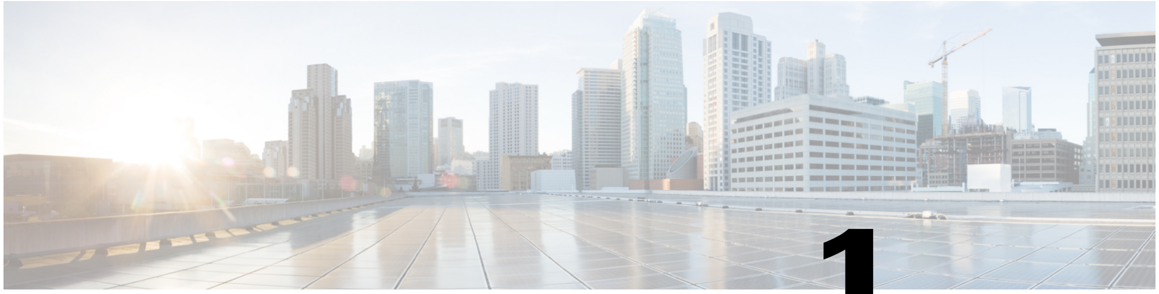
Cisco Nexus 1000V for KVM System Management Configuration Guide, Release 5.x

First Published: August 01, 2014

Last Modified: November 21, 2014

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

New and Changed Information

This chapter contains the following sections:

New and Changed Information

Table 1: New and Changed Features

Content	Description	Changed in Release	Where Documented
vTracker	This feature is introduced.	5.2(1)SK3(2.1)	Enabling vTracker, on page 129
Local SPAN and ERSPAN	This feature is introduced.	5.2(1)SK31(2.1)	Configuring Local SPAN and ERSPAN, on page 53

CHAPTER 2

Overview

This chapter contains the following sections:

Cisco Nexus 1000V for KVM and OpenStack

The Cisco Nexus 1000V for KVM consists of two main components:

- Virtual Ethernet Module (VEM)—A software component that is deployed on each kernel-based virtual machine (VM) host. Each VM on the host is connected to the VEM through virtual Ethernet (vEth) ports.
- Virtual Supervisor Module (VSM)—The Management component that controls multiple VEMs and helps in the definition of VM-focused network policies. It is deployed either as a virtual appliance on any KVM host or on the Cisco Cloud Services Platform appliance.

Each of these components is tightly integrated with the OpenStack environment:

- The VEM is a hypervisor-resident component and is tightly integrated with the KVM architecture.
- The VSM is integrated with OpenStack using the OpenStack Neutron Plug-in.

- The OpenStack Neutron API has been extended to include two additional user-defined resources:
    - Network profiles are logical groupings of network segments.
    - Policy profiles group port policy information, including security.

Using OpenStack, you create VMs, networks, and subnets on the Cisco Nexus 1000V for KVM, by defining components such as the following:

- Tenants
- Network segments, such as VLANs, VLAN trunks, and VXLANs
- IP address pools (subnets)

Using the Cisco Nexus 1000V for KVM VSM, you create port profiles (called policy profiles in OpenStack), which define the port policy information, including security settings.

When a VM is deployed, a port profile is dynamically created on the Cisco Nexus 1000V for KVM for each unique combination of policy port profile and network segment. All other VMs deployed with the same policy to this network reuse this dynamic port profile.

Note You must consistently use OpenStack for all VM network and subnet configuration. If you use *both* OpenStack and the VSM to configure VM networks and subnets, the OpenStack and the VSM configurations can become out-of-sync and result in faulty or inoperable network deployments.

CDP

The Cisco Discovery Protocol (CDP) runs over the data link layer and is used to advertise information to all attached Cisco devices and to discover and view information about attached Cisco devices. CDP runs on all Cisco-manufactured equipment.

Domains

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

Configuration Management

The Cisco Nexus 1000V 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.

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.

NetFlow

NetFlow gives visibility into traffic that transits the virtual switch by characterizing IP traffic based on its source, destination, timing, and application information. You can use this information to assess network availability and performance, assist in meeting regulatory requirements (compliance), and help with troubleshooting.

You can also use the Cisco Network Analysis Module (NAM) to monitor NetFlow data sources.

System Messages

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

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

Troubleshooting

Ping and trace route are among the available troubleshooting tools. For more information, see the *Cisco Nexus 1000V for KVM Troubleshooting Guide*.

CHAPTER 3

Configuring CDP

This chapter contains the following sections:

Information About CDP

The Cisco Discovery Protocol (CDP), which runs over the data link layer, is used to advertise information to all attached Cisco devices and to discover and view information about attached Cisco devices. CDP runs on all Cisco-manufactured equipment.

Each device that you configure for CDP sends periodic advertisements to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain hold time information, which indicates the length of time that a receiving device should hold CDP information before discarding it. You can configure the advertisement or refresh timer and the hold timer.

CDP Version 2 (CDPv2) allows you to track instances where the native VLAN ID or port duplex states do not match between connecting devices.

CDP advertises the following type-length-value fields (TLVs):

- Device ID
- Address
- Port ID
- Capabilities

- Version
- Platform
- Native VLAN
- Full/half duplex
- Maximum Transmission Unit (MTU)
- Sysname
- SysObjectID
- Management address
- Physical location

All CDP packets include a VLAN ID. The CDP packet is untagged, so it goes over the native/access VLAN, which is then also added to the packet.

High Availability

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

Guidelines and Limitations

- CDP gathers protocol addresses of neighboring devices and discovers the platform of those devices. CDP runs over the data link layer only. With CDP, two systems that support different Layer 3 protocols can learn about each other.
- CDP can discover up to 256 neighbors per port if the port is connected to a hub with 256 connections.
- CDP must be enabled globally before you can configure CDP on an interface. CDP is enabled globally by default.
- You can configure CDP on physical interfaces and port channels only.

Default Settings

Parameters	Default
CDP	Enabled globally and on all interfaces
CDP version	Version 2
CDP device ID	System name
CDP timer	60 seconds
CDP hold timer	180 seconds

Configuring CDP

This section includes the following topics:

- CDP Global Configuration
- Enabling CDP on an Interface
- Disabling CDP on an Interface

Enabling or Disabling CDP Globally

Be sure you understand that when you globally disable the CDP feature, all CDP configurations are removed.

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	switch# **config t**	Places you in global configuration mode.
Step 2	switch(config)# [**no**] **cdp enable**	Enables or disables the CDP feature globally.

```
switch# config t
switch(config)# no cdp enable
```

Enabling or Disabling CDP on an Interface

You can enable or disable CDP on an interface.

Note Although CDP is enabled by default on all interfaces, should it become disabled, you can use this procedure to enable it again.

Procedure

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

	Command or Action	Purpose
Step 2	switch(config)# **interface** *interface-type number*	Places you in interface configuration mode for the specific interface.
Step 3	switch(config-if)# [**no**] **cdp enable**	Disables or enables CDP on this interface.
Step 4	switch(config-if)# **show cdp interface** *interface-type number*	(Optional) Displays CDP information for the specified interface.
Step 5	switch(config-if)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

```
switch# config terminal
switch(config)# interface ethernet 3/1
switch(config-if)# no cdp enable
switch(config-if)# show cdp interface mgmt0
mgmt0 is up
    CDP disabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
switch(config)# copy running-config startup-config
```

Configuring CDP Options

You can configure the following for CDP:

- The device ID format to use

  Note Only the system-name device ID format is supported

- The maximum hold time for neighbor information
- The refresh time for sending advertisements

Note You can view output from the upstream Catalyst 6500 Series switch by using the **show cdp neighbor command**.

Before You Begin

Before beginning this procedure, be sure you know the following information:

- How long you want CDP to retain neighbor information if you are setting the holdtime.
- How often you want CDP to advertise if you are setting the CDP timer.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **cdp format device-id system-name**	(Optional) Specifies that CDP uses the system name for the device ID format.
Step 3	switch(config)# **show cdp neighbors**	Displays the upstream device from your device.
Step 4	switch(config)# **cdp holdtime** *seconds*	(Optional) Sets the maximum amount of time that CDP holds onto neighbor information before discarding it. • The range for the *seconds* argument is from 10 to 255 seconds. • The default is 180 seconds.
Step 5	switch(config)# **cdp timer** *seconds*	Sets the refresh time for CDP to send advertisements to neighbors. • The range for the *seconds* argument is from 5 to 254 seconds.
Step 6	switch(config)# **show cdp global**	(Optional) Displays the CDP version that is being advertised or sent to other devices.
Step 7	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

```
switch# config terminal
switch(config)# cdp format device-id system-name
switch(config)# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device ID              Local Intrfce   Hldtme  Capability  Platform      Port ID

swordfish-6k-2         Eth2/2          169     R S I    WS-C6503-E    Gig1/14
swordfish-6k-2         Eth2/3          139     R S I    WS-C6503-E    Gig1/15
swordfish-6k-2         Eth2/4          135     R S I    WS-C6503-E    Gig1/16
swordfish-6k-2         Eth2/5          177     R S I    WS-C6503-E    Gig1/17
swordfish-6k-2         Eth2/6          141     R S I    WS-C6503-E    Gig1/18
switch(config)# cdp holdtime 10
switch(config)# cdp timer 5
switch(config)# show cdp global
Global CDP information:
    CDP enabled globally
    Sending CDP packets every 5 seconds
    Sending a holdtime value of 10 seconds
    Sending CDPv2 advertisements is disabled
    Sending DeviceID TLV in Mac Address Format
switch(config-if)# copy running-config startup-config
```

Advertising a CDP Version

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

- The version of CDP currently supported on the device.
- Only one version of CDP (version 1 or version 2) is advertised at a time for all uplinks and port channels on the switch.

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	switch# **config t**	Places you in global configuration mode.
Step 2	switch(config)# **cdp advertise** {**v1** | **v2**}	Assigns the CDP version to advertise: • CDP Version 1 • CDP Version 2
Step 3	switch(config)# **show cdp global**	(Optional) Displays the CDP version that is being advertised or sent to other devices.
Step 4	switch(config)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

```
switch# config t
switch(config)# cdp advertise v1
switch(config)# show cdp global
Global CDP information:
    CDP enabled globally
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is disabled
    Sending DeviceID TLV in Default Format
switch(config)# copy running-config startup-config
```

Verifying the CDP Configuration

Use one of the following commands to verify the configuration:

Command	Purpose
show cdp all	Displays all interfaces that have CDP enabled.
show cdp entry {**all** | **name** *entry-name*}	Displays the CDP database entries.
show cdp global	Displays the CDP global parameters.
show cdp interface *interface-type slot/port*	Displays the CDP interface status.
show cdp neighbors {**detail** | **interface** *interface-type slot/port*}	Displays the CDP neighbor status.

Monitoring CDP

Monitoring CDP Statistics

Command	Purpose
show cdp traffic interface *interface-type slot/port*	Displays the CDP traffic statistics on an interface.

Clearing CDP Statistics

Use one of the following commands to clear CDP statistics:

Command	Purpose
clear cdp counters	Clears CDP statistics on all interfaces.
clear cdp counters interface *number*	Clears CDP statistics on the specified interface.
clear cdp table	Clears the CDP cache for one or all interfaces.

Configuration Example for CDP

This example shows how to enable the CDP feature and configures the refresh and hold timers:

```
switch# config t
switch(config)# cdp enable
switch(config)# cdp timer 50
switch(config)# cdp holdtime 100
```

Feature History for CDP

Feature	Releases	Feature Information
CDP	Release 5.2(1)SK1(2.1)	This feature was introduced.

CHAPTER 4

Configuring the Domain

This chapter contains the following sections:

Information About Domains

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

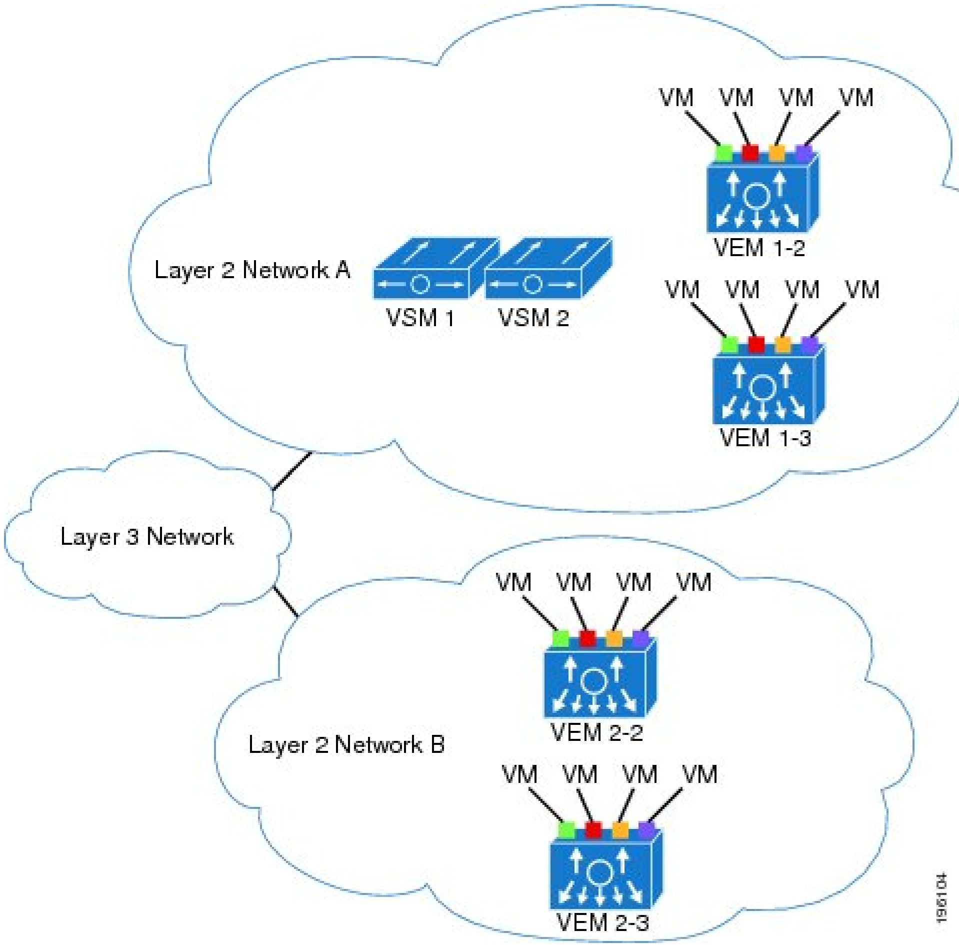
Layer 3 Control

The Cisco Nexus 1000V for KVM supports Layer 3 control by default, and this setting cannot be changed. Layer 3 control, or IP connectivity, is supported between the Virtual Supervisor Module (VSM) and the Virtual Ethernet Module (VEM) for control and packet traffic. With Layer 3 control, a VSM can be Layer 3 accessible and can control hosts that reside in a separate Layer 2 network. In the Layer 3 mode, all the VEMs hosts that are managed by VSM and the VSM can be in different networks.

To implement Layer 3 control, you must configure the VSM in Layer 3 mode.

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

Figure 1: Example of Layer 3 Control IP Connectivity



Configuring a Domain

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

Before You Begin

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

You must know the following information:

- A unique domain ID for this Cisco Nexus 1000V instance.

Procedure

	Command or Action	Purpose
Step 1	switch# **config terminal**	Places you in global configuration mode.
Step 2	switch(config)# **svs-domain**	Places you in SVS domain configuration mode.
Step 3	switch(config-svs-domain)# **svs mode L3 interface** {**mgmt0** | **control0**}	Designates which interface to use, mgm0 or control0. **Note** The interface must already have an IP address configured.
Step 4	switch(config-svs-domain)# **domain id** *number*	Creates the domain ID for this Cisco Nexus 1000V instance.
Step 5	switch(config--svs-domain)# **show svs domain**	(Optional) Displays the domain configuration.
Step 6	switch(config-svs-domain)# **exit**	Returns you to global configuration mode.
Step 7	switch(config)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

```
switch# configuration terminal
switch(config)# svs-domain
switch(config-svs-domain)# svs mode L3 interface mgmt0
switch(config-svs-domain)# domain id 1
switch(config-vlan)# exit

switch(config)# show svs domain
SVS domain config:
  Domain id:    1
  Control vlan:  NA
  Packet vlan:   NA
  Control mode: L3
  Switch guid: 07da7e1a-2bff-6833-b416-f5d83204a55c
  L3 control interface: mgmt0
  Status: Config push to VC successful.
  Control type multicast: No

Note: Control VLAN and Packet VLAN are not used in L3 mode

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

Verifying the Domain

Use this procedure to view and verify the configured domain.

Before You Begin

- You are logged in to the CLI in any command mode.
- You have configured a domain using the Creating a Domain procedure.

Procedure

show svs domain

Example:

```
switch# show svs domain
SVS domain config:
  Domain id:    1
  Control vlan:  NA
  Packet vlan:   NA
  Control mode: L3
  Switch guid: 07da7e1a-2bff-6833-b416-f5d83204a55c
  L3 control interface: mgmt0
  Status: Config push to VC successful.
  Control type multicast: No

Note: Control VLAN and Packet VLAN are not used in L3 mode
```

Display the domain configured on the Cisco Nexus 1000V.

Feature History for the VSM Domain

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

Feature Name	Releases	Feature Information
VSM Domain	Release 5.2(1)SK1(2.1)	This feature was introduced.

CHAPTER 5

Managing Host Server Connections

This chapter contains the following sections:

Information about Host Server Connections

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

Configuring Host Server Connections

Mapping a VEM to a New Host

Before You Begin

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

- Logged in to the CLI in EXEC mode
- Removed the host from the Cisco Nexus 1000V DVS on the OpenStack controller

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Places you in global configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# **no vem** *module number*	(Optional) Removes the existing module-to-host mapping **Note** If you are changing the mapping on a module, you must remove the existing host mapping first. If you do not remove the existing host mapping first, the new host is assigned a different module number.
Step 3	switch(config)# **vem** *module number*	Places you in configuration mode for the specified module.
Step 4	switch(config-vem-slot)# **host id** *server-bios-uuid*	Assigns a different host server UUID to the specified module. The host ID must match the host UUID in the /etc/n1kv/n1kv.conf file. The valid range is from 0 to 64 characters.
Step 5	switch(config-vem-slot)# **show module vem mapping**	(Optional) Displays the mapping of modules to hosts.
Step 6	switch(config-vem-slot)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

```
switch# configure terminal
switch(config)# no vem 3
switch(config)# vem 3
switch(config-vem-slot)# host id 93312881-309e-11db-afa1-0015170f51a8
switch(config-vem-slot)# show module vem mapping
Mod     Status          UUID                                    License Status
---     -----------     ------------------------------------    --------------
  3      powered-up     93312881-309e-11db-afa1-0015170f51a8    licensed
  4          absent     6dd6c3e3-7379-11db-abcd-000bab086eb6    licensed

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

Removing Host Mapping from a Virtual Ethernet Module

You can remove the host mapping from a module.

Before You Begin

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

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

Procedure

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

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

Viewing Host Mapping

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

Procedure

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

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

Verifying the Configuration

Use one of the following commands to verify the configuration:

show running-config

Displays the current configuration.

If the Cisco Nexus 1000V is not connected to a OpenStack controller or KVM server, the output is limited to connection-related information.

```
switch(config)# show running-config

!Command: show running-config
!Time: Fri Jul 26 01:59:50 2013

version 5.2(1)SK1(1.1)
switchname n1000v-VSM-Primary

no feature telnet

username adminbackup password 5 !  role network-operator
username admin password 5 $1$uaNy2mFT$Sy6fo2j8Q/uxc0fWMpBLz1  role network-admi
n
username admin keypair rsa

banner motd #Nexus 1000v Switch
#

ip domain-lookup
ip host n1000v-VSM-Primary 10.106.202.182
errdisable recovery cause failed-port-state
vem 3
  host id 10
vem 4
  host id 64
snmp-server user admin network-admin auth md5 0xb64ad6879970f0e57600c443287a79f
0 priv 0xb64ad6879970f0e57600c443287a79f0 localizedkey


vrf context management
  ip route 0.0.0.0/0 10.106.202.161
vlan 1,2166-2170

cdp advertise v1
cdp holdtime 10
cdp timer 5
port-channel load-balance ethernet source-mac
port-profile default max-ports 32
port-profile default port-binding static
port-profile type vethernet N1K_Cloud_Default_Trunk
  switchport mode trunk
  no shutdown
  guid 51e1095a-61ea-50b5-9f3c-19842dcff6e7
  max-ports 64
  description Port Profile created for Nexus 1000V internal usage. Do not use.
  state enabled
port-profile type ethernet uplink_sys
  switchport mode trunk
  switchport trunk allowed vlan 2167-2170
  no shutdown
  guid 53502d18-9ffb-411a-b665-d830081136e5
  max-ports 512
  state enabled
port-profile type ethernet uplink_sys_pc
  switchport mode trunk
  switchport trunk allowed vlan 2167
  channel-group auto mode active
  no shutdown
  guid 7aa26801-1e00-2684-97ec-a7cc1a4615af
  max-ports 512
  state enabled
port-profile type vethernet vm_access_sys
  switchport mode access
  guid 78dc356e-1fe5-7c72-8c2c-6286065720a8
port-profile type vethernet DEFAULT_DATA_VNIC1
  switchport mode access
  switchport access vlan 2170
  no shutdown
  guid 5cb014fe-3d4f-014a-b673-869700f70425
  state enabled
port-profile type vethernet DEFAULT_DATA_VNIC2
  switchport mode access
  switchport access vlan 2167
  no shutdown
  guid 42dbc174-30ec-2ab7-8796-c92e15ea4167
  state enabled
port-profile type vethernet DEFAULT_DATA_VNIC3
  switchport mode access
  switchport access vlan 2169
  no shutdown
  guid 090dc703-caca-102c-869a-86e433531d77
  state enabled
port-profile type vethernet mx-nlb
  guid 2505614c-2107-5f97-9f21-45d70b57aa3e
port-profile type vethernet hsrp-1
  switchport mode trunk
  disable-loop-detection hsrp
  no shutdown
  guid 6d2b8903-94c5-2e9a-923d-182408301feb
  state enabled
port-profile type vethernet vrrp-1
  disable-loop-detection vrrp
  switchport mode trunk
  no shutdown
  guid 3262b6ec-1333-2665-bc78-37a31ea6a71e
  state enabled
port-profile type vethernet LynnTest
  guid 5a5e3644-8cf9-1f4a-bf63-97912048f20e
port-profile type vethernet LynnPP
  switchport mode access
  switchport access vlan 10
  no shutdown
  capability l3control
  guid 754ab04a-6979-3f5f-a0ec-aef11dd83ff0
  state enabled


interface port-channel2

interface mgmt0
  ip address 10.106.202.182/27

interface control0
  no snmp trap link-status
line console
line vty
boot kickstart bootflash:/n1000v-dk9-kickstart.5.2.1.SK1.1.0.345.gbin sup-1
boot system bootflash:/n1000v-dk9.5.2.1.SK1.1.0.345.gbin sup-1
boot kickstart bootflash:/n1000v-dk9-kickstart.5.2.1.SK1.1.0.345.gbin sup-2
boot system bootflash:/n1000v-dk9.5.2.1.SK1.1.0.345.gbin sup-2
svs-domain
  domain id 1
  control vlan 1
  packet vlan 1
  svs mode L3 interface mgmt0
  switch-guid 07da7e1a-2bff-6833-b416-f5d83204a55c
svs connection svs_system
  max-ports 8192
vservice global type vsg
  tcp state-checks invalid-ack
  tcp state-checks seq-past-window
  no tcp state-checks window-variation
  no bypass asa-traffic
vnm-policy-agent
  registration-ip 0.0.0.0
  shared-secret **********
  log-level info
```

show svs connections

Displays the current connections to the Cisco Nexus 1000V.

Note Network connectivity issues may shut down your connection to theOpenStack controller. When network connectivity is restored, the Cisco Nexus 1000V will not automatically restore the connection. In this case, you must restore the connection manually using the following command sequence:

no connect

connect

```
switch(config)# show svs connections

connection svs_system:
    hostname: -
    ip address: -
    remote port: 80
    protocol: -
    certificate: default
    datacenter name: -
    admin:
    max-ports: 8192
    DVS uuid: -
    config status: Disabled
    operational status: Disconnected
    sync status: -
    version: -
    vc-uuid: -
switch(config)#
```

show module

Displays the module information.

```
swtich# show module
Mod  Ports  Module-Type                       Model               Status
---  -----  --------------------------------  ------------------  ------------
1    0      Virtual Supervisor Module         Nexus1000V          active *
2    0      Virtual Supervisor Module         Nexus1000V          ha-standby

Mod  Sw                  Hw
---  ------------------  ------------------------------------------------
1    5.2(1)SK1(1)        0.0
2    5.2(1)SK1(1)        0.0

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
2    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
1    10.105.225.180   NA                                    NA
2    10.105.225.180   NA                                    NA

* this terminal session
```

Feature History for Host Server Connections

Feature Name	Releases	Feature Information
Host Mapping	Release 5.2(1)SK1(2.1)	This feature was introduced.

CHAPTER 6

Managing the Configuration

This chapter contains the following sections:

Information About Configuration Management

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

Changing the Switch Name

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

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

Before You Begin

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

Procedure

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

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

Configuring a Message of the Day

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

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

Before You Begin

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

Procedure

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

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

Saving a Configuration

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

Before You Begin

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

Procedure

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

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

Erasing a Configuration

Use this procedure to erase a startup configuration.

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

Before You Begin

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

Procedure

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

	Command or Action	Purpose
		• boot: Erases the boot variables and the mgmt0 IP configuration. • debug: Erases the debug configuration.

```
switch# write erase debug
```

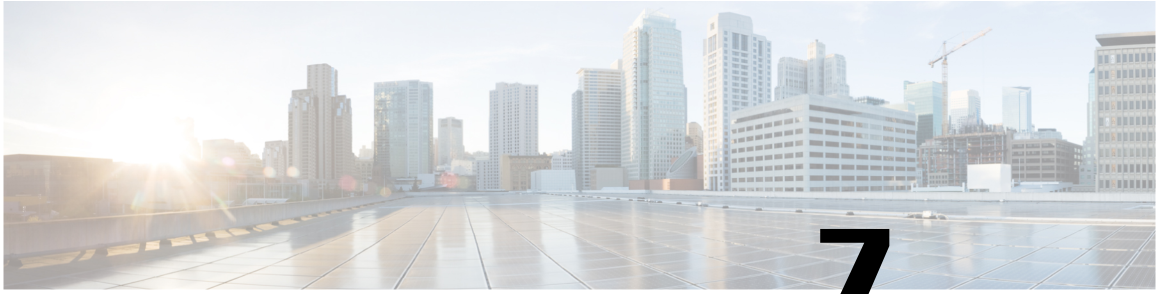
Verifying the Configuration

Use the following commands to verify the configuration of interfaces, system settings, and hardware and software versions. For detailed information, including sample output, see the *Cisco Nexus 1000V for KVM Command Reference.*

Command	Description
show version	Displays the versions of system software and hardware that are currently running on the switch.
show running-config	Displays the versions of system software and hardware that are currently running on the switch.
show running-config diff	Displays the difference between the startup configuration and the running configuration currently on the switch.
show interface {*type*} {*name*} *brief*	Displays a brief version of information about the specified interface configuration.
show interface {*type*} {*name*}	Displays details about the specified interface configuration.
show interface brief	Displays a brief version of all interface configurations on your system.
show running-config interface	Displays the running configuration for all interfaces on your system.

Feature History for Configuration Management

Feature Name	Releases	Feature Information
Configuration Management	Release 5.2(1)SK1(2.1)	This feature was introduced.



CHAPTER 7

Working with Files

This chapter contains the following sections:

Information About Files

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

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

Navigating the File System

Specifying File Systems

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

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

Identifying the Directory You are Working From

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

Before You Begin

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

Procedure

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

```
switch# pwd
bootflash:
```

Changing Your Directory

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

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

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

Before You Begin

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

Procedure

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

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

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

Listing the Files in a File System

Procedure

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

```
switch(config)# dir
      77824    Jul 26 01:48:13 2013  accounting.log
       4096    Jun 24 21:08:18 2013  core/
       4096    Jun 24 21:08:18 2013  log/
      16384    Jun 24 21:07:59 2013  lost+found/
        875    Jun 28 04:19:00 2013  mts.log
    1955033    Jun 24 21:08:11 2013  n1000v-dk9-dplug.5.2.1.SK1.1.0.345.gbin
   31329792    Jun 24 21:08:11 2013  n1000v-dk9-kickstart.5.2.1.SK1.1.0.345.gbin
   98044335    Jun 24 21:08:15 2013  n1000v-dk9.5.2.1.SK1.1.0.345.gbin
       4096    Jun 24 21:08:43 2013  vdc_2/
       4096    Jun 24 21:08:43 2013  vdc_3/
       4096    Jun 24 21:08:43 2013  vdc_4/
    8401501    Jun 24 21:08:17 2013  vsmcpa.3.0.0.112.bin

Usage for bootflash://
  498884608 bytes used
 5905084416 bytes free
 6403969024 bytes total
switch(config)#
```

Identifying Available File Systems for Copying Files

Before You Begin

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

Procedure

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

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

```
sftp: Select source filesystem
startup-config Copy startup configuration to destination
system: Select source filesystem
tftp: Select source filesystem
volatile: Select source filesystem
```

Using Tab Completion

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

Procedure

	Command or Action	Purpose
Step 1	switch# **show file** *filesystem name: partial filename* <Tab>	Completes the filename when you type a partial filename and then press Tab and if the characters you typed are unique to a single file. If not, the CLI lists a selection of file names that match the characters that you typed. You can then retype enough characters to make the file name unique; and CLI completes the filename for you.
Step 2	switch# **show file bootflash:nexus-1000v-** <Tab>	Completes the file name for you

```
switch# show file bootflash:nexus-1000v-
bootflash:nexus-n1000v-dk9-dplug.5.2.1.SK1.1.0.345.gbin
bootflash:nexus-1000v-mzg.5.2.1.SK1.1.0.345.gbin
bootflash:nexus-1000v-kickstart-mzg.5.2.1.SK1.1.0.345.gbin
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

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

- You are logged in to the CLI through a Telnet, or SSH connection.

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

Procedure

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

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

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

Creating a Directory

Procedure

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

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

Removing an Existing Directory

This command is valid only on Flash file systems.

Before You Begin

Before beginning this procedure, be sure of the following:

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

Procedure

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

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

Moving Files

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

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

Before You Begin

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

Procedure

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

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

Deleting Files or Directories

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

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

Before You Begin

You must understand the following information:

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

Procedure

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

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

Compressing Files

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	switch# **gzip** [*path*] *filename*	Compresses the specified file.
Step 2	switch# **dir**	Displays the contents of the specified directory, including the newly-compressed file. The compressed filename suffix becomes **.gz** indicating that it is a compressed gzip file. Shows the file size of the newly-compressed file.

```
switch# gzip csafile
switch# dir
      77824    Aug 21 13:37:25 2013  accounting.log
       4096    Jun 24 21:08:18 2013  core/
      14278    Aug 21 13:36:54 2013  csafile.gz
       4096    Jul 26 02:47:21 2013  log/
      16384    Jun 24 21:07:59 2013  lost+found/
        875    Jun 28 04:19:00 2013  mts.log
    1955033    Jun 24 21:08:11 2013  n1000v-dk9-dplug.5.2.1.SK1.1.0.345.gbin
   31329792    Jun 24 21:08:11 2013  n1000v-dk9-kickstart.5.2.1.SK1.1.0.345.gbi
n
   98044335    Jun 24 21:08:15 2013  n1000v-dk9.5.2.1.SK1.1.0.345.gbin
       4096    Jun 24 21:08:43 2013  vdc_2/
       4096    Jun 24 21:08:43 2013  vdc_3/
       4096    Jun 24 21:08:43 2013  vdc_4/
    8401501    Jun 24 21:08:17 2013  vsmcpa.3.0.0.112.bin

Usage for bootflash://
  499183616 bytes used
 5904785408 bytes free
 6403969024 bytes total
```

Uncompressing Files

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

Before You Begin

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

Procedure

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

```
switch# gunzip bootflash:errorsfile.gz
switch# dir bootflash:
       2687     Jul 01 18:17:20 2013  errorsfile
      16384     Jun 30 05:17:51 2013  lost+found/
       4096     Jun 30 05:18:29 2013  routing-sw/
         49     Jul 01 17:09:18 2013  sample_test.txt
    1322843     Jun 30 05:17:56 2013  nexus-1000v-dplug-mzg.5.2.1.SK1.1.0.345.gbin
   21629952     Jun 30 05:18:02 2013  nexus-1000v-kickstart-mzg.5.2.1.SK1.1.0.345.gbin
   39289400     Jun 30 05:18:14 2013  nexus-1000v-mzg.5.2.1.SK1.1.0.345.gbin

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

Directing Command Output to a File

Procedure

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

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

Verifying a Bootable Image

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# **show version image** [**bootflash:** | **modflash:** |**volatile:**]	Validates the specified image. bootflash:—specifies bootflash as the directory name. volatile:—Specifies volatile as the directory name. modflash:—Specifies modflash as the directory name.

```
switch# show version image bootflash:n1000v-dk9-dplug.5.2.1.SK1.1.0.345.gbin
  MD5 Verification Passed
  image name: n1000v-dk9-dplug.5.2.1.SK1.1.0.345.gbin
  plugin:     version 5.2(1)SK1(1.1) [build 5.2(1)SK1(1.0.345)] [gdb]
  compiled:   6/17/2013 0:00:00 [06/17/2013 12:16:57]
switch#
```

Loading a File into the Running Configuration

You can load an image into the running configuration

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

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

Rolling Back to a Previous Configuration

You can recover your configuration from a previously saved version.

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

Procedure

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

```
switch# copy bootflash:June13 startup-config
```

Displaying Files

Displaying File Contents

Before You Begin

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

Procedure

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

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

switch#
```

Displaying Directory Contents

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

Before You Begin

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

Procedure

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

```
switch# pwd
bootflash:
switch# dir

Usage for volatile://
          0 bytes used
```

```
   20971520 bytes free
   20971520 bytes total
switch#
```

Displaying File Checksums

You can display checksums for checking file integrity.

Procedure

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

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

Displaying the Last Lines in a File

Before You Begin

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

Procedure

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

```
switch# tail mts.log 5
AT 60000 usecs after 6/24/2013 21:8:37: MTS node 4: state changed from 'offline' to
'supervisor'
AT 820000 usecs after 6/24/2013 21:8:41: MTS node 4: state changed from 'supervisor' to
'active alone'

AT 310000 usecs after 6/24/2013 21:29:57: MTS state 'offline': last_sync_msg opc=0,
seq_no=0x0, next_seqno=0x0
AT 310000 usecs after 6/24/2013 21:29:57: MTS node 4: state changed from 'offline' to
'supervisor'
AT 740000 usecs after 6/24/2013 21:30:7: MTS node 4: state changed from 'supervisor' to
'active alone'
```

Feature History for File Management

Feature Name	Releases	Feature Information
File Management	Release 5.2(1)SK1(2.1)	This feature was introduced.

CHAPTER 8

Managing Users

This chapter contains the following sections:

Information About User Management

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

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

Displaying Current User Access

You can display all users currently accessing the switch.

Before You Begin

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

Procedure

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

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

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

Sending a Message to Users

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

Before You Begin

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

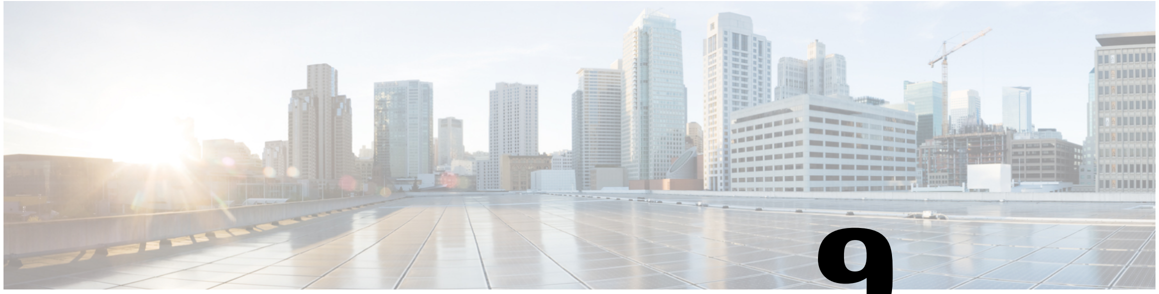
Procedure

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

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

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

Hello. Shutting down the system in 10 minutes.


switch#
```

Feature History for User Management

Feature Name	Releases	Feature Information
User Management	Release 5.2(1)SK1(2.1)	This feature was introduced.



CHAPTER 9

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.

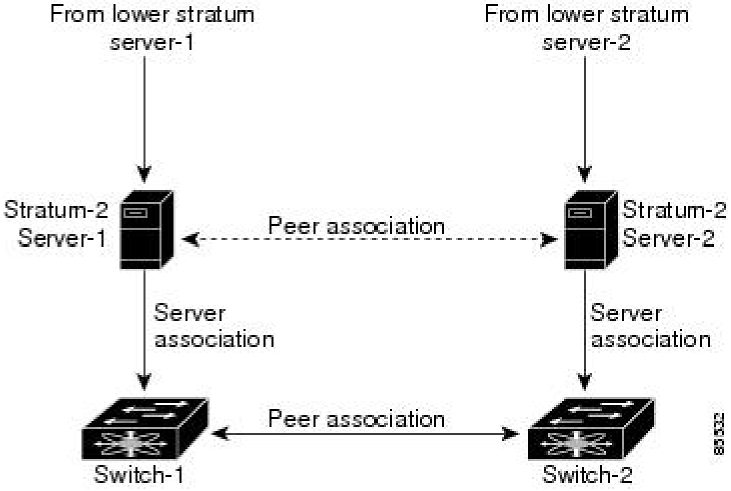
If the network is isolated from the Internet, Cisco NX-OS allows you to configure a network device so that the device acts as though it is synchronized through NTP, when it has determined the time by using other means. Other network devices can then synchronize to that network device through NTP.

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

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

Procedure

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

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

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

Clearing NTP Sessions

Command	Purpose
clear ntp session	Clears the NTP sessions.

Clearing NTP Statistics

Command	Purpose
clear ntp statistics	Clears the NTP sessions.

Verifying the NTP Configuration

Use one of the following commands to verify the configuration:

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

Feature History for NTP

Feature Name	Releases	Feature Information
NTP	Release 5.2(1)SK1(2.1)	This feature was introduced.

CHAPTER 10

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 channel, 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 Ethernet Module (VEM) 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 or virtual Ethernet port, a port channel, 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 VEM. 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 (VEM)
- 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

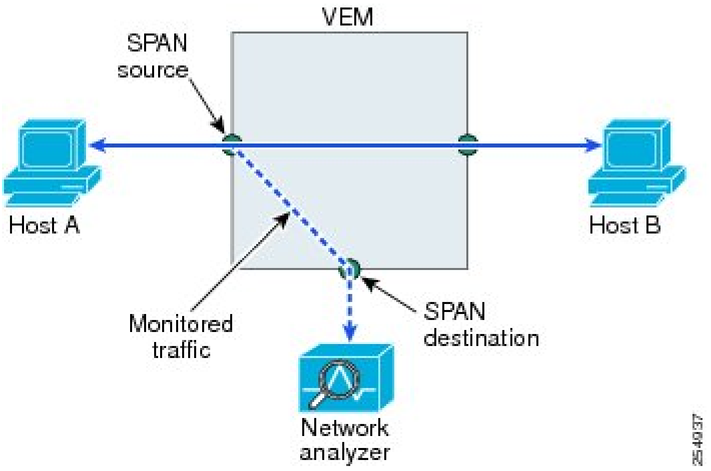
In Local SPAN, the source interface and destination interface are on the same VEM. The network analyzer is attached directly to the SPAN destination port. The SPAN source can be a port, a VLAN interface, or a port profile.The destination can be a port or port profile.

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

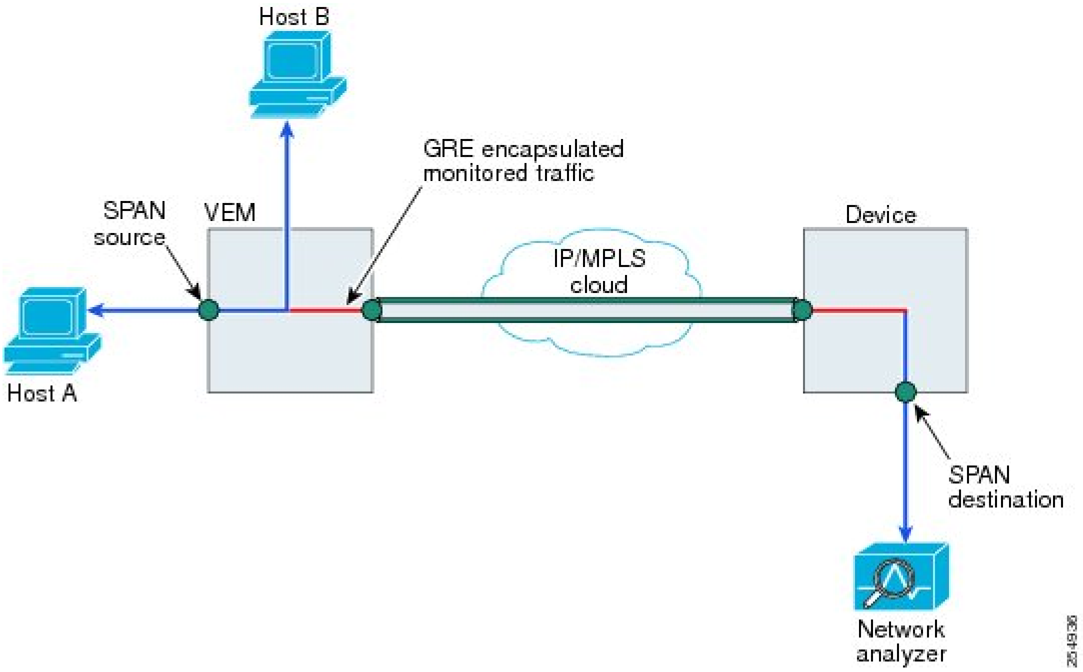


Encapsulated Remote SPAN

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.

To use NAM for monitoring the Cisco Nexus 1000V ERSPAN data sources, see the *Cisco Nexus 1010 Network Analysis Module Installation and Configuration Note.*

SPAN Sessions

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

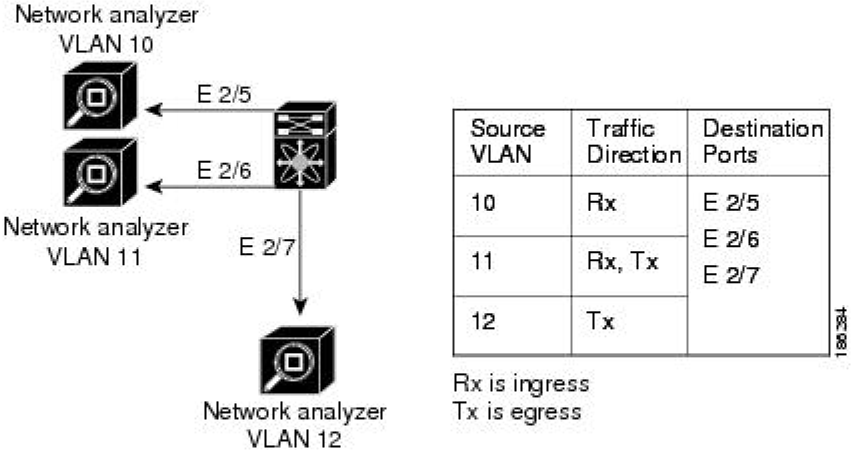
You must configure an ERSPAN session ID that is added to the ERSPAN header of the encapsulated frame to differentiate between ERSPAN streams of traffic at the termination box. You can also configure the range of flow ID numbers.

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



Source VLAN	Traffic Direction	Destination Ports
10	Rx	E 2/5 E 2/6 E 2/7
11	Rx, Tx	
12	Tx	

Rx is ingress
Tx is egress

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.

- 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.

- Dynamic port profiles such as a source or destination cannot be added to the SPAN/ERSPAN session. To add these port profiles, create a static port profile and then add it to the SPAN/ERSPAN 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 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 1000V Interface Configuration Guide*.

Before You Begin

- Log into the CLI in EXEC mode
- Determine the number of the SPAN session 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*	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” section on page 9-9 • For the **traffic direction** keywords, specify as follows: ◦ **rx** which is the VLAN default indicates receive. ◦ **tx** indicates transmit.

	Command or Action	Purpose
		◦ **both**is the default keyword
Step 6	Repeat Step 5 to configure additional SPAN sources.	(Optional)
Step 7	switch(config-monitor)# **filter vlan** {*id* | *range*}	(Optional) For the specified SPAN session, configures the filter from among the source VLANs.
Step 8	Repeat Step 7 to configure all source VLANs to filter.	(Optional)
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	Repeat Step 9 to configure all SPAN destination ports.	(Optional)
Step 11	switch(config-monitor)# **no shut**	Enables the SPAN session. By default, the session is created in the shut state.
Step 12	switch(config-monitor)# **exit**	(Optional) Exits monitor configuration mode and places you in interface configuration mode.
Step 13	switch(config-if)# **show monitor session** *session-number*	(Optional) 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	switch(config-if)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

```
switch# configure terminal
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 the OpenStack Horizon server.

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 ERSPAN local Layer 3 interface can be assigned to this Layer 3 control port profile per host as follows:

- If more than one ERSPAN local Layer 3 interface is assigned to a host, the first one assigned takes effect. The second one is not considered a Layer 3 interface.
- If more than one ERSPAN local Layer 3 interface is assigned to a host, and you remove the second assigned one, the VEM does not use the first assigned one. Instead, you must remove both the ERSPAN local Layer 3 interfaces and then add one back.

Before You Begin

- Log into the CLI in EXEC mode
- Ensure that a name has been established for this port profile

Note The port profile name is used to configure the ERSPAN local Layer 3 interface. An ERSPAN local Layer 3 interface is required on each KVM host to send ERSPAN-encapsulated IP packets; and must have IP connectivity to the ERSPAN destination IP address.

- Ensure that a name has been established for the OpenStack policy profile to which this profile maps. For information, see the *Cisco Nexus 1000V for KVM Virtual Network Configuration Guide*.
- Created the system VLAN that sends IP traffic to the ERSPAN destination; and you know the VLAN ID that will be used in this configuration.

- Obtained the documentation for adding a new virtual adapter.

For more information about system port profiles, see the *Cisco Nexus 1000V Port Profile Configuration Guide*.

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 places you in 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 1000V.
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)# **publish port-profile***name*	Designates the port profile as an OpenStack policy profile and adds the name of the OpenStack policy profile to which this profile maps. This command saves the settings in the running configuration. The port profile is mapped to a OpenStack policy profile of the same name. When an OpenStack Horizon server connection is established, the port group created in Cisco Nexus 1000V is then distributed to the virtual switch on the OpenStack Horizon 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).
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)# **state enabled**	Enables the port profile in the running configuration. This port profile is now ready to send out ERSPAN packets on all KVM hosts with ERSPAN sources.

	Command or Action	Purpose
Step 9	switch(config-prot-prof)# **show port-profile name** *port_profile_name*	(Optional) Displays the configuration for the specified port profile as it exists in the running configuration.
Step 10	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.
Step 11	To configure the ERSPAN local Layer 3 interface, navigate to the `/etc/n1kv/n1kv.conf` file and enter the details such as, the portname, port profile, IP address, subnet, and the MAC address. For example, virt erspan0 profile erspan-pp mode static address 30.30.30.20 netmask 255.255.255.0 mac 00:22:44:34:ab:cd.	

```
switch# configure terminal
switch(config)# port-profile erspan_profile
switch(config-port-prof)# capability l3control
switch(config-port-prof)# publish port-profile
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)# 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. The step to do this is included in the procedure.

Before You Begin

- Log into 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

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* **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** which is the VLAN default indicates receive. ◦ **tx** indicates transmit. ◦ **both**is the default keyword
Step 6	Repeat Step 5 to configure additional ERSPAN sources.	(Optional)

	Command or Action	Purpose
Step 7	switch(config-erspan-src)# **filter vlan** {*number* | *range*}	(Optional) 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.
Step 8	Repeat Step 7 to configure all source VLANs to filter.	(Optional)
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	switch(config-erspan-src)# **ip ttl** *ttl_value*	(Optional) 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	switch(config-erspan-src)# **mtu** *mtu_value*	(Optional) Specifies an MTU size (from 50 to 1500) 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 switch, truncated ERSPAN packets are dropped unless the **no mls verify ip length consistent** command is configured on the Cisco 6500.
Step 12	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.)
Step 13	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 14	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.

	Command or Action	Purpose
Step 15	switch(config-erspan-src)# **show monitor session** *session_id*	(Optional) Displays the ERSPAN session configuration as it exists in the running configuration
Step 16	switch(config-erspan-src)# **copy running-config startup-config**	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

```
switch# configure terminal
switch(config)# 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)# 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 Monitor Configuration Mode

Before You Begin

- Log into the CLI in EXEC mode.
- Determine which session you want to shutdown

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. • The *session-range* argument specifies a range of SPAN sessions from 1 to 64. • The **all** keyword specifies all SPAN monitor sessions.

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

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

Shutting Down a SPAN Session from Monitor Configuration Mode

Before You Begin

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

- Logged in to the CLI in EXEC mode.
- Determined which session you want to shutdown

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. • 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.

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

```
switch# configure terminal
switch(config)# 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 into 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. • The **all** keyword specifies all SPAN monitor sessions.
Step 3	switch(config)# **show monitor**	(Optional) Displays the status of the SPAN sessions.

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

```
switch# configure terminal
switch(config)# 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 into 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	switch(config-monitor)# **show monitor**	(Optional) Displays the status of the SPAN sessions.
Step 4	switch(config-monitor)# **show monitor session** *session-id*	(Optional) Displays detailed configuration and status of a specific SPAN session for verification.

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

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

Use this procedure to 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 into 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 = 1 The maximum value = 1023 The **no** form of this command removes any configured values and restores default values.
Step 3	switch(config)# **show running monitor**	(Optional) Displays changes to the default limit-resource erspan-flow-id values for verification

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

```
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 vem *module-number* **execute vemcmd show span**	Displays the configured SPAN sessions on a VEM module.
show port-profile name *port_profile_name*	Displays a port profile.

Configuration Example for an ERSPAN Session

The following example shows how to create an ERSPAN session for a source Ethernet interface and destination IP address on the Cisco Nexus 1000V.CSCtn56340 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 3/3
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 vem 3 execute vemcmd show span

VEM 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

```
 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 port-channel 2
  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 Eth2/2 Eth2/3
    tx            : Eth2/1 Eth2/2 Eth2/3
    both          : Eth2/1 Eth2/2 Eth2/3
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 : Eth2/5
destination port-profile : my_profile_dst

switch# module vem 3 execute vemcmd show span

VEM SOURCE IP NOT CONFIGURED.

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

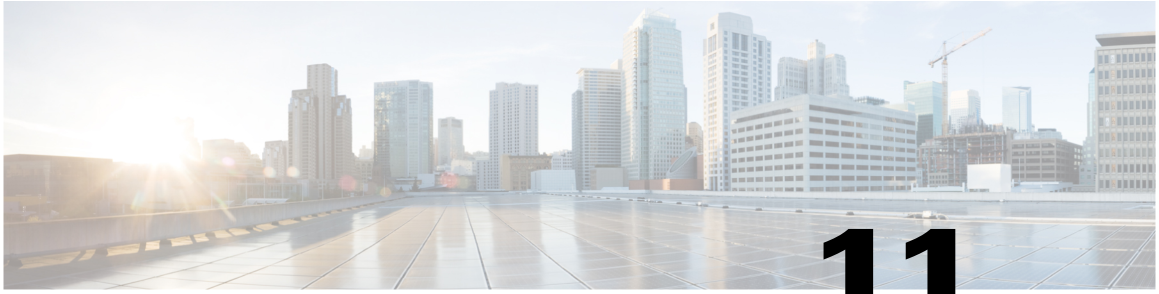
Example of a Configuration to Enable SPAN Monitoring

This example shows how to configure destination ports in access or trunk mode, and enable SPAN monitoring.

```
switch# configure terminal
  switch(config)# interface ethernet 2/5
  switch(config-if)# switchport
  switch(config-if)# switchport mode trunk
  switch(config-if)# no shut
  switch(config-if)# exit
  switch(config)#
```

Feature History for SPAN and ERSPAN

Feature Name	Releases	Feature Information
SPAN and ERSPAN	5.2(1)SK3(2.1)	SPAN and ERSPAN were introduced.



CHAPTER 11

Configuring SNMP

This chapter contains the following sections:

Information About SNMP

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

SNMP Functional Overview

The SNMP framework consists of three parts:

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

SNMP is defined in RFCs 3411 to 3418.

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

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

SNMP Notifications

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

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

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

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

SNMPv3

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

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

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

Security Models and Levels for SNMPv1, v2, v3

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

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

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

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

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	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. See for information on how to modify this default value.

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

Configuring SNMP Users

Before You Begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Places you in global configuration mode.
Step 2	switch(config)# **snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv**	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**

	Command or Action	Purpose
	[**aes-128**] *passphrase*] [**engineID** *id*] [**localizedkey**]]	keyword, the *passphrase* can be any case-sensitive, alphanumeric string up to 130 characters. The *name* argument is the name of a user who can access the SNMP engine. The **auth** keyword enables one-time authentication for SNMP over a TCP session. It is optional. The **md5** keyword specifies HMAC MD5 algorithm for authentication. It is optional. The **sha** keyword specifies HMAC SHA algorithm for authentication. It is optional. The **priv** keyword specifies encryption parameters for the user. It is optional. The **aes-128** keyword specifies a 128-byte AES algorithm for privacy. It is optional. The **engineID** keyword specifies the engineID for configuring the notification target user (for V3 informs). It is optional. The *id* is a 12-digit colon-separated decimal number.
Step 3	switch(config-callhome)# **show snmp user**	(Optional) Displays information about one or more SNMP users.
Step 4	switch(config-callhome)# **copy running-config startup-config**	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

```
switch(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(config)# **snmp-server globalEnforcePriv**	Enforces SNMP message encryption for all users.

Creating SNMP Communities

You can create SNMP communities for SNMPv1 or SNMPv2c.

Before You Begin

You must be in global configuration mode.

Procedure

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

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 over UDP and TCP. After creating the ACL, assign the ACL to the SNMP community. For more information on creating ACLs, see the Nexus 1000V for Microsoft Hyper-V Security Configuration Guide.

Use the following commands in global configuration mode to assign an ACL to a community to filter SNMP requests:

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.
Step 2	switch(config)# **ip access-list acl_for_community**	Creates the named access list or places you in configuration mode for the specified access list.
Step 3	switch(config-acl)# **statistics per-entry**	Configures statistics.
Step 4	switch(config-acl)# **permit udp any any**	Permits UDP protocol.
Step 5	switch(config-acl)# **show ip access-lists**	(Optional) Displays show command output.
Step 6	switch(config-acl)# **exit**	Exits the current configuration mode.
Step 7	switch(config)# **snmp community** *community-name*	Configures SNMP community.
Step 8	switch(config)# **snmp community** *community-name* **use-acl** *acl-name*	Assigns an ACL to an SNMP community to filter SNMP requests.
Step 9	switch(config)# **show snmp community**	(Optional) Displays show command output.

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip access-list acl_for_community
switch(config-acl)# statistics per-entry
switch(config-acl)# permit udp any any
switch(config-acl)# show ip access-lists

IPV4 ACL acl_for_community
        statistics per-entry
        10 permit udp any any [match=0]

switch(config-acl)# exit
switch(config)# snmp community public
switch(config)# snmp community public use-acl acl_for_community
switch(config)# show snmp community
SNMP_svr1                       network-operator
public                          network-operator               acl_for_community

switch(config)#
```

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. The community can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

Configuring a Host Receiver for SNMPv2c Traps or Informs

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** | **informs**} **version 2c** *community* [**udp_port** *number*]	Configures a host receiver for SNMPv2c traps or informs. The community can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

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 device to authenticate and decrypt the SNMPv3 messages

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** | **informs**} **version 3** {**auth** | **noauth** | **priv**} *username* [**udp_port** *number*]	Configures a host receiver for SNMPv2c traps or informs. The username can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

```
switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS
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 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 inform s

Before You Begin

You must be in global configuration mode to configure the notification target user.

Procedure

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

Enabling SNMP Notifications

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

The following table lists the commands that enable the notifications for Cisco 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.

Before You Begin

You must be in global configuration mode.

Procedure

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

	Command or Action	Purpose
Step 6	switch(config)# **snmp-server enable traps snmp** [**authentication**]	Enables the SNMP agent notifications.

```
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 this limit notifications on flapping interface (an interface that transitions between up and down repeatedly).

Before You Begin

You must be in interface configuration mode.

Procedure

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

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(config)# **snmp-server tcp-session** [**auth**]	Enables a one-time authentication for SNMP over a TCP session. The default is disabled.

```
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	switch(config)# **show snmp**	(Optional) Displays information about one or more destination profiles.
Step 5	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

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

Disabling SNMP

Before You Begin

You must be in global configuration mode.

Procedure

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

Modifying the AAA Synchronization Time

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

Before You Begin

You must be in global configuration mode.

Procedure

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

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

Verifying the SNMP Configuration

Use one of the following commands to verify the configuration:

Command	Purpose
show 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.

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

MIBs

Following is information about the supported SNMP MIBs.
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
- 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-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

Feature History for SNMP

Feature Name	Releases	Feature Information
SNMP	Release 5.2(1)SK1(2.1)	This feature was introduced.

CHAPTER 12

Configuring NetFlow

This chapter contains the following sections:

Information About NetFlow

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

What is a Flow

You create a flow using a flow record to define the criteria for your flow. All criteria must match for the packet to count in the given flow. Flows are stored in the NetFlow cache. Flow information tells you the following:

- Source address tells you who is originating the traffic.
- Destination address tells who is receiving the traffic
- Ports characterize the application that uses the traffic

- Class of service examines the priority of the traffic
- The device interface tells how traffic is being used by the network device
- Tallied packets and bytes show the amount of traffic

Flow Record Definition

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

Predefined Flow records use 32-bit counters and are not recommended for data rates above 1 Gbps. For data rates that are higher than 1 Gbps, Cisco recommends that you manually configure the records to use 64-bit counters.

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

Table 2: Flow Record Criteria

Flow Record Criteria	Description
Match	Defines the information that is matched for collection in the flow record. • ip—Data collected in the flow record matches one of the following IP options: ◦ Protocol ◦ tos (type of service) • iIPv4—Data collected in the flow record matches one of the following IPv4 address options: ◦ Source address ◦ Destination address • Transport—Data collected in the flow record that matches one of the following transport options: ◦ Destination port ◦ Source port • datalink—Data collected in the flow record matches one of the following datalink options: ◦ mac source-address ◦ mac destination-address ◦ ethertype ◦ vlan ◦ vxlan **Note** Layer 2 fields can be matched only then IP fields are not present in the record.

Flow Record Criteria	Description
Collect	Defines how the flow record collects information. • Counter—Collects flow record information in one of the following formats: ◦ Bytes—32-bit counter. (default) ◦ Bytes long—64-bit counter (recommended for data rates that are higher than 1 Gbps). ◦ Packets—32-bit counter (default) ◦ Packets long—64-bit counters (recommended for data rates that are higher than 1 Gbps) • timestamp sys-uptime—Collects the system up time for the first or last packet in the flow. • transport tcp flags—Collects the TCP transport layer flags for the packets in the flow. **Note** 64-bit counters are recommended.

Predefined Flow Records

Cisco Nexus 1000V Predefined Flow Record: Netflow-Original

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

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

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

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

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

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

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

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

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

Accessing NetFlow Data

You can use two methods to access NetFlow data:

- Command-line interface (CLI)
- NetFlow collector (a separate product from the Cisco Nexus 1000V for KVM)

Command-line Interface for NetFlow

You can use the CLI to access NetFlow data and to view what is happening in your network now.

The CLI uses a flow monitor and a flow exporter to capture and export flow records to the Netflow collector. Cisco Nexus 1000V supports the NetFlow Version 9 export format.

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

Flow Monitor

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

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

This flow monitor enables a set, which consists of a record and an exporter. You can define this set once and reuse it multiple times. You can create multiple flow monitors for different needs. A flow monitor is applied to a specific interface or port-profile in a specific direction.

Flow Exporter

The flow exporter is used to define the source and destination of the flow records. The source is from the VEM module and the destination is the reporting server, called the Netflow Collector. An IP packet is sent from the source to the destination with the collected information. The packet will originate from the VEM, but the user can configure which IP address is placed in the source field of the IP packet. The destination requires an IP address as well as a UDP port number for which the Netflow Collector will listen for packets.

An exporter definition includes the following:

- Destination IP address
- UDP port number (where the collector is listening)
- Source IP Address to spoof (not the actual source location, but the address placed in in the IP packet sent to the collector)
- Export format version

NetFlow Collector

NetFlow data reporting process is as follows:

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

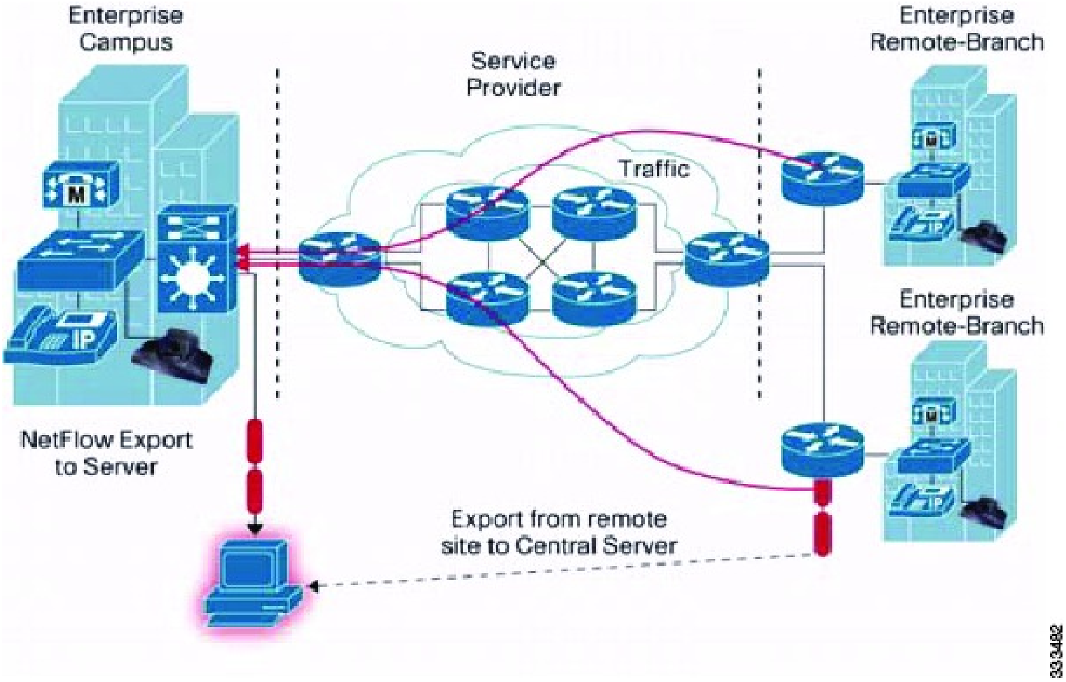
Exporting Flows to the NetFlow Collector Server

Timers determine when a flow is exported to the NetFlow collector server. See the followling figure where a flow is ready for export when one of the following occurs:

- The flow is inactive for a certain time amount of time, inactive timer, during which no new packets are received for the flow.

- The flow has lived longer than the active timer, such as, a long FTP download.

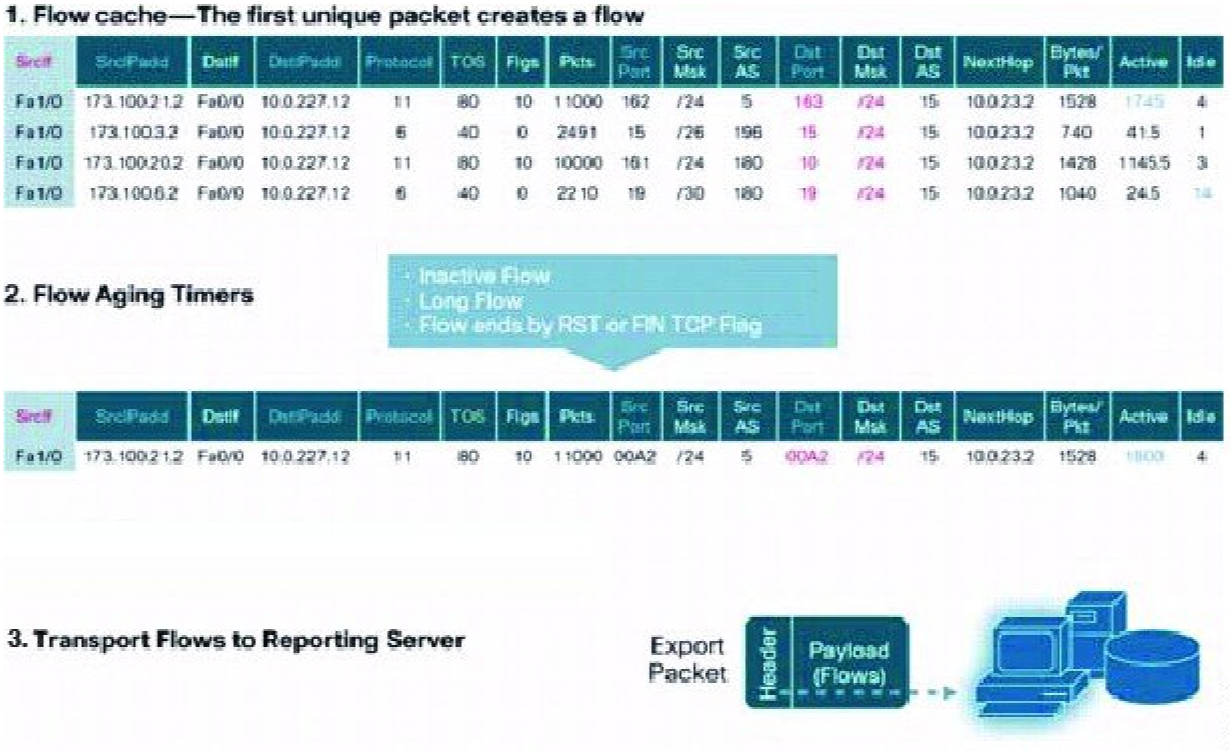
Figure 6: Exporting Flows to the NetFlow Collector Server



What NetFlow Data Looks Like

The following figure shows an example of NetFlow data.

Figure 7: NetFlow Cache Example



1. Flow cache—The first unique packet creates a flow

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	NextHop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	162	/24	5	163	/24	15	10.0.23.2	1528	1745	4
Fa1/0	173.100.3.2	Fa0/0	10.0.227.12	6	40	0	2491	15	/26	196	15	/24	15	10.0.23.2	740	41.5	1
Fa1/0	173.100.20.2	Fa0/0	10.0.227.12	11	80	10	10000	161	/24	180	10	/24	15	10.0.23.2	1428	1145.5	3
Fa1/0	173.100.6.2	Fa0/0	10.0.227.12	6	40	0	2210	19	/30	180	19	/24	15	10.0.23.2	1040	24.5	14

2. Flow Aging Timers

- Inactive Flow
- Long Flow
- Flow ends by RST or FIN TCP Flag

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	NextHop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.0.23.2	1528	1800	4

3. Transport Flows to Reporting Server

Network Analysis Module

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

High Availability for NetFlow

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

Guidelines and Limitations for NetFlow

- In Cisco Nexus 1000V, the mgmt0 interface IP address of the VSM is configured by default as the source IP address for an exporter.

- Predefined Flow records use 32-bit counters are recommended for data rates above 1 Gbps. For data rates that are higher than 1 Gbps, Cisco recommends that you manually configure the records to use 64-bit counters.
- The Cisco Nexus 1000V includes the following predefined flow records:
  - netflow-original—The Cisco Nexus 1000V predefined traditional IPv4 input NetFlow with origin ASs

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

  - netflow ipv4 original-input—The Cisco Nexus 1000V predefined traditional IPv4 input NetFlow
  - netflow ipv4 original-output—The Cisco Nexus 1000V predefined traditional IPv4 output NetFlow
  - netflow protocol-port—The Cisco Nexus 1000V predefined protocol and ports aggregation scheme
- Up to 8,000 NetFlow instances are allowed per Distributed Virtual Switch (DVS).
- Up to 300 NetFlow instances are allowed per host.
- A maximum of one flow monitor per interface per direction is allowed.
- Up to two flow exporters are permitted per monitor.
- Up to 64 NetFlow monitors, exporters, or records are allowed per DVS.
- NetFlow is not supported on on port channels or interfaces in a portchannel.

Default Settings for NetFlow

Table 3: Default NetFlow Parameters

Parameters	Default
NetFlow version	9
source	line card export with spoofed mgmt0 IP address of the VSM
match	direction and interface (incoming/outgoing)
flow monitor active timeout[1]	1800
flow monitor inactive timeout [2]	45
DSCP	default/best-effort (0)
VRF	management (1)

[1] Cisco recommends that the difference between the flow active timeout and the flow inactive timeout be a minimum of 1600 seconds.

[2] Cisco recommends that the difference between the flow active timeout and the flow inactive timeout be a minimum of 1600 seconds.

Enabling the NetFlow Feature

Before You Begin

You are logged in to the CLI in EXEC mode.

Procedure

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

This example shows how to enable the NetFlow feature:

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

Configuring Netflow

Defining a Flow Record

Before You Begin

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

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

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

Procedure

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td><b>Step 1</b></td><td>switch# <b>configure terminal</b></td><td>Enters global configuration mode.</td></tr>
<tr><td><b>Step 2</b></td><td>switch(config)# <b>flow record</b> <i>name</i></td><td>Creates a Flow Record by name, and places you in the CLI Flow Record Configuration mode for that specific record.</td></tr>
<tr><td><b>Step 3</b></td><td>switch(config-flow-record)# <b>description</b> <i>string</i></td><td>(Optional) Adds a description of up to 63 characters to the Flow Record and saves it to the running configuration.</td></tr>
<tr><td><b>Step 4</b></td><td>switch(config-flow-record)# <b>match</b> {<b>ip</b> {<b>protocol</b> | <b>tos</b>} | <b>ipv4</b> {<b>destination</b> | <b>source</b>} | <b>transport</b> {<i>destination-port</i> | <i>source-port</i>} | <b>datalink</b> {{<b>mac</b> {<i>source-address</i> | <i>destination-address</i>}} | <b>ethertype</b> | <b>vlan</b> | <b>vxlan</b> }}</td><td>Defines the Flow Record to match one of the following and saves it in the running configuration.
• ip—Matches one of the following IP options:
◦ protocol
◦ tos (type of service)
• ipv4—Matches one of the following ipv4 address options:
◦ source address
◦ destination address
• transport—Matches one of the following transport options:
◦ destination port
◦ source port
• datalink— Data collected in the flow record matches one of the following datalink options:
◦ mac source-address
◦ mac destination-address
◦ ethertype
◦ vlan
◦ vxlan</td></tr>
</table>

	Command or Action	Purpose
		Note Netflow does not support mixing datalink fields with other field types in the same record.
Step 5	switch(config-flow-record)# **collect** {**counter** {**bytes** [**long**] | **packets** [**long**]} | **timestamp sys-uptime**{*first* | *last*} | **transport tcp flags**}	Specifies a collection option to define the information to collect in the Flow Record and saves it in the running configuration. • counter—Collects Flow Record information in one of the following formats: ◦ bytes: collected in 32-bit counters unless the long 64-bit counter is specified. ◦ packets: collected in 32-bit counters unless the long 64-bit counter is specified. **Note** Cisco recommends that the 64-bit counters be used for systems with data rates in excess of 1 Gbps. • timestamp sys-uptime—Collects the system up time for the first or last packet in the flow. • transport tcp flags—Collects the TCP transport layer flags for the packets in the flow.
Step 6	switch(config-flow-record)# **show flow record** [**name**]	(Optional) Displays information about Flow Records.
Step 7	switch(config-flow-record)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to create a flow record:

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

Defining a Flow Exporter

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

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

Before You Begin

- You know the destination IP address of the NetFlow Collector Server.
- You know the transport UDP port that the Collector is listening on.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)#**flow exporter** *name*	Creates a Flow Exporter, saves it in the running configuration, and then places you in CLI Flow Exporter Configuration mode.
Step 3	switch(config-flow-exporter)# **description** *string*	Adds a description of up to 63 characters to this Flow Exporter and saves it in the running configuration.
Step 4	switch(config-flow-exporter)# **destination** *ipv4-address*	Specifies the IP address of the destination interface for this Flow Exporter and saves it in the running configuration.
Step 5	switch(config-flow-exporter)# **dscp** *value*	Specifies the differentiated services codepoint value for this Flow Exporter, between 0 and 63, and saves it in the running configuration.
Step 6	switch(config-flow-exporter)# **source lc-exp** *ipv4-address/subnet-mask*	(Optional) Specifies the IP address to spoof, from which the Flow Records are sent to the NetFlow Collector Server, and saves it in the running configuration.
Step 7	switch(config-flow-exporter)# **transport udp** *port-number*	Specifies the destination UDP port, between 1 and 65535, used to reach the NetFlow collecton, and saves it in the running configuration.
Step 8	switch(config-flow-exporter)# **version** {**9**}	Specifies NetFlow export version 9, saves it in the running configuration, and places you into the export version 9 configuration mode.
Step 9	switch(config-flow-exporter-version-9)# **option** {**exporter-stats** | **interface-table**} **timeout** *value*	Specifies one of the following version 9 exporter resend timers and its value, between 1 and 86400 seconds, and saves it in the running configuration. • exporter-stats

	Command or Action	Purpose
		• interface-table
Step 10	switch(config-flow-exporter-version-9)# **template data timeout** *seconds*	Sets the template data resend timer and its value, between 1 and 86400 seconds, and saves it in the running configuration.
Step 11	switch(config-flow-exporter-version-9)# **show flow exporter** [*name*]	(Optional) Displays information about the Flow Exporter.
Step 12	switch(config-flow-exporter-version-9)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to create a flow exporter:

```
switch# configure terminal
switch(config)# flow exporter ExportTest
switch(config-flow-exporter)# description ExportHamilton
switch(config-flow-exporter)# destination 192.0.2.1
switch(config-flow-exporter)# dscp 2
switch(config-flow-exporter)# source lc-exp 192.0.2.2/24
switch(config-flow-exporter)# transport udp 200
switch(config-flow-exporter)# version 9
switch(config-flow-exporter-version-9)# option exporter-stats timeout 1200
switch(config-flow-exporter-version-9)# template data timeout 1200
switch(config-flow-exporter-version-9)# show flow exporter ExportTest
Flow exporter ExportTest:
    Description: ExportHamilton
    Destination: 192.0.2.1
    VRF: management (1)
    Destination UDP Port 200
    Source IP Address 192.0.2.2
    Export from Line Card
    DSCP 2
    Export Version 9
        Exporter-stats timeout 1200 seconds
        Data template timeout 1200 seconds
    Exporter Statistics
        Number of Flow Records Exported 0
        Number of Templates Exported 0
        Number of Export Packets Sent 0
        Number of Export Bytes Sent 0
        Number of Destination Unreachable Events 0
        Number of No Buffer Events 0
        Number of Packets Dropped (No Route to Host) 0
        Number of Packets Dropped (other) 0
        Number of Packets Dropped (LC to RP Error) 0
        Number of Packets Dropped (Output Drops) 1
        Time statistics were last cleared: Never
switch(config-flow-exporter-version-9)# copy running-config startup-config
switch(config-flow-exporter-version-9)#
```

Defining a Flow Monitor

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

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

Before You Begin

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

Note Cisco recommends that you use the predefined flow records for systems with a lower data rate. For systems operating at a higher data rate of more than 1 Gbps, Cisco recommends that you manually configure the flow record and use the 64-bit long counters.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **flow monitor** *name*	Creates a flow monitor by name, saves it in the running configuration, and then places you in the CLI Flow Monitor Configuration mode.
Step 3	switch(config-flow-monitor)# **description** *string*	(Optional) For the specified flow monitor, adds a descriptive string of up to 63 alphanumeric characters, and saves it in the running configuration.
Step 4	switch(config-flow-monitor)# **exporter** *name*	For the specified flow monitor, adds an existing flow exporter and saves it in the running configuration.
Step 5	switch(config-flow-monitor)# **record** { [*name* | **netflow** {**ipv4**}] | **netflow-original** | **original-input** |**original-output** |**protocol-port**}	For the specified flow monitor, adds an existing flow record and saves it in the running configuration. • name: The name of a flow record you have previously created, or the name of a Cisco provided pre-defined flow record. • netflow: Traditional NetFlow collection schemes ipv4: Traditional IPv4 NetFlow collection schemes
Step 6	switch(config-flow-monitor)# **show flow monitor** [*name*]	(Optional) Displays information about existing flow monitors.

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

The following example shows how to create a flow exporter:

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

Assigning a Flow Monitor to an Interface

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *interface-type interface-number*	Places you in the CLI Interface Configuration mode for the specified interface.
Step 3	switch(config-if)# **ip flow monitor** *name* {**input** | **output**}	For the specified interface, assigns a flow monitor for input or output packets and saves it in the running configuration.
Step 4	switch(config-if)# **show flow interface** *interface-type interface-number*	(Optional) For the specified interface, displays the NetFlow configuration.
Step 5	switch(config-if)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

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

```
switch# configure terminal
switch(config)# interface veth 2
switch(config-if)# ip flow monitor MonitorTest output
switch(config-if)# show flow interface veth 2
Interface Vethernet2:
    Monitor: MonitorTest
    Direction: Output
switch(config-if)#
```

Adding a Flow Monitor to a Port Profile

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** [**type** {**ethernet** | **vethernet**}] *name*	Enters port profile configuration mode for the named port profile.
Step 3	switch(config-port-prof)# **ip flow monitor** *name* {**input** | **output**}	Applies a named flow monitor to the port profile for either incoming (input) or outgoing (output) traffic.
Step 4	switch(config-port-prof)# **show port-profile** [**expand-interface**] [**name** *profile-name*]	(Optional) Displays the configuration for verification.
Step 5	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

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

```
switch# configure terminal
switch(config)# port-profile AccessProf
switch(config-port-prof)# ip flow monitor access4 output
switch(config-port-prof)# show port-profile name AccessProf
port-profile AccessProf
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    ip flow monitor access4 output
  evaluated config attributes:
    ip flow monitor access4 output
  assigned interfaces:
switch(config-port-prof)#
```

Verifying the NetFlow Configuration

Use one of the following commands to verify the configuration:

Command	Purpose
show flow cache	Displays information about NetFlow flow cache.
show flow exporter [*name*]	Displays information about NetFlow flow exporter.
show flow interface [*interface-type number*]	Displays information about NetFlow interfaces.
show flow monitor [*name* [**cache module** *number* | **statistics module** *number*]]	Displays information about NetFlow flow monitors. **Note** The **show flow monitor cache module** command differs from the **show flow monitor statistics module** command in that the cache command also displays cache entries.
show flow record [*name*]	Displays information about NetFlow flow records.
show flow timeout	Displays the NetFlow flow timeout setting.

Example: show flow exporter

```
switch(config-flow-exporter-version-9)# show flow exporter ExportTest
Flow exporter ExportTest:
    Description: ExportHamilton
    Destination: 192.0.2.1
    VRF: management (1)
    Destination UDP Port 200
    Source IP address 192.0.2.2
    Export from Line Card
    DSCP 2
    Export Version 9
        Exporter-stats timeout 1200 seconds
        Data template timeout 1200 seconds
    Exporter Statistics
        Number of Flow Records Exported 0
        Number of Templates Exported 0
        Number of Export Packets Sent 0
        Number of Export Bytes Sent 0
        Number of Destination Unreachable Events 0
        Number of No Buffer Events 0
        Number of Packets Dropped (No Route to Host) 0
        Number of Packets Dropped (other) 0
        Number of Packets Dropped (LC to RP Error) 0
        Number of Packets Dropped (Output Drops) 1
        Time statistics were last cleared: Never
switch(config-flow-exporter-version-9)#
```

Example: show flow interface

```
switch(config-if)# show flow interface veth2
Interface Vethernet2:
    Monitor: MonitorTest
    Direction: Output
switch(config-if)#
```

Example: show flow monitor

```
switch(config-flow-monitor)# show flow monitor
Flow Monitor MonitorTest:
    Use count: 1
    Flow Record: test
    Flow Exporter: ExportTest
Flow Monitor MonitorIpv4:
    Use count: 70
    Flow Record: RecordTest
    Flow Exporter: ExportTest
switch(config-flow-monitor)#
```

Example: show flow monitor cache module

```
switch(config-port-prof)# show flow monitor mDocs cache module 5
Cache type:                          Normal
Cache size (Bytes):                  224
Active Flows:                        8
Flows added:                         8
Packets added:                       228
Flows aged:                          0
    - Watermark aged                 0
    - Inactive timeout               0
    - Active timeout                 0
    - Event aged                     0
    - Emergency aged                 0
    - Permanent                      0
    - Immediate aged                 0
    - Session aged                   0
    - Fast aged                      0
    - Counters Overflow              0

            *  Denotes interface no longer exists, so just the IF Handle is displayed


  IPV4 SRC ADDR    IPV4 DST ADDR           INTF INPUT           INTF OUTPUT  FLOW DIRN
bytes       pkts
===============  ===============  ====================  ====================  =========
==========  ==========
   192.168.0.15     192.168.0.11                 Veth4                 Veth6      Input
5390        55
   192.168.0.11     192.168.0.15                 Veth6                 Veth4      Input
5390        55
   192.168.0.14     192.168.0.10                 Veth1                 Veth5      Input
5292        54
   192.168.0.10     192.168.0.14                 Veth5                 Veth1      Input
5292        54
```

Example: show flow monitor statistics module

```
switch(config)# show flow monitor m1 statistics module 3
Cache type:                          Normal
Cache size:                          0
Active Flows:                        1
Flows added:                         149
Packets added:                       350
Flows aged:                          148
```

```
    - Watermark aged                 0
    - Active timeout                 0
    - Inactive timeout               148
    - Event aged                     0
    - Emergency aged                 0
    - Permanent                      0
    - Immediate aged                 0
    - Session aged                   0
    - Fast aged                      0
    - Counters Overflow              0
switch(config)#
```

Example: show flow record

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

Netflow Example Configuration

The following example shows how to configure flow monitor using a new flow record and apply it to an interface:

```
switch# configure terminal
switch(config)# flow record RecordTest
switch(config-flow-record)# description Ipv4flow
switch(config-flow-record)# match ipv4 destination address
switch(config-flow-record)# collect counter packets
switch(config-flow-record)# exit
switch(config)# flow exporter ExportTest
switch(config-flow-exporter)# description ExportHamilton
switch(config-flow-exporter)# destination 192.0.2.1
switch(config-flow-exporter)# dscp 2
switch(config-flow-exporter)# source lc-exp 192.0.2.2/24
switch(config-flow-exporter)# transport udp 200
switch(config-flow-exporter)# version 9
switch(config-flow-exporter-version-9)# option exporter-stats timeout 1200
switch(config-flow-exporter-version-9)# template data timeout 1200
switch(config-flow-exporter-version-9)# exit
switch(config-flow-exporter)# exit
switch(config)# flow monitor MonitorTest
switch(config-flow-monitor)# description Ipv4Monitor
switch(config-flow-monitor)# exporter ExportTest
switch(config-flow-monitor)# record RecordTest
switch(config-flow-monitor)# exit
switch(config)# interface veth 2
switch(config-if)# ip flow monitor MonitorTest output
switch(config-if)# show flow interface veth 2
Interface Vethernet2:
    Monitor: MonitorTest
    Direction: Output
switch(config-if)#
```

The following example shows how to configure flow monitor using a pre-defined record and apply it to an interface:

```
switch# configure terminal
switch(config)# flow exporter ExportTest
switch(config-flow-exporter)# description ExportHamilton
switch(config-flow-exporter)# destination 192.0.2.1
switch(config-flow-exporter)# dscp 2
switch(config-flow-exporter)# source lc-exp 192.0.2.2/24
switch(config-flow-exporter)# transport udp 200
switch(config-flow-exporter)# version 9
switch(config-flow-exporter-version-9)# option exporter-stats timeout 1200
switch(config-flow-exporter-version-9)# template data timeout 1200
switch(config-flow-exporter-version-9)# exit
switch(config-flow-exporter)# exit
switch(config)# flow monitor MonitorTest
switch(config-flow-monitor)# description Ipv4Monitor
switch(config-flow-monitor)# exporter ExportTest
switch(config-flow-monitor)# record netflow-original
switch(config-flow-monitor)# exit
switch(config)# interface veth 2
switch(config-if)# ip flow monitor MonitorTest output
switch(config-if)# show flow interface veth 2
Interface Vethernet2:
    Monitor: MonitorTest
    Direction: Output
switch(config-if)#
```

Related Documents for NetFlow

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

Feature History for NetFlow

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

Feature Name	Releases	Feature Information
NetFlow	Release 5.2(1)SK1(2.1)	Distributed NetFlow was introduced.

CHAPTER 13

Configuring System Message Logging

This chapter contains the following sections:

Information About System Message Logging

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

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

By default, the device outputs messages to terminal sessions.

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

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

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

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

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

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

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

System Message Logging Facilities

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

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

Facility	Description
cdp	CDP manager
cert-enroll	Certificate enroll daemon
cfs	CFS manager
clis	CLIS manager
cmpproxy	CMP proxy manager
copp	CoPP manager
core	Core daemon
cron	Cron and at scheduling service
daemon	System daemons
dhcp	DHCP manager
diagclient	GOLD diagnostic client manager
diagmgr	GOLD diagnostic manager
eltm	ELTM manager
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

Facility	Description
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
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

Facility	Description
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
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

Facility	Description
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

Parameter	Default
syslog server logging	Disabled
syslog server configuration distribution	Disabled

Configuring System Message Logging

Configuring System Message Logging to Terminal Sessions

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

Procedure

	Command or Action	Purpose
Step 1	switch# **terminal monitor**	Enables the device to log messages to the console.
Step 2	switch# **configure terminal**	Enters global configuration mode.
Step 3	switch(config)# **logging console** [*severity-level*]	Configures the device to log messages to the console session based on a specified severity level or higher. The default severity level is 2.
Step 4	switch(config)# **show logging console**	(Optional) Displays the console logging configuration.
Step 5	switch(config)# **logging monitor** [*severity-level*]	Enables the device to log messages to the monitor based on a specified severity level or higher. The configuration applies to telnet and SSH sessions. The default severity level is 2.
Step 6	switch(config)# **show logging monitor**	(Optional) Displays the monitor logging configuration.
Step 7	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

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

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

Restoring System Message Logging Defaults for Terminal Sessions

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

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

Configuring System Message Logging for Modules

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **logging module** [*severity-level*]	Enables module log messages that have the specified severity level or higher. If the severity level is not specified, the default of 5 is used.
Step 3	switch(config)# **show logging module**	
Step 4	switch(config)# **logging timestamp** {**microseconds** | **milliseconds** | **seconds**}	Sets the logging time-stamp units. The default unit is seconds.
Step 5	switch(config)# **show logging timestamp**	(Optional) Displays the logging time-stamp units configured.
Step 6	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

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

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

Restoring System Message Logging Defaults for Modules

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

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

Configuring System Message Logging for Facilities

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **logging module** [*severity-level*]	Enables module log messages that have the specified severity level or higher. If the severity level is not specified, the default of 5 is used.
Step 3	switch(config)# **show logging module**	(Optional) Displays the module logging configuration.
Step 4	switch(config)# **logging timestamp** {**microseconds** | **milliseconds** | **seconds**}	Sets the logging time-stamp units. The default unit is seconds.
Step 5	switch(config)# **show logging timestamp**	(Optional) Copies the running configuration to the startup configuration.
Step 6	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

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

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

```
Logging timestamp: Microseconds
switch(config)# copy running-config startup-config
switch(config)#
```

Restoring System Message Logging Defaults for Facilities

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

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

Configuring syslog Servers

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

Procedure

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

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

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

Restoring System Message Logging Defaults for Servers

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

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

Using a UNIX or Linux System to Configure Logging

Before You Begin

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

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

Procedure

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

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

$ chmod 666 /var/log/myfile.log

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

Displaying Log Files

Use this procedure to display messages in the log file.

Procedure

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

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

```
switch# show logging last 5
2013 Jun 30 09:37:04 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
2013 Jun 30 09:37:04 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
2013 Jun 30 09:37:05 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
2013 Jun 30 09:37:05 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
2013 Jun 30 09:37:05 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
switch#
```

Verifying the System Message Logging Configuration

Use one of the following commands to verify the configuration:

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

Command	Purpose
show logging timestamp	Displays the logging time-stamp units configuration.

Example: show logging console

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

Example: show logging info

```
switch# show logging info

Logging console:                enabled (Severity: critical)
Logging monitor:                enabled (Severity: notifications)
Logging linecard:               enabled (Severity: notifications)
Logging fex:                    enabled (Severity: notifications)
Logging timestamp:              Seconds
Logging server:                 disabled
Logging logfile:                enabled
        Name - messages: Severity - notifications Size - 10485760

Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     3                       3
aclcomp                 2                       2
acllog                  2                       2
aclmgr                  3                       3
auth                    0                       0
authpriv                3                       3
bootvar                 5                       5
capability              2                       2
capability              2                       2
cdm                     5                       5
cdp                     2                       2
cert_enroll             2                       2
clis                    7                       7
confcheck               2                       2
cron                    3                       3
daemon                  3                       3
eth-port-sec            2                       2
eth_port_channel        5                       5
ethpm                   5                       5
evmc                    5                       5
evms                    2                       2
feature-mgr             2                       2
fs-daemon               2                       2
ftp                     3                       3
fwm                     6                       6
ifmgr                   5                       5
igmp_1                  5                       5
ip                      3                       3
ipv6                    3                       3
kern                    3                       3
l3vm                    5                       5
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
m2rib                   2                       2
mail                    3                       3
```

```
module                  5                       5
monitor                 3                       3
msp                     5                       5
mvsh                    2                       2
news                    3                       3
ntp                     2                       2
platform                5                       5
plugin                  2                       2
port-profile            2                       2
radius                  3                       3
redun_mgr               4                       4
res_mgr                 5                       5
rpm                     5                       5
sal                     2                       2
securityd               3                       3
sksd                    3                       3
smm                     4                       4
snmpd                   2                       2
span                    3                       3
stp                     3                       3
syslog                  3                       3
sysmgr                  3                       3
u6rib                   5                       5
ufdm                    2                       2
urib                    5                       5
user                    3                       3
uucp                    3                       3
vdc_mgr                 6                       6
vem_mgr                 5                       5
vim                     5                       5
vlan_mgr                2                       2
vmm                     5                       5
vms                     5                       5
vns_agent               6                       6
vntag_mgr               6                       6
vshd                    5                       5
xmlma                   3                       3

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

Example: show logging last

```
switch# show logging last 5
2013 Jun 29 17:52:42 S22-DCOS %ETHPORT-5-IF_UP: Interface Ethernet2/5 is up in mode access
2013 Jun 29 17:52:43 S22-DCOS %ETHPORT-5-IF_UP: Interface Ethernet2/2 is up in mode trunk
2013 Jun 29 17:52:43 S22-DCOS %ETHPORT-5-IF_UP: Interface Ethernet2/4 is up in mode access
2013 Jun 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 .
2013 Jun 29 17:53:04 S22-DCOS clis[2558]: CLI-3-NVDB: Batched send failed for component:
clic
switch#
```

Example: show logging level aaa

```
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#
```

Example: show logging module

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

Example: show logging monitor

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

Example: show logging server

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

Example: show logging session status

```
switch# show logging session status
Last Action Time Stamp     : Fri Jul 26 11:28:55 2013
Last Action                : Distribution Enable
Last Action Result         : Success
Last Action Failure Reason : none
switch#
```

Example: show logging status

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

Example: show logging timestamp

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

Feature History for System Message Logging

Feature Name	Releases	Feature Information
System Message Logging	Release 5.2(1)SK1(2.1)	This feature was introduced.

CHAPTER 14

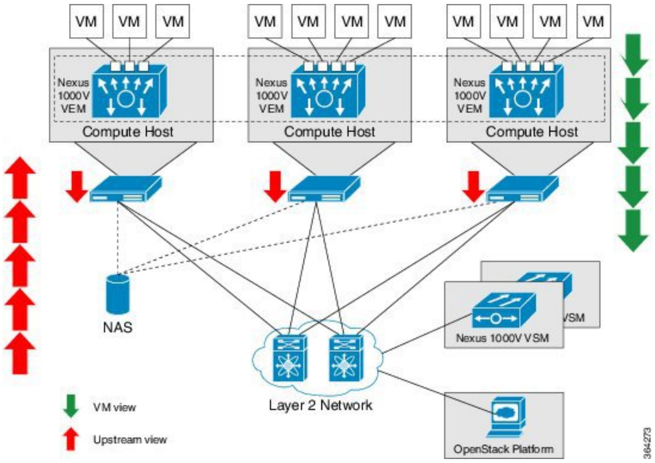
Enabling vTracker

This chapter contains the following sections:

Information About vTracker

The following illustration displays the vTracker setup diagram:

Figure 8: vTracker Setup Diagram in the KVM Cisco Nexus 1000V Environment



The vTracker feature on the Cisco Nexus 1000V 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 RedHat OSP, 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 the following data:

  VM vNIC View—Provides information about the virtual machines (VMs) that are managed by the Cisco Nexus 1000V switch. The vNIC view is from the bottom to the top of the network.
- Module pNIC View—Provides information about the physical network interface cards (pNIC) that are connected to each Virtual Ethernet Module (VEM).
- VLAN View—Provides information about all the VMs that are connected to specific VLANs.

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

Guidelines and Limitations

vTracker has the following configuration guidelines and limitations:

- For VM views, you should connect the Virtual Supervisor Module (VSM) with the OpenStack Horizon for the vTracker **show** commands to work.

- vTracker is disabled by default.

- While the Cisco Nexus 1000V switch information is validated, the information sourced by vTracker from the OpenStack Horizon 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 VEMs and OpenStack Horizon, 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.

	Command or Action	Purpose
Step 3	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example enables vTracker:

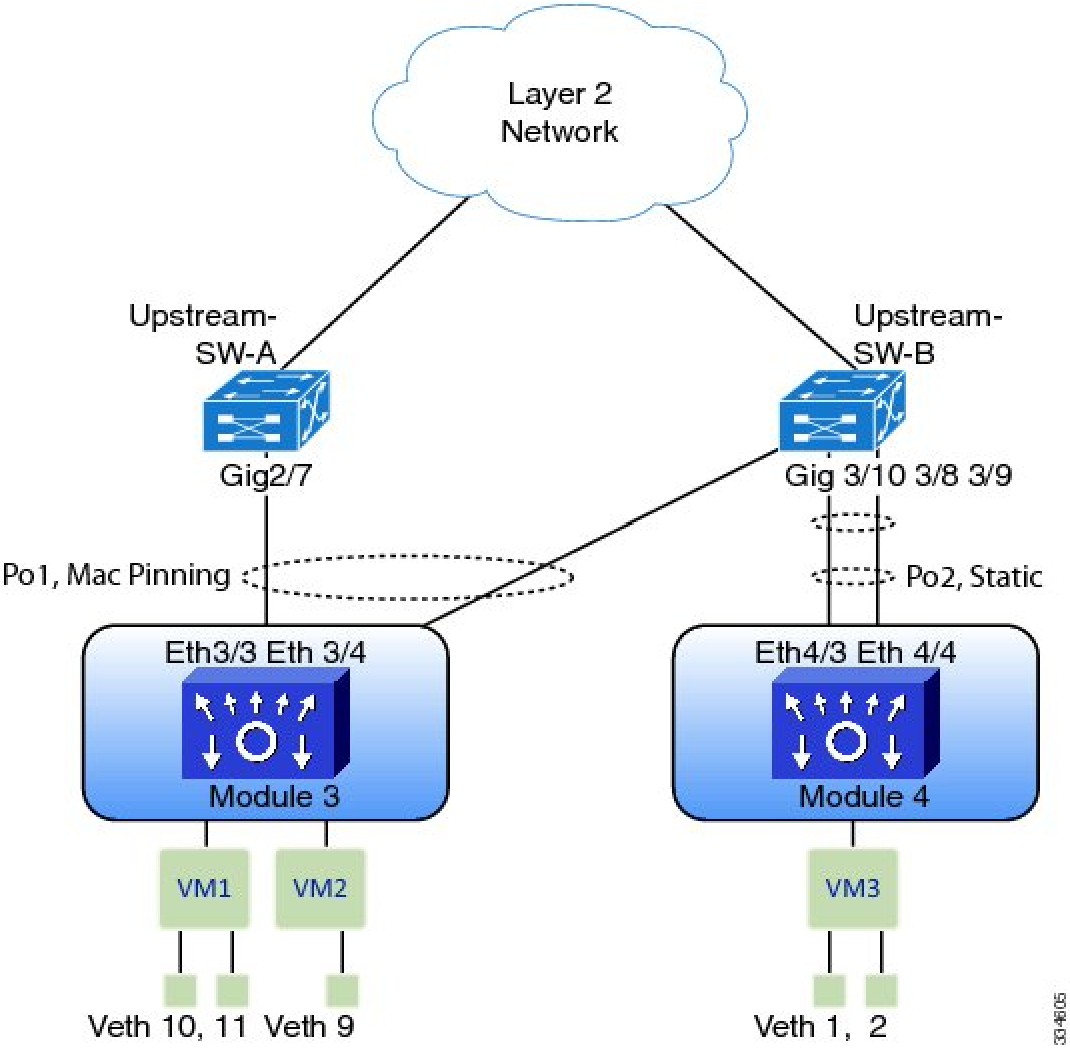
```
switch# configure terminal
switch(config)# feature vtracker
switch(config)# copy running-config startup-config
```

Upstream View

Upstream View Overview

The upstream view provides end-to-end network information from the VM to the physical switch. The following is the upstream view set-up diagram:

Figure 9: Upstream View Setup Diagram in the Cisco Nexus 1000V Environment



Note Cisco Discovery Protocol (CDP) neighbor information must be accessible to generate the required upstream view output. CDP must be enabled on the hosts as well as on the VSM or the Cisco Cloud Services Platform (CSP) in order for the **show vtracker upstream-view** command to work.

Displaying Upstream View

To display the upstream view, follow the given step.

Procedure

show vtracker upstream-view [**device-id** *name* | **device-ip** *IP address*]
The following examples show the vTracker upstream view in a VSM:

Example:

```
switch(config)# show vtracker upstream-view
--------------------------------------------------------------------------------
Device-Name               Device-Port   Server-Name        PC-Type    Veth-interfaces
Device-IP                 Local-Port    Adapter Status     PO-Intf
--------------------------------------------------------------------------------
JWALA-N5K-1(SSI153307R9)  Eth103/1/24   biju-1-237         MacPinn    None
10.197.128.14             Eth3/1        enp133s up         Po3

                          Eth103/1/23   biju-1-237         MacPinn    None
                          Eth3/4        enp133s up         Po3

                          Eth105/1/11   biju-1-237         MacPinn    1-3,5-6,35-36
                          Eth3/8        enp3s0f up         Po1
JWALA-N5K-2(SSI15330LPA)  Eth104/1/22   biju-1-237         MacPinn    None
10.197.128.15             Eth3/2        enp132s up         Po3

                          Eth104/1/23   biju-1-237         LACP-A     17,65,70,110
                          Eth3/3        enp1s0f up         Po2        114


                          Eth104/1/24  biju-1-237          LACP-A     17,65,70,110
                          Eth3/6       enp1s0f up          Po2        114

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

Example:

```
switch(config)# show vtracker upstream-view device-id JWALA-N5K-1(SSI153307R9)
--------------------------------------------------------------------------------
Device-Name              Device-Port   Server-Name        PC-Type    Veth-interfaces
Device-IP                Local-Port    Adapter Status     PO-Intf
--------------------------------------------------------------------------------
JWALA-N5K-1(SSI153307R9) Eth103/1/24   biju-1-237         MacPinn    None
10.197.128.14            Eth3/1        enp133s up         Po3

                         Eth103/1/23   biju-1-237         MacPinn    None
                         Eth3/4        enp133s up         Po3

                         Eth105/1/11   biju-1-237         MacPinn    1-3,5-6,35-36
                         Eth3/8        enp3s0f up         Po1
--------------------------------------------------------------------------------
```

Upstream View Field Description

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

Column	Description
Device-Name	Name of the neighboring device.

Column	Description
Device-IP	IP address of the device.
Device-Port	Port interface of the device that is connected to the Cisco Nexus 1000V Ethernet (local) port.
Local-Port	Local port interface, which is connected to the neighboring device port.
Server-Name	Name or IP address of the server module to which the local port is connected.
Adapter	Local port name as known by the hypervisor. For KVM, it is known as VTEP.
Status	Local port's operational status.
PC-Type	Port-channel type of the local port. Each PC-Type has a corresponding channel-group configuration in the port profile or the interface. Supported values are as follows: • Default—channel-group auto or channel-group auto mode on • MacPinn—channel-group auto mode on mac-pinning • MacPinnRel—channel-group auto mode on mac-pinning relative • SubGrpCdp—channel-group auto mode on sub-group cdp • SubGrpMan—channel-group auto mode on sub-group manual • LACP-A—channel-group auto mode active • LACP-P—channel-group auto mode passive
PO-Intf	Port channel interface of the local port.
veth-interfaces	Available virtual Ethernet interfaces for which traffic can flow through the upstream switch. **Note** You can get similar information by entering the **show int virtual pinning** command at the VSM prompt.

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 1000V switch. The VM perspective is divided into two views:

- VM vNIC View—Provides information about all the vNICs (virtual network interface cards) adapters that are managed by the Cisco Nexus 1000V switch.
- VM Info View—Provides information about all the VMs that run on each server module. The data is fetched from the attributes of each VM via the OpenStack Horizon.

Note The VSM must be connected with the OpenStack Horizon 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
    Port-UUID                                Adapter      Mode       IP-Addr
------------------------------------------------------------------------------------------
3                                            Veth65       n/a        0000.3737.4437   up
 1280      Po2
    52cf5c78-8c2f-40d5-9107-2347a525fc59  vtep137-ovs  access     n/a

3                                            Veth70       n/a        6663.d067.5d23   up
 1280      Po2
    07eceb05-f31d-479a-9ee8-4a1750e067de  vtep37-ovs   access     n/a

4                                            Veth110      n/a        0011.2233.4437   up
 1280      Po2
    b4732e9b-3d6a-473b-b154-76c729fc3a7b  vtep237-ovs  access     n/a

4                                            Veth114      n/a        0000.3737.a737   up
 1280      Po2
    fad17ad5-b8c0-48e1-99fb-023bf662a166  vtep7-ovs    access n/a
```

```
5   TVM-TVM-1-013                         Veth35       n/a        0050.5600.000d   up
 1251      Eth3/8
    7e822cef-0902-4ae4-b357-be54c916bcb8  vnet438      access     n/a

5   TVM-TVM-1-013                         Veth36       n/a        5254.004b.77e6   up
 1251      Eth3/8
    4c9437d3-a413-4545-8b2e-181dfa4a3a3d  vnet440      access     n/a
--------------------------------------------------------------------------------
```

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
    Port-UUID       Adapter     Mode      IP-Addr
--------------------------------------------------------------------------------
4                   Veth114     n/a       0000.3737.a737  up    1280   Po2
                                          fad17ad5-b8c0-48e1-99fb-023bf662a166
                    vtep7-ovs   access     n/a
--------------------------------------------------------------------------------
```

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.
Port-uuid	Port uuid generated by OpenStack.
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.
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.
State	Operational status of the network adapter.

Column	Description
Network	Network interface ID. Supported values are as follows: • access interface—Access VLAN • 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.

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 VEM 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(config)# show vtracker module-view pnic
-------------------------------------------------------------------------------
Mod  EthIf     Adapter     Mac-Address    Driver    DriverVer           FwVer
               Description
-------------------------------------------------------------------------------
4    Eth4/4    vmnic3      0050.565e.df75 e1000     8.0.3.2-1vmw-NAPI   N/A
               Intel Corporation 82546GB Gigabit Ethernet Controller
3    Eth3/1    enp133s0f0000a.f701.06bc bnx2 2.2.5 bc 7.4.0
               Broadcom Corporation NetXtreme II BCM5709 Gigabit Ethernet (rev 20)

3    Eth3/2    enp132s0f0000a.f701.06b8 bnx2 2.2.5 bc 7.4.0
               Broadcom Corporation NetXtreme II BCM5709 Gigabit Ethernet (rev 20)
4    Eth4/1    enp1s0f1 b0fa.eb97.9bfb igb 5.0.5-k 1.61, 0x800009c
               Intel Corporation I350 Gigabit Network Connection (rev 01)

4    Eth4/2    enp130s0f10000.c9b0.149e be2net 10.0.600.0r 2.702.200.1702
               Emulex Corporation OneConnect 10Gb NIC (rev 02)
5    Eth5/1    enp133s0f1000a.f71b.d3be bnx2 2.2.5 bc 7.4.0
               Broadcom Corporation NetXtreme II BCM5709 Gigabit Ethernet (rev 20)

5    Eth5/2    enp1s0f1 c067.af03.d3bb igb 5.0.5-k 1.61, 0x800009c
               Intel Corporation I350 Gigabit Network Connection (rev 01)

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

Example:

```
switch(config)# show vtracker module-view pnic module 3
--------------------------------------------------------------------------------
Mod  EthIf     Adapter     Mac-Address    Driver    DriverVer           FwVer
               Description
--------------------------------------------------------------------------------
3    Eth3/8    vmnic7      0050.5652.f935 igb       2.1.11.1            1.4-3
               Intel Corporation 82576 Gigabit Network Connection


4    Eth4/3    vmnic2      0050.565e.df74 e1000     8.0.3.2-1vmw-NAPI   N/A
               Intel Corporation 82546GB Gigabit Ethernet Controller


4    Eth4/4    vmnic3      0050.565e.df75 e1000     8.0.3.2-1vmw-NAPI   N/A
               Intel Corporation 82546GB Gigabit Ethernet Controller
--------------------------------------------------------------------------------
```

Module pNIC View Field Description

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

Column	Description
Mod	Module ID of the server on the VSM.
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.

Column	Description
Driver	Driver type of the interface.
DriverVer	Driver version of the interface.
FwVer	Firmware version 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 of the Veth interface.
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.

Feature History for vTracker

Feature Name	Releases	Feature Information
vTracker	5.2(1)SK3(2.1)	This feature was introduced.