CHAPTER 7

Ports and Port Profiles

This chapter describes how to identify and resolve problems with ports and includes the following topics:

Overview

Before a switch can relay frames from one data link to another, the characteristics of the interfaces through which the frames are received and sent must be defined. The configured interfaces can be Ethernet (physical) interfaces, virtual Ethernet interfaces, and the management interface (mgmt0),.

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 may not be valid when the interface is down (such as the operation speed).

For a complete description of port modes, administrative states, and operational states, see the *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)*.

Guidelines for Configuring a Port Interface

Use the following guidelines when configuring a port interface.

- Using the procedure, Verifying the Module State, page 7-2, make sure that the module is active.

Verifying the Module State

Use this procedure to verify the state of a module.

BEFORE YOU BEGIN

- The output of this command should indicate that the module is OK (active)

DETAILED STEPS

Step 1 From EXEC mode, enter the following command:

show module *module-number*

Example:

```
n1000v# 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
```

Diagnostic Checklist

Use the following checklist to begin diagnosing port interface activity.

Checklist	√
Verify that the VSM is connected to the vCenter Server by using the **show svs connections** command.	
Verify that appropriate port profiles are assigned to the physical NICS and the virtual NICS by verifying the same on the vSphere Client connected to vCenter Server.	

Checklist (continued)	√
Verify that the ports have been created using the **show interface brief** command.	
Using the procedure, Viewing the Port State, page 7-3, verify the state of the interface. For more information about port states, see the *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)*.	

Use the following commands to troubleshoot ports:

- **show interface status**
- **show interfaces capabilities**
- **show system internal ethpm errors**
- **show system internal ethpm event-history**
- **show system internal ethpm info**
- **show system internal ethpm mem-stats**
- **show system internal ethpm msgs**
- **show system internal vim errors**
- **show system internal vim event-history**
- **show system internal vim info**
- **show system internal vim mem-stats**
- **show system internal vim msgs**

Viewing the Port State

Use this procedure to view the port state.

BEFORE YOU BEGIN

- The output of this command includes the following:
  - Administrative state
  - Speed
  - Trunk VLAN status
  - Number of frames sent and received
  - Transmission errors, including discards, errors, CRCs, and invalid frames

DETAILED STEPS

Step 1 From EXEC mode, enter the following command:

show interface ethernet *slot-number*

Example:

```
n1000v# show int 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
n1000v#
```

Using Port Counters

Counters can identify synchronization problems by showing a significant disparity between received and transmitted frames.

BEFORE YOU BEGIN

- Create a baseline first by clearing the counters.

  The values stored in the 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 this time.

DETAILED STEPS

Step 1 From EXEC mode, enter the following command to zero out the counters for the interface:

clear counters interface ethernet *slot-number*

Example:

```
n1000v# clear counters interface eth 2/45
n1000v#
```

Step 2 Enter the following command to view the port counters:

show interface ethernet *slot number* **counters**

Example:

```
n1000v# 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
```

Port Interface Symptoms and Solutions

This section includes possible causes and solutions for the following symptoms:

Cannot Enable an Interface

Symptom	Possible Cause	Solution
Cannot enable an interface.	Layer 2 port is not associated with an access VLAN or the VLAN is suspended.	Use the **show interface brief** CLI command to see if the interface is configured in a VLAN. Use the **show vlan brief** CLI command to determine the status of the VLAN. Use the **state active** CLI command in VLAN configuration mode to configure the VLAN as active.

Port Remains in a Link Failure or Not Connected State

Symptom	Possible Cause	Solution
Port remains in a link-failure state.	Port connection is bad.	Use the **show system internal ethpm info** CLI command to verify the port status is in link-failure. Use the **shut** command followed by the **no shut** command to disable and enable the port. If this does not clear the problem, try moving the connection to a different port on the same or another module.
	Link is stuck in initialization state or the link is in a point-to-point state.	Use the **show logging** CLI command to check for a `Link Failure, Not Connected` system message. Use the **shut CLI** command followed by the **no shut** command to disable and enable the port. If this does not clear the problem, try moving the connection to a different port on the same or another module.
	—	If these steps are inconclusive on the VSM, use the **vss-support** command to collect the ESX side NIC configuration.

Link Flapping

This section includes the following topics:

About the Link Flapping Cycle

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.

Troubleshooting Prerequisites

When troubleshooting unexpected link flapping, it is important to know the following information:

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

Symptoms, Causes, and Solutions

Symptom	Possible Cause	Solution
Unexpected link flapping occurs.	The bit rate exceeds the threshold and puts the port into an error disabled state.	Right-click the port in Device Manager and select **disable** and then **enable**, or use the **shut CLI** command followed by the **no shut** command to return the port to the normal state.
	Some problem in the switch triggers the link flap action by the end device. Some of the causes are: • Packet drop in the switch, because of either a hardware failure or an intermittent hardware error. • Packet drop resulting from a software error. • A control frame is erroneously sent to the device.	Determine link flap reason as indicated by the MAC driver. Use the debug facilities on the end device to troubleshoot the problem. An external device may choose to initialize the link again when encountering the error. If so, the exact method of link initialization varies by device.
	The link flapping can be caused by ESX errors, or link flapping on the upstream switch.	

Port State Is ErrDisabled

This section includes the following topics:

About the ErrDisabled Port State

The ErrDisabled state indicates that the switch detected a problem with the port and disabled the port. This state could be caused by a flapping port or a high amount of bad frames (CRC errors), potentially indicating something wrong with the media.

Verifying the ErrDisable State

To resolve the ErrDisable state using the CLI, follow these steps:

Step 1 Use the **show interface** command to verify that the switch detected a problem and disabled the port. Check cables.

```
n1000v# show interface e1/14
e1/7 is down (errDisabled)
```

Step 2 Use the **show port internal event-history interface** command to view information about the internal state transitions of the port. In this example, porte1/7 entered the ErrDisabled state because of a capability mismatch, or “CAP MISMATCH.” You might not know how to interpret this event, but you can look for more information with other commands.

```
n1000v# 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]
```

Step 3 Use the **show logging logfile** command to display the switch log file and view a list of port state changes. In this example, an error was recorded when someone attempted to add port e1/7 to port channel 7. The port was not configured identically to port channel 7, so the attempt failed.

```
n1000v# 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
```

MTU Configuration Failure on ESX

An MTU configuration fails if you attempt to configure a value that is not supported by the physical NIC on the ESX host and VEM. A system message similar to the following is generated as a warning:

```
2010 Nov 15 04:35:27 my-n1k %VEM_MGR-SLOT3-1-VEM_SYSLOG_ALERT: vssnet :
sf_platform_set_mtu: Failed setting MTU for VMW port wiht portID 33554475.
```

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 MACs can be manually configured or dynamically learned.

There are two type of security violations:

- Addr-Count-Exceed Violation
- MAC Move Violation

The following port types support port security:

- VEthernet access ports
- VEthernet trunk ports

VEthernet SPAN destination ports do not support port security. In addition, port security is not supported on standalone Ethernet interfaces or on members of a Port Channel.

Troubleshooting Port Security Problems

This section describes how to troubleshoot the following connectivity issues when you have port security enabled on an interface:

- Cannot Ping from a VM with Port Security Enabled
- Port Enabled with Port Security is Error Disabled

Cannot Ping from a VM with Port Security Enabled

If you cannot send a ping from a VM with port security enabled, follow these steps:

Step 1 Enter the **module vem 3 execute vemcmd show portsec stats** command to view the actual port security configuration applied on the port.

Syntax: **module vem** *vem number* **execute vemcmd show portsec stats**

```
n1000V#module vem 3 execute vemcmd show portsec stats
  LTL   if_index  cp-cnt  Max         Aging   Aging     DSM  Sticky   VM
                          Secure      Time    Type      Bit  Enabled  Name
                          Addresses
   47   1b020000       0          1       0   Absolute  Clr       No  VM-Pri.eth1
```

The output shows that port security is enabled on the interface with LTL 47 connected to the Network Adapter 1 of the VM-Pri Virtual Machine

In addition, it shows other port security configuration attributes: Maximum No of Secured Addresses is 1, Aging Type is Absolute, Aging Time is 0 seconds (which means aging is disabled), and Sticky MAC is disabled.

Caution If Drop on Source Miss (DSM) is set, it means that no new MAC addresses can be learned by this port.

To clear the DSM bit, enter the **no port-security stop learning** command on the VSM:

```
n1000V# no port-security stop learning
```

If the DSM bit is not set, proceed to step 2.

Step 2 Log in to the ESX Host containing the VM and enter the **module vem 3 execute vemcmd show portsec macs all** command to view all secure MACs on that VEM.

```
~ #module vem 3 execute vemcmd show portsec macs all
VLAN 65's Secure MAC list:
     cp MAC 08:66:5c:99:72:f2  LTL    48  timeout       960
```

cp means currently being processed, which means that the packet is not yet acknowledged by the port security process running on the VSM.

This verification notification is sent over the inband channel.

Because the verification notification is sent through the inband channel, the inband VLAN must be on one of the uplink ports on the VEM as well as the corresponding ports on the upstream switch.

Step 3 Use the **show svs domain** command to find out the packet VLAN (inband VLAN)

```
n1000v(config-port-prof)# show svs domain
SVS domain config:
  Domain id:    559
```

```
  Control vlan: 3002
  Packet vlan:  3003
  L2/L3 Aipc mode: L2
  L2/L3 Aipc interface: mgmt0
  Status: Config push to VC successful.
```

In this output, the packet VLAN is 69

Step 4 Verify that the packet VLAN is allowed on any of the uplink ports of the VEM.

Assume there is one uplink and it is bound to a port-profile uplink-profile. Enter the **show port-profile na uplink-all** command:

```
n1000v# show port-profile na uplink-all
port-profile uplink-all
description:
type: vethernet
status: enabled
capability l3control: no
pinning control-vlan: -
pinning packet-vlan: -
system vlans: 69-69
port-group: uplink-all
max ports:
inherit: port-profile xyz
config attributes:
 switchport mode trunk
 switchport access vlan 1
 switchport trunk allowed vlan 1, 68-69,231-233
 channel-group auto mode on sub-group cdp
 no shutdown
evaluated config attributes:
 switchport mode trunk
 switchport trunk allowed vlan 1,68-69,231-233
 channel-group auto mode on sub-group cdp
 no shutdown
assigned interfaces:
  Ethernet3/2
```

As shown in the output, the uplink profile is assigned to Ethernet 3/2 and the inband VLAN (69) is allowed on the port. If it is not, add the packet VLAN (69) to the allowed VLAN list.

Step 5 Enter the **show cdp neighbors** command to find out the upstream neighbors connected to Ethernet interface 3/2.

```
n1000V#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
```

The output shows that Ethernet interface 3/2 is connected to the switch n1000v-6k-2 on Gigabit interface 1/38.

Log in to n1000v-6k-2 and verify that the packet VLAN is allowed on the port.

```
n1000v-6k-2#show running-config interface gigabitEthernet 1/38
Building configuration...

Current configuration : 161 bytes
!
```

```
interface GigabitEthernet1/38
 description sfish-srvr-100:vmnic1
 switchport
 switchport trunk allowed vlan 1,60-69,231-233
 switchport mode trunk
end
```

The output shows that the packet VLAN 69 is allowed on the port. If it is not, add the packet VLAN to the allowed VLAN list.

Port Enabled with Port Security is Error Disabled

The ErrDisabled state of a port indicates that the VSM detected a problem with the port and disabled the port. Port security could be responsible for error disabling the port for the following reasons:

- Address Count Exceed Violation
- MAC Move Violation

Address Count Exceed Violation

This issues occurs when more than the configured maximum number of secured addresses are seen on the port. The default violation action is to error disable the port. One way to discover this is to use a **grep** command for the search pattern PORT-SECURITY-2- on the output of a **show logging** command.

```
n1000v#show port-security address interface vethernet 1
Total Secured Mac Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

------------------------------------------------------------------------
                    Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address             Type             Ports      Remaining age
                                                               (mins)
----    -----------            ------            -----     ---------------
  65    0050.56B7.7DE2        DYNAMIC        Vethernet1         0
========================================================================
```

The output shows that MAC 0050.56B7.7DE2 is secured on veth1.

```
n1000V#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
==============================================================================
```

The Max Secured Address is 1.

Another MAC E276.DECF.7DE2 appears on VEthernet 1. Now the port is error disabled.

```
n1000v# show logging | inc "PORT-SECURITY-2-ETH_PORT_SEC_SECURITY_VIOLATION_MAX_MAC_VLAN"

2008 Dec 20 21:33:44 N1KV %PORT-SECURITY-2-ETH_PORT_SEC_SECURITY_VIOLATION_MAX_MAC_VLAN:
Port Vethernet1 moved to SHUTDOWN state as host E276.DECF.7DE2 is trying to access the
port in vlan 65
```

MAC Move Violation

A MAC Move Violation occurs when a MAC that is already secured on one port, such as port A, is seen on another secure port, such as port B.

```
n1000v#show port-security address interface vethernet 1
Total Secured Mac Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

------------------------------------------------------------------------
                    Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address             Type             Ports      Remaining age
                                                               (mins)
----    -----------             ------           -----      ---------------
  65    0050.56B7.7DE2        DYNAMIC        Vethernet1        0
========================================================================
```

The output shows that MAC 0050.56B7.7DE2 is secured on veth1

```
n1000v#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
==============================================================================
```

The output shows the Max Secured Address is 1.

MAC E276.DECF.7DE2 appears on VEthernet 1. Now the port is error disabled.

```
n1000v# show logging | inc "PORT-SECURITY-2-ETH_PORT_SEC_SECURITY_VIOLATION_MAX_MAC_VLAN"
```

2008 Dec 20 21:33:44 N1KV
%PORT-SECURITY-2-ETH_PORT_SEC_SECURITY_VIOLATION_MAX_MAC_VLAN: Port Vethernet1 moved to SHUTDOWN state as host E276.DECF.7DE2 is trying to access the port in vlan 65

Port Security Restrictions and Limitations

When troubleshooting port security issues, make sure you follow these guidelines:

- Dynamic secure MACs cannot be cleared using the **clear mac address-table** command. Use the **clear port-security** command instead.
- Port security cannot be enabled on a Veth on a VLAN if there are static MACs configured on the same VLAN. You need to delete any static MACs that are present on the VLAN on any interface to enable port security on a Veth on that VLAN.
- Restrict Violation Action is not supported. Only Shutdown and Protect Violation Modes can be configured as a Port Security Violation Action.

Collecting Debugging Output for Port Security

Use the following commands to troubleshoot port security:

- **show port-security**
- **show port-security interface veth**
- **show port -security address**

On the VSM, use the following commands to collect information and troubleshoot port security:

- **show system internal port-security msgs**
- **show system internal port-security errors**
- **show system internal l2fm msgs**
- **show system internal l2fm errors**
- **show system internal l2fm info detail**
- **show system internal pktmgr interface brief**
- **show system internal pktmgr client detail**

Symptoms, Causes, and Solutions

Symptom	Possible Causes	Solution
A ping from the VM fails on an interface that has Port Security enabled on it.	—	Verify that the first packet from the VM has been sent to the VSM. Ensure that the uplink port on the ESX host and the port on the uplink switch is carrying the inband VLAN. Ensure that the uplink port on the ESX port (and the corresponding port on the uplink switch) hosting the CPVA is carrying the inband VLAN. Check that the Veth interface state is up in Packet Manager. If it is not, enter a **shutdown** command followed by a **no shutdown** command on the Veth interface.

Port Profiles

Port profiles are used to configure interfaces. A port profile can be assigned to multiple interfaces giving them all the same configuration. Changes to the port profile will be propagated automatically to the configuration of any interface assigned to it.

In the VMware vCenter Server, a port profile is represented as a port group. The VEthernet or Ethernet interfaces are assigned in vCenter Server to a port profile for:

- Defining port configuration by policy.
- Applying a single policy across a large number of ports.
- Supporting both VEthernet and Ethernet ports.

Port profiles that are configured as uplinks, can be assigned by the server administrator to physical ports (a vmnic or a pnic). Port profiles that are not configured as uplinks can be assigned to a VM virtual port.

Note While manual interface configuration overrides that of the port profile, it is not recommended. Manual interface configuration is only used, for example, to quickly test a change or allow a port to be disabled without having to change the inherited port profile.

For more information about assigning port profiles, see your VMware documentation.

To verify that the profiles are assigned as expected, use the following show commands:

- **show port-profile usage**
- **show running-config interface** *interface-id*

The output of the **show running-config interface** *interface-id* command shows a config line such as, `inherit port-profile MyProfile`, indicating the inherited port profile.

Note Inherited port profiles cannot be changed or removed from an interface using the CLI. This can only be done through the vCenter Server.

Note Inherited port profiles are automatically configured when the ports are attached on the hosts. This is done by matching up the VMware port group assigned by the system administrator with the port profile that created it.

For detailed information about port profiles, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3).*

Troubleshooting Commands for Port Profiles

To collect detailed logs for port profiles, execute the following commands that enable debug logs:

- **debug port-profile trace**
- **debug port-profile error**
- **debug port-profile all**

After enabling the debug log, re-execute a port-profile operation and capture the output in a log file.

Use the following commands to troubleshoot port profiles:

- **show port-profile**

```
n1000v# show port-profile
port-profile UpLinkProfile1
  description:
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
```

```
  inherit:
  config attributes:
    channel-group auto mode on mac-pinning
  evaluated config attributes:
    channel-group auto mode on mac-pinning
  assigned interfaces:
port-profile UpLinkProfile2
  description:
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    channel-group auto mode on sub-group cdp
  evaluated config attributes:
    channel-group auto mode on sub-group cdp
  assigned interfaces:
port-profile UpLinkProfile3
  description:
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    channel-group auto mode on sub-group manual
  evaluated config attributes:
    channel-group auto mode on sub-group manual
  assigned interfaces:n1000v#
```

- **show port-profile expand-interface**

```
n1000v# show port-profile expand-interface

port-profile uplink1
Ethernet3/2
    switchport mode trunk
    switchport trunk allowed vlan 1,110-119
    no shutdown
Ethernet4/2
    switchport mode trunk
    switchport trunk allowed vlan 1,110-119
    no shutdown

port-profile data
Vethernet1
    switchport mode access
    switchport access vlan 118
    no shutdown
n1000v#
```

- **show port-profile usage**

```
n1000v# show port-profile usage
```

```
--------------------------------------------------------------------------------
Port Profile                 Port         Adapter         Owner
--------------------------------------------------------------------------------
uplink1                      Eth3/2       vmnic1          172.23.232.57
                           Eth4/2       vmnic1          172.23.232.58
data                         Veth1        Net Adapter 1   ubuntu-2
n1000v#
```

- **show port-profile internal info**

```
n1000v# show port-profile internal info
port-profile Unused_Or_Quarantine_Uplink
  ppid: 00000001
  flags: 00000000
  fsm_state: PPM_PROFILE_FSM_ST_CREATED
  state: enabled
  capability: 00000002
  description: "Port-group created for Nexus1000V internal usage. Do not use."
  alias_id: Unused_Or_Quarantine_Uplink (type=1)
  num_aliases: 1
  alias (type=2):
    name: dvportgroup-1060
    flags: 00000000
  alias name: dvportgroup-1060 type: 2 (pss)
  parent port-profile: none
  num_child_profiles: 0
  num_active_ifs: 0
port-profile Unused_Or_Quarantine_Veth
  ppid: 00000002
  flags: 00000000
  fsm_state: PPM_PROFILE_FSM_ST_CREATED
  state: enabled
  capability: 00000000
  description: "Port-group created for Nexus1000V internal usage. Do not use."
  alias_id: Unused_Or_Quarantine_Veth (type=1)
  num_aliases: 1
  alias (type=2):
    name: dvportgroup-1061
    flags: 00000000
  alias name: dvportgroup-1061 type: 2 (pss)
  parent port-profile: none
  num_child_profiles: 0
  num_active_ifs: 0
port-profile uplink1
  ppid: 00000003
  flags: 00000000
  fsm_state: PPM_PROFILE_FSM_ST_CREATED
  state: enabled
  capability: 00000003
  description: ""
  alias_id: uplink1 (type=1)
  num_aliases: 1
  alias (type=2):
    name: dvportgroup-1062
    flags: 00000000
  alias name: dvportgroup-1062 type: 2 (pss)
  parent port-profile: none
  num_child_profiles: 0
  num_active_ifs: 1
  Ethernet3/2:
    flags: 00000000
    is_active: true
    is_user_configured: false
    bind_count: 1
```

```
    is_bound_by_eth_attach: 1
port-profile data
  ppid: 00000005
  flags: 00000000
  fsm_state: PPM_PROFILE_FSM_ST_CREATED
  state: enabled
  capability: 00000000
  description: ""
  alias_id: data (type=1)
  num_aliases: 1
  alias (type=2):
    name: dvportgroup-1064
    flags: 00000000
  alias name: dvportgroup-1064 type: 2 (pss)
  parent port-profile: none
  num_child_profiles: 0
  num_active_ifs: 0
vms info flag: 00000001
n1000v#
```

- **show port-profile internal event-history msgs**

```
n1000v# show port-profile internal event-history msgs
1) Event:E_MTS_RX, length:60, at 553112 usecs after Thu May 14 00:28:52 2009
    [REQ] Opc:MTS_OPC_SDWRAP_DEBUG_DUMP(1530), Id:0X0028B018, Ret:SUCCESS
    Src:0x00000101/3929, Dst:0x00000101/429, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x0028B018, Sync:NONE, Payloadsize:212
    Payload:
    0x0000:  01 00 2f 74 6d 70 2f 64 62 67 64 75 6d 70 31 37

2) Event:E_MTS_RX, length:60, at 472402 usecs after Thu May 14 00:28:48 2009
    [REQ] Opc:MTS_OPC_SDWRAP_DEBUG_DUMP(1530), Id:0X0028AF64, Ret:SUCCESS
    Src:0x00000101/3928, Dst:0x00000101/429, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x0028AF64, Sync:NONE, Payloadsize:212
    Payload:
    0x0000:  01 00 2f 74 6d 70 2f 64 62 67 64 75 6d 70 31 37

3) Event:E_MTS_RX, length:60, at 897349 usecs after Thu May 14 00:24:59 2009
    [REQ] Opc:MTS_OPC_VSH_CMD_TLV(7679), Id:0X00289DB3, Ret:SUCCESS
    Src:0x00000101/3899, Dst:0x00000101/429, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x00289DB3, Sync:NONE, Payloadsize:228
    Payload:
    0x0000:  04 03 02 01 e4 00 00 00 00 00 00 00 00 00 00 00

4) Event:E_MTS_RX, length:60, at 171002 usecs after Thu May 14 00:19:27 2009
    [REQ] Opc:MTS_OPC_VSH_CMD_TLV(7679), Id:0X00288A62, Ret:SUCCESS
    Src:0x00000101/3899, Dst:0x00000101/429, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x00288A62, Sync:NONE, Payloadsize:220
    Payload:
    0x0000:  04 03 02 01 dc 00 00 00 00 00 00 00 00 00 00 00
```

- **show port-profile internal event-history port-profile** *profile-name*

```
n1000v# show port-profile internal event-history port-profile data

>>>>FSM: <port-profile/5> has 6 logged transitions<<<<<

1) FSM:<port-profile/5> Transition at 212488 usecs after Mon May 11 19:45:02 2009
    Previous state: [PPM_PROFILE_FSM_ST_NOT_EXISTENT]
    Triggered event: [PPM_PROFILE_FSM_EV_INIT]
    Next state: [PPM_PROFILE_FSM_ST_CREATED]

2) FSM:<port-profile/5> Transition at 212494 usecs after Mon May 11 19:45:02 2009
    Previous state: [PPM_PROFILE_FSM_ST_CREATED]
```

```
    Triggered event: [PPM_PROFILE_FSM_EV_CFG_CHANGED]
    Next state: [PPM_PROFILE_FSM_ST_UPDATING_EVAL_CFG]

3) FSM:<port-profile/5> Transition at 212516 usecs after Mon May 11 19:45:02 2009
    Previous state: [PPM_PROFILE_FSM_ST_UPDATING_EVAL_CFG]
    Triggered event: [PPM_PROFILE_FSM_EV_EVAL_CFG_CHANGED]
    Next state: [PPM_PROFILE_FSM_ST_MSP_HANDSHAKE_CFG_CHANGE]

4) FSM:<port-profile/5> Transition at 212535 usecs after Mon May 11 19:45:02 2009
    Previous state: [PPM_PROFILE_FSM_ST_MSP_HANDSHAKE_CFG_CHANGE]
    Triggered event: [PPM_PROFILE_FSM_EV_MSP_HANDSHAKE_FAIL]
    Next state: [PPM_PROFILE_FSM_ST_UPDATING_CLIENTS]

5) FSM:<port-profile/5> Transition at 212542 usecs after Mon May 11 19:45:02 2009
    Previous state: [PPM_PROFILE_FSM_ST_UPDATING_CLIENTS]
    Triggered event: [PPM_PROFILE_FSM_EV_UPDATE_DONE]
    Next state: [PPM_PROFILE_FSM_ST_WAIT_FOR_CHILD]

6) FSM:<port-profile/5> Transition at 213668 usecs after Mon May 11 19:45:02 2009
    Previous state: [PPM_PROFILE_FSM_ST_WAIT_FOR_CHILD]
    Triggered event: [PPM_PROFILE_FSM_EV_CHILD_PROFILE_DONE]
    Next state: [PPM_PROFILE_FSM_ST_CREATED]
```

System Port Profiles

System port profiles are special port profiles that must be configured before the VSM and the VEM can communicate with each other. System port profiles are used to convey the control and packet VLAN IDs from the VSM to the VEM via the vCenter Server.

When configuring system port profiles, follow these guidelines:

- For trunk ports, the system VLAN list must be a subset of the allowed VLAN list.
- For access ports, there must be one system VLAN, and it must the same as the access VLAN.
- Issue the **no system vlan** command only when no interface is using the profile.
- Once a system profile is in use by at least one interface, you can only add to the list of system VLANs, but not delete any VLANs from the list.
- For a profile with system VLANs, the **no port-profile** command, the **no vmware port-group** command, and the **no state enabled** command can be issued only when no interface is using the profile.
- The maximum number of port profiles is 128.

Port Profiles Symptoms and Solutions

Symptom	Possible Causes	Solution
You do not see a port group on a vCenter Server or see the message Warning: Operation succeeded locally but update failed on vCenter server. Please check if you are connected to vCenter Server.	—	Issue the **show svs connections** command to verify that the connection to the vCenter Server is active. The switch output should display Enabled and Connected. Issue the **show svs domain** command and check the status for success. Also verify that the following commands have been specified for the port profile: • **vmware port-group** • **state enabled**
A port configuration is not applied to an interface.	—	Issue the **show port-profile usage** command to show the interface. Use the **show run** command and the **show port-profile expand-interface** command to verify that the interface level configuration did not overwrite the port profile configuration.
An Ethernet interface or Veth interface is administratively down.	The interface is inheriting one of the quarantine port profiles. Use the **show port-profile usage** command to verify this situation.	Reassign the vnic or pnic to a non-quarantine port group to enable the Veth or Ethernet interface to be up and able to forward traffic. This action requires changing the port group on the vCenter Server.

Transferring Port Profiles from the VSM to the vCenter Server

When transferring a Port Profile from the VSM to the vCenter Server, follow these guidelines:

- Make sure that an Uplink Port Profile (UPP) has the following essential attributes:
  - Uplink capability.
  - System VLANs configured if it is a system port profile.

Note For a privileged profile, make sure you explicitly allow VLANs in the profile if you are configuring trunk mode. Enter the **switchport trunk allowed vlan** *your-vlan -list* command for this type of configuration.

  - Vmware port group.
  - Switchport mode trunk or access.
  - No shutdown.

  - State enabled.
- Make sure you explicitly create any VLANs which you configure in the Port Profiles.