: For Access interface - Access vlan, Trunk interface - Native vlan,
           VXLAN interface - Segment Id.
--------------------------------------------------------------------------------
Mod VM-Name         VethPort    Drv Type  Mac-Addr        State Network Pinning
    HypvPort        Adapter     Mode      IP-Addr
--------------------------------------------------------------------------------
4   Fedora-VM1      Veth7       E1000     0050.56bb.4fc1  up    406     Eth4/3
```

```
   4258           Adapter 2   pvlan     10.104.249.49
--------------------------------------------------------------------------------
```

VM vNIC View Field Description

The column headings in the VM vNIC view examples above are described in the following table:

Column	Description
Mod	Module number on which the VM resides.
VM-Name	VM name.
HypvPort	Generated port ID in the hypervisor. For VMware hypervisor, it is called the dvPort ID.
VethPort	vEthernet interface number in the Cisco Nexus 1000V switch.
Adapter	Network adapter number of the vEthernet interface.
Drv Type	Driver type of the network adapter. Supported values are as follows: • E1000 • E1000e • PCNet32 • Vmxnet2 • Vmxnet3
Mode	Interface modes. Supported values are as follows: • access—Access port/Virtual Extensible Local Area Network (VXLAN) port • trunk—Trunk port • pvlan—Private VLAN (PVLAN) host mode or pvlan promiscuous mode
Mac-Addr	MAC address of the network adapter.
IP-Addr	IPv4 address of the network adapter, if the VMware tools are installed on the OS.
State	Operational status of the network adapter.

Column	Description
Network	Network interface ID. Supported values are as follows: • access vlan—Access interface • trunk interface—Native VLAN • vxlan interface—Segment ID • pvlan interface—Promiscous - primary VLAN; Isolated - secondary VLAN; Community-secondary VLAN **Note** To know the interface type, refer the Mode value.
Pinning	• For LACP or static port-channels, pinning columns only display the port-channel number. The link the VM traffic travels depends upon the hashing algorithm the port-channel is using. • For a vPC CDP/Manual/MAC Pinning port-channel, each vEthernet port is pinned to a sub-group of the port-channel. The sub-group corresponds to an Ethernet or its uplink interface. This column shows the Ethernet port members of the sub-group. • If the Ethernet ports are not part of the port channel in any module, this column is blank.

Displaying the VM Info View

To display the VM Info view, follow the given step.

Procedure

show vtracker vm-view info [**module** *number* | **vm** *name*]

Note The timeout for this command is 180 seconds.

The following examples show the vTracker VM Info view in a VSM:

Example:

```
switch(config)# show vtracker vm-view info
Module 4:
   VM Name:                Fedora-VM1
   Guest Os:               Other Linux (32-bit)
   Power State:            Powered On
   VM Uuid:                421871bd-425e-c484-d868-1f65f4f1bc50
   Virtual CPU Allocated:  1
   CPU Usage:              1 %
```

```
   Memory Allocated:       256 MB
   Memory Usage:           1 %
   VM FT State:            Unknown
   Tools Running status:   Not Running
   Tools Version status:   not installed
   Data Store:             NFS1_4
   VM Uptime:              1 day 29 minutes 46 seconds

   VM Name:                Fedora-VM2
   Guest Os:               Other Linux (32-bit)
   Power State:            Powered On
   VM Uuid:                4218ab37-d56d-63e4-3b00-77849401071e
   Virtual CPU Allocated:  1
   CPU Usage:              1 %
   Memory Allocated:       256 MB
   Memory Usage:           1 %
   VM FT State:            Unknown
   Tools Running status:   Not Running
   Tools Version status:   not installed
   Data Store:             NFS1_4
   VM Uptime:              58 minutes 30 seconds

Module 5:
   VM Name:                gentoo-cluster2-1
   Guest Os:               Other (64-bit)
   Power State:            Powered Off
   VM Uuid:                4235edf5-1553-650f-ade8-39565ee3cd57
   Virtual CPU Allocated:  1
   CPU Usage:              0 %
   Memory Allocated:       512 MB
   Memory Usage:           0 %
   VM FT State:            Unknown
   Tools Running status:   Not Running
   Tools Version status:   not installed
   Data Store:             datastore1 (2)
   VM Uptime:              n/a
```

Example:

```
switch(config)# show vtracker vm-view info vm Fedora-VM1
Module 4:
   VM Name:                Fedora-VM1
   Guest Os:               Other Linux (32-bit)
   Power State:            Powered On
   VM Uuid:                421871bd-425e-c484-d868-1f65f4f1bc50
   Virtual CPU Allocated:  1
   CPU Usage:              1 %
   Memory Allocated:       256 MB
   Memory Usage:           1 %
   VM FT State:            Unknown
   Tools Running status:   Not Running
   Tools Version status:   not installed
   Data Store:             NFS1_4
   VM Uptime:              1 day 29 minutes 46 seconds
```

VM Info View Field Description

The column headings in the VM Info view examples above are described in the following table:

Column	Description
Module	Module number on which the VM resides.
VM Name	VM name.
Guest OS	Guest operating system name, which is running on the VM.
Power State	Operational state of the VM. Supported status values are as follows: • Unknown • Powered On • Powered Off • Suspended • Non Available
VM Uuid	UUID of the VM.
Virtual CPU Allocated	Number of the virtual CPUs allocated for the VM.
CPU Usage	VM usage in percentage.
Memory Allocated	Memory allocated to the VM in megabytes.
Memory Usage	VM memory usage in percentage.
VM FT State	Fault tolerance state of the VM. Supported values are as follows: • Unknown • FT Primary • FT Secondary • Not Available
Tools Running status	VMware tools running status. Supported values are as follows: • Unknown • Starting • Running • Not Running • Not Available

Column	Description
Tools Version status	VMware tools that display the version status. Supported values are as follows: • Unknown • Current • Need Upgrade • Not Installed • Unmanaged • Blacklisted • Supported New • Supported Old • Too New • Too Old • Not Available
Data Store	Data store name on which the VM resides.
VM Uptime	How long the VM has been running.

Module pNIC View

Module pNIC View Overview

The Module pNIC View provides information about the physical network interface cards (pNICs) that are connected to each of the VSE server module in the network.

Displaying the Module pNIC View

To display the Module pNIC view, follow the given step.

Procedure

show vtracker module-view pnic [**module** *number*]

The following examples show the vTracker Module pNIC view in a VSM:

Example:

```
switch#  show vtracker module-view pnic

--------------------------------------------------------------------------------
```

```
Mod  EthIf     Adapter        Mac-Address         Driver
               Description
-------------------------------------------------------------------------------
3    Eth3/1    eth1           000c.2983.4b53      uio_pci_generic
               VMXNET3 Ethernet Controller 07b0

4    Eth4/1    eth1           000c.29d1.2373      uio_pci_generic
               VMXNET3 Ethernet Controller 07b0

-------------------------------------------------------------------------------
```

Example:

```
switch(config)# show vtracker module-view pnic module 3
-------------------------------------------------------------------------------
Mod  EthIf     Adapter        Mac-Address         Driver
               Description
-------------------------------------------------------------------------------
3    Eth3/1    eth1           000c.2983.4b53      uio_pci_generic
               VMXNET3 Ethernet Controller 07b0

-------------------------------------------------------------------------------
```

Module pNIC View Field Description

The column headings in the Module pNIC view examples above is described in the following table:

Column	Description
Mod	Server module name on which the VM resides.
EthIf	Ethernet interface ID of the server module.
Adapter	Ethernet adapter name as seen by the Hypervisor.
Description	Manufacturer name of the above adapter.
Mac-Address	MAC address of the Ethernet interface.
Driver	Driver type of the interface.

VLAN View

VLAN View Overview

The VLAN view provides information about all the VMs that are connected to a specific VLAN or a range of VLANs. It is a view from the VLAN perspective.

Displaying the VLAN View

To display the VLAN view, follow the given step.

Procedure

show vtracker vlan-view vnic [**vlan** *number/range*]

The following examples show the vTracker VLAN view in a VSM:

Example:

```
switch(config)# show vtracker vlan-view
* R = Regular Vlan,  P = Primary Vlan, C = Community Vlan
  I = Isolated Vlan, U = Invalid

--------------------------------------------------------------------------------
VLAN   Type VethPort  VM Name                  Adapter Name     Mod
--------------------------------------------------------------------------------
1      R    -         -                        -                -
233    R    -         -                        -                -
335    R    -         -                        -                -
336    R    -         -                        -                -
337    R    -         -                        -                -
338    R    -         -                        -                -
339    R    Veth3     gentoo-2                 Net Adapter 3    3
            Veth4     gentoo-2                 Net Adapter 4    3
            Veth5     gentoo-2                 Net Adapter 2    3
340    R    -         -                        -                -
341    R    -         -                        -                -
400    R    Veth1     Fedora-VM2               Net Adapter 1    5
401    R    Veth1     Fedora-VM2               Net Adapter 1    5
402    R    Veth1     Fedora-VM2               Net Adapter 1    5
403    R    -         -                        -                -
404    P    Veth6     Fedora-VM1               Net Adapter 1    4
405    C    Veth2     Fedora-VM2               Net Adapter 3    5
406    I    Veth7     Fedora-VM1               Net Adapter 2    4
--------------------------------------------------------------------------------
```

Example:

```
switch(config)# show vtracker vlan-view vlan 233-340
* R = Regular Vlan,  P = Primary Vlan, C = Community Vlan
  I = Isolated Vlan, U = Invalid

--------------------------------------------------------------------------------
VLAN   Type VethPort  VM Name                  Adapter Name     Mod
--------------------------------------------------------------------------------
233    R    -         -                        -                -
335    R    -         -                        -                -
336    R    -         -                        -                -
337    R    -         -                        -                -
338    R    -         -                        -                -
339    R    Veth3     gentoo-2                 Net Adapter 3    3
            Veth4     gentoo-2                 Net Adapter 4    3
            Veth5     gentoo-2                 Net Adapter 2    3
340    R    -         -                        -                -
--------------------------------------------------------------------------------
```

VLAN View Field Description

The column headings in the VLAN view examples above are described in the following table:

Column	Description
VLAN	VLAN ID on which the VM resides.
Type	VLAN type. Supported types are as follows: • R—Regular VLAN • P—Primary VLAN • C—Community VLAN • I—Isolated VLAN • U—Invalid VLAN
VethPort	vEthernet interface port number used by the VLAN.
VM Name	VM name of the interface.
Adapter Name	Adapter name of the interface.
Mod	Module number on which the interface resides.

VMotion View

VMotion View Overview

The vMotion view provides information about all the ongoing (if any) as well as previous VM migration events. However, only VMs that are currently being managed by the Cisco Nexus 1000VE switch are displayed in the output.

Note The VSM must be connected with the vCenter in order to generate the required VMotion view output. You can enter the **show svs connections** command on the VSM to verify the connection.

Displaying the VMotion View

To display the VMotion view, follow the given step.

Procedure

show vtracker vmotion-view [**now** | **last** *number 1-100*]

Note The timeout for this command is 180 seconds.

The following examples show the vTracker VMotion view in a VSM:

Example:

```
switch(config)# show vtracker vmotion-view last 20
Note: Command execution is in progress...

Note: VM Migration events are shown only for VMs currently
      managed by Nexus 1000ve.

* '-' = Module is offline or no longer attached to Nexus1000ve DVS
--------------------------------------------------------------------------------
VM-Name               Src Dst   Start-Time               Completion-Time
                      Mod Mod
--------------------------------------------------------------------------------
rk-ubt-1-0046         6    4    Mon Sep  3 10:42:27 2012 OnGoing

rk-ubt-1-0045         6    4    Mon Sep  3 10:42:27 2012 OnGoing

rk-ubt-1-0031         6    4    Mon Sep  3 10:42:27 2012 Mon Sep  3 10:44:10 2012

rk-ubt-1-0021         6    4    Mon Sep  3 10:42:27 2012 Mon Sep  3 10:43:42 2012

rk-ubt-1-0023         6    3    Thu Aug 16 14:25:26 2012 Thu Aug 16 14:27:55 2012

rk-ubt-1-0029         6    3    Thu Aug 16 14:25:26 2012 Thu Aug 16 14:27:50 2012

rk-ubt-1-0024         6    3    Thu Aug 16 14:25:26 2012 Thu Aug 16 14:26:13 2012

rk-ubt-1-0025         6    3    Thu Aug 16 14:25:26 2012 Thu Aug 16 14:26:12 2012

rk-ubt-1-0026         6    3    Thu Aug 16 14:25:26 2012 Thu Aug 16 14:26:09 2012

RHEL-Tool-VmServer    -    3    Wed Aug  8 12:57:48 2012 Wed Aug  8 12:58:37 2012

--------------------------------------------------------------------------------
```

Example:

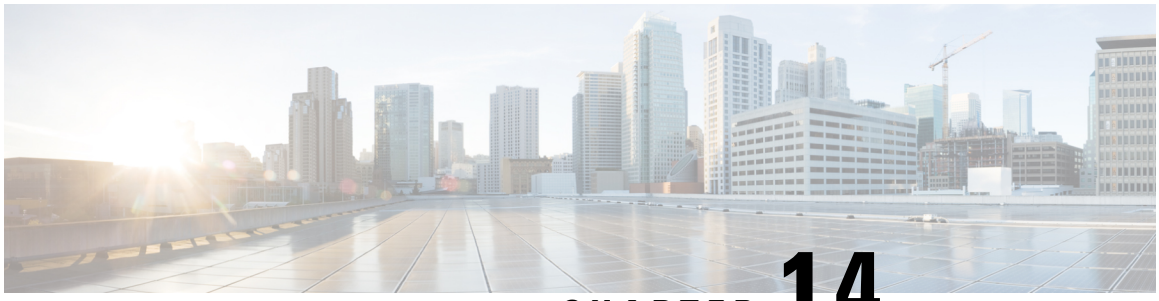
```
switch(config)# show vtracker vmotion-view now
Note: Command execution is in progress...

*Note: VM Migration events are shown only for VMs currently
      managed by Nexus 1000ve.

* '-' = Module is offline or no longer attached to Nexus1000ve DVS
--------------------------------------------------------------------------------
VM-Name               Src Dst   Start-Time               Completion-Time
                      Mod Mod
--------------------------------------------------------------------------------
rk-ubt-1-0046         6    4    Mon Sep  3 10:42:27 2012 OnGoing

rk-ubt-1-0045         6    4    Mon Sep  3 10:42:27 2012 OnGoing
--------------------------------------------------------------------------------
```

VMotion View Field Description

The column headings in the VMotion view examples above are described in the following table:

Column	Description
VM-Name	VM name.

Column	Description
Src Mod	Source module number of the migration.
Dst Mod	Destination module number of the migration.
Start-Time	Migration start time per the time zone defined in the Virtual Supervisor Module (VSM).
Completion-Time	Migration completion time in VSM time zone. For migration in progress, the status shows as “OnGoing.”



CHAPTER 14

Configuring Virtualized Workload Mobility

This chapter contains the following sections:

Information About Virtualized Workload Mobility (DC to DC vMotion)

This section describes the Virtualized Workload Mobility (DC to DC vMotion) configurations and includes the following topics:

- Stretched Cluster
- Split Cluster

Stretched Cluster

Note A stretched cluster is a cluster with ESX/ESXi hosts in different physical locations.

In an environment where the same Cisco Nexus 1000 instance spans two data centers, this configuration allows you to have Virtual Service Engine (VSEs) in different data centers be part of the same vCenter Server cluster.

By choosing this configuration, you are ensure that the VSEs in either data center (in a two data center environment) are a part of the same Dynamic Resource Scheduling (DRS) / VMware High Availability (VMW HA) / Fault Tolerance (FT) domain that allows for multiple parallel virtual machine (VM) migration events.

Split Cluster

The Split Cluster configuration is an alternate to the Stretched Cluster deployment. With this configuration, the deployment consists of one or more clusters on either physical site with no cluster that contains VSEs in multiple data centers. While this configuration allows for VM migration between physical data centers, these events are not automatically scheduled by DRS.

Prerequisites for Virtualized Workload Mobility (DC to DC vMotion)

Virtualized Workload Mobility (DC to DC vMotion) has the following prerequisite:

- Layer 2 extension between the two physical data centers over the DCI link.

Guidelines and Limitations

Virtualized Workload Mobility (DC to DC vMotion) has the following guidelines and limitations:

- The VSM HA pair must be located in the same site as their storage and the active vCenter Server.
- Quality of Service bandwidth guarantees for control traffic over the DCI link.
- Limit the number of physical data centers to two.
- A maximum latency of 10 ms is supported for VSM-VSM control traffic when deployed across datacenters.
- A maximum latency of 100 ms is supported for VSM-VSE control traffic for both L2 and L3 mode of deployments.

Physical Site Considerations

When you are designing a physical site, follow these guidelines:

- Check the average and maximum latency between a Virtual Supervisor Module (VSM) and VSE.
- Follow the procedures to perform actions you would intend to do in normal operation. For example, VSM migration.
- Design the system to handle the high probability of VSM-VSE communication failures where a VSE must function in headless mode due to data center interconnect (DCI) link failures.

Handling Inter-Site Link Failures

If the DCI link or Layer 2 extension mechanism fails, a set of VSE modules might run with their last known configuration for a period of time.

Headless Mode of Operation

For the period of time that the VSM and VSE cannot communicate, the VSE continues to operate with its last known configuration. Once the DCI link connectivity is restored and the VSM-VSE communication is reestablished, the system should come back to its previous operational state. This mode type is no different than the headless mode of operation within a data center and has the following limitations for the headless VSE:

- No new VM ports will be brought up on Cisco N1KVE during headless mode as VSM-to-VSE communication is essential to bring up ports.
- Queries on BRIDGE and IF-MIB processed at the VSM give the last known status for the hosts in headless mode.

Handling Additional Distance/Latency Between the VSM and VSE

In a network where there is a considerable distance between the VSM and VSE, latency becomes a critical factor.

Because the control traffic between the VSM and VSE faces a sub-millisecond latency within a data center, latency can increase to a few milliseconds depending on the distance.

With an increased round-trip time, communication between the VSM and VSE takes longer. As you add VSEs and vEthernet interfaces, the time it takes to perform actions such as configuration commands, module insertions, port bring-up, and **show**show commands increase because that many tasks are serialized.

Migrating a VSM

This section describes how migrate a VSM from one physical site to another.

Note If you are migrating a VSM on a Cisco Nexus 1010, see the Cisco Nexus 1010 Software Configuration Guide, Release 4.2(1)SP1(3).

Migrating a VSM Hosted on an ESX

Use the following procedure to migrate a VSM that is hosted on an ESX or ESXi host from the local data center to the remote data center:

Note For information on vMotion or storage vMotion, see the VMware documentation.

Before you begin

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

- Reduce the amount of time where the VSM runs with remote storage in another data center.

- Do not bring up any new VMs or vMotion VMs that are hosted on any VSEs corresponding to the VSM that is being migrated.

Procedure

Step 1 Migrate the standby VSM to the backup site.

Step 2 Perform a storage vMotion for the standby VSM storage.

Step 3 switch#**system switchover**

Initiates a system switchover.

Step 4 Migrate the original active VSM to the backup site.

Step 5 Perform a storage vMotion for the original active VSM storage.

Verifying and Monitoring the Virtualized Workload Mobility (DC to DC vMotion) Configuration

Refer to the following section for verifying and monitoring the Virtualized Workload Mobility (DC to DC vMotion) configuration:

Procedure

switch#**show module**

Displays the virtualized workload mobility (DC to DC vMotion) configuration.