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#
```