Cisco Virtual Security Gateway for Microsoft Hyper-V Command Reference, Release 5.2(1)VSG2(1.1a)

January 31, 2014

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number: OL-31175-01

Cisco Virtual Security Gateway for Microsoft Hyper-V Command Reference, Release 5.2(1)VSG2(1.1a)

CONTENTS

CHAPTER 4

Cisco vPath and vServices Overview

This chapter provides an overview of the Cisco vPath and vServices and includes the following sections:

Information About the Cisco vPath and vServices

This section provides an overview of the Cisco vPath and vServices and includes the following topics:

Overview of vPath

Cisco Virtual Service Data Path (vPath) is the service intelligence embedded in the Cisco Nexus 1000V Series switch.

vPath provides the forwarding plane abstraction and programmability required to implement the Layer 3 to Layer 7 network services such as segmentation firewalls, edge firewalls, load balancers, WAN optimization, and others. It is embedded in the Cisco Nexus 1000V Series switch Virtual Ethernet Module (VEM). It intercepts the traffic whether external to the virtual machine or traffic from virtual machine to virtual machine and then redirects the traffic to the appropriate virtual service node (VSN) such as Cisco Virtual Security Gateway (VSG) for processing. vPath uses overlay tunnels to steer the traffic to the virtual service node and the virtual service node can be Layer 3 adjacent.

The basic functions of vPath includes traffic redirection to a virtual service node (VSN). Apart from the basic functions, vPath also includes advanced functions such as traffic off load, acceleration and others.

vPath steers traffic, whether external to the virtual machine or from a virtual machine to a virtual machine, to the virtual service node. Initial packet processing occurs in the VSN for policy evaluation and enforcement. Once the policy decision is made, the virtual service node may off-load the policy enforcement of remaining packets to vPath.

Figure 1-1 Virtual Service Datapath (vPath)

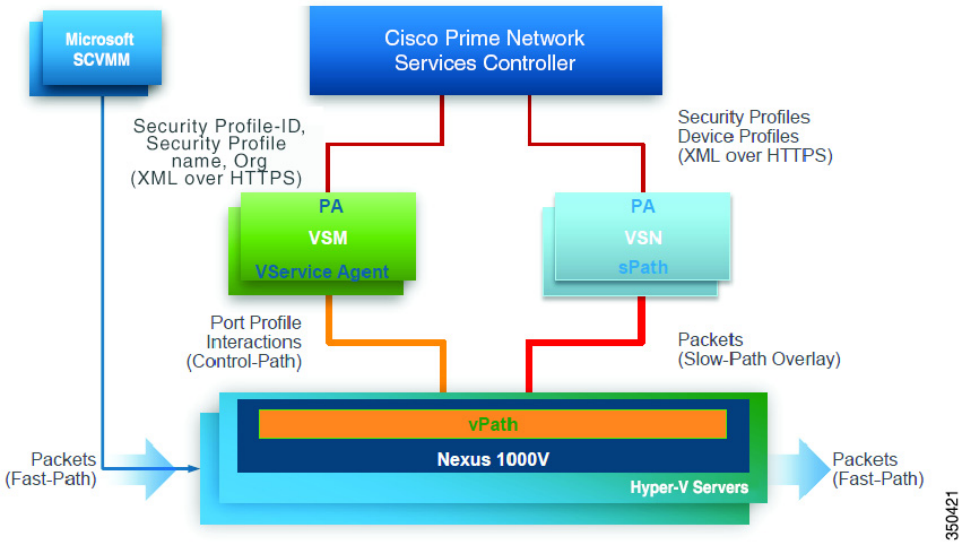
Overview of Virtual Services (vServices)

Virtual Services include the various Layer 4 through Layer 7 network services such as firewalls(VSG), edge firewalls, load balancers, WAAN optimization and others which are virtualized and delivered as virtual machines.

VSG: Povides trusted multitenant access with granular zone-based security policies for VMs. Cisco VSG delivers security policies across multiple servers. It supports VM mobility across physical servers for workload balancing, availability, or scale.

Virtual Services Architecture

Figure 1-2 Virtual Services Architecture



The Virtual Services Architecture provides a framework for delivering virtual services. vPath is the main component of the architecture and it is embedded in the Cisco Nexus 1000V Series switchVEM. It acts as a service traffic classifier and as a service dispatcher. It selects the traffic requiring service and steers it to the appropriate virtual service node for service delivery. vPath performs all its functions on tenant boundaries in order to provide tenant isolation.

The other components of the virtual service architecture includes:

- The Cisco Prime Network Services Controller (Prime NSC), a multi tenant policy manager responsible for device and policy management . The Cisco Prime NSC is the overall management and orchestration component of the virtual service architecture.
- The Cisco Nexus 1000V Series switch VSM, responsible for all the interactions with vPath and Prime NSC.The Virtual Service Agent on theCisco Nexus 1000V Series switch is responsible for all the control aspects of vPath such as traffic classification, traffic redirection, traffic off loading and accleration.
- Virtual Service Node (VSN), responsible for the service processing. The various virtual services supported include VSG. The VSNs can include many instances of the same virtual service or different virtual service types.

Benefits of vPath and Virtual Services Architecture

vPath and virtual services architecture include the following benefits:

- Dynamic Service Provisioning, page 1-4
- Service Binding, page 1-4
- Service Overlay, page 1-5
- Mobility, page 1-5
- Multi-Tenancy, page 1-6

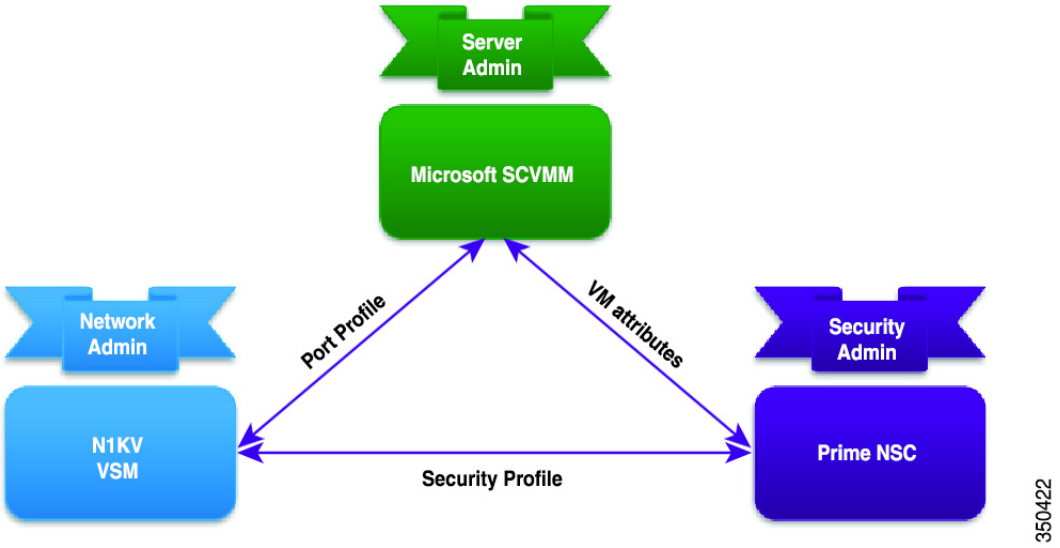
Dynamic Service Provisioning

vPath supports dynamic provisioning of virtual machines via service profiles and ensures that the service profiles follow vMotion events. In a service profile you can configure the service parameters. In VSGthe service profiles map to a policy. In VSG, the service profile is referred to as a security profile.

The service parameters are configured in a service profile and then attached to a port profile. When the virtual machines get instantiated and attached to a port profile, the service profile also gets dynamically attached to the virtual machine.Once associated all the policies are dynamically provisioned to a virtual machine as the virtual machine comes up or moves from one server to another.

The virtual services architecture supports a collaborative management model where the roles and responsibilities of network administrator, server administrator and service administrator are clearly defined.

Figure 1-3 Dynamic Service Provisioning



Service Binding

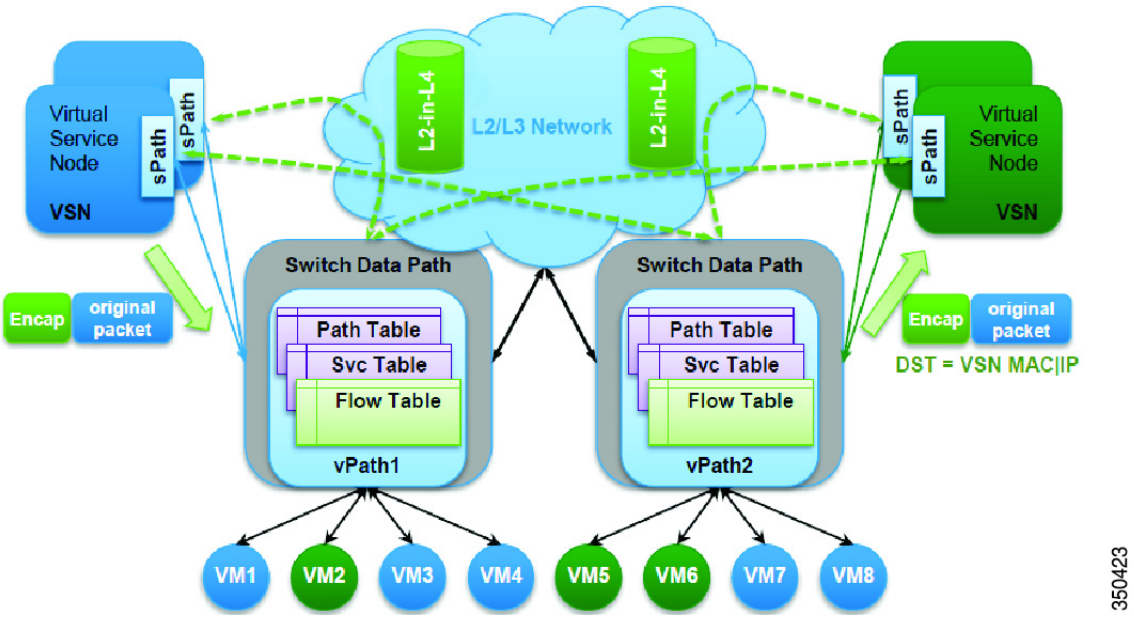
Due to dynamic service provisioning, a service profile is associated with the virtual machines as they are instantiated. vPath then assigns a service profile identifier to the service profile. vPath thus enables different service profile bindings on traffic associated with the different virtual machines. Virtual service nodes then use the service profile identifier to choose the appropriate policy to apply to the traffic or deliver the service.

Service Overlay

vPath uses overlay tunnels to steer the traffic to the virtual service node and the virtual service node can be either Layer 2 or Layer 3 adjacent. As shown in the following figure, the tunnels can be L2 or L4. MAC-in-MAC encapsulation is used in the L2 tunnel and MAC in UDP encapsulation is used in the L4 tunnel.

In L4 tunnel, UDP encapsulation enables load balancing of the packets onto the links at the network elements and enables NICs to support Receive Side Scaling (RSS).

Figure 1-4 Service Overlay



Mobility

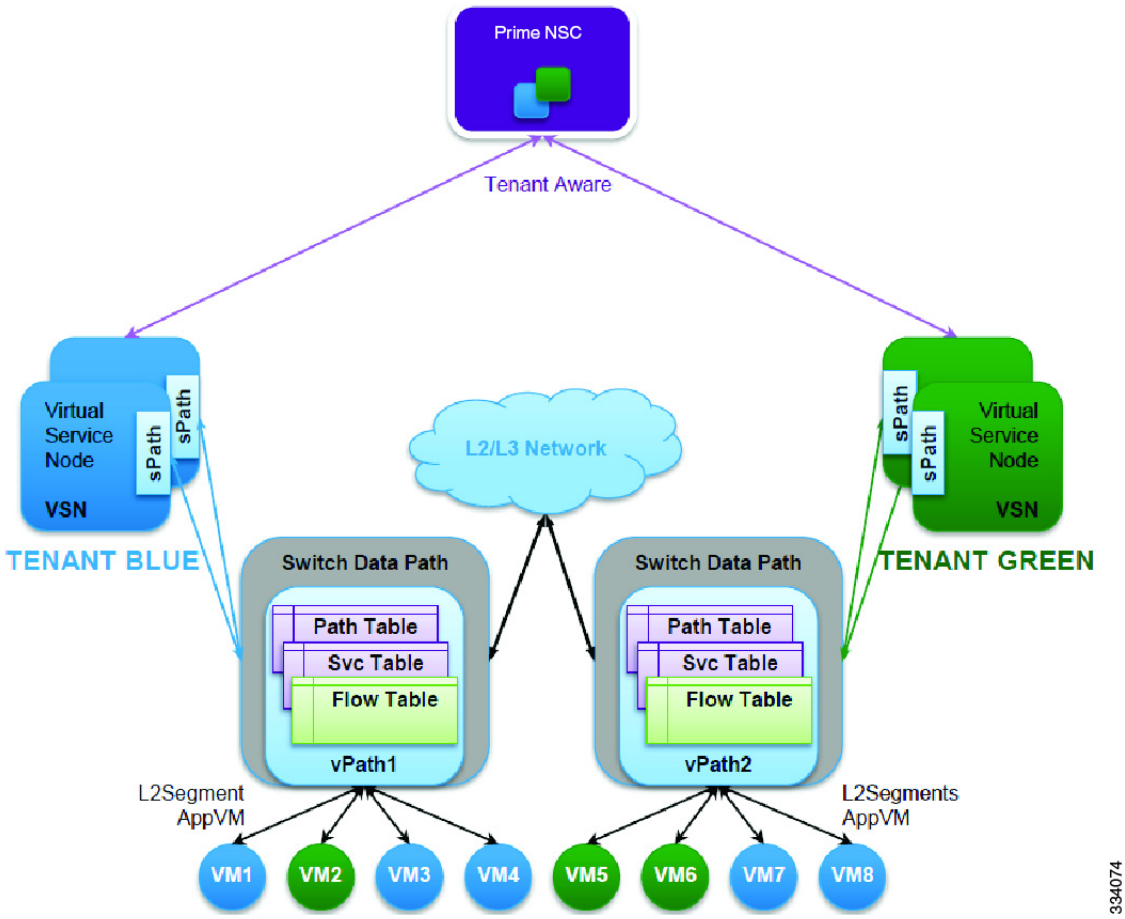
The virtual services architecture enables the mobility of the virtual machine as well as the virtual service node. Dynamic service provisioning ensures that the virtual machine traffic flow continues to be handled by the appropriate virtual service node. This is possible since the service profile remains the same in the port profile and the port profile moves along with the virtual machine. As a result the virtual machine in the new host will continue to use the same virtual service node for service processing.

Service overlay ensures that the virtual service node is reachable on the new host and the virtual machines continue to forward traffic to the same virtual service node.

Multi-Tenancy

vPath is tenant aware and it can serve virtual service nodes belonging to different tenants. The virtual services architecture enables vPath to support overlapping IP addresses among different tenants. vPath steers traffic from the virtual machines to the virtual service nodes in the same tenant thus enabling tenant separation.

Figure 1-5 Multi-tenancy

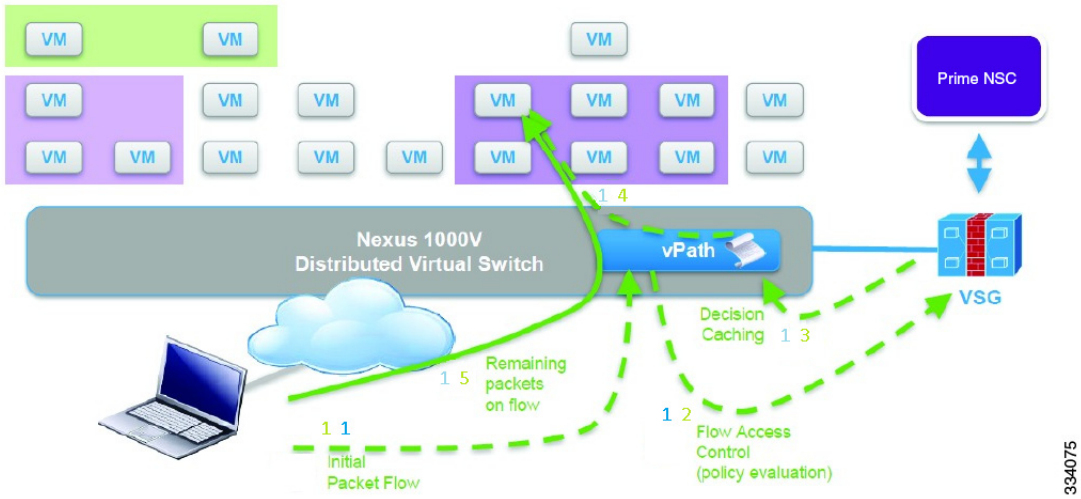


Service Acceleration and Programmability

vPath steers traffic, whether external to the virtual machine or from a virtual machine to a virtual machine, to the virtual service node. The virtual service node can either continue to process the redirected traffic or off load the traffic to vPath. The off loaded traffic is processed by vPath leading to increased performance in service delivery of the Cisco Nexus 1000V Series switch.

vPath also has the ability to enforce the actions on the traffic as specified by the virtual service node. Virtual service nodes can then choose to intercept reverse traffic without any static configurations on the switch or choose to off load some traffic.

Figure 1-6 Service Accleration



Version Compatibility

The following table lists the version compatibility of the virtual service nodes with Cisco Nexus 1000V Series switch.

Table 1-1 Virtual Service Node and Nexus 1000V Release Compatibility

Virtual Service Node	Minimum Required Version of Cisco Nexus 1000V
Cisco Virtual Service Gateway (VSG)	5.2(1)SM1(5.1)

Licensing

Cisco Virtual Service Data Path (vPath) is an intelligent service embedded in the Cisco Nexus 1000V Series switch. See *Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV2(2.1)* for more information on Cisco Nexus 1000V Series switch license.

Obtaining Documentation and Submitting a Service Request

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

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

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

Configuring Nodes and Services for vPath

This chapter describes how to configure the virtual service nodes and virtual network services for vPath.

This chapter includes the following sections:

Guidelines and Limitations

vPath and vServices has the following configuration guidelines and limitations:

- If the jumbo frames are enabled in the network, make sure that the MTU of the client and server VMs are reduced by the vPath encapsulation size.
- If the Cisco VSN is deployed on a Vitual Extensible Local Area Network, an additional header with 50 bytes is added in front of the vPath encapsulation. Adjust the MTU by this amount.
- When the VEM communicates with the Cisco VSN in the Layer 3 mode, an additional header with 82 bytes is added to the original packet. The VEM does not support fragmentation in Layer 3 mode and the ports/network- elements that carry the vPath encapsulated packets must be configured so that the vPath overhead is accommodated.

Configuring Virtual Service Nodes

This section includes the following topics:

Configuring the vService Node on VSM

BEFORE YOU BEGIN

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

- Setup the vService node.
- You have the Virtual Service Node (VSN) software installed and the basic installation completed.
- Default license is installed.

SUMMARY STEPS

1. **configure**
2. **vservice node** *node_name* **type** {**vsg** }
3. {**ip address** *ip_addr* | **no ip address**}
4. {**adjacency** { **l3** | **no adjacency**}
5. {{**failmode** {**close** | **open**} | **no failmode**}

DETAILED STEPS

	Command	Purpose
Step 1	**configure** **Example:** n1000v# configure n1000v(config)#	Places you in global configuration mode.
Step 2	**vservice node** *node_name* **type** {**vsg**} **Example:** n1000v(config)# vservice node test type vsg n1000v(config-vservice-node)#	Configures the vservice node name for the Cisco VSN. The name will be used to associate with port profile. A node can be deleted only if it is not bound to any virtual machines or not used in any port profile. **type** is needed only for creation of a node. Once a node is created, **type** is not needed.
Step 3	{**ip address** *ip_addr*	**no ip address**} **Example:** n1000v(config-vservice-node)# ip address 10.0.0.1 n1000v(config-vservice-node)#	Configures the vservice node IP address for the Cisco VSN. **Note** The IP address must match the control interface (control0) IP address on the Cisco VSN.
Step 4	{**adjacency** {**l3**	**no adjacency**} **Example:** n1000v(config-vservice-node)# or n1000v(config-vservice-node)# adjacency l3 n1000v(config-vservice-node)#	Configures the adjacency for the Cisco VSN. If the Cisco VSN is operating in Layer 3 mode, specify Layer 3 as keyword.
Step 5	{**failmode** {**close**	**open**}	**no failmode**} **Example:** n1000v(config-vservice-node)# fail-mode close n1000v(config-vservice-node)#	The failmode default value is close. Fail mode specifies the behavior when the VEM does not have connectivity to the service node. The default fail mode for VSG is close, which means that the packets will be dropped.

Associating a Port Profile to a Virtual Service Node

BEFORE YOU BEGIN

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

- You have the Cisco VSN software installed and the basic installation completed.
- Default license is installed.
- You have completed creating the Cisco VSG port profiles for the service and high-availability (HA) interface. See the *Cisco Virtual Security Gateway for Microsoft Hyper-V Configuration Guide, Release 5.2(1)VSG2(1.1a)*.
- You have defined the vservice node that will be added to the port profile.
- You are logged in to the switch CLI in EXEC mode.

SUMMARY STEPS

1. **configure**
2. **port-profile** *port-profile-name*
3. state enabled
4. no shutdown
5. **org** *org-name*
6. **vservice node** *node name* **profile** [*security-profile-name*]
7. **publish port-profile**
8. (Optional) **copy running-config startup-config**
9. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**configure**
	
	Example:
	`n1000v# configure`
	`n1000v(config)#`
		Places you in global configuration mode.

Step 2	**port-profile** *port-profile-name*
	
	Example:
	`n1000v(config-port-prof)# port-profile host-profile`
	`n1000v(config-port-prof)#`
		Enters the port profile configuration mode for the named port profile. If the port profile does not exist, it is created using the following characteristics:
		port-profile-name—The port profile name can be up to 80 alphanumeric characters and must be unique for each port profile on the Cisco VSN.

Step 3	**state enabled**
	
	Example:
	`n1000v(config-port-prof)# state enabled`
	`n1000v(config-port-prof)#`
		Sets the operational state of a port profile.

	Command	Purpose

Step 4	**no shutdown**
	
	Example:
	`n1000v(config-port-prof)# no shutdown`
	`n1000v(config-port-prof)#`
		Administratively enables all ports in the profile.

Step 5	**org** *org-name*
	
	Example:
	`n1000v(config-port-prof)# org root/Tenant-A`
	`n1000v(config-port-prof)#`
		Designates an organization name for the Cisco VSN port profile.

Step 6	**vservice node** node name **profile** [*security-profile-name*]
	
	Example:
	`n1000v (config-port-prof)# vservice node vsg1 profile profile-1`
	`n1000v (config-port-prof)#`
		Associate the port profile with the previously defined vservice node and the security profile name.
		
		Note If you do not pick a security profile name, the default name is used. The security profile name must match the security profile created on the Cisco Prime NSC.

Step 7	**publish port-profile** **Example:** `n1000v(config-port-prof)# publish port-profile`	Publishes the port-profile.

Step 8	**copy running-config startup-config**
	
	Example:
	`n1000v(config-port-prof)# copy running-config startup-config`
	`n1000v(config-port-prof)#`
		(Optional) Saves configuration changes.

Step 9	**exit**
	
	Example:
	`n1000v(config-port-prof)# exit`
	`n1000v(config)#`
		Exits the configuration mode and returns you to the global configuration mode.

vService Specific Configurations

This topic includes the following topics:

Configuring Virtual Network Adapter for the Layer 3 Mode VSN Encapsulation

You can configure virtual network adapters for a Cisco VSN in the Layer 3 mode encapsulation.

BEFORE YOU BEGIN

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

- Identify a VLAN to be used in Router for transporting the Cisco VSN in Layer 3 mode-encapsulation traffic. Ensure that the VLAN is configured on the uplink port profile for all VEMs on which the Cisco VSN in Layer 3 mode can be configured.

SUMMARY STEPS

1. **port-profile type vethernet** *vsm_gs_l3vns*
2. **capability** *l3-vservice*
3. **no shutdown**
4. **state enabled**
5. **publish port-profile**

DETAILED STEPS

	Command	Purpose

Step 1	**port-profile** type vethernet *profilename*
	
	Example:
	switch(config)# port-profile vnadp-pp
	switch(config-port-prof)
		Enters port profile configuration mode for the named port profile. If the port profile does not already exist, it is created using the following characteristics:
		
		The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V.

Step 2	**capability** *l3-vservice* **Example:** switch(config-port-prof)# capability l3-vservice switch(config-port-prof)	Set the port-profile capability to Layer3 service.

Step 3	**no shutdown**
	
	Example:
	switch(config-port-prof)# no shutdown
	switch(config-port-prof)
		Administratively enables all ports in the profile.

Step 4	**state enabled**
	
	Example:
	switch(config-port-prof)# state enabled
	switch(config-port-prof)
		Sets the operational state of a port profile.

Step 5	**publish port-profile** **Example:** switch(config-port-prof)# publish port-profile	Publishes the port-profile.

Configuring TCP State-Checks for All Cisco VSGs in the vPath

The Transmission Control Protocol (TCP) state checks performs three checks on TCP traffic that is routed through the Cisco VSG:

- **invalid-ack**—When the ACK (acknowledge) number of a received TCP packet is greater than the sequence number of the TCP packet to be sent next, it is an invalid ACK.
- **seq-past-window**—The sequence number of a received TCP packet is greater than the right edge of the TCP receiving window.
- **window-variation**—The window size mechanism allows TCP to advertise a large window and to subsequently advertise a much smaller window without accepting a lot of data. From the TCP specification, it is recommended not to make the window size smaller.

When the state check is turned on, the data packets are dropped by the Cisco VSG if they meet either of the three TCP traffic check criteria. By default, TCP state checks functionality is disabled, use the **tcp state-checks** command to enable or disable TCP state checks.

BEFORE YOU BEGIN

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

- You have the Cisco VSG software installed and the basic installation completed. For details, see the *Cisco Virtual Security Gateway, Release 5.2(1)VSG2(1.1a) and Cisco Virtual Network Management Center, Release 2.1 Installation Guide*.
- Default license must be installed.
- You have completed creating the Cisco VSG port profiles for the service and HA interface.
- You are logged in to the switch CLI in EXEC mode.

SUMMARY STEPS

1. **configure**
2. **vservice global type vsg**
3. **[no] tcp state-checks**
4. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**configure**
	
	Example:
	`n1000v# configure`
	`n1000v(config)#`
		Places you in global configuration mode.

Step 2	**vservice global type vsg**
	
	Example:
	`n1000v(config)# vservice global type vsg`
	`n1000v(config-vservice-global)#`
		Enters vservice global configuration mode.

	Command	Purpose

Step 3	**[no] tcp state-checks**
	
	Example 1:
	`n1000v(config-vservice-global)# tcp state-checks`
	`n1000v(config-vservice-global)#`
		Enables or disables the TCP state checks for Cisco VSGs in the vPath.
		
		The **no** form of this command reverses the above respective default state.

Step 4	**exit**
	
	Example:
	`n1000v(config-vservice-global)# exit`
	`n1000v(config)#`
		Exits vservice global configuration mode and returns you to the global configuration mode.

Verifying the Cisco VSN Configuration

To display information related to a Cisco VSN, perform one of the following tasks on the switch CLI:

- Show Commands, page 2-7
- vPath Ping Command for the Layer 3 Mode, page 2-7

Show Commands

Command	Purpose
show license usage **Example:** `vsm# show license usage`	Displays a table with the Cisco VSN license usage information for the Cisco Nexus 1000V Series switch.
show vservice {**statistics** | **brief** | {**detail** [{[**ip** *ip-addr*] | **module** *module-num*}]}} **Example:** `vsm# show vservice statistics detail module m1-vsm-stats`	Displays Virtual Service Node (VSN) statistics for all VEM modules.

vPath Ping Command for the Layer 3 Mode

Examples

This example shows how to see the vsn connections:

```
vsm# ping vsn ip 10.1.1.40 src-module vpath-all
ping vsn 10.1.1.40 vlan 0 from module 9 11 12, seq=0 timeout=1-sec
  module(usec)    :  9(698) 11(701) 12(826)

ping vsn 10.1.1.40 vlan 0 from module 9 11 12, seq=1 timeout=1-sec
  module(usec)    :  9(461) 11(573) 12(714)

ping vsn 10.1.1.40 vlan 0 from module 9 11 12, seq=2 timeout=1-sec
  module(usec)    :  9(447) 11(569) 12(598)

ping vsn 10.1.1.40 vlan 0 from module 9 11 12, seq=3 timeout=1-sec
  module(usec)    :  9(334) 11(702) 12(559)
```

```
ping vsn 10.1.1.40 vlan 0 from module 9 11 12, seq=4 timeout=1-sec
  module(usec)   :  9(387) 11(558) 12(597)

vsm#
```

This example shows how VSN ping options are dispalyed for all sources modules:

```
vsm# ping vsn all src-module all
ping vsn 10.1.1.44 vlan 0 from module 9 10 11 12, seq=0 timeout=1-sec
  module(usec)   :  9(508)
  module(failed) : 10(VSN ARP not resolved) 11(VSN ARP not resolved)
                   12(VSN ARP not resolved)
ping vsn 10.1.1.40 vlan 0 from module 9 10 11 12, seq=0 timeout=1-sec
  module(usec)   :  9(974) 11(987) 12(1007)
  module(failed) : 10(VSN ARP not resolved)

ping vsn 10.1.1.44 vlan 0 from module 9 10 11 12, seq=1 timeout=1-sec
  module(usec)   :  9(277) 10(436) 11(270) 12(399)
ping vsn 10.1.1.40 vlan 0 from module 9 10 11 12, seq=1 timeout=1-sec
  module(usec)   :  9(376) 10(606) 11(468) 12(622)

ping vsn 10.1.1.44 vlan 0 from module 9 10 11 12, seq=2 timeout=1-sec
  module(usec)   :  9(272) 10(389) 11(318) 12(357)
ping vsn 10.1.1.40 vlan 0 from module 9 10 11 12, seq=2 timeout=1-sec
  module(usec)   :  9(428) 10(632) 11(586) 12(594)

ping vsn 10.1.1.44 vlan 0 from module 9 10 11 12, seq=3 timeout=1-sec
  module(usec)   :  9(284) 10(426) 11(331) 12(387)
ping vsn 10.1.1.40 vlan 0 from module 9 10 11 12, seq=3 timeout=1-sec
  module(usec)   :  9(414) 10(663) 11(644) 12(698)

ping vsn 10.1.1.44 vlan 0 from module 9 10 11 12, seq=4 timeout=1-sec
  module(usec)   :  9(278) 10(479) 11(334) 12(469)
ping vsn 10.1.1.40 vlan 0 from module 9 10 11 12, seq=4 timeout=1-sec
  module(usec)   :  9(397) 10(613) 11(560) 12(593)

vsm#
```

Troubleshooting vPath and vServices

This chapter includes the following sections:

See the *Cisco Virtual Security Gateway for Microsoft Hyper-V Troubleshooting Guide, Release 5.2(1)VSG2(1.1a)* for more information on troubleshooting VSG.

VNS Agent

Virtual Network Service (VNS) agent-related event logs are maintained on the Virtual Supervisor Module (VSM), not on the Cisco VSG.

This section includes the following topics:

Core Module

Core events are those events that are related to port attach, port detach, Internet Protocol Database (IPDB), and to port-profile CLI.

This example shows how to enable/disable error messages for the vns_agent core module:

```
vsm# event-log vns-agent core-error [terminal] ----->enable messages to the terminal
vsm# no event-log vns-agent core-error [terminal] ----->disable messages to the terminal
```

This example shows how to enable/disable informational messages for the vns_agent core module:

```
vsm# event-log vns-agent core-info [terminal] ----->enable messages to the terminal
vsm# no event-log vns-agent core-info [terminal] ----->disable messages to the terminal
```

VPath Module

Because the vPath module works based on core-module events, you should always enable core module event logs before you enable the vPath module events.

This example shows how to enable/disable error messages for the vns_agent vPath module:

```
vsm# event-log vns-agent vpath-error [terminal] ----->enable messages to the terminal
vsm# no event-log vns-agent vpath-error [terminal] ----->disable messages to the terminal
```

This example shows how to enable/disable informational messages for the vns_agent vPath module:

```
vsm# event-log vns-agent vpath-info [terminal] ----->enable messages to the terminal
vsm# no event-log vns-agent vpath-info [terminal] ----->disable messages to the terminal
```

Using vPath Ping to Determine Connectivity

You can use the vpath **ping** command to determine the connectivity between the Cisco VSG and the VEM.

This example shows how to ping the Cisco VSG connections and if they are reachable:

```
VSM-1# ping vsn all src-module all
ping vsn 106.1.1.1 vlan 0 from module 3 5, seq=0 timeout=1-sec
  module(usec)   :  3(156)  5(160)
ping vsn 110.1.1.1 vlan 0 from module 3 5, seq=0 timeout=1-sec
  module(failed) :  3(VSN ARP not resolved)  5(VSN ARP not resolved)

ping vsn 106.1.1.1 vlan 0 from module 3 5, seq=1 timeout=1-sec
  module(usec)   :  3(230)  5(151)
ping vsn 110.1.1.1 vlan 0 from module 3 5, seq=1 timeout=1-sec
  module(failed) :  3(VSN ARP not resolved)  5(VSN ARP not resolved)

ping vsn 106.1.1.1 vlan 0 from module 3 5, seq=2 timeout=1-sec
  module(usec)   :  3(239)  5(131)
ping vsn 110.1.1.1 vlan 0 from module 3 5, seq=2 timeout=1-sec
  module(failed) :  3(VSN ARP not resolved)  5(VSN ARP not resolved)

ping vsn 106.1.1.1 vlan 0 from module 3 5, seq=3 timeout=1-sec
  module(usec)   :  3(248)  5(153)
ping vsn 110.1.1.1 vlan 0 from module 3 5, seq=3 timeout=1-sec
  module(failed) :  3(VSN ARP not resolved)  5(VSN ARP not resolved)

ping vsn 106.1.1.1 vlan 0 from module 3 5, seq=4 timeout=1-sec
  module(usec)   :  3(259)  5(126)
ping vsn 110.1.1.1 vlan 0 from module 3 5, seq=4 timeout=1-sec
  module(failed) :  3(VSN ARP not resolved)  5(VSN ARP not resolved)
```

This example shows how to display VSN ping options:

```
VSM-1# ping vsn ?
  all   All VSNs associated to VMs
  ip    IP Address
```

This example shows how to display VSN ping options for all source modules:

```
VSM-1# ping vsn all src-module ?
  <3-66>     Module number
  all        All modules in VSM
  vpath-all  All modules having VMs associated to VSNs
```

This example shows how to set up a ping for all source modules from a specified IP address:

```
VSM-1# ping vsn ip 10.1.1.60 src-module all
ping vsn 10.1.1.60 vlan o from module 4 5 7, seq=0 timeout=1-sec
  module(usec)   :  4(301)  5(236)
  module(failed) :  7(VSN ARP not resolved)

ping vsn 10.1.1.60 vlan 0 from module 4 5 7, seq=1 timeout=1-sec
  module(usec)   :  4(241)  5(138)  7(270)

ping vsn 10.1.1.60 vlan 0 from module 4 5 7, seq=2 timeout=1-sec
  module(usec)   :  4(230)  5(155)  7(256)
```

```
ping vsn 10.1.1.60 vlan 0 from module 4 5 7, seq=3 timeout=1-sec
  module(usec)    :  4(250)  5(154)  7(284)

ping vsn 10.1.1.60 vlan 0 from module 4 5 7, seq=4 timeout=1-sec
  module(usec)    :  4(231)  5(170)  7(193)
```

This example shows to set up a ping for all vPath source modules for a specified IP address:

```
VSM-1# ping vsn ip 10.1.1.60 src-module vpath-all
ping vsn 10.1.1.60 vlan 0 from module 4 5, seq=0 timeout=1-sec
  module(usec)    :  4(223)  5(247)

ping vsn 10.1.1.60 vlan 0 from module 4 5, seq=1 timeout=1-sec
  module(usec)    :  4(206)  5(167)

ping vsn 10.1.1.60 vlan 0 from module 4 5, seq=2 timeout=1-sec
  module(usec)    :  4(241)  5(169)
```

This example shows how to set up a ping for all source modules of a specified IP address with a time-out and a count:

```
VSM-1# ping vsn ip 10.1.1.60 src-module all timeout 2 count 3
ping vsn 10.1.1.60 vlan 0 from module 4 5 7, seq=0 timeout=2-sec
  module(usec)    :  4(444)  5(238)  7(394)

ping vsn 10.1.1.60 vlan 0 from module 4 5 7, seq=1 timeout=2-sec
  module(usec)    :  4(259)  5(154)  7(225)

ping vsn 10.1.1.60 vlan 0 from module 4 5 7, seq=2 timeout=2-sec
  module(usec)    :  4(227)  5(184)  7(216)
```

vPath and vServices Commands

This chapter provides information about the vPath and vServices related commands on the Cisco Nexus 1000V Series switch and the Cisco Cloud Service Platform networking appliance.

capability l3-vservice

To configure a port profile to be used with l3-vservice, use the **capability l3-vservice** command. To remove the capability from a port profile, use the **no** form of this command.

capability l3-vservice

no capability l3-vservice

Syntax Description

l3-vservice	Configure virtual network adapter to carry l3-vservice traffic.

Defaults

None

Command Modes

Port-profile configuration (config-port-prof)

network-admin

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

If you are configuring a port profile for **l3-vservice**, ensure that the port profile is configured in switchport mode.

Examples

This example shows how to configure a port profile to be used with l3-vservice:

```
n1000v# config t
n1000v(config)# port-profile testprofile
n1000v(config-port-prof)# capability l3-vservice
n1000v(config-port-prof)#
```

This example shows how to remove the l3-vservice configuration from the port profile:

```
n1000v# config t
n1000v(config)# port-profile testprofile
n1000v(config-port-prof)# no capability l3-vservice
n1000v(config-port-prof)#
```

Related Commands

Command	Description
show port-profile	Displays information about the port profiles.

clear vservice connection

To clear the Cisco vservice connections, use the **clear vservice connection** command.

clear vservice connection [**module** *module-num*]

Syntax Description

module	(Optional) Clears a specific module.
module-num	Module number. The range is from 3 to 66.

Defaults

None

Command Modes

EXEC

Global configuration (config)

SupportedUserRoles

network-admin

network-operator

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Examples

This example shows how to clear Cisco VSG connections:

```
vsm# clear vservice connection
```

Related Commands

Command	Description
show vservice	Displays Cisco VSG information.

clear vservice statistics

To clear the Cisco vservice statistics, use the **clear vservice statistics** command.

clear vservice statistics [**module** *module-number* | **ip** <*ip-address*>]

Syntax Description

module	(Optional) Clears a module.
module-number	Module number. The range of values is from 3 to 66.
ip	IP address.
ip-address	IP address.

Defaults

None

Command Modes

EXEC

Global configuration (config)

SupportedUserRoles

network-admin

network-operator

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Examples

This example shows how to clear Cisco vservice statistics for existing modules:

```
vsm# clear vservice statistics
Cleared statistics successfully in module 4
Cleared statistics successfully in module 6
```

Related Commands

Command	Description
show vservice	Displays Cisco VSG information.

copy running-config startup-config

To copy the running configuration to the startup configuration, use the **copy running-config startup-config** command.

copy running-config startup-config

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

Use this command to save configuration changes in the running configuration to the startup configuration in persistent memory. When a device reload or switchover occurs, the saved configuration is applied.

Examples

This example shows how to save the running configuration to the startup configuration:

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

Related Commands

Command	Description
show running-config	Displays the running configuration.
show running-config diff	Displays the differences between the running configuration and the startup configuration.
show startup-config	Displays the startup configuration.
write erase	Erases the startup configuration in the persistent memory.

log-level

To set logging severity levels for the Cisco Prime Network Services Controller (Prime NSC) policy agent, use the **log-level** command. To reset logging levels, use the **no** form of this command.

log-level {**critical** | **debug0** | **debug1** | **debug2** | **debug3** | **debug4** | **info** | **major** | **minor** | **warn**}

no {**critical** | **debug0** | **debug1** | **debug2** | **debug3** | **debug4** | **info** | **major** | **minor** | **warn**}

Syntax Description

critical	Sets the logging level to critical.
debug0	Sets the logging level to debug 0.
debug1	Sets the logging level to debug 1.
debug2	Sets the logging level to debug 2.
debug3	Sets the logging level to debug 3.
debug4	Sets the logging level to debug 4.
info	Sets the logging level to information.
major	Sets the logging level to major.
minor	Sets the logging level to minor.
warn	Sets the logging level to warning.

Command Default

None

Command Modes

Cisco Prime NSC policy agent configuration (config-nsc-policy-agent)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Examples

This example shows how to set the logging level to critical:

```
vsm# configure
vsm(config)# nsc-policy-agent
vsm(config-nsc-policy-agent)# log-level critical
```

Related Commands

Command	Description
nsc-policy-agent	Enables the Cisco Prime NSC policy agent configuration mode.

org

To create a Cisco Prime NSC organization (domain), use the **org** command in VSM. To delete a Cisco Prime NSC organization, use the **no** form of the command.

org *organization-name*

no org [*organization-name*]

Syntax Description

organization-name	Organization name. The range of values is from 1 to 251.

Command Default

None

Command Modes

Port profile configuration (config-port-prof)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

Cisco Prime NSC organizations are Cisco Prime NSC domains.

You can hierarchically manage Cisco Prime NSC organizations. A user that is assigned at a top level organization has automatic access to all organizations under it. For example, an engineering organization can contain a software engineering organization and a hardware engineering organization. A locale containing only the software engineering organization has access to system resources only within that organization. However, a locale that contains the engineering organization has access to the resources for both the software engineering and hardware engineering organizations.

Examples

This example shows how to create an organization:

```
vsm# configure
Enter configuration commands, one per line. End with CNTL/Z.
vsm(config)# port-profile pP1
vsm(config-port-prof)# org root/tenant1
vsm(config-port-prof)#
```

Related Commands

Command	Description
vservice	Sets the IP address for a virtual firewall.

ping vsn

To ping the virtual service nodes (VSN) from the vPath, use the **ping vsn** command. There is no **no** form of this command.

ping vsn {**all** | {**ip** <*ip-addr*>}} **src-module** {**all** | **vpath-all** | <*module-num*>} [**timeout** <*secs*>] [**count** {**unlimited** | <*count*>}]

Syntax Description

ip	Designates that a specific IP address is to be pinged.
ip-addr	IP address of the specific VSN.
all	Indicates that all VSNs must be pinged.
src-module	Designates the source module for the ping.
module-num	Module number for the source path.
vpath all	Designates that all source vPaths will be used.
timeout	(Optional) Designates a timeout.
secs	Duration of the pinging operation in seconds.
count	(Optional) Designates a count of pings.
count	Number of pings to be counted.

Command Default

None

Command Modes

EXEC

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

There is no **no** form of this command.

Examples

This example shows how to ping a Cisco VSG:

```
vsm# ping ?
<CR>
  A.B.C.D or Hostname  IP address of remote system
  WORD                 Enter Hostname
  vsn                  VSNs to be pinged

vsm# ping vsn

Input parameters:
```

- vsn : VSNs to be pinged.
  - all : All VSNs that are currently associated to at least one VM. In other words, all VSNs specified in port-profiles that are bound to at least one VM.
  - ip-addr <ip-addr> : All VSNs configured with this IP address.
- src-module : Source modules to orginate ping request from.
  - all : All online modules.
  - vpath-all : All modules having VMs associated to port-profiles that has vn-service defined.
  - <module-num> : A online module number.
- timeout <secs> : Time to wait for response from VSNs, in seconds. Default is 1 sec.
- count : Number of ping packets to be sent.
  - <count> : Sepcifies number of ping packets to be sent. Default is 5. Min 1, Max 2147483647.
  - unlimited : Send ping packets until command is stopped.

Specify the IP address if the VSN to be pinged is not associated to any VMs yet.

In the output, the status of the ping request for each VSN for each module is shown. On a successful ping, the round-trip-time of ping request/response for a VSN is shown in microseconds next to the module number. On a failure, the failure message is shown next to the module number.

```
Various forms:
ping vsn all src-module all                (Ping all VSNs from all modules)
ping vsn all src-module vpath-all              (Ping all VSNs from all modules having
                                                VMs associated to VSNs)
ping vsn all src-module 3                      (Ping all VSNs from the specified module)
ping vsn ip 106.1.1.1 src-module all           (Ping specified VSN from all modules)
ping vsn ip 106.1.1.1 src-module vpath-all   (Ping specified VSN from all modules
                                                having VMs associated to VSNs)
```

The options timeout and count apply to all of the above commands:

```
ping vsn all src-vpath all timeout 2 count 10
ping vsn all ip 106.1.1.1 count unlimited

Errors:
VSN response timeout – VSN is down, not reachable or not responding.
VSN ARP not resolved – VEM couldn't resolve MAC address of VSN.
no response from VEM – VEM is not sending ping response to VSM. Can happen when VEM
                       is down and VSM not detected it yet.
```

These examples show how to display all of the source module traffic:

```
vsm# ping vsn all src-module all
ping vsn 10.1.1.44 vlan 0 from module 9 10 11 12, seq=0 timeout=1-sec
  module(usec)   :  9(508)
  module(failed) : 10(VSN ARP not resolved) 11(VSN ARP not resolved)
                   12(VSN ARP not resolved)
ping vsn 10.1.1.40 vlan 0 from module 9 10 11 12, seq=0 timeout=1-sec
  module(usec)   :  9(974) 11(987) 12(1007)
  module(failed) : 10(VSN ARP not resolved)

ping vsn 10.1.1.44 vlan 0 from module 9 10 11 12, seq=1 timeout=1-sec
  module(usec)   :  9(277) 10(436) 11(270) 12(399)
ping vsn 10.1.1.40 vlan 0 from module 9 10 11 12, seq=1 timeout=1-sec
  module(usec)   :  9(376) 10(606) 11(468) 12(622)

ping vsn 10.1.1.44 vlan 0 from module 9 10 11 12, seq=2 timeout=1-sec
  module(usec)   :  9(272) 10(389) 11(318) 12(357)
ping vsn 10.1.1.40 vlan 0 from module 9 10 11 12, seq=2 timeout=1-sec
  module(usec)   :  9(428) 10(632) 11(586) 12(594)
```

```
ping vsn 10.1.1.44 vlan 0 from module 9 10 11 12, seq=3 timeout=1-sec
  module(usec)   :  9(284) 10(426) 11(331) 12(387)
ping vsn 10.1.1.40 vlan 0 from module 9 10 11 12, seq=3 timeout=1-sec
  module(usec)   :  9(414) 10(663) 11(644) 12(698)

ping vsn 10.1.1.44 vlan 0 from module 9 10 11 12, seq=4 timeout=1-sec
  module(usec)   :  9(278) 10(479) 11(334) 12(469)
ping vsn 10.1.1.40 vlan 0 from module 9 10 11 12, seq=4 timeout=1-sec
  module(usec)   :  9(397) 10(613) 11(560) 12(593)
```

vsm# **ping vsn ip 10.1.1.40 src-module vpath-all**

```
ping vsn 10.1.1.40 vlan 0 from module 9 11 12, seq=0 timeout=1-sec
  module(usec)   :  9(698) 11(701) 12(826)

ping vsn 10.1.1.40 vlan 0 from module 9 11 12, seq=1 timeout=1-sec
  module(usec)   :  9(461) 11(573) 12(714)

ping vsn 10.1.1.40 vlan 0 from module 9 11 12, seq=2 timeout=1-sec
  module(usec)   :  9(447) 11(569) 12(598)

ping vsn 10.1.1.40 vlan 0 from module 9 11 12, seq=3 timeout=1-sec
  module(usec)   :  9(334) 11(702) 12(559)

ping vsn 10.1.1.40 vlan 0 from module 9 11 12, seq=4 timeout=1-sec
  module(usec)   :  9(387) 11(558) 12(597)

vsm#
```

Related Commands

Command	Description
ping	Activates a signal to verify connections with other devices on a path.

policy-agent-image

To designate the policy agent image local URL as bootflash, use the **policy-agent-image** command. To remove the designation, use the no form of the command.

policy-agent-image bootflash:<nsc-pa name>

no policy-agent-image bootflash:<nsc-pa name>

Syntax Description

bootflash:	Designates the policy agent image local URL as bootflash.

Command Default

None

Command Modes

Prime NSC policy agent configuration (config-nsc-policy-agent)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Examples

This example shows how to designate the local URL that contains the policy agent image:

```
vsm# configure
vsm(config)# nsc-policy-agent
vsm(config-nsc-policy-agent)# policy-agent-image bootflash:nsc_pa
```

Related Commands

Command	Description
nsc-policy-agent	Enables the NSC policy agent configuration mode.

pop

To pop a mode off the stack or to restore a mode, use the **pop** command.

pop *file-name*

Syntax Description

file-name	Name of the file.

Command Default None

Command Modes EXEC

SupportedUserRoles network-admin

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Examples This example shows how to restore from a file called file1:

```
vsm# pop file1
```

Related Commands

Command	Description
push	Pushes the current mode onto the stack.

port-profile

To create a port profile and enter port profile configuration mode, use the **port-profile** command. To remove the port profile configuration, use the **no** form of this command.

port-profile *profile-name*

no port-profile *profile-name*

Syntax Description

profile-name	Port profile name. The range of valid values is from 1 to 80.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

The port profile name must be unique for each port profile.

Examples

This example shows how to create a port profile called AccessProf:

```
vsm# configure
vsm(config)# port-profile AccessProf
vsm(config-port-prof)#
```

This example shows how to remove the port profile called AccessProf:

```
vsm# configure
vsm(config)# no port-profile AccessProf
vsm(config)#
```

Related Commands

Command	Description
show port-profile	Displays information about the port profiles.

push

To push the current mode onto stack or to save it, use the **push** command.

push *file-name*

Syntax Description

file-name	Name of the file.

Command Default None

Command Modes EXEC

SupportedUserRoles network-admin

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Examples

This example shows how to push file1 onto the stack:

```
vsm# push file1
```

Related Commands

Command	Description
pop	Pops the current mode off the stack.

registration-ip

To set the service registry IP address, use the **registration-ip** command. To discard the service registry IP address, use the **no** form of this command.

registration-ip *ip-address*

no registration-ip

ip-address	Service registry IP address. The format is A.B.C.D.

Command Default

None

Command Modes

Cisco Prime NSC policy agent configuration mode (config-nsc-policy-agent)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Examples

This example shows how to set the service registry IP address:

```
vsm# configure
vsm(config)# nsc-policy-agent
vsm(config-nsc-policy-agent)# registration-ip 209.165.200.233
vsm(config-nsc-policy-agent)#
```

Related Commands

Command	Description
nsc-policy-agent	Enters the Cisco Prime NSC policy agent configuration mode.

shared-secret

To set the shared secret password for communication between the Cisco Virtual Security Gateway (VSG), the Virtual Supervisor Module (VSM), and the Cisco Prime Network Services Controller (Prime NSC), use the **shared-secret** command. To discard the shared secret password, use the **no** form of this command.

shared-secret *shared-secret-password*

no shared-secret

Syntax Description

shared-secret-password	Shared secret password. The range of valid values is from 1 to 64. You must use at least one uppercase character.

Command Default

None

Command Modes

Cisco Prime NSC policy agent configuration mode (config-nsc-policy-agent)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Examples

This example shows how to set the shared secret password:

```
vsm# configure
vsm(config)# nsc-policy-agent
vsm(config-nsc-policy-agent)# shared-secret Password123
vsm(config-nsc-policy-agent)#
```

Related Commands

Command	Description
nsc-policy-agent	Enters NSC policy agent configuration mode.

show org port brief

To display the ports attached to the port profile where org is configured, use the show org port brief command.

show org port brief [port-profile *pp_name* **| vethernet** *veth_num***] [module** *module_num***]**

Syntax Description

port-profile	Filters the port information for the specified port-profile name.
pp_name	Specifies the port-profile name.
vethernet	Filters the port information for the specified virtual ethernet number.
vethernet_num	Specifies the virtual ethernet number.
module	Filters the display by module number.
module_num	Specifies the module number to see the virtual ethernet connections on the module.

Command Modes

EXEC

SupportedUserRoles

Network-admin

Network-operator

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

You can use the following operators with the **show org port brief** command:

- **>**—Redirects the output to a file.
- **>>**—Redirects the output to a file in append mode.
- module—Filter the output per a specific module number.
- **|**—Pipes the command output to a filter.

Examples

This example shows how to display the port information:

```
vsm# show org port brief
Veth Mod VM-Name vNIC IP-Address
2 4 traffic-vm-ubuntu-50 192.170.0.50,
3 4 traffic-vm-win-70 192.170.0.70,
5 3 traffic-vm-win-30 192.170.0.30,
8 3 traffic-vm-ubuntu-10 192.170.0.10,
```

show running-config

To display the running configuration, use the **show running-config** command.

show running-config [**aaa | diff| ip| port-profile | vlan | acllog | eem | ipqos | port-security | vrf | aclmgr | exclude | ipv6 | radius | vservice | adjmgr | exclude-provision | l3vm | rpm| vshd | all | expand-port-profile | license | security | arp | icmpv6 | monitor | snmp | cdp | igmp | network | spanning-tree | cert-enroll | interface | ntp | vdc-all]**

Syntax Description

aaa	(Optional) Displays the Authentication, Authorization and Accounting (AAA) configuration.
aclmgr	(Optional) Displays the running configuration for Access Control List (ACL) manager.
adjmgr	(Optional) Displays adjacency manager information.
all	(Optional) Displays the current operating configurations.
arp	(Optional) Displays Address Resolution Protocol (ARP) information.
cdp	(Optional) Displays the Cisco- Discovery Protocol (CDP) configuration.
cert-enroll	(Optional) Displays the certificate configuration.
diff	(Optional) Displays the difference between the running and startup configurations.
eem	(Optional) Displays the event manager running configuration.
exclude	(Optional) Excludes the running configuration of specified features.
exclude-provision	(Optional) Exclude configuration for offline pre-provisioned interfaces.
expand-port-profile	(Optional) Displays port profile information.
icmpv6	(Optional) Displays Internet Control Message Protocol (ICMPv6) information.
igmp	(Optional) Displays Internet Group Management Protocol (IGMP) information.
interface	(Optional) Displays interface configurations.
ip	(Optional) Displays Internet Protocol (IP) information.
ipqos	(Optional) Displays the running configuration for the IP Quality of Service (QoS) manager.
ipv6	(Optional) Displays IPv6 information.
l3vm	(Optional) Displays Layer 3 Virtual Machine (L3VM) information.
license	(Optional) Displays the licensing configuration.
monitor	(Optional) Displays Ethernet Switched Port Ananlyzer (SPAN) session information.
network	(Optional) Displays network information.
ntp	(Optional) Displays Network Time Protocol (NTP) information.
port-profile	(Optional) Displays port-profile configurations.
port-security	(Optional) Displays port-security configurations.
radius	(Optional) Displays the Remote Authentication Dial In User Service (RADIUS) configuration.
rpm	(Optional) Displays RPM information.

security	(Optional) Displays the security configurations.
snmp	(Optional) Displays the Simple Network Management Protocol (SNMP) configuration.
spanning-tree	(Optional) Displays spanning-tree protocol information.
vdc-all	(Optional) Displays all Virtual Device Context (VDC) configurations.
vlan	(Optional) Displays virtual large area network (VLAN) information.
vrf	(Optional) Displays Virtual Routing and Forwarding (VRF) information.
vshd	(Optional) Displays the running configuration for virtual shared hardware device (VSHD).
acllog	Displays acllog information.
vservice	Displays virtual service node.

Command Default

None

Command Modes

EXEC

SupportedUserRoles

network-admin

network-operator

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

You can use the following operators with the **show running-config** command:

- **>**—Redirects the output to a file.
- **>>**—Redirects the output to a file in append mode.
- **|**—Pipes the command output to a filter.

Examples

This example shows how to display the running configuration:

```
vsm-hpv# show running-config

!Command: show running-config
!Time: Sun May  5 20:04:22 2013

version 5.2(1)SM1(5.1)
svs switch edition essential

hostname VSM-hpv

no feature telnet
feature network-segmentation-manager
```

```
username admin password 5 $1$KxvwqWCb$8PqeCVrfY6QDy9nau.hBf.  role network-admin

banner motd #Nexus 1000V Switch
#

ip domain-lookup
errdisable recovery cause failed-port-state
svs license volatile
vem 3
  host id 0F5A5036-A5BF-1244-896D-760C4E3AC29C
vem 4
  host id 1022F40A-D033-FB44-B228-6B48FBD14928
snmp-server user admin network-admin auth md5 0xda2d510adcc26f463fc5c476a19be55b priv
0xda2d510adcc26f463fc5c476a19be55b localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO

vrf context management
  ip route 0.0.0.0/0 10.2.0.1
vlan 1,550-555,914

port-channel load-balance ethernet source-mac
port-profile default max-ports 32
port-profile default port-binding static
port-profile type vethernet NSM_template_vlan
  no shutdown
  guid 86ceec5b-7a9c-4df4-9218-333bfc6f40a5
  description NSM default port-profile for VLAN networks. Do not delete.
  state enabled
port-profile type vethernet NSM_template_segmentation
  no shutdown
  guid 4a6cf01d-80df-48b2-87d8-0b0a15e7d450
  description NSM default port-profile for VXLAN networks. Do not delete.
  state enabled
port-profile type ethernet Uplink
  no shutdown
  guid 2122b8d9-8d21-4fb3-9e75-971fbb1a266d
  max-ports 512
  state enabled
port-profile type ethernet uplink_network_default_policy
  no shutdown
  guid bf7bd8ce-9a90-4af2-98c9-d7f8bafa9cb2
  max-ports 512
  description NSM created profile. Do not delete.
  state enabled
port-profile type vethernet N1K
  no shutdown
  guid 70cff39e-9136-434c-8f36-f17e82210031
  state enabled
  publish port-profile
port-profile type vethernet service
  no shutdown
  guid 6b9b60fd-4aff-40da-896c-7df7bc252908
  state enabled
  publish port-profile
port-profile type vethernet ha
  no shutdown
  guid 7f598f09-68d6-47a3-97e0-158ce8558292
  state enabled
  publish port-profile
port-profile type vethernet vnadp
```

```
  capability l3-vservice
  no shutdown
  guid d41c34d0-7c93-4fec-92ef-1f4383276b28
  state enabled
  publish port-profile
port-profile type vethernet veth-1
  org root/Tenant-1
  vservice node VSG-138 profile SP11
  no shutdown
  guid 14fa09d3-6cf8-4c55-b7f5-ad0ae4e4c8bd
  state enabled
  publish port-profile
port-profile type vethernet veth-2
  org root/Tenant-1/VDC-1/App-1/Tier-1
  vservice node VSG-138 profile SP14
  no shutdown
  guid 4be00543-2965-4d4e-be39-2f0ed5c606e6
  state enabled
  publish port-profile
port-profile type vethernet veth-3
  org root/Tenant-1/VDC-1/App-1/Tier-1
  vservice node VSG-N1010 profile SP11
  no shutdown
  guid 335f49a3-95e8-4c88-b078-7a5424f4537b
  state enabled
  publish port-profile
vsm#
```

Related Commands

Command	Description
show aaa	Displays AAA information.

show running-config vservice node

To display the configuration details of the virtual service nodes in the network, use the **show running-config vservice node** command.

show running-config vservice node

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC

SupportedUserRoles

Network-admin

Network-operator

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

You can use the following operators with the **show running-config vservice node** command:

- **>**—Redirects the output to a file.
- **>>**—Redirects the output to a file in append mode.
- node-name—Displays the configuration of the specified vservice node name.
- **|**—Pipes the command output to a filter.

Examples

This example shows how to display the information of the configured vservice nodes:

```
vsm# show running-config vservice node

!Command: show running-config vservice node
!Time: Wed May  8 06:54:03 2013

version 5.2(1)SM1(5.1)
logging level vns_agent 2
vservice node VSGl3 type vsg
  ip address 192.168.180.33
  adjacency l3
  fail-mode close
vservice node VSGhv-l3 type vsg
  ip address 192.168.180.31
  adjacency l3
  fail-mode close
```

Related Commands

Command	Description
vservice node	Configures a virtual service node.

show nsc-pa status

To display the installation status of a policy agent, use the **show nsc-pa status** command.

show nsc-pa status

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Global configuration (config)

SupportedUserRoles network-admin
network-operator

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines You can use the following operators with the **show nsc-pa status** command:

- >—Redirects the output to a file.
- >>—Redirects the output to a file in append mode.
- |—Pipes the command output to a filter.

Examples This example shows how to display the installation status of the policy agent:

```
VSM-hpv# configure
VSM-hpv(config)# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 3.2(1c)-`vsm
```

Related Commands

Command	Description
nsc-policy-agent	Enters the Cisco Prime NSC policy agent configuration mode.

show vservice brief

To display only a brief summary about the Virtual Service Nodes (VSN), use the **show vservice brief** command.

show vservice brief {[node-name <*node name***>] | { [node-l3] [node-ipaddr <***ip-addr***>}} | [module <***module-num***>]}}**

Syntax Description

node-name	(Optional) Displays service node name.
node-name	Specifies the service node.
node-l3	Displays the port information for the Layer 3 adjacency of a node.
node-ipaddr	Displays the port information for the specified IP address of the node.
ip-addr	Specifies the IP address of the service node.
module	(Optional) Displays module number.
module-num	Specifies the module number to see all the VSN connections on the module.

Command Default

None

Command Modes

EXEC

SupportedUserRoles

network-admin

network-operator

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

You can use the following operators with the **show vservice brief** command:

- **>**—Redirects the output to a file.
- **>>**—Redirects the output to a file in append mode.
- **|**—Pipes the command output to a filter.

Examples

This example shows how to display brief information about the Cisco VSGs:

```
VSM-hpv# sh vservice brief
------------------------------------------------------------------------------
Node Information
------------------------------------------------------------------------------
ID Name Type IP-Address Mode State Module
```

```
1 VSG-Node-L3 vsg 70.1.0.75 l3 Alive 4,5,
------------------------------------------------------------------------------
Path Information
------------------------------------------------------------------------------
------------------------------------------------------------------------------
Port Information
------------------------------------------------------------------------------
PortProfile:PP-VM-VNS
Org:root/T1
Node:VSG-Node-L3(70.1.0.75) Profile(Id):SP1(10)
Veth Mod VM-Name vNIC
5       4   ub-31
6       5   ub-11
8       5   ub-12
9       4       ub-32
```

Related Commands

Command	Description
show vservice port	Displays vEth port information.

show vservice connection

To display VSN connections, use the **show vservice connection** command.

show vservice connection [**port-profile** <*pp_name*> | **service-profile** <*sp_name*> | **node-name** <*node_name*> | {[**node-l3**] [**node-ipaddr** <*ip_addr*>]}] [**module** <*module_num*>]

Syntax Description

port-profile	Filters the port information for the specified port-profile name.
port-profile	Specifies the port-profile name.
service-profile	Filters the port information for the specified service-profile name.
service_profile	Specifies the service-profile name.
node-name	(Optional) Displays service node name.
node-name	Specifies the service node.
node-l3	Displays the port information for the Layer 3 adjacency of a node.
node-ipaddr	Displays the port information for the specified IP address of the node.
ip-addr	Specifies the IP address of the service node.
module	(Optional) Displays module number.
module-num	Specifies the module number to see all the VSN connections on the module.

Command Default

None

Command Modes

EXEC

SupportedUserRoles

network-admin

network-operator

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

You can use the following operators with the **show vservice connection** command:

- **>**—Redirects the output to a file.
- **>>**—Redirects the output to a file in append mode.
- **|**—Pipes the command output to a filter.

Examples

This example shows how to display Cisco VSG connections:

```
vsm-hpv# show vservice connection
```

```
Actions(Act):
d - drop s - reset
p - permit t - passthrough
r - redirect e - error
_ - not processed yet upper case - offloaded
Flags:
A - seen ack for syn/fin from src a - seen ack for syn/fin from dst
E - tcp conn established (SasA done)
F - seen fin from src f - seen fin from dst
R - seen rst from src r - seen rst from dst
S - seen syn from src s - seen syn from dst
T - tcp conn torn down (FafA done) x - IP-fragment connection

#Port-Profile:PP-VM-VNS2 Node:VSG-Node74
#Module 3
Proto SrcIP[:Port] SAct DstIP[:Port] DAct Flags Bytes
icmp 80.1.0.53 P 80.1.0.80 592
#Module 5
Proto SrcIP[:Port] SAct DstIP[:Port] DAct Flags Bytes
icmp 80.1.0.53 80.1.0.80 P 592
```

Related Commands

Command	Description
show vservice port	Displays port information.

show vservice detail

To display detailed information about the Virtual Service Nodes (VSN), use the **show vservice detail** command.

show vservice detail{[node-name <*node name***>] | { [node-l3] [node-ipaddr <***ip-addr***>}} | [module <***module-num***>]}}**

Syntax Description

node-name	(Optional) Displays service node name.
node-name	Specifies the service node.
node-l3	Displays the port information for the Layer 3 adjacency of a node.
node-ipaddr	Displays the port information for the specified IP address of the node.
ip-addr	Specifies the IP address of the service node.
module	(Optional) Displays module number.
module-num	Specifies the module number to see all the VSN connections on the module.

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC

Global Configuration (config)

SupportedUserRoles

network-admin

network-operator

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

You can use the following operators with the **show vservice detail** command:

- **>**—Redirects the output to a file.
- **>>**—Redirects the output to a file in append mode.
- **|**—Pipes the command output to a filter.

Examples

This example shows how to display detailed information about Cisco VSGs:

```
vsm-hpv# show vservice detail
------------------------------------------------------------------------------
                                  Node Information
------------------------------------------------------------------------------
Node ID:3      Name:VSG-Root
Type:vsg       IPAddr:10.1.0.150       Fail:close  L3
Mod  State     MAC-Addr                VVer
  4  Alive     --                         2

------------------------------------------------------------------------------
                                  Path Information
------------------------------------------------------------------------------
------------------------------------------------------------------------------
                                  Port Information
------------------------------------------------------------------------------
PortProfile:veth-10
Org:root/Tenant-1/VDC-1/App-1/Tier-1
Node:VSG-Root(10.1.0.150)                     Profile(Id):SP100(16)
Veth5
Module  :4
VM-Name :vm-win-16
vNIC:Network Adapter
DV-Port :884f1580-0ad6-4958-a74a-c27b3febbe28--8884a888-09e1-4503-8074-de32e3e2
af85
VM-UUID :884F1580-0AD6-4958-A74A-C27B3FEBBE28
DVS-UUID:633a90b8-98bd-4264-b3b6-7a0d77b73ba1

vsm#
-------------------
```

Related Commands

Command	Description
show vservice port	Displays information about virtual Ethernet (vEth) ports.

show vservice node mac brief

To display only summary about the MAC address of the virtual service node, use the **show vservice node mac brief** command.

show vservice node mac brief

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC

SupportedUserRoles

network-admin

network-operator

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

You can use the following operators with the **show vservice node mac brief** command:

- **>**—Redirects the output to a file.
- **>>**—Redirects the output to a file in append mode.
- **|**—Pipes the command output to a filter.

Examples

This example shows how to display the MAC address of the Cisco virtual service node

```
VSM-hpv# show vservice node mac brief
------------------------------------------------------------------------------
                                  Node Information
------------------------------------------------------------------------------
ID Type   IP-Address      MAC-Addr          Mode   Fail  State   Module
  3 vsg    10.1.0.150      00:00:00:00:00:00 l3     close Alive    4,
```

Related Commands

Command	Description
show vservice node brief	Displays summary of virtual service node.

show vservice node brief

To display only the summary about the Cisco virtual service node, use the **show vservice node brief** command.

show vservice node brief {[**name** <*name*>] | {[**l3**] [**ipaddr** <*ip_addr*>]} } [**module** <*module_num*>]}

Syntax Description

name	(Optional) Displays service node name.
name	Service node.
l3	Displays the port information for the Layer 3 adjacency.
ipaddr	Displays the port information for the specified IP address of the node.
ip_addr	Node's IP address.
module	(Optional) Displays module keyword.
module-num	Module number to see all the VSN connections on the module.

Command Default

None

Command Modes

EXEC

Global configuration (config)

Supported User Roles

network-admin

network-operator

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

You can use the following operators with the **show vservice node brief** command:

- **>**—Redirects the output to a file.
- **>>**—Redirects the output to a file in append mode.
- **|**—Pipes the command output to a filter.

Examples

This example shows how to display summary information about Cisco VSN.

```
VSM-hpv# show vservice  node brief
------------------------------------------------------------------------
                                  Node Information
------------------------------------------------------------------------
```

```
ID Name                     Type   IP-Address      Mode   State   Module
  3 VSG-Root                 vsg    10.1.0.150      l3     Alive  4,
```

Related Commands

Command	Description
show vservice node detail	Displays detailed information about virtual service node.

show vservice node detail

To display the detail about the Cisco virtual service node, use the **show vservice node detail** command.

show vservice node detail {[**name** <*name*>] | {[**l3**] [**ipaddr** <*ip_addr*>]} } [**module** <*module_num*>]}

SyntaxDescription

name	(Optional) Displays service node name.
name	Service node.
l3	Displays the port information for the Layer 3 adjacency.
ipaddr	Displays the port information for the specified IP address of the node.
ip_addr	Node's IP address.
module	(Optional) Displays module keyword.
module-num	Module number to see all the VSN connections on the module.

Command Default

None

Command Modes

EXEC

Global configuration (config)

SupportedUserRoles

network-admin

network-operator

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

You can use the following operators with the **show vservice node detail** command:

- **>**—Redirects the output to a file.
- **>>**—Redirects the output to a file in append mode.
- **|**—Pipes the command output to a filter.

Examples

This example shows how to display Cisco VSG service node:

```
VSM-hpv# show vservice node detail
------------------------------------------------------------------------------
                                  Node Information
------------------------------------------------------------------------------
```

```
Node ID:3       Name:VSG-Root
Type:vsg        IPAddr:10.1.0.150       Fail:close  L3
Mod  State      MAC-Addr                VVer
  4  Alive      --                         2
```

Related Commands

Command	Description
show vservice node brief	Displays brief information about virtual service node.

show vservice port brief

To display a brief summary of the configured ports in the network, use the **show vservice port brief** command.

show vservice port brief [**port-profile** <*pp_name*> | **vethernet** <*veth_if*> | **service-profile** <*sp_name*> | **node-name** <*node_name*> | {[**node-l3**] [**node-ipaddr** <*ip_addr*>]}] [**module** <*module_num*>]}

Syntax Description

port-profile	Displays the port information for the specified port-profile name.
pp_name	Port-profile name.
vethernet	Displays the virtual ethernet interface for the specified port-profile name.
veth_if	Virtual ethernet interface.
service-profile	Displays the port information for the specified service-profile name.
service_profile	Service-profile name.
node-name	(Optional) Displays service node name.
node-name	Service node.
node-l3	Displays the port information for the Layer 3 adjacency of a node.
node-ipaddr	Displays the port information for the specified IP address of the node.
ip_addr	Node's IP address.
module	(Optional) Displays module keyword.
module-num	Module number to see all the VSN connections on the module.

Command Modes

EXEC

Global configuration (config)

SupportedUserRoles

Network-admin

Network-operator

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

You can use the following operators with the **show vservice port brief** command:

- **>**—Redirects the output to a file.
- **>>**—Redirects the output to a file in append mode.
- module—Filter the output per a specific module number.
- **|**—Pipes the command output to a filter.

Examples

This example shows how to display the brief summary information of the vservice ports per module number 4:

```
vsm# show vservice port brief module 4

--------------------------------------------------------------------------------
                                  Port Information
--------------------------------------------------------------------------------
PortProfile:
Org:root/Tenant-1/VDC-1/App-1/Tier-1
Node:VSG-Root(10.1.0.150)                     Profile(Id):SP100(16)
Veth Mod VM-Name                              vNIC
   5   4 vm-win-16
```

Related Commands

Command	Description
vservice port detail	Displays details of the configured ports in the network.

show vservice port detail

To display details of the configured ports in the network, use the **show vservice port detail** command.

show vservice port detail [**port-profile** <*pp_name*> | <*veth_if*> | **service-profile** <*sp_name*> | **node-name** <*node_name*> | {[**node-l3**] [**node-ipaddr** <*ip_addr*>]}] [**module** <*module_num*>]}

Syntax Description

port-profile	Displays the port information for the specified port-profile name.
pp_name	Port-profile name.
veth_if	Virtual ethernet interface.
service-profile	Displays the port information for the specified service-profile name.
service_profile	Service-profile name.
node-name	(Optional) Displays service node name.
node-name	Service node.
node-l3	Displays the port information for the Layer 3 adjacency of a node.
node-ipaddr	Displays the port information for the specified IP address of the node.
ip_addr	Node's IP address.
module	(Optional) Displays module keyword.
module-num	Module number to see all the VSN connections on the module.

Command Modes

EXEC

SupportedUserRoles

Network-admin

Network-operator

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

You can use the following operators with the **show vservice port detail** command:

- **>**—Redirects the output to a file.
- **>>**—Redirects the output to a file in append mode.
- module—Filter the output per a specific module number.
- **|**—Pipes the command output to a filter.

Examples

This example shows how to display the detailed information of the vservice ports per module number 4:

```
vsm# show vservice port detail module 4
```

```
--------------------------------------------------------------------------------
                                  Port Information
--------------------------------------------------------------------------------
PortProfile:
Org:root/Tenant-1/VDC-1/App-1/Tier-1
Node:VSG-Root(10.1.0.150)                     Profile(Id):SP100(16)
Veth5
Module  :4
VM-Name :vm-win-16
vNIC:Network Adapter
DV-Port :884f1580-0ad6-4958-a74a-c27b3febbe28--8884a888-09e1-4503-8074-de32e3e2a
f85
VM-UUID :884F1580-0AD6-4958-A74A-C27B3FEBBE28
DVS-UUID:633a90b8-98bd-4264-b3b6-7a0d77b73ba1
```

Related Commands

Command	Description
show vservice port brief	Displays a brief summary of the configured ports in the network.

show vservice statistics

To display the information about the configuration, MAC address, state of associated Cisco VSG and Virtual Ethernet Module (VEM), Veths to which Cisco VSGs are bound, and Virtual Service Node (VSN) statistics for all VEM modules associated with Cisco VSGs, use **show vservice statistics** command.

show vservice statistics [**ip** *ip-addr* | **module** *module-num*]

Syntax Description

ip	(Optional) Displays IP address statistics.
ip-addr	Specifies the MAC address
module	(Optional) Displays VEM module statistics.
module-num	Specifies the VSG and VEM module

Command Default

None

Command Modes

EXEC

SupportedUserRoles

network-admin
network-operator

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

You can use the following operators with the **show vservice statistics** command:

- **>**—Redirects the output to a file.
- **>>**—Redirects the output to a file in append mode.
- **|**—Pipes the command output to a filter.

Examples

This example shows how to display statistics for a module:

```
VSM-hpv# show vservice statistics module 4
#VSN  VLAN: 0, IP-ADDR: 10.1.0.150
  Module: 4
    #VPath Packet Statistics     Ingress         Egress           Total
    Total Seen                         2              2               4
    Policy Redirects                   2              2               4
    No-Policy Passthru                 0              0               0
    Policy-Permits Rcvd                1              2               3
    Policy-Denies  Rcvd                0              0               0
    Permit Hits                        0              0               0
    Deny   Hits                        0              0               0
    Decapsulated                       1              2               3
```

```
    Fail-Open                          0             0             0
    Badport Err                        0             0             0
    VSN Config Err                     0             0             0
    VSN State Down                   228          1288          1516
    Encap Err                          0             0             0
    Version Mismatch                   0             0             0
    V1 In svcPath                      0             0             0
    All-Drops                        228          1288          1516
    Flow Notificns Sent                                           0
    Total Rcvd From VSN                                           5
    Non-Cisco Encap Rcvd                                          0
    VNS-Port Drops                                                2
    Policy-Action Err                                             0
    Decap Err                                                     0
    L2-Frag Sent                                                  0
    L2-Frag Rcvd                                                  0
    L2-Frag Coalesced                                             0
    Encap exceeded MTU                                            0
    ICMP Too Big Rcvd                                             0

    #VPath Flow Statistics
    Active Flows                       0  Active Connections                0
    Forward Flow Create                1  Forward Flow Destroy              1
    Reverse Flow Create                1  Reverse Flow Destroy              2
    Flow ID Alloc                      3  Flow ID Free                      3
    Connection ID Alloc                1  Connection ID Free                1
    L2 Flow Create                     1  L2 Flow Destroy                   1
    L3 Flow Create                     0  L3 Flow Destroy                   0
    L4 TCP Flow Create                 0  L4 TCP Flow Destroy               0
    L4 UDP Flow Create                 2  L4 UDP Flow Destroy               2
    L4 Oth Flow Create                 0  L4 Oth Flow Destroy               0
    Embryonic Flow Create              0  Embryonic Flow Bloom              0
    L2 Flow Timeout                    2  L2 Flow Offload                   3
    L3 Flow Timeout                    0  L3 Flow Offload                   0
    L4 TCP Flow Timeout                0  L4 TCP Flow Offload               0
    L4 UDP Flow Timeout                5  L4 UDP Flow Offload               0
    L4 Oth Flow Timeout                0  L4 Oth Flow Offload               0
    Flow Lookup Hit                    5  Flow Lookup Miss                  3
    Flow Dual Lookup                   8  L4 TCP Tuple-reuse                0
    TCP chkfail InvalACK               0  TCP chkfail SeqPstWnd             0
    TCP chkfail WndVari                0
    Flow Classify Err                  0  Flow ID Alloc Err                 0
    Conn ID Alloc Err                  0  Hash Alloc Err                    0
    Flow Exist                         0  Flow Entry Exhaust                0
    Flow Removal Err                   0  Flow Entry Miss                   0
    Flow Full Match Err                0  Bad Action Receive                0
    Invalid Flow Pair                  3  Invalid Connection                0
    Hash Alloc                         0  Hash Free                         0
    InvalFID Lookup Err                0  Deferred Delete                   0

vsm#
```

Related Commands

Command	Description
show vservice port vethernet	Displays information about virtual Ethernet (vEth) ports.

show vsn port vethernet

To display information about virtual Ethernet (vEth) ports, use the **show vsn port vethernet** command.

show vsn port vethernet *port-number*

Syntax Description

port-number	Port number. The range is from 1 to 1048575.

Command Default

None

Command Modes

EXEC

SupportedUserRoles

network-admin
network-operator

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

You can use the following operators with the **show vsn port vethernet** command:

- **>**—Redirects the output to a file.
- **>>**—Redirects the output to a file in append mode.
- **|**—Pipes the command output to a filter.

Examples

This example shows how to display information about vEth port 2:

```
vsm# show vsn port vethernet 2

Veth             : Veth2
VM Name          : UD136-1
VM uuid          : 42 3b e1 60 17 e6 92 c4-3b 47 f4 b7 4c a0 be 1b
DV Port          : 7458
DVS uuid         : 90 33 3b 50 c2 11 2a 50-ae c5 0f 07 b2 b3 23 2c
Flags            : 0x148
VSN Data IP      : 192.168.136.1
Security Profile : sp1
Org              : Not set
VNSP id          : 1
IP addresses:
vsm#
```

Related Commands

Command	Description
show vservice statistics	Displays virtual service node statistics.

tcp state-checks

To configure the Cisco Nexus 1000V switch to perform TCP state checks, use the **tcp state-checks** command. To disable TCP state checks, use the **no** form of the command.

tcp state-checks

no tcp state-checks

Syntax Description

There are no arguments.

Command Modes

vservice global configuration (config-vservice-global)

SupportedUserRoles

network-admin

system-admin

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

Use this command to enable or disable TCP state checks. The TCP state check is disabled by default.

Examples

This example shows how to enable the switch to perform the TCP state checks:

```
n1000v(config)# vservice global type vsg
n1000v(config-vservice-global)# tcp state-checks
```

Related Commands

Command	Description
vservice global type vsg	Enters the vservice global configuration mode.

vservice

To associate a port-profile with a service node, use the **vservice** command from the config-port-profile mode of the port-profile. To delete a port-profile configuration, use the **no** form of this command.

vservice {**node** *node_name* [**profile** *profile_name*] }

no vservice

Syntax Description

node	Specifies the service node to associate the port-profile with.
node_name	The pre-defined service node name.
profile	(Optional) Specifies the service profile the service node is to be associated with.
profile_name	The pre-defined service profile name.

Defaults

None

Command Modes

Port-profile configuration (config-port-prof)

SupportedUserRoles

Network-admin

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

You can associate either the service node to the chosen port-profile entity. If the node is of type VSG, then specifying a profile is mandatory.

Examples

This example shows how to configure a port-profile with a node and service profile:

```
vsm(config)# port-profile port1 <-------- Enter the mode of the port-profile entity you
want to configure
vsm(config-port-prof)# vservice node vsg1 profile sp1
vsm(config-port-prof)#
```

Related Commands

Command	Description
show port-profile	Displays information about the port profiles.

vservice node

To configure a service node, use the **vservice node** command. To disable a service node, use the **no** form of the command.

vservice node *node_name* **type** {**vsg**}
ip address *ip-address* | **no ip address**
adjacency {**l3**} | **no adjacency failmode** {**close** | **open**} | **no failmode**

no vservice node *node_name*
no ip address
no adjacency
no failmode

Syntax Description

node_name	Displays the service node name to identify it in the network.
type	Displays the type of service node to be configured. The values include vsg.
vsg	Cisco virtual security gateway (VSG) service node.
ip-address	Displays IP address of the associated service node.
ip-address	IP address of the associated service node. This IP address should match the IP address of the data interface node.
adjacency	Specifies the adjacency for l3 mode.
l3	Specifies Layer 3 (using IP address) mode for the service node.
failmode	Sets state to be in either fail close, or fail open mode.
close	Drops packets if the Cisco VSG is down. This is the default value.
open	Allows the packets to pass through if the Cisco VSG is down.

Command Default

None

Command Modes

Global configration (config)

SupportedUserRoles

Network-admin

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

Use the **vservice node** command to configure a service node with an existing Cisco VSG. That node in turn is associated with either a port profile or a vservice path.

You can only delete inactive vservice nodes. The inactive nodes are not configured with any virtual machines or service paths.

Examples

This example shows how to enter the vservice-node mode, and configure the IP address of a vservice node, adjacency, and fail-mode settings:

```
vsm(config)# vservice node test type vsg <------- enter the vservice-node mode
vsm(config-vservice-node)# ip address 1.1.11.11
vsm(config-vservice-node)# adjacency l3
vsm(config-vservice-node)# fail-mode close
vsm(config-vservice-node)#
```

Related Commands

Command	Description
show vservice node brief	Displays the vservice node information, in brief.
show vservice node detail	Displays the vservice node information, in detail.

nsc-policy-agent

To enter Cisco Prime Network Services Controller (Prime NSC) policy agent mode, use the **nsc-policy-agent** command.

nsc-policy-agent

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Usage Guidelines

Use the Cisco Prime NSC policy agent configuration mode to configure policy agents.

Examples

This example shows how enter policy agent mode:

```
vsm# configure
vsm(config)# nsc-policy-agent
vsm(config-nsc-policy-agent)#
```

Related Commands

Command	Description
configure	Enters global configuration mode.

vservice global type vsg

To enter the vservice global configuration mode, use the **vservice global type vsg** command.

vservice global type vsg

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

vservice global configration (config-vservice-global)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SM1(5.1)	This command was introduced.

Examples

This example shows how to enter the vservice global configuration mode:

```
n1000v# configure <------ enter the config mode
n1000v(config)# vservice global type vsg
n1000v(config-vservice-global)#
```

Related Commands

Command	Description
tcp state-checks	Configures selective TCP state checks on the switch traffic.