Ports

This chapter describes how to identify and resolve problems related to ports. This chapter contains the following sections:

Information about Ports

Information About Interface Characteristics

Before a switch can relay frames from one data link to another, you must define the characteristics of the interfaces through which the frames are received and sent. The configured interfaces can be Ethernet (physical) interfaces, virtual Ethernet interfaces, and the management interface.

Each interface has the following:

- Administrative Configuration—The administrative configuration does not change unless you modify it. This configuration has attributes that you can configure in administrative mode.
- Operational State—The operational state of a specified attribute, such as the interface speed. This state cannot be changed and is read-only. Some values might not be valid when the interface is down (such as the operation speed).

For detailed information about port modes, administrative states, and operational states, see the *Cisco Nexus 1000V Interface Configuration Guide*.

Information About Interface Counters

Port counters are used to identify synchronization problems. Counters can show a significant disparity between received and transmitted frames. To display interface counters, use the **show interface ethernet counters** command shown in show interface ethernet counters, on page 11.

Values stored in counters can be meaningless for a port that has been active for an extended period. Clearing the counters provides a better idea of the actual link behavior at the present time. Create a baseline first by clearing the counters using the **clear counters interface ethernet** command.

Information About Link Flapping

When a port continually goes up and down, it is said to be flapping, or link flapping. When a port is flapping, it cycles through the following states in this order and then starts over again:

1. Initializing—The link is initializing.
2. Offline—The port is offline.
3. Link failure or not connected—The physical layer is not operational and there is no active device connection.

To troubleshoot link flapping, see Link Flapping, on page 4.

Information About Port Security

The port security feature allows you to secure a port by limiting and identifying the MAC addresses that can access the port. Secure MAC addresses can be manually configured or dynamically learned.

For detailed information about port security, see the *Cisco Nexus 1000V Security Configuration Guide*.

Type of Port	Is Port Security Supported?
vEthernet access	Yes
vEthernet trunk	Yes
vEthernet SPAN destination	No
Standalone Ethernet interfaces	No
Port channel members	No

To troubleshoot problems related to port security, see the following:

- VM Cannot Ping a Secured Port, on page 6
- Port Security Violations, on page 7

Port Diagnostic Checklist

Use the following checklist to diagnose port interface activity.

For more information about port states, see the *Cisco Nexus 1000V Interface Configuration Guide*.

Table 1: Port Diagnostic Checklist

Checklist	Example
Verify that the module is active. **show module**	See show module, on page 9.

Checklist	Example
Verify that the VSM is connected to vCenter Server. **show svs connections**	See show svs, on page 10.
On vSphere Client connected to vCenter Server, verify that the required port profiles are assigned to the physical NICs and the virtual NICs.	—
Verify that the ports have been created. **show interface brief**	See show interface brief, on page 11.
Verify the state of the interface. **show interface ethernet**	See show interface ethernet, on page 11.

Problems with Ports

An Interface Cannot be Enabled

Possible Cause	Solution
A layer 2 port is not associated with an access VLAN or the VLAN is suspended.	1. Verify that the interface is configured in a VLAN by using the **show interface brief** command. 2. If not already, associate the interface with an access VLAN. 3. Determine the VLAN status by using the **show vlan brief** command. 4. If not already active, configure the VLAN as active by using the following commands: 1. **config t** 2. **vlan** *vlan-id* 3. **state active**

Port Link Failure or Port Not Connected

Possible Cause	Solution
The port connection is bad.	1. Verify the port state by using the **show system internal ethpm info** command. 2. Disable and then enable the port. 1. **shut** 2. **no shut** 3. Move the connection to a different port on the same module or a different module. 4. Collect the ESX-side NIC configuration by using the **vss-support** command.
The link is stuck in initialization state or the link is in a point-to-point state.	1. Check for the link failure system message `Link Failure, Not Connected` by using the **show logging** command. 2. Disable and then enable the port. 1. **shut** 2. **no shut** 3. Move the connection to a different port on the same module or a different module. 4. Collect the ESX-side NIC configuration by using the **vss-support** command.

Link Flapping

When you are troubleshooting unexpected link flapping, it is important to have the following information:

- Who initiated the link flap?
- The actual reason for the link being down.

For information about link flapping, see Information About Link Flapping, on page 2.

Possible Cause	Solution
The bit rate exceeds the threshold and puts the port into an error-disabled state.	Disable and then enable the port. 1. **shut** 2. **no shut** The port should return to the normal state.

Possible Cause	Solution
One of the following: • A hardware failure or intermittent hardware error causes a packet drop in the switch. • A software error causes a packet drop. • A control frame is erroneously sent to the device.	An external device might choose to initialize the link again when encountering the error. If so, the exact method of link initialization varies by device. 1. Determine the reason for the link flap as indicated by the MAC driver. 2. Use the debug facilities on the end device to troubleshoot the problem.
ESX errors or link flapping occurs on the upstream switch.	Use the troubleshooting guidelines in the documentation for your ESX or upstream switch.

Port ErrDisabled

Possible Cause	Solution
The cable is defective or damaged.	1. Verify the physical cabling. 2. Replace or repair defective cables. 3. Re-enable the port. 1. **shut** 2. **no shut**
You attempted to add a port to a port channel that was not configured identically and the port is then errdisabled.	1. Display the switch log file and identify the exact configuration error in the list of port state changes by using the **show logging logfile** command. 2. Correct the error in the configuration and add the port to the port channel. 3. Re-enable the port. 1. **shut** 2. **no shut**
A VSM application error has occurred.	1. Identify the component that had an error while you were bringing up the port by using the **show logging logfile | grep** *interface_number* command. See show logging logfile, on page 10. 2. Identify the error transition by using the **show system internal ethpm event-history interface** *interface_number* command. 3. Open a support case and submit the output of the above commands. For more information, see Cisco Support Information.

VM Cannot Ping a Secured Port

Possible Cause	Solution
The vEthernet interface is not up.	1. Verify the state of the vEthernet interface. **show interface vethernet** *number* 2. If the interface is down, enable it. 1. **shut** 2. **no shut**
One of the following: • Drop on Source Miss (DSM) is set. • New MAC addresses cannot be learned by this port.	1. Verify the port security configuration. **module vem 3 execute vemcmd show portsec stats** 2. If DSM is set, clear the DSM bit on the VSM. **no port-security stop learning**
The packet VLAN is not allowed on the port.	1. Identify the packet VLAN ID. **show svs domain** 2. Verify that the packet VLAN is allowed on VEM uplink ports. **show port-profile na uplink-all** 3. If the packet VLAN is not allowed on the uplink port profile, add it to the allowed VLAN list.
The packet VLAN is not allowed on the upstream switch port.	1. Identify the upstream neighbors connected to the interface. **show cdp neighbors** 2. Log in to the upstream switch and verify that the packet VLAN is allowed on the port. **show running-config interface gigabitEthernet** *slot/port* 3. If the packet VLAN is not allowed on the port, add it to the allowed VLAN list.

Port Security Violations

Possible Cause	Solution
The configured maximum number of secured addresses on the port is exceeded.	1. Display the secure addresses. **show port-security address vethernet** *number* **show port-security address interface vethernet** *number* 2. Identify ports with security violation. **show logging |** **inc "PORT-SECURITY-2-** **ETH_PORT_SEC_SECURITY** **_VIOLATION_MAX_MAC_VLAN"** 3. Correct the security violation. 4. Enable the interface. 1. **shut** 2. **no shut**

For detailed information about port security, see the *Cisco Nexus 1000V for VMware vSphere Security Configuration Guide*.

Port State is Blocked on a VEM

Possible Cause	Solution
The VLAN is not created on the VSM.	1. Verify the status of the vEthernet interface by using the **show interface vethernet number** command. It should be up and not inactive. 2. Verify that the VLAN on the VSM is created by using the **show vlan** *vlan-id* command. 3. On the VEM module, do the following: 1. Verify that the VLAN is programmed by using the **vemcmd show vlan** *vlan-id* command. 2. Verify that the VLAN is allowed on the ports by using the **vemcmd show port vlan** command. 3. Create the VLAN on the VSM by using the **vlan** *vlan-id* command.

Possible Cause	Solution
The VEM modules are unlicensed.	1. Verify that all modules are in licensed state by using the **show module** command. 2. Verify the status of the vEthernet interface by using the **show interface vethernet number** command. It should be up and not `VEM Unlicensed`. 3. Verify the license status of VEM modules by using the **show module vem license-info** command. 4. On the VEM module, do the following: 1. Verify that the card details show `Licensed: Yes` by using the **vemcmd show card** command. 2. Install the necessary licenses or move the switch to essential mode by using the **svs switch edition essential** command.

Port Troubleshooting Commands

Command	Purpose	Examples
show module *module-number*	Displays the state of a module.	show module, on page 9
show svs domain	Displays the domain configuration.	show svs, on page 10
show svs connections	Displays the Cisco Nexus 1000V connections.	show svs, on page 10
show cdp neighbors	Displays the neighbors connected to an interface.	show cdp neighbors, on page 10
show port internal event-history interface	Displays information about the internal state transitions of the port.	show port internal event-history interface, on page 10
show logging logfile	Displays logged system messages.	show logging logfile, on page 10
show logging logfile | grep *interface_number*	Displays logged system messages for a specified interface.	show logging logfile, on page 10
show interface brief	Displays a table of interface states.	show interface brief, on page 11

Command	Purpose	Examples
show interface ethernet	Displays the configuration for a named Ethernet interface, including the following: • Administrative state • Speed • Trunk VLAN status • Number of frames sent and received • Transmission errors, including discards, errors, CRCs, and invalid frames	show interface ethernet, on page 11
show interface ethernet counters	Displays port counters for identifying synchronization problems.	show interface ethernet counters, on page 11
show interface vethernet	Displays the vEthernet interface configuration.	show interface vEthernet, on page 12
show interface status	Displays the status of the named interface.	—
show interface capabilities	Displays a tabular view of all configured port profiles.	show interface capabilities, on page 12
show interface virtual port-mapping	Displays the virtual port mapping for all vEthernet interfaces.	show interface virtual port-mapping, on page 14
module vem execute vemcmd show portsec status	Displays the port security status of the port. If enabled, the output shows an LTL connected to the VM network adapter.	module vem execute vemcmd show portsec status, on page 14
show port-security interface veth	Displays secure vEthernet interfaces.	show port-security, on page 14
show port-security address interface vethernet	Displays information about secure addresses on an interface.	show port-security, on page 14

Command Examples

show module

```
switch# show mod 3
Mod Ports Module-Type Model Status
--- ----- -------------------------------- ------------------ ------------
3 248 Virtual Ethernet Module ok
Mod Sw Hw
--- -------------- ------
3 NA 0.0
Mod MAC-Address(es) Serial-Num
--- -------------------------------------- ----------
3 02-00-0c-00-03-00 to 02-00-0c-00-03-80 NA
Mod Server-IP Server-UUID Server-Name
```

```
--- --------------- ------------------------------------ --------------------
3 192.168.48.20 496e48fa-ee6c-d952-af5b-001517136344 frodo
```

show svs

```
switch# show svs domains
SVS domain config:
Domain id: 559
Control vlan: 3002
Packet vlan: 3003
L2/L3 Aipc mode: L2
L2/L3 Aipc interface: management interface0
Status: Config push to VC successful.
switch#
```

```
switch# show svs connections
connection VC:
ip address: 192.168.0.1
protocol: vmware-vim https
certificate: default
datacenter name: Hamilton-DC
DVS uuid: ac 36 07 50 42 88 e9 ab-03 fe 4f dd d1 30 cc 5c
dvs version: 5.0
config status: Enabled
operational status: Connected
switch#
```

show cdp neighbors

```
switch# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute
Device ID Local Intrfce Hldtme Capability Platform Port ID
swordfish-6k-2 Eth3/2 149 R S I WS-C6506-E Gig1/38
switch#
```

show port internal event-history interface

```
switch# show port internal event-history interface e1/7
>>>>FSM: <e1/7> has 86 logged transitions<<<<<
1) FSM:<e1/7> Transition at 647054 usecs after Tue Jan 1 22:44..
Previous state: [PI_FSM_ST_IF_NOT_INIT]
Triggered event: [PI_FSM_EV_MODULE_INIT_DONE]
Next state: [PI_FSM_ST_IF_INIT_EVAL]
2) FSM:<e1/7> Transition at 647114 usecs after Tue Jan 1 22:43..
Previous state: [PI_FSM_ST_IF_INIT_EVAL]
Triggered event: [PI_FSM_EV_IE_ERR_DISABLED_CAP_MISMATCH]
Next state: [PI_FSM_ST_IF_DOWN_STATE]
```

show logging logfile

```
switch# show logging logfile
. . .
Jan 4 06:54:04 switch %PORT_CHANNEL-5-CREATED: port-channel 7 created
Jan 4 06:54:24 switch %PORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-channel 7
is down (No operational members)
Jan 4 06:54:40 switch %PORT_CHANNEL-5-PORT_ADDED: e1/8 added to port-channel 7
Jan 4 06:54:56 switch %PORT-5-IF_DOWN_ADMIN_DOWN: Interface e1/7 is down (Admnistratively
down)
Jan 4 06:54:59 switch %PORT_CHANNEL-3-COMPAT_CHECK_FAILURE: speed is not compatible
```

```
Jan 4 06:55:56 switch%PORT_CHANNEL-5-PORT_ADDED: e1/7 added to port-channel 7
switch#
```

```
switch# show logging logfile | grep Vethernet3626
2011 Mar 25 10:56:03 n1k-bl %VIM-5-IF_ATTACHED: Interface Vethernet3626
is attached to Network Adapter 8 of gentoo-pxe-520 on port 193 of module
13 with dvport id 6899
2011 Mar 25 11:10:06 n1k-bl %ETHPORT-2-IF_SEQ_ERROR: Error ("Client data
inconsistency") while communicating with component MTS_SAP_ACLMGR for
opcode MTS_OPC_ETHPM_PORT_PRE_CFG (RID_PORT: Vethernet3626)
2011 Mar 25 11:10:06 n1k-bl %ETHPORT-2-IF_DOWN_ERROR_DISABLED: Interface
Vethernet3626 is down (Error disabled. Reason:Client data inconsistency)
```

show interface brief

```
switch# show int brief
--------------------------------------------------------------------------------
Port VRF Status IP Address Speed MTU
--------------------------------------------------------------------------------
management interface0 -- up 172.23.232.141 1000 1500
--------------------------------------------------------------------------------
Ethernet VLAN Type Mode Status Reason Speed Port
Interface Ch #
--------------------------------------------------------------------------------
Eth3/2 1 eth trunk up none 1000(D) --
Eth3/3 1 eth access up none 1000(D) --
switch#
```

show interface ethernet

```
switch# show interface e1/14
e1/7 is down (errDisabled)
```

```
switch# show interface eth3/2
Ethernet3/2 is up
Hardware: Ethernet, address: 0050.5653.6345 (bia 0050.5653.6345)
MTU 1500 bytes, BW -598629368 Kbit, DLY 10 usec,
reliability 0/255, txload 0/255, rxload 0/255
Encapsulation ARPA
Port mode is trunk
full-duplex, 1000 Mb/s
Beacon is turned off
Auto-Negotiation is turned off
Input flow-control is off, output flow-control is off
Auto-mdix is turned on
Switchport monitor is off
Rx
  18775 Input Packets 10910 Unicast Packets
  862 Multicast Packets 7003 Broadcast Packets
  2165184 Bytes
Tx
  6411 Output Packets 6188 Unicast Packets
  216 Multicast Packets 7 Broadcast Packets 58 Flood Packets
  1081277 Bytes
  1000 Input Packet Drops 0 Output Packet Drops
1 interface resets
switch#
```

show interface ethernet counters

```
switch# show interface eth3/2 counters
--------------------------------------------------------------------------------
Port InOctets InUcastPkts InMcastPkts InBcastPkts
```

```
--------------------------------------------------------------------------------
Eth3/2 2224326 11226 885 7191
--------------------------------------------------------------------------------
Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts
--------------------------------------------------------------------------------
Eth3/2 1112171 6368 220 7
```

show interface vEthernet

```
switch# show interface veth1
Vethernet1 is up
Port description is gentoo1, Network Adapter 1
Hardware is Virtual, address is 0050.56bd.42f6
Owner is VM "gentoo1", adapter is Network Adapter 1
Active on module 33
VMware DVS port 100
Port-Profile is vlan48
Port mode is access
Rx
491242 Input Packets 491180 Unicast Packets
7 Multicast Packets 55 Broadcast Packets
29488527 Bytes
Tx
504958 Output Packets 491181 Unicast Packets
1 Multicast Packets 13776 Broadcast Packets 941 Flood Packets
714925076 Bytes
11 Input Packet Drops 0 Output Packet Drops
switch#
```

show interface capabilities

```
switch# show interface capabilities
management interface0
Model: --
Type: --
Speed: 10,100,1000,auto
Duplex: half/full/auto
Trunk encap. type: 802.1Q
Channel: no
Broadcast suppression: none
Flowcontrol: rx-(none),tx-(none)
Rate mode: none
QOS scheduling: rx-(none),tx-(none)
CoS rewrite: yes
ToS rewrite: yes
SPAN: yes
UDLD: yes
Link Debounce: no
Link Debounce Time: no
MDIX: no
Port Group Members: none
port-channel1
Model: unavailable
Type: unknown
Speed: 10,100,1000,10000,auto
Duplex: half/full/auto
Trunk encap. type: 802.1Q
Channel: yes
Broadcast suppression: percentage(0-100)
Flowcontrol: rx-(off/on/desired),tx-(off/on/desired)
Rate mode: none
QOS scheduling: rx-(none),tx-(none)
CoS rewrite: yes
```

```
ToS rewrite: yes
SPAN: yes
UDLD: no
Link Debounce: no
Link Debounce Time: no
MDIX: no
Port Group Members: none
port-channel2
Model: unavailable
Type: unknown
Speed: 10,100,1000,10000,auto
Duplex: half/full/auto
Trunk encap. type: 802.1Q
Channel: yes
Broadcast suppression: percentage(0-100)
Flowcontrol: rx-(off/on/desired),tx-(off/on/desired)
Rate mode: none
QOS scheduling: rx-(none),tx-(none)
CoS rewrite: yes
ToS rewrite: yes
SPAN: yes
UDLD: no
Link Debounce: no
Link Debounce Time: no
MDIX: no
Port Group Members: none
port-channel12
Model: unavailable
Type: unknown
Speed: 10,100,1000,10000,auto
Duplex: half/full/auto
Trunk encap. type: 802.1Q
Channel: yes
Broadcast suppression: percentage(0-100)
Flowcontrol: rx-(off/on/desired),tx-(off/on/desired)
Rate mode: none
QOS scheduling: rx-(none),tx-(none)
CoS rewrite: yes
ToS rewrite: yes
SPAN: yes
UDLD: no
Link Debounce: no
Link Debounce Time: no
MDIX: no
Port Group Members: none
control0
Model: --
Type: --
Speed: 10,100,1000,auto
Duplex: half/full/auto
Trunk encap. type: 802.1Q
Channel: no
Broadcast suppression: none
Flowcontrol: rx-(none),tx-(none)
Rate mode: none
QOS scheduling: rx-(none),tx-(none)
CoS rewrite: yes
ToS rewrite: yes
SPAN: yes
UDLD: yes
Link Debounce: no
Link Debounce Time: no
MDIX: no
```

```
Port Group Members: none
switch#
```

show interface virtual port-mapping

```
switch# show interface virtual port-mapping
------------------------------------------------------------------------------
Port Hypervisor Port Binding Type Status Reason
------------------------------------------------------------------------------
Veth1 DVPort5747 static up none
Veth2 DVPort3361 static up none
switch#
```

show port-security

```
switch# show port-security
Total Secured Mac Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8192
------------------------------------------------------------------------------
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
(Count) (Count) (Count)
------------------------------------------------------------------------------
Vethernet1 1 0 0 Shutdown
==============================================================================


switch# show port-security address interface vethernet 11
Secure Mac Address Table
------------------------------------------------------------------------
Vlan/Vxlan Mac Address Type Ports Configured Age
(mins)
---------- ----------- ------ ----- ---------------
50 0050.56a4.38ec STATIC Vethernet11 0
50 0000.0000.0011 DYNAMIC Vethernet11
```

module vem execute vemcmd show portsec status

```
cyp1-switch# module vem 3 execute vemcmd show portsec status
LTL if_index Max Aging Aging DSM Sticky VM
Secure Time Type Bit Enabled Name
Addresses
56 1c0000a0 5 0 Absolute Clr No Ostinato-Upgrade-VM1.eth1
```