CHAPTER 7

VSM and VEM Modules

This chapter describes how to identify and resolve problems that relate to modules and includes the following sections:

Information About Modules

Cisco Nexus 1000V manages a data center defined by a VirtualCenter. Each server in the data center is represented as a module in Nexus 1000V and can be managed as if it were a module in a physical Cisco switch.

The Cisco Nexus 1000V implementation has 2 parts:

- Virtual supervisor module (VSM) – This is the control software of the Cisco Nexus 1000V distributed virtual switch. It runs on a virtual machine (VM) and is based on NX-OS software.
- Virtual Ethernet module (VEM) – This is the part of Cisco Nexus 1000V that actually switches data traffic. It runs on a VMware ESX 4.0 host. Several VEMs are controlled by one VSM. All the VEMs that form a switch domain should be in the same virtual Data Center as defined by VMware VirtualCenter.

Troubleshooting a Module Not Coming Up on the VSM

This section describes the process you can use when a module does not come up on the VSM. This section includes the following topics:

Guidelines for Troubleshooting Modules

Follow these guidelines when troubleshooting a module controlled by the VSM.

- You must have a VSM VM and a VEM up and running.
- Make sure you are running compatible versions of vCenter Server and VSM.

  For more information, see the *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV2(1.1)*.
- To verify network connectivity between the VSM and vCenter Server, ping the IP address of the vCenter Server. If you are using a domain name service (DNS) name, use the DNS name in the ping. If a ping to the vCenter Server fails, check to see if you can ping the gateway. Otherwise, check the mgmt0 interface configuration settings.
- Make sure the firewall settings are OFF on the vCenter Server. If you want the firewall settings, then check to see if these ports are open.
  - Port 80
  - Port 443
- If you see the following error, verify that the VSM extension was created from vCenter Server.
  - ERROR: [VMware vCenter Server 4.0.0 build-150489]
    Extension key was not registered before its use

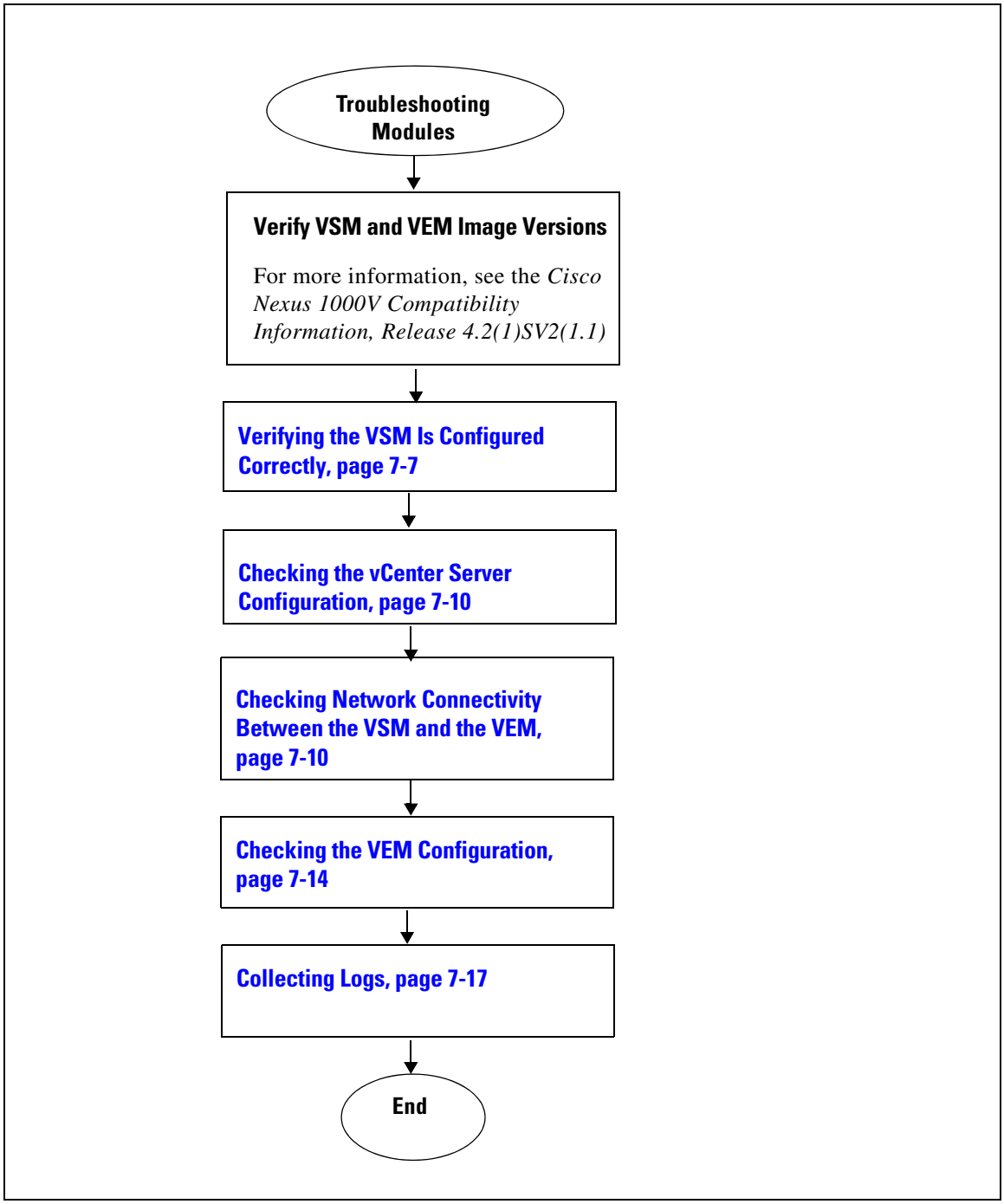
  To verity that the extension or plugin was created, see the "Finding the Extension Key Tied to a Specific DVS" procedure on page 3-8.

  For more information about extension keys or plugins, see the "Managing Extension Keys" section on page 3-6.
- If you see the following error, see the "Checking the vCenter Server Configuration" procedure on page 7-10.
  - ERROR: Datacenter not found
- For a list of terms used with Cisco Nexus 1000V, see the *Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(5.1)*.

Flow Chart for Troubleshooting Modules

Use the following flowchart to troubleshoot modules.

Flowchart: Troubleshooting Modules



Problems with the VSM

The following are symptoms, possible causes, and solutions for problems with the VSM.

Table 7-1 Problems with the VSM

Symptom	Possible Causes	Solution
You see the following error on the VSM: `ERROR: [VMware vCenter Server 4.0.0 build-150489] Extension key was not registered before its use`	A extension or plug-in was not created for the VSM.	1. Verify that the extension or plugin was created. "Finding the Extension Key Tied to a Specific DVS" procedure on page 3-8 2. If the plug-in is not found, then create one using the following procedure in the *Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(5.1)*: Creating a Cisco Nexus 1000V Plug-In on the vCenter Server
Following a reboot of the VSM, the system stops functioning in one of the following states and does not recover on its own. Attempts to debug fail.		
After boot, VSM in loader prompt.	Corrupt VSM kickstart image.	1. Boot the VSM from the CD ROM. 2. From the CD Boot menu, choose Option 1, Install Nexus1000v and bring up new image. Follow the VSM installation procedure.
	Boot variables are not set.	1. Boot the VSM from the CD ROM. 2. From the CD Boot menu, choose Option 3, Install Nexus1000v only if the disk unformatted and bring up new image. 3. Set the boot variables used to boot the VSM: **boot system bootflash:***system-boot-variable-name* **boot kickstart bootflash:***kickstart-boot-variable-name* 4. Reload the VSM. **reload**
After boot, VSM in boot prompt.	Corrupt VSM system image.	1. Boot the VSM from the CD ROM. 2. From the CD Boot menu, choose Option 1, Install Nexus1000v and bring up new image. 3. Follow the VSM installation procedure.

Table 7-1 Problems with the VSM (continued)

Symptom	Possible Causes	Solution
After boot, VSM re-configured.	Startup configuration is deleted.	Do one of the following: • If you have a saved backup copy of your configuration file, restore the configuration on the VSM. **copy** *source filesystem: filename* **system:running-config** • If not, reconfigure the VSM using the following section in the *Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(5.1)*: Setting Up the Software
After boot, VSM stopped at "Loader Loading."	Corrupt boot menu file.	1. Boot the VSM from the CD ROM. 2. From the CD Boot menu, choose Option 3, Install Nexus1000v only if the disk unformatted and bring up new image. 3. Do one of the following: • If you have a saved backup copy of your configuration file, restore the configuration on the VSM. **copy** *source filesystem: filename* **system:running-config** • If not, reconfigure the VSM using the following section in the *Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(5.1)*: Setting Up the Software
After boot, secondary VSM reboots continuously.	Control VLAN or control interface down	Check control connectivity between the active and standby VSM.
	Active and standby VSMs fail to synchronize.	From active VSM, check gsyncstats to identify which application caused the failure. **show logging**
After a host reboot, the absence of a VLAN, or the wrong system VLAN on the VSM management port profile, the control and management connectivity of the VSM is lost.	The VSM is running on a VEM that it manages, but the VSM ports are not configured with system port profiles.	Run the VEM connect script locally in the ESX host where the VEM is running. Then go to the VSM and configure the system VLANs in the port profile used for management. "Recovering Management and Control Connectivity of a Host when a VSM is Running on a VEM" section on page 7-12

Verifying the VSM Is Connected to the vCenter Server

You can use the following procedure to verify that the VSM is connected to the vCenter Server.

Step 1 Verify the connection between the VSM and vCenter Server.

show svs connections

The output should indicate that the operational status is **Connected**.

```
Example:
n1000v# show svs connections
connection vc:
    ip address: 172.23.231.223
    protocol: vmware-vim https
    certificate: user-installed
    datacenter name: hamilton-dc
    DVS uuid: 92 7a 14 50 05 11 15 9c-1a b0 f2 d4 8a d7 6e 6c
    config status: Disabled
    operational status: Disconnected
```

Step 2 Do one of the following:

- If the status is **Connected**, then return to the Flowchart: Troubleshooting Modules, page 7-3.
- If not, then continue with the next step.

Step 3 Connect to the vCenter Server.

config t

svs connection *connection_name*

connect

```
Example:
n1000v# conf t
n1000v(config)# svs connection HamiltonDC
n1000v(config-svs-conn)# connect

Example:
n1000v# conf t
n1000v(config)# svs connection HamiltonDC
n1000v(config-svs-conn)# connect
ERROR: [VMWARE-VIM] Extension key was not registered before its use.
```

Step 4 Do one of the following:

- If you see an error message about the Extension key, continue with the next stepTable 7-1.
- If not, go to Step 6.

Step 5 Do the following and then go to Step 6.

- Unregister the extension key using the "Unregister the Extension Key in the vCenter Server" procedure on page 3-12.
- Install a new extension key using the following procedure in the *Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(5.1)*.
  - *Creating a Cisco Nexus 1000V Plug-In on the vCenter Server*

Step 6 Verify the connection between the VSM and vCenter Server.

show svs connections

The output should indicate that the operational status is **Connected**.

```
Example:
n1000v# show svs connections
connection vc:
    ip address: 172.23.231.223
    protocol: vmware-vim https
    certificate: user-installed
    datacenter name: hamilton-dc
    DVS uuid: 92 7a 14 50 05 11 15 9c-1a b0 f2 d4 8a d7 6e 6c
    config status: Disabled
    operational status: Disconnected
```

Step 7 Do one of the following:

- If the status is **Connected**, then you have completed this procedure.
- If not, then return to the Flowchart: Troubleshooting Modules, page 7-3.

Verifying the VSM Is Configured Correctly

This section includes the following procedures to verify the VSM configuration.

Verifying the Domain Configuration

You can use the following procedure to verify the domain configuration.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- The output of the show **svs domain** command should indicate the following:
  - The presence of a control VLAN and a packet VLAN.
  - The domain configuration was successfully pushed to VC.

Step 1 On the VSM, verify the domain configuration.

show svs domain

```
Example:
n1000v# show svs domain
SVS domain config:
  Domain id:    682
  Control vlan: 3002
  Packet vlan:  3003
  L2/L3 Control VLAN mode: L2
  L2/L3 Control VLAN interface: mgmt0
  Status: Config push to VC successful
```

Verifying the System Port Profile Configuration

You can use the following procedure to verify the port profile configuration.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- The output of the **show port-profile name** command should indicate the following:
  - The control and packet VLANs are assigned.
  - The port profile is enabled.
  - If you have configured a non-default system mtu setting, then it is of the correct size.

Step 1 On the VSM, verify the system port profile configuration.

show port-profile name *system-port-profile-name*

Example:

```
n1000v# show port-profile name SystemUplink
port-profile SystemUplink
  description:
  type: ethernet
  status: enabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: 114,115
  port-group: SystemUplink
  max ports: 32
  inherit:
  config attributes:
    switchport mode trunk
    switchport trunk allowed vlan all
    system mtu 1500
    no shutdown
  evaluated config attributes:
    switchport mode trunk
    switchport trunk allowed vlan all
    no shutdown
  assigned interfaces:
```

Verifying the Control and Packet VLAN Configuration

You can use the following procedure to verify that the control and packet VLANs are configured on the VSM.

Note The procedure documented is for troubleshooting VSM and VEM connectivity with layer 2 mode.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- The output of the **show running-config** command should show control and packet VLAN ID numbers among the VLANs configured,

Step 1 On the VSM, verify that the control and packet VLANs are present.

```
n1000v# show running-config vlan 260-261
version 4.0(4)SV1(3)
vlan 260
  name cp_control
vlan 261
  name cp_packet

n1000v#
. . .
```

Step 2 Find the AIPC MAC address of the VSM by running **show svs neighbors** on the VSM.

```
switch(config-svs-domain)# show svs neighbors

Active Domain ID: 27

AIPC Interface MAC: 0050-56bc-74f1 <-------------
Inband Interface MAC: 0050-56bc-62bd

Src MAC           Type   Domain-id    Node-id     Last learnt (Sec. ago)
--------------------------------------------------------------------------

0050-56bc-6a3d     VSM        27         0201     771332.97
0002-3d40-1b02     VEM        27         0302        51.60
0002-3d40-1b03     VEM        27         0402        51.60
```

Step 3 Find the DPA MAC address of the VEM by running vemcmd show card on the ESX host.

```
# vemcmd show card
Card UUID type  2: 24266920-d498-11e0-0000-00000000000f
Card name:
Switch name: Nexus1000v
Switch alias: DvsPortset-0
Switch uuid: ee 63 3c 50 04 b1 6d d6-58 61 ff ba 56 05 14 fd
Card domain: 27
Card slot: 3
VEM Tunnel Mode: L2 Mode
VEM Control (AIPC) MAC: 00:02:3d:10:1b:02
VEM Packet (Inband) MAC: 00:02:3d:20:1b:02
VEM Control Agent (DPA) MAC: 00:02:3d:40:1b:02 <-------------
VEM SPAN MAC: 00:02:3d:30:1b:02
Primary VSM MAC : 00:50:56:bc:74:f1
Primary VSM PKT MAC : 00:50:56:bc:62:bd
Primary VSM MGMT MAC : 00:50:56:bc:0b:d5
Standby VSM CTRL MAC : 00:50:56:bc:6a:3d
Management IPv4 address: 14.17.168.1
Management IPv6 address: 0000:0000:0000:0000:0000:0000:0000:0000
Primary L3 Control IPv4 address: 0.0.0.0
Secondary VSM MAC : 00:00:00:00:00:00
Secondary L3 Control IPv4 address: 0.0.0.0
Upgrade : Default
Max physical ports: 32
Max virtual ports: 216
Card control VLAN: 168
```

```
Card packet VLAN: 168
Control type multicast: No
Card Headless Mode : No
       Processors: 16
  Processor Cores: 8
Processor Sockets: 2
  Kernel Memory:   25102148
Port link-up delay: 5s
Global UUFB: DISABLED
Heartbeat Set: True
PC LB Algo: source-mac
Datapath portset event in progress : no
Licensed: Yes
```

Step 4 Check the upstream switches for these MAC addresses in the correct VLANs.

```
switch1 # show mac address-table | grep 1b02
* 168      0002.3d20.1b02    dynamic   20          F    F  Veth854
* 168      0002.3d40.1b02    dynamic   0           F    F  Veth854
* 1        0002.3d40.1b02    dynamic   1380        F    F  Veth854

switch2 # show mac address-table | grep 74f1
* 168      0050.56bc.74f1    dynamic   0           F    F  Eth1/1/3
```

Checking the vCenter Server Configuration

You can use the following procedure from vSphere client to verify the configuration on the vCenter Server.

Step 1 Confirm that the host is added to the data center and the Cisco Nexus 1000V DVS in that data center.

Step 2 Confirm that at least one pnic of the host is added to the DVS, and that pnic is assigned to the **system-uplink** profile.

Step 3 Confirm that the three VSM vnics are assigned to the port groups containing the control VLAN, packet VLAN, and management network.

Checking Network Connectivity Between the VSM and the VEM

You can use the following procedure to verify Layer 2 network connectivity between the VSM and VEM.

Step 1 On the VSM, find its MAC address.

show svs neighbors

The VSM MAC address displays as the AIPC Interface MAC.

The user VEM Agent MAC address of the host displays as the Src MAC.

Example:

```
n1000v# show svs neighbors

Active Domain ID: 1030
```

```
AIPC Interface MAC: 0050-568e-58b7
Inband Interface MAC: 0050-568e-2a39

Src MAC           Type   Domain-id    Node-id     Last learnt (Sec. ago)
--------------------------------------------------------------------------

0002-3d44-0602     VEM      1030         0302     261058.59
```

Step 2 Do one of the following:

- If the output of the **show svs neighbors** command in Step 1 does not display the VEM MAC address, then there is a problem with connectivity between the server hosting the VSM and the upstream switch. Recheck the VSM configuration and vCenter Server configuration.
- Otherwise, continue with the next step.

Step 3 On the VEM, run the vem-health script using the VSM MAC address you found in Step 1.

Note If the vem-health script is not in the PATH, you can find it under /usr/lib/ext/cisco/nexus/vem*/sbin/.

vem-health check *vsm_mac_address*

The vem-health script output shows the cause of the connectivity problem and recommends next steps in troubleshooting.

Example:

```
~ # vem-health check  00:50:56:a3:36:90
VSM Control MAC address: 00:50:56:a3:36:90
Control VLAN: 90
DPA MAC: 00:02:3d:40:5a:03

VSM heartbeats are not reaching the VEM.
Your uplink configuration is correct.
Recommended action:
Check if the VEM's upstream switch has learned the VSM's Control MAC.
```

Step 4 Do one of the following:

- If the VEM health check in Step 3 indicates a problem with connectivity to the upstream switch. continue with the next step.
- Otherwise, go to Step 7.

Step 5 On the upstream switch, display the MAC address table to verify the network configuration.

Example:

```
switch# show mac address-table interface Gi3/1 vlan 3002
Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

  vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
Active Supervisor:
* 3002  0050.56be.7ca7   dynamic  Yes          0   Gi3/1

switch# show mac address-table interface Gi3/2 vlan 3002
Legend: * - primary entry
        age - seconds since last seen
        n/a - not available
```

```
  vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
Active Supervisor:
* 3002  00:02:3d:40:0b:0c   dynamic  Yes          0   Gi3/2
```

Step 6 Do one of the following:

- If the output from Step 5 does not display the MAC address of the VSM, then there is a problem with connectivity between the server hosting the VSM and the upstream switch. Recheck the VSM configuration and vCenter Server configuration.
- Otherwise, continue with the next step.

Step 7 On the VEM, enter the following commands to verify that the VSM MAC appears in the control and packet VLANs.

config t

module vem *module_number* **execute vemcmd show l2** *control_vlan_id*

module vem *module_number* **execute vemcmd show l2** *packet_vlan_id*

The VSM eth0 and eth1 MAC addresses should display in the host control and packet VLANs.

Example:

```
n100v# config t
n1000v(config)# module vem 3 execute vemcmd show l2 3002
Bridge domain 3002 brtmax 100, brtcnt 3, timeout 120
    Dynamic MAC 00:50:56:be:7c:a7  LTL    16 pvlan     0 timeout   110
    Dynamic MAC 00:02:3d:40:0b:0c  LTL    10 pvlan     0 timeout   110

n1000v(config)# module vem 3 execute vemcmd show l2 3003
Bridge domain 3002 brtmax 100, brtcnt 3, timeout 120
    Dynamic MAC 00:50:56:be:7c:a7  LTL    16 pvlan     0 timeout   110
    Dynamic MAC 00:02:3d:20:0b:0c  LTL    10 pvlan     0 timeout   110
```

Step 8 Do one of the following:

- If the MAC address of the VSM does not appear in the output of Step 7, then check the VEM configuration as explained in "Checking the VEM Configuration" section on page 7-14.
- Otherwise, you have completed this procedure.

Recovering Management and Control Connectivity of a Host when a VSM is Running on a VEM

When the VSM is running on a VEM that it manages, but the VSM ports are not configured with system port profiles, the control and management connectivity of the VSM can be lost after a host reboot or similar event. To recover from the loss, you can run the VEM connect script locally in the ESX host where the VEM is running. Then go to the VSM and configure the system VLANs in the port profile used for management.

Using the VEM Connect Script

The VEM connect script sets a given VLAN as a system VLAN on the vmknic that has the given IP address, and also sets the VLAN on all the required uplinks.

If no uplink is carrying this VLAN, you also need to specify the uplink (vmnicN) on which this VLAN needs to be applied. The uplink can be a single port or a port-channel member. If it is the latter, then the script will apply the VLANs as a system VLAN to all member uplinks of that port channel.

vem-connect -i <*ip_address*> **-v** <*vlan*> **[-p <vmnicN>]**

The -p parameter to the script is optional. If you run the script without the -p parameter, it will try to locate an uplink that carries this VLAN. If no such uplink exists, it will report this as an error. You need to specify the -p parameter and re-run the script.

You can use the following procedure to recover management and control connectivity of a host when a VSM is running on a VEM.

SUMMARY

Step 1 Enter the following command to display the VEM ports:

vemcmd show port

Example:

```
~ # vemcmd show port
  LTL   VSM Port  Admin Link  State  PC-LTL  SGID  Vem Port  Type
   18     Eth9/2     UP   UP    F/B*     305     1    vmnic1
   20     Eth9/4     UP   UP    F/B*     305     3    vmnic3
   49      Veth1     UP   UP    FWD        0     3  VM-T-125.eth0
   50     Veth10     UP   UP    FWD        0     1      vmk1
  305        Po2     UP   UP    F/B*       0

* F/B: The port is blocked on some of the VLANs.
```

Note The output `*F/B The port is blocked on some of the VLANs` means that the trunk is not forwarding all vlans. This may be normal depending on the port profile allowed VLAN list. Compare the output of the `vemcmd show port vlans` against the list of allowed VLANs in the trunk port profile. If the lists match, then all of the expected VLANs are forwarding and the Cisco Nexus 1000V is blocking non-allowed VLANs.

Step 2 Enter the following command to display details about the system VLANS**:**

vemcmd show port vlans system

Example:

```
~ # vemcmd show port vlans system
                         Native  VLAN   Allowed
  LTL   VSM Port  Mode   VLAN/   State  Vlans/SegID
                         SegID
    6   Internal   A        1    FWD    1
    8   Internal   A     3969    FWD    3969
    9   Internal   A     3969    FWD    3969
   10   Internal   A      210    FWD    210
   11   Internal   A     3968    FWD    3968
   12   Internal   A      211    FWD    211
   13   Internal   A        1    BLK    1
   14   Internal   A     3971    FWD    3971
   15   Internal   A     3971    FWD    3971
   16   Internal   A        1    FWD    1
   18     Eth9/2   T        1    FWD    210-211
   20     Eth9/4   T        1    FWD    210-211
   49      Veth1   A        1    FWD    1
   50     Veth10   A        1    FWD    1
```

```
  305        Po2   T          1   FWD    210-211
```

Step 3 Enter the following command to recover connectivity:

vem-connect -i <*ip_address*> **-v** <*vlan*> **[-pnic <vmnicN>]**

Example:

```
~ # vem-connect -i 172.23.232.67 -v 232 -p vmnic3
ltl 50 and veth Veth10 vmk1
Uplink port Po2 carries vlan 232
Set System Vlan 232 port Po2 305
Uplink port Eth9/2 carries vlan 232
Set System Vlan 232 port Eth9/2 18
Uplink port Eth9/4 carries vlan 232
Set System Vlan 232 port Eth9/4 20
Set System 232 for vmk
```

Step 4 Enter the following command to confirm management connectivity:

vemcmd show port vlans system

Example:

```
~ # vemcmd show port vlans system
                          Native  VLAN   Allowed
  LTL   VSM Port  Mode    VLAN/   State  Vlans/SegID
                          SegID
    6   Internal   A          1   FWD    1
    8   Internal   A       3969   FWD    3969
    9   Internal   A       3969   FWD    3969
   10   Internal   A        210   FWD    210
   11   Internal   A       3968   FWD    3968
   12   Internal   A        211   FWD    211
   13   Internal   A          1   BLK    1
   14   Internal   A       3971   FWD    3971
   15   Internal   A       3971   FWD    3971
   16   Internal   A          1   FWD    1
   18     Eth9/2   T          1   FWD    210-211,232
   20     Eth9/4   T          1   FWD    210-211,232
   49      Veth1   A          1   FWD    1
   50     Veth10   A        232   FWD    232
  305        Po2   T          1   FWD    210-211,232
```

Checking the VEM Configuration

You can use the following procedure to verify that the ESX host received the VEM configuration and setup.

Step 1 On the ESX host, use the following command to confirm that the VEM Agent is running, and that the correct host uplinks are added to the DVS.

vem status

Example:

```
~ # vem status
VEM modules are loaded

Switch Name    Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0       64          3           64                1500    vmnic0
```

```
DVS Name        Num Ports   Used Ports  Configured Ports  Uplinks
n1000v          256         9           256               vmnic1 VEM Agent is running
```

Step 2 Use the following commands to restore connectivity that is lost due to an incorrect MTU value on an uplink:

vemcmd show port *port-LTL-number*

vemcmd set mtu *value* **ltl** *port-LTL-number*

Example:

```
~ # vemcmd show port 48
LTL    IfIndex   Vlan    Bndl  SG_ID Pinned_SGID  Type  Admin State  CBL Mode Name
. . .
17   1a030100      1 T   304      1          32  PHYS     UP    UP    1  Trunk vmnic1
~# vemcmd set mtu 9000 ltl 17
```

Note Use these **vemcmds** only as a recovery measure and then update the MTU value in the port profile configuration for system uplinks or in the interface configuration for non-system uplinks.

Step 3 Use the following command to verify that the domain ID, control VLANs, and packet VLANs are configured correctly on the host.

vemcmd show card

Example:

```
~ # vemcmd show card
Card UUID type  2: 58f8afd7-e1e3-3c51-85e2-6e6f2819a7b8
Card name: sfish-srvr-1
Switch name: n1000v
Switch alias: DvsPortset-0
Switch uuid: 56 e0 36 50 91 1c 32 7a-e9 9f 31 59 88 0c 7f 76
Card domain: 1024
Card slot: 4
VEM Control (Control VLAN) MAC: 00:02:3d:14:00:03
VEM Packet (Inband) MAC: 00:02:3d:24:00:03
VEM Control Agent (DPA) MAC: 00:02:3d:44:00:03
VEM SPAN MAC: 00:02:3d:34:00:03
Management IP address: 172.23.232.102
Max physical ports: 32
Max virtual ports: 216
Card control VLAN: 3002
Card packet VLAN: 3003
       Processors: 4
  Processor Cores: 4
Processor Sockets: 2
  Physical Memory: 4290351104
```

Step 4 Use the following command to verify that the ports of the host added to the DVS are listed, and that the ports are correctly configured as access or trunk on the host.

vemcmd show port

Example:

```
~ # vemcmd show port
LTL    IfIndex   Vlan    Bndl  SG_ID Pinned_SGID  Type  Admin State  CBL Mode   Name
8          0   3969       0      2           2  VIRT     UP    UP    1 Access 120
9          0   3969       0      2           2  VIRT     UP    UP    1 Access 121
10         0   3002       0      2           2  VIRT     UP    UP    1 Access 122
11         0   3968       0      2           2  VIRT     UP    UP    1 Access 123
12         0   3003       0      2           2  VIRT     UP    UP    1 Access 124
13         0      1       0      2           2  VIRT     UP    UP    0 Access 125
```

```
14          0   3967       0      2           2  VIRT     UP    UP    1 Access l26
16   1a030100      1 T     0      2           2  PHYS     UP    UP    1 Trunk vmnic1
```

The last line of output indicates that vmnic1 should be in Trunk mode, with the CBL value of 1. The CBL value of the native VLAN does not have to be 1. It will be 0 if it is not allowed, or 1 if it is VLAN 1 and not allowed. This is not an issue unless the native VLAN is the Control VLAN.The Admin state and Port state should be UP.

Step 5 Use the following commands to verify that the vmnic port that is supposed to carry the control VLAN and packet VLAN is present.

vemcmd show bd *control_vlan*
vemcmd show bd *packet_vlan*

Example:

```
~ # vemcmd show bd 3002
BD 3002, vdc 1, vlan 3002, 2 ports
Portlist:
     10  l22
     16  vmnic1
~ # vemcmd show bd 3003
BD 3003, vdc 1, vlan 3003, 2 ports
Portlist:
     12  l24
     16  vmnic1
```

Step 6 Use the **vemcmd show trunk** command to verify the following:

- The control and packet VLANs are shown in the command output, indicating that the DV port groups are successfully pushed from the vCenter Server to the host.
- The correct physical trunk port vmnic is used.

Example:

```
~ # vemcmd show trunk
Trunk port 16 native_vlan 1 CBL 1vlan(1) cbl 1, vlan(3002) cbl 1, vlan(3003) cbl 1,
```

At least one physical uplink must be carrying the control and packet VLANs. If more than one uplink is carrying the control and packet VLANs, the uplinks must be in a port channel profile. The port channel itself would not be visible because the VEM is not yet added to the VSM.

Step 7 Use the following commands to restore connectivity that is lost due to incorrect port and system VLAN settings:

vemcmd show port *port-ltl-number*

vemcmd set system-vlan *vlan_id* **ltl** *port-ltl-number*

Example:

```
~ # vemcmd show port 48
LTL    IfIndex   Vlan    Bndl  SG_ID Pinned_SGID  Type  Admin State  CBL Mode   Name
. . .
48     1b030000     1       0     32           1 VIRT     UP  DOWN     0 Access vmk1
~ # vemcmd set system-vlan 99 ltl 48
```

Note Use these **vemcmds** only as a recovery measure and then update the port profile configuration with correct system VLANs.

Collecting Logs

After you have verified network connectivity between the VEM and the VSM, you can use the following procedure to collect log files to help identify the problem.

Step 1 On the VEM, use the following command to verify its UUID.

vemcmd show card info

Example:

```
~ # module vem 3 vemcmd show card info
Card UUID type  0: 4908a717-7d86-d28b-7d69-001a64635d18
Card name: sfish-srvr-7
Switch name: N1000v
Switch uuid: 50 84 06 50 81 36 4c 22-9b 4e c5 3e 1f 67 e5 ff
Card domain: 11
Card slot: 12
Control VLAN MAC: 00:02:3d:10:0b:0c
Inband MAC: 00:02:3d:20:0b:0c
SPAN MAC: 00:02:3d:30:0b:0c
USER DPA MAC: 00:02:3d:40:0b:0c
Management IP address: 172.28.30.56
Max physical ports: 16
Max virtual ports: 32
Card control VLAN: 3002
Card packet VLAN: 3003
```

Step 2 On the VSM, use the following command to verify the module number to which the corresponding UUID entry is mapped.

show module vem mapping

Example:

```
n1000v# show module vem mapping
Mod     Status          UUID                                    License Status
---     -----------     ------------------------------------    --------------
60      absent          33393935-3234-5553-4538-35314e355400    unlicensed
66      powered-up      33393935-3234-5553-4538-35314e35545a    licensed
n1000v#
```

Step 3 Using the module number from Step 2, collect the output of the following commands:

- **show platform internal event-history module 13**
- **show module internal event-history module 13**
- **show system internal im event-history module 13**
- **show system internal vmm event-history module 13**
- **show system internal ethpm event-history module 13**

Note If you need to contact Cisco TAC for assistance in resolving an issue, you will need the output of the commands listed in Step 3.

VSM and VEM Troubleshooting Commands

You can use the commands in this section to troubleshoot problems related to VSM.

Command	Description
show svs neighbors	Displays all svs neighbors. See Example 7-1 on page 7-19.
show svs connections	Displays the Cisco Nexus 1000V connections. See Example 7-2 on page 7-20.
show svs domain	Displays the domain configuration. See Example 7-3 on page 7-20.
show port-profile name *name*	Displays the configuration for a named port profile. See Example 7-4 on page 7-20.
show running-config vlan *vlanID*	Displays the VLAN information in the running configuration. See Example 7-5 on page 7-20.
vem-health check *vsm_mac_address*	Displays the cause of a connectivity problem and recommends next steps in troubleshooting. See Example 7-6 on page 7-21.
show mac address-table interface	Displays the MAC address table on an upstream switch to verify the network configuration. See Example 7-7 on page 7-21.
module vem *module_number* **execute vemcmd show l2** [*control_vlan_id* | *packet_vlan_id*]	Displays the VLAN configuration on the VEM to verify that the VSM MAC appears in the control and packet VLANs. See Example 7-8 on page 7-21.
vem status	Displays the VEM status to confirm that the VEM Agent is running, and that the correct host uplinks are added to the DVS. See Example 7-9 on page 7-21.
vemcmd show card	Displays information about cards on the VEM to verify that the domain ID, control VLANs, and packet VLANs are configured correctly on the host. See Example 7-10 on page 7-21.
vemcmd show port [*port-LTL-number*]	Displays information about ports on the VEM to verify that the ports of the host added to the DVS are listed, and that the ports are correctly configured as access or trunk on the host. See Example 7-11 on page 7-22. See Example 7-12 on page 7-22.

Command	Description
vemcmd show bd [*control_vlan_id* | *packet_vlan_id*]	Displays configured information on the VEM to verify that the VM NIC port that is supposed to carry the control VLAN and packet VLAN is present. See Example 7-14 on page 7-23.
vemcmd show trunk	Displays configured information on the VEM to verify that the DV port groups are successfully pushed from the vCenter Server to the host and that the correct physical trunk port VM NIC is used. See Example 7-15 on page 7-23.
vem-connect -i <*ip_address*> **-v** <*vlan*> **[-pnic <vmnicN>]**	Recovers management and control connectivity of a host when a VSM is running on a VEM.
show module vem mapping	Displays information about the VEM a VSM maps to, including VEM module number, status, UUID, and license status See Example 7-16 on page 7-23.
show platform internal event-history module *module-number*	Displays platform FSM event information.
show module internal event-history module *module-number*	Displays the event log for a module.
show system internal im event-history module *module-number*	Displays the module IM event logs for the system.
show system internal vmm event-history module *module-number*	Displays the module VMM event logs for the system.
show system internal ethpm event-history module *module-number*	Displays the module Ethernet event logs for the system.
show system internal ethpm event-history int *type slot*	Displays the Ethernet interface logs for the system.

Example 7-1 show svs neighbors

```
n1000v# show svs neighbors

Active Domain ID: 113

AIPC Interface MAC: 0050-56b6-2bd3
Inband Interface MAC: 0050-56b6-4f2d

Src MAC           Type   Domain-id    Node-id     Last learnt (Sec. ago)
------------------------------------------------------------------------

0002-3d40-7102     VEM       113         0302     71441.12
0002-3d40-7103     VEM       113         0402       390.77

n1000v#
```

Example 7-2 show svs connections

```
n1000v# show svs connections
connection vc:
    ip address: 172.23.231.223
    protocol: vmware-vim https
    certificate: user-installed
    datacenter name: hamilton-dc
    DVS uuid: 92 7a 14 50 05 11 15 9c-1a b0 f2 d4 8a d7 6e 6c
    config status: Disabled
    operational status: Disconnected
```

Example 7-3 show svs domain

```
n1000v# show svs domain
SVS domain config:
  Domain id:    682
  Control vlan: 3002
  Packet vlan:  3003
  L2/L3 Control VLAN mode: L2
  L2/L3 Control VLAN interface: mgmt0
  Status: Config push to VC successful
```

Example 7-4 show port-profile

```
n1000v# show port-profile name SystemUplink
port-profile SystemUplink
  description:
  type: ethernet
  status: enabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: 114,115
  port-group: SystemUplink
  max ports: 32
  inherit:
  config attributes:
    switchport mode trunk
    switchport trunk allowed vlan all
    system mtu 1500
    no shutdown
  evaluated config attributes:
    switchport mode trunk
    switchport trunk allowed vlan all
    no shutdown
  assigned interfaces:
```

Example 7-5 show running-configuration vlan

```
n1000v# show running-config vlan 260-261
version 4.0(4)SV1(3)
vlan 260
  name cp_control
vlan 261
  name cp_packet

n1000v#
```

Example 7-6 vem-health check

```
~ # vem-health check  00:50:56:a3:36:90
VSM Control MAC address: 00:50:56:a3:36:90
Control VLAN: 90
DPA MAC: 00:02:3d:40:5a:03

VSM heartbeats are not reaching the VEM.
Your uplink configuration is correct.
Recommended action:
Check if the VEM's upstream switch has learned the VSM's Control MAC.
```

Example 7-7 show mac address-table interface

```
switch# show mac address-table interface Gi3/1 vlan 3002
Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

  vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
Active Supervisor:
* 3002  0050.56be.7ca7   dynamic  Yes          0   Gi3/1
```

Example 7-8 module vem execute vemcmd show l2

```
n1000v# config t
n1000v(config)# module vem 3 execute vemcmd show l2 3002
Bridge domain 3002 brtmax 100, brtcnt 3, timeout 120
    Dynamic MAC 00:50:56:be:7c:a7  LTL    16 pvlan     0 timeout   110
    Dynamic MAC 00:02:3d:40:0b:0c  LTL    10 pvlan     0 timeout   110

n1000v(config)# module vem 3 execute vemcmd show l2 3003
Bridge domain 3002 brtmax 100, brtcnt 3, timeout 120
    Dynamic MAC 00:50:56:be:7c:a7  LTL    16 pvlan     0 timeout   110
    Dynamic MAC 00:02:3d:20:0b:0c  LTL    10 pvlan     0 timeout   110
```

Example 7-9 vem status

```
~ # vem status
VEM modules are loaded

Switch Name    Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0       64          3           64                1500    vmnic0
DVS Name       Num Ports   Used Ports  Configured Ports  Uplinks
n1000v         256         9           256               vmnic1 VEM Agent is running
```

Example 7-10 vemcmd show card

```
~ # vemcmd show card
Card UUID type  2: 58f8afd7-e1e3-3c51-85e2-6e6f2819a7b8
Card name: sfish-srvr-1
Switch name: n1000v
Switch alias: DvsPortset-0
Switch uuid: 56 e0 36 50 91 1c 32 7a-e9 9f 31 59 88 0c 7f 76
Card domain: 1024
Card slot: 4
VEM Control (Control VLAN) MAC: 00:02:3d:14:00:03
VEM Packet (Inband) MAC: 00:02:3d:24:00:03
VEM Control Agent (DPA) MAC: 00:02:3d:44:00:03
VEM SPAN MAC: 00:02:3d:34:00:03
```

```
Management IP address: 172.23.232.102
Max physical ports: 32
Max virtual ports: 216
Card control VLAN: 3002
Card packet VLAN: 3003
       Processors: 4
  Processor Cores: 4
Processor Sockets: 2
  Physical Memory: 4290351104
```

Example 7-11 vemcmd show port

```
~ # vemcmd show port
LTL    IfIndex   Vlan    Bndl  SG_ID Pinned_SGID  Type  Admin State  CBL Mode   Name
8          0   3969       0      2           2  VIRT     UP    UP    1 Access l20
9          0   3969       0      2           2  VIRT     UP    UP    1 Access l21
10         0   3002       0      2           2  VIRT     UP    UP    1 Access l22
11         0   3968       0      2           2  VIRT     UP    UP    1 Access l23
12         0   3003       0      2           2  VIRT     UP    UP    1 Access l24
13         0      1       0      2           2  VIRT     UP    UP    0 Access l25
14         0   3967       0      2           2  VIRT     UP    UP    1 Access l26
16  1a030100      1 T     0      2           2  PHYS     UP    UP    1 Trunk vmnic1
```

Example 7-12 vemcmd show port

```
~ # vemcmd show port 48
LTL    IfIndex   Vlan    Bndl  SG_ID Pinned_SGID  Type  Admin State  CBL Mode
Name  . . .
17   1a030100      1 T   304      1          32  PHYS     UP    UP    1  Trunk vmnic1
```

Example 7-13 vemcmd show port

```
~ # module vem 5 e vemcmd show port
  LTL   VSM Port  Admin Link  State  PC-LTL  SGID  Vem Port
   17     Eth5/1     UP   UP    FWD     305     0  vmnic0
   18     Eth5/2     UP   UP    FWD     305     1  vmnic1
   49     Veth11     UP   UP    FWD       0     0  vmk0
   50     Veth14     UP   UP    FWD       0     1  vmk1
   51     Veth15     UP   UP    FWD       0     0  vswif0
  305        Po1     UP   UP    FWD       0

* F/B: Port is BLOCKED on some of the vlans.
 Please run "vemcmd show port vlans" to see the details.

~ # module vem 5 e vemcmd show port vlans
                       Native  VLAN   Allowed
  LTL   VSM Port  Mode  VLAN    State  Vlans
   17     Eth5/1   T        1   FWD    1,100,119,219,319
   18     Eth5/2   T        1   FWD    1,100,119,219,319
   49     Veth11   A      119   FWD    119
   50     Veth14   A      119   FWD    119
   51     Veth15   A      119   FWD    119
  305        Po1   T        1   FWD    1,100,119,219,319
```

Note The output `*F/B The port is blocked on some of the VLANs` means that the trunk is not forwarding all vlans. This may be normal depending on the port profile allowed VLAN list. Compare the output of the `vemcmd show port vlans` against the port profile trunk allowed VLANs. If the lists match, then all of the expected VLANs are forwarding and the Cisco Nexus 1000V is blocking non-allowed VLANs.

Example 7-14 vemcmd show bd

```
~ # vemcmd show bd 3002
BD 3002, vdc 1, vlan 3002, 2 ports
Portlist:
     10  l22
     16  vmnic1
```

Example 7-15 vemcmd show trunk

```
~ # vemcmd show trunk
Trunk port 16 native_vlan 1 CBL 1vlan(1) cbl 1, vlan(3002) cbl 1, vlan(3003) cbl 1,
```

Example 7-16 show module vem mapping

```
n1000v# show module vem mapping
Mod     Status          UUID                                    License Status
---     -----------     ------------------------------------    --------------
60      absent          33393935-3234-5553-4538-35314e355400    unlicensed
66      powered-up      33393935-3234-5553-4538-35314e35545a    licensed
n1000v#
```