

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Theory](#)

[PVLAN Implementation in UCS](#)

[Goal](#)

[Configure](#)

[Network Diagrams](#)

[PVLAN on vSwitch: Isolated PVLAN with Promiscuous Port on an Upstream Device](#)

[Configuration in UCS](#)

[Configuration of Upstream Devices](#)

[Troubleshooting](#)

[Isolated PVLAN on N1K with Promiscuous Port on an Upstream Device](#)

[Configuration in UCS](#)

[Configuration of Upstream Devices](#)

[Configuration of N1K](#)

[Troubleshooting](#)

[Isolated PVLAN on N1K with Promiscuous Port on the N1K Uplink Port-Profile](#)

[Configuration in UCS](#)

[Configuration of Upstream Devices](#)

[Configuration of N1K](#)

[Troubleshooting](#)

[Community PVLAN on N1K with Promiscuous Port on the N1K Uplink Port-Profile](#)

[Troubleshooting](#)

[Isolated PVLAN and Community PVLAN on VMware DVS Promiscuous Port on the DVS](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes private VLAN (PVLAN) support in the Cisco Unified Computing System (UCS), a feature introduced in Release 1.4 of the Cisco UCS Manager (UCSM). It also details the features, the caveats, and the configuration when PVLANS are used in a UCS environment.

THIS DOCUMENT IS FOR USE WITH UCSM VERSION 2.2(2C) AND EARLIER VERSIONS. In versions later than Version 2.2(2C), changes have been made to UCSM and ESXi DVS is supported. There are also changes in how tagging works for the PVLAN NIC.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- UCS
- Cisco Nexus 1000 V (N1K)
- VMware
- Layer 2 (L2) switching

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

Theory

A private VLAN is a VLAN configured for L2 isolation from other ports within the same private VLAN. Ports that belong to a PVLAN are associated with a common set of support VLANs, which are used in order to create the PVLAN structure.

There are three types of PVLAN ports:

- A **promiscuous port** communicates with all other PVLAN ports and is the port used in order to communicate with devices outside of the PVLAN.
- An **isolated port** has complete L2 separation (including broadcasts) from other ports within the same PVLAN with the exception of the promiscuous port.
- A **community port** can communicate with other ports in the same PVLAN as well as the promiscuous port. Community ports are isolated at L2 from ports in other communities or isolated PVLAN ports. Broadcasts are only propagated to other ports in the community and the promiscuous port.

Refer to [RFC 5517, Cisco Systems' Private VLANs: Scalable Security in a Multi-Client Environment](#) in order to understand the theory, operation, and concepts of PVLANS.

PVLAN Implementation in UCS

UCS closely resembles the Nexus 5000/2000 architecture, where the Nexus 5000 is analogous to the UCS 6100 and the Nexus 2000 to the UCS 2104 Fabric Extenders.

Many limitations of PVLAN functionality in UCS are caused by the limitations found in the Nexus 5000/2000 implementation.

Important points to remember are:

- Only isolated ports are supported in UCS. With the N1K incorporated, you can use community VLANs, but the promiscuous port must be on the N1K as well.
- There is no support for promiscuous ports/trunks, community ports/trunks, or isolated trunks.
- Promiscuous ports need to be outside the UCS domain, such as an upstream switch/router or a downstream N1K.

Goal

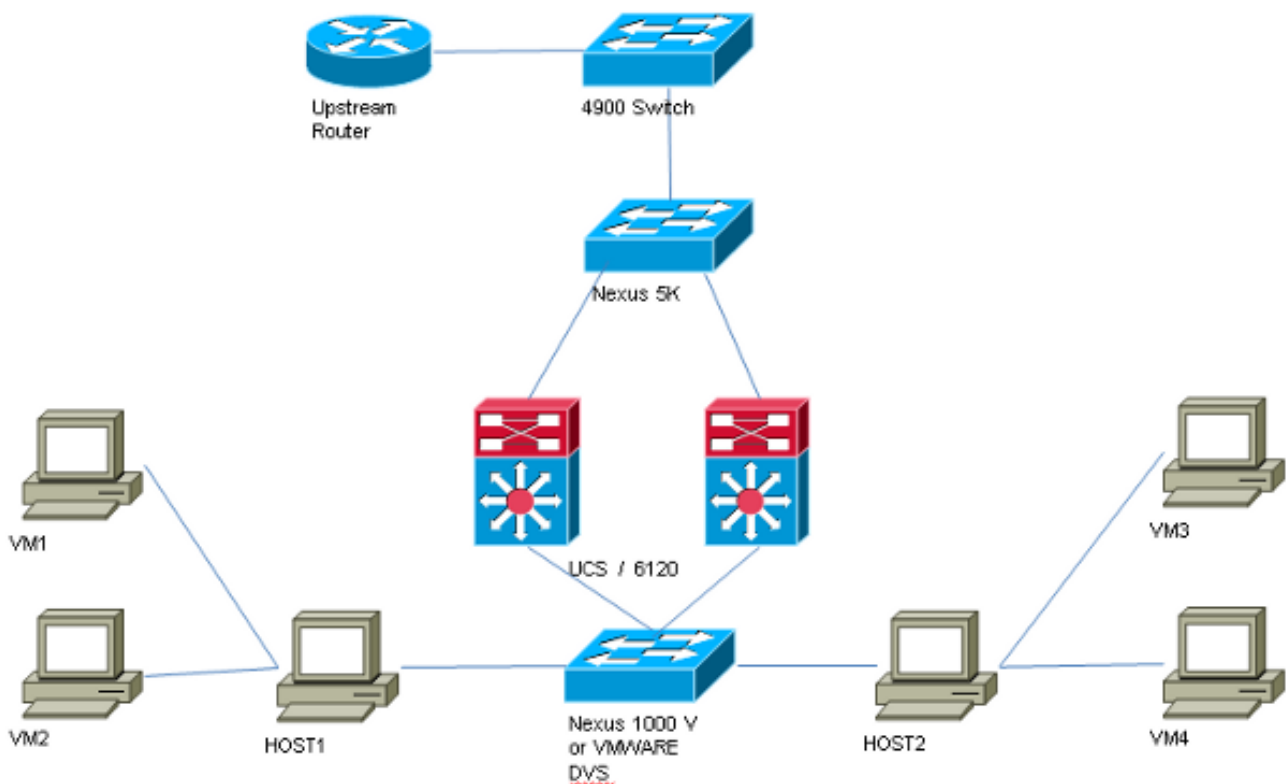
This document covers several different configurations available for PVLAN with UCS:

1. Isolated PVLAN with promiscuous port on an upstream device.
2. Isolated PVLAN on N1K with promiscuous port on an upstream device.
3. Isolated PVLAN on N1K with promiscuous port on the N1K uplink port-profile
4. Community PVLAN on N1K with promiscuous port on the N1K uplink port-profile.
5. Isolated PVLAN on VMware Distributed Virtual Switch (DVS) promiscuous port on the DVS.
6. Community PVLAN on VMware DVS switch promiscuous port on the DVS.

Configure

Network Diagrams

The topology for all examples with a distributed switch is:



The topology for all examples with no distributed switch is:



PVLAN on vSwitch: Isolated PVLAN with Promiscuous Port on an Upstream Device

In this configuration, you are passing PVLAN traffic through UCS to a promiscuous port that is upstream. Because you cannot send both primary and secondary VLANs on the same vNIC, you need one vNIC for each blade for each PVLAN, in order to carry the PVLAN traffic.

Configuration in UCS

This procedure describes how to create both the primary and any isolated VLANs.

Note: This example uses 266 as the primary and 166 as the isolated; the VLAN IDs will be determined by the site.

1. In order to create the primary VLAN, click **Primary** as the Sharing Type, and enter a **VLAN ID** of 266:

The screenshot displays the UCS configuration interface. The **Properties** section is at the top, showing the following settings:

- Name: 266
- Native VLAN: No
- Network Type: Lan
- Locale: External
- Multicast Policy Name: <not set>
- Multicast Policy Instance: org-root/mc-policy-default
- Sharing Type: Primary
- VLAN ID: 266
- Fabric ID: Dual
- If Type: Virtual
- Transport Type: Ether
- + Create Multicast Policy

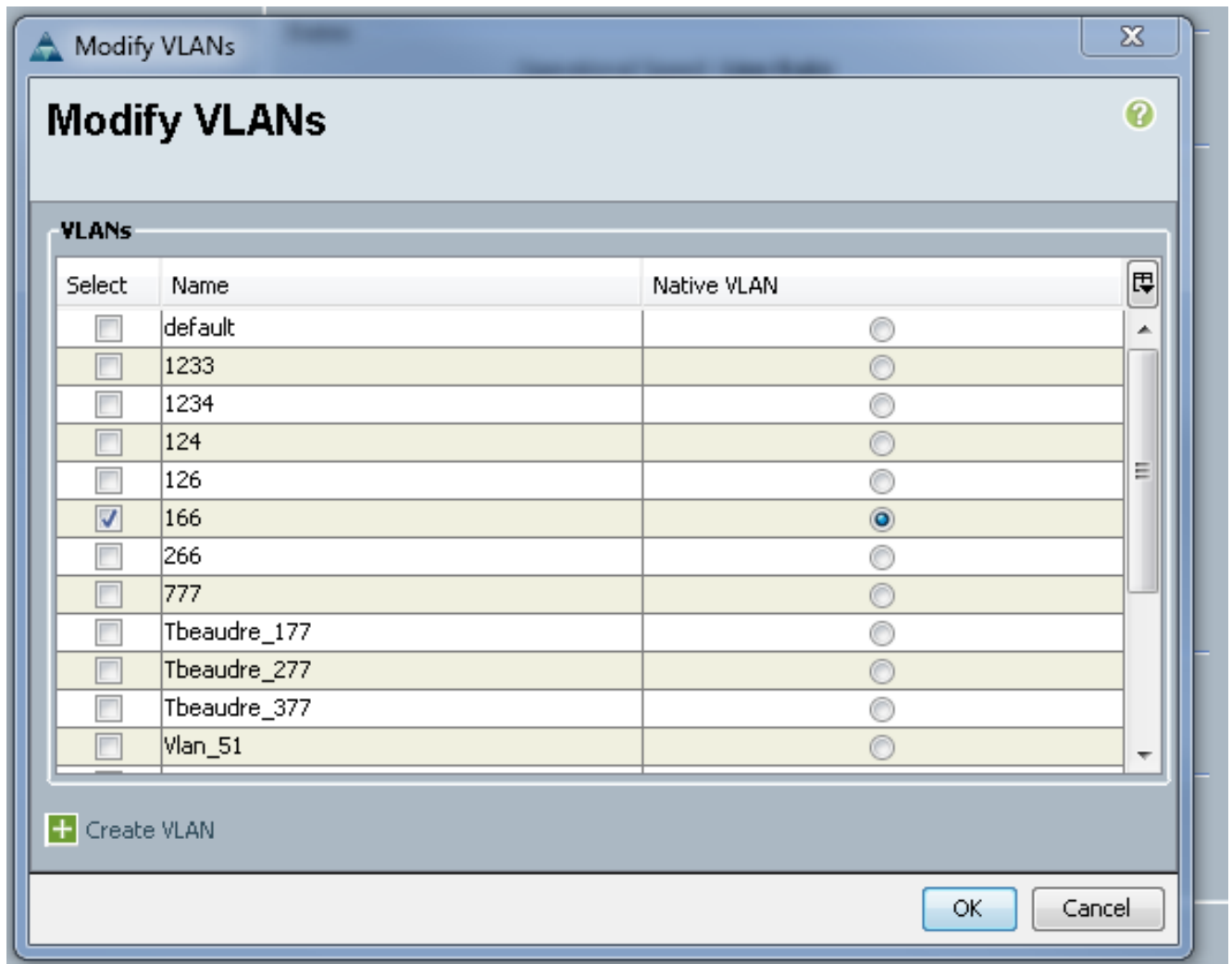
The **Secondary VLANs** section is below, featuring a table with the following data:

Name	ID	Type	Transport	Native	VLAN Sharing
166	166	Lan	Ether	No	Isolated

2. In order to create the isolated VLAN, click **Isolated** as the Sharing Type, enter a **VLAN ID** of 166, and choose **VLAN 266 (266)** as the Primary VLAN:



3. In order to add the VLAN to the vNIC, click the **Select** checkbox for VLAN 166, and click the associated **Native VLAN** radio button.



Only the isolated VLAN is added, it must be set as primary, and there can only be one for each vNIC. Because the Native VLAN is defined here, do not configure VLAN tagging on the VMware port groups.

Configuration of Upstream Devices

These procedures describe how to configure a Nexus 5K to pass the PVLAN through to an upstream 4900 switch where the promiscuous port is. While this might not be necessary in all environments, use this configuration in the event that you must pass the PVLAN through another switch.

On the Nexus 5K, enter these commands, and check uplink configuration:

1. Turn on the PVLAN feature:

```
Nexus5000-5(config)# feature private-vlan
```

2. Add the VLANs as primary and isolated:

```
Nexus5000-5(config)# vlan 166
```

```
Nexus5000-5(config-vlan)# private-vlan isolated
Nexus5000-5(config-vlan)# vlan 266
Nexus5000-5(config-vlan)# private-vlan primary
```

3. Associate VLAN 266 with the isolated VLAN 166:

```
Nexus5000-5(config-vlan)# private-vlan association 166
```

4. Make sure that all uplinks are configured in order to trunk the VLANs:

```
interface Ethernet1/1description Connection to 4900switchport mode trunkspeed
1000interface Ethernet1/3description Connection to FIB Port 5switchport mode trunkspeed
1000interface Ethernet1/4description Connection to FIA port 5switchport mode trunkspeed
1000
```

On the 4900 switch, take these steps, and set up the promiscuous port. The PVLAN ends at the promiscuous port.

1. Turn on PVLAN feature if required.
2. Create and associate the VLANs as done on the Nexus 5K.
3. Create the promiscuous port on the egress port of the 4900 switch. From this point on, the packets from VLAN 166 are seen on VLAN 266 in this case.

```
Switch(config-if)#switchport mode trunk
switchport private-vlan mapping 266 166
switchport mode private-vlan promiscuous
```

On the upstream router, create a subinterface for the VLAN 266 only. At this level, the requirements depend upon the network configuration you are using:

1. interface GigabitEthernet0/1.1
2. encapsulation dot1Q 266
3. IP address 209.165.200.225 255.255.255.224

Troubleshooting

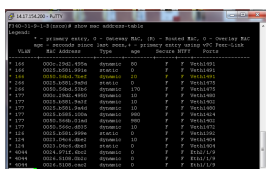
This procedure describes how to test the configuration.

1. Configure the switch virtual interface (SVI) on each switch, which allows you to ping the SVI from the PVLAN:

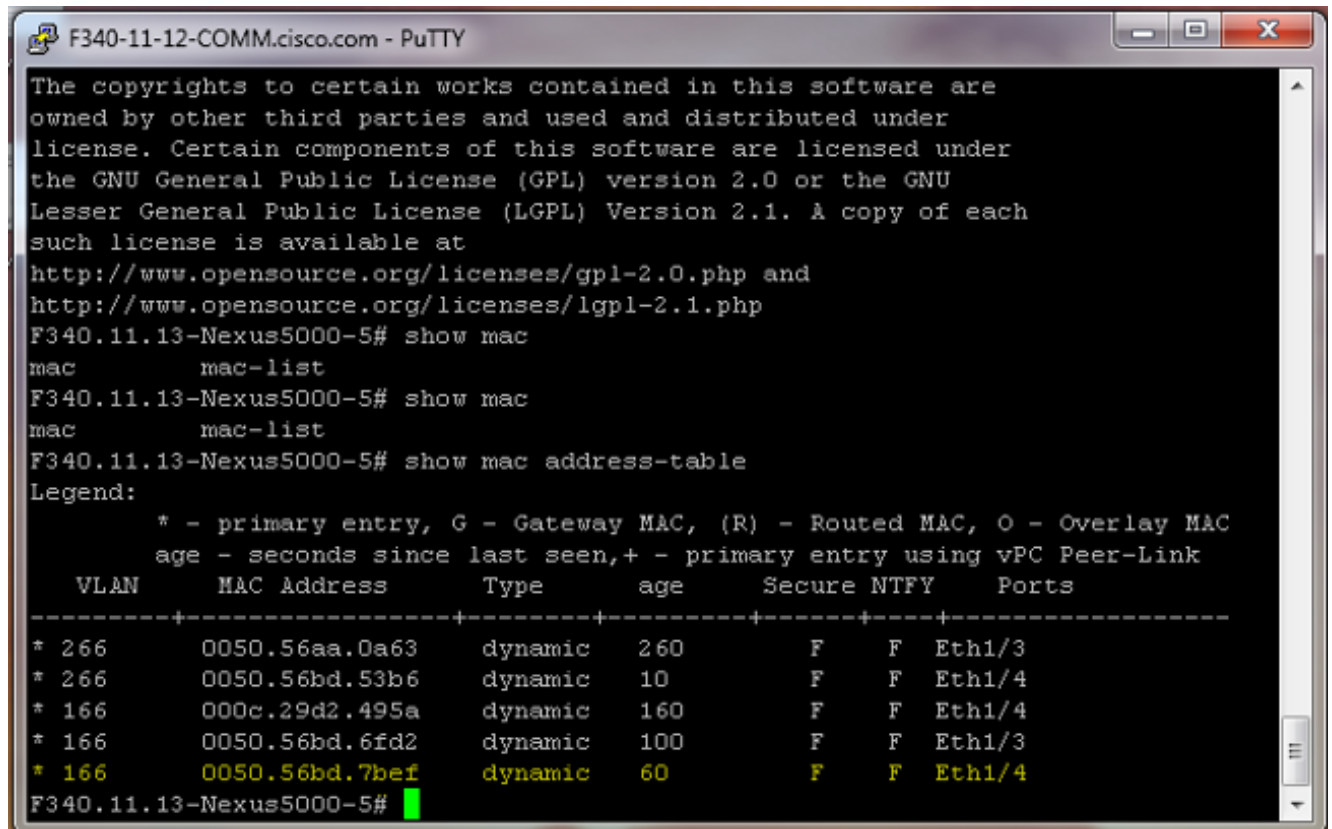
```
(config)# interface vlan 266
(config-if)# ip address 209.165.200.225 255.255.255.224
(config-if)# private-vlan mapping 166
(config-if)# no shut
```

2. Check the MAC address tables in order to see where your MAC is being learned. On all switches, the MAC should be in the isolated VLAN except on the switch with the promiscuous port. On the promiscuous switch, note that the MAC is in the primary VLAN.

On the Fabric Interconnect, MAC address 0050.56bd.7bef is learned on Veth1491:

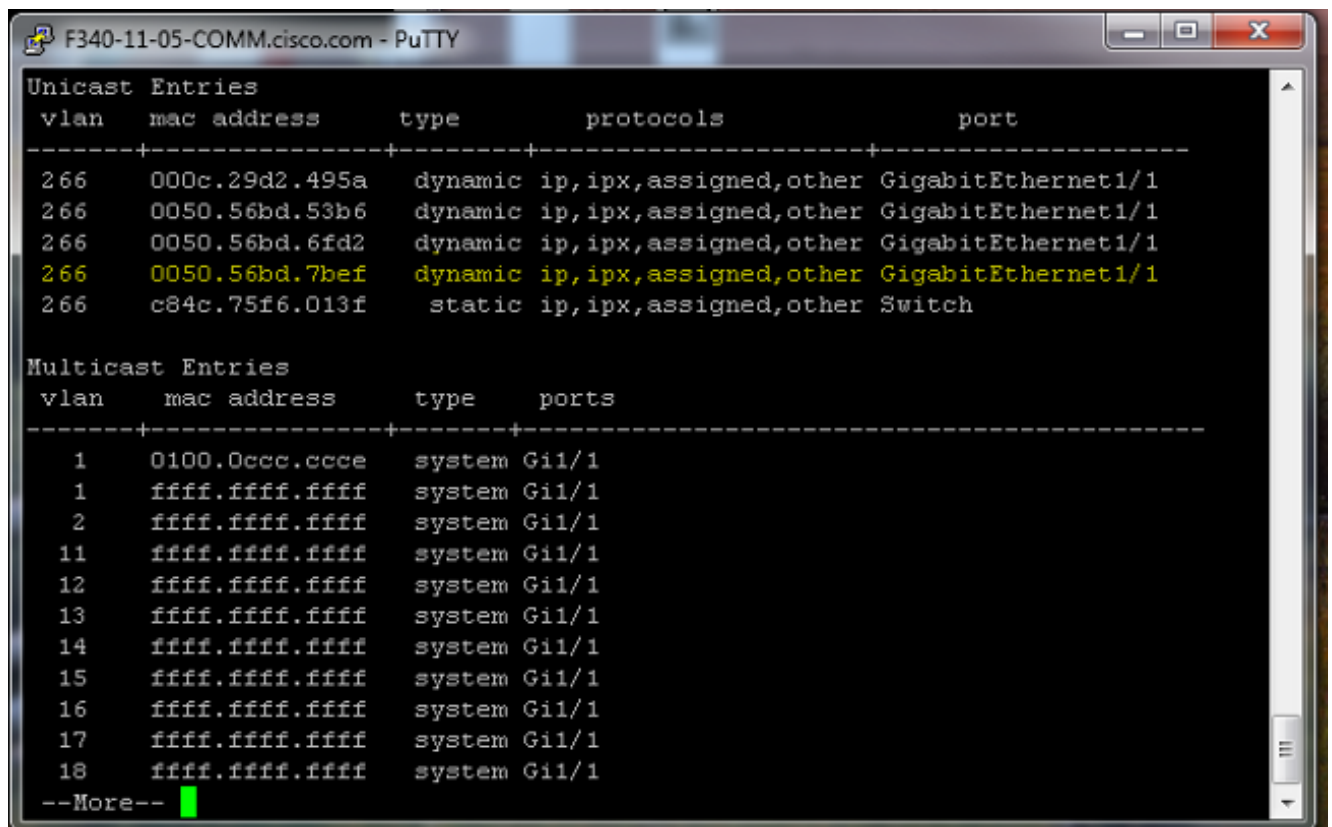


On the Nexus 5K, MAC address 0050.56bd.7bef is learned on Eth1/4:



```
F340-11-12-COMM.cisco.com - PuTTY
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
F340.11.13-Nexus5000-5# show mac
mac          mac-list
F340.11.13-Nexus5000-5# show mac
mac          mac-list
F340.11.13-Nexus5000-5# show mac address-table
Legend:
    * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
    age - seconds since last seen,+ - primary entry using vPC Peer-Link
VLAN      MAC Address      Type      age      Secure NTFY      Ports
-----+-----+-----+-----+-----+-----
* 266     0050.56aa.0a63    dynamic   260      F      F      Eth1/3
* 266     0050.56bd.53b6    dynamic   10       F      F      Eth1/4
* 166     000c.29d2.495a    dynamic   160      F      F      Eth1/4
* 166     0050.56bd.6fd2    dynamic   100      F      F      Eth1/3
* 166     0050.56bd.7bef    dynamic   60       F      F      Eth1/4
F340.11.13-Nexus5000-5#
```

On the 4900 switch, MAC address 0050.56bd.7bef is learned on GigabitEthernet1/1:



```
F340-11-05-COMM.cisco.com - PuTTY
Unicast Entries
vlan      mac address      type      protocols      port
-----+-----+-----+-----+-----
266       000c.29d2.495a    dynamic   ip,ipx,assigned,other GigabitEthernet1/1
266       0050.56bd.53b6    dynamic   ip,ipx,assigned,other GigabitEthernet1/1
266       0050.56bd.6fd2    dynamic   ip,ipx,assigned,other GigabitEthernet1/1
266       0050.56bd.7bef    dynamic   ip,ipx,assigned,other GigabitEthernet1/1
266       c84c.75f6.013f    static    ip,ipx,assigned,other Switch

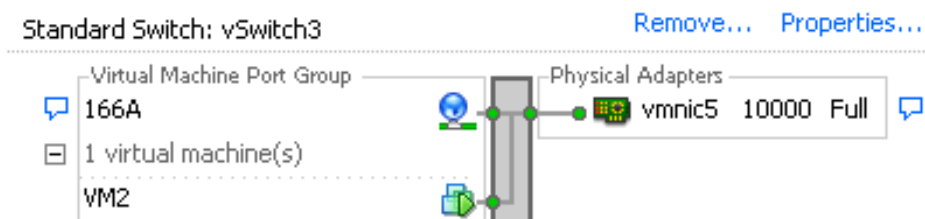
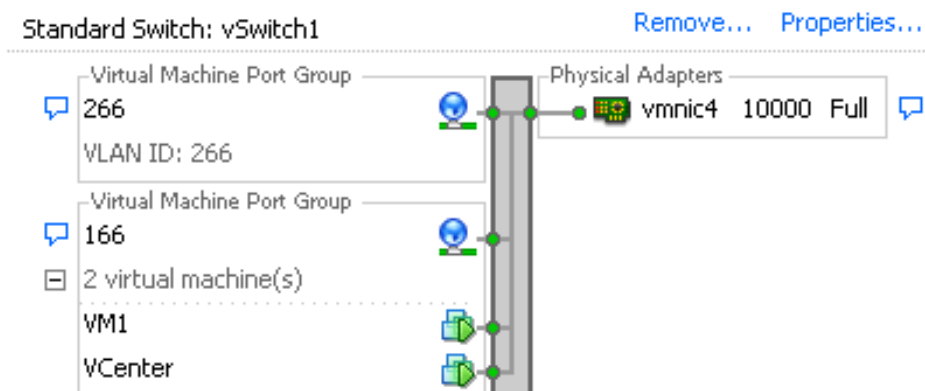
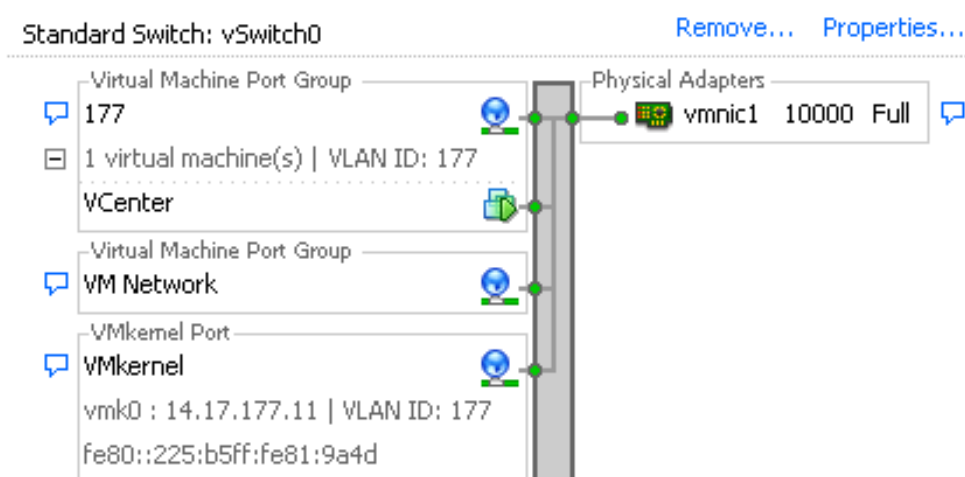
Multicast Entries
vlan      mac address      type      ports
-----+-----+-----+-----
1         0100.0ccc.ccce    system    Gi1/1
1         ffff.ffff.ffff    system    Gi1/1
2         ffff.ffff.ffff    system    Gi1/1
11        ffff.ffff.ffff    system    Gi1/1
12        ffff.ffff.ffff    system    Gi1/1
13        ffff.ffff.ffff    system    Gi1/1
14        ffff.ffff.ffff    system    Gi1/1
15        ffff.ffff.ffff    system    Gi1/1
16        ffff.ffff.ffff    system    Gi1/1
17        ffff.ffff.ffff    system    Gi1/1
18        ffff.ffff.ffff    system    Gi1/1
--More--
```

In this configuration, the systems in this isolated VLAN cannot communicate with each other, but can communicate with other systems through the promiscuous port on the 4900 switch. One issue is how to configure downstream devices. In this case, you are using VMware and two hosts.

Remember that you must use one vNIC for each PVLAN. These vNICs are presented to VMware vSphere ESXi, and you can then create port groups and have guests to these port groups.

If two systems are added to the same port group on the same switch, they can communicate with each other because their communications are switched locally on the vSwitch. In this system, there are two blades with two hosts each.

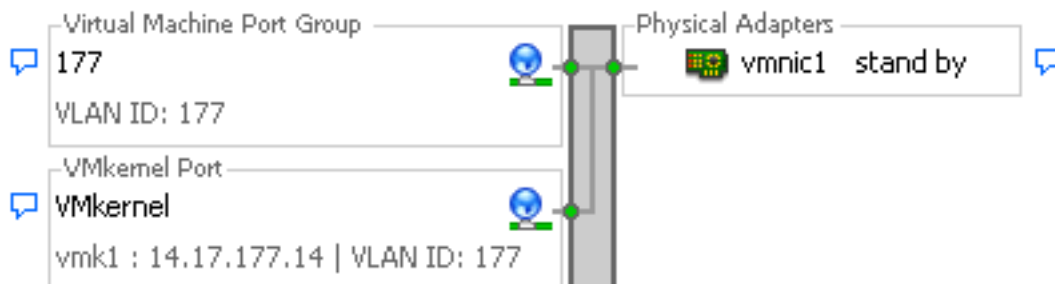
On the first system, two different port groups have been created - one called 166, and one called 166A. Each is connected to a single NIC, which is configured in the isolated VLAN on UCS. There is currently only one guest for each port group. In this case, because these are separated on ESXi, they cannot talk to each other.



On the second system, there is only one port group called 166. There are two guests in this port group. In this configuration, VM3 and VM4 can communicate with each other even though you do not want this to happen. In order to correct this, you need to configure a single NIC for each virtual machine (VM) that is in the isolated VLAN, and then create a port group attached to that vNIC. Once this is configured, put only one guest into the port group. This is not a problem with a bare metal Windows install because you do not have these underlying vSwitches.

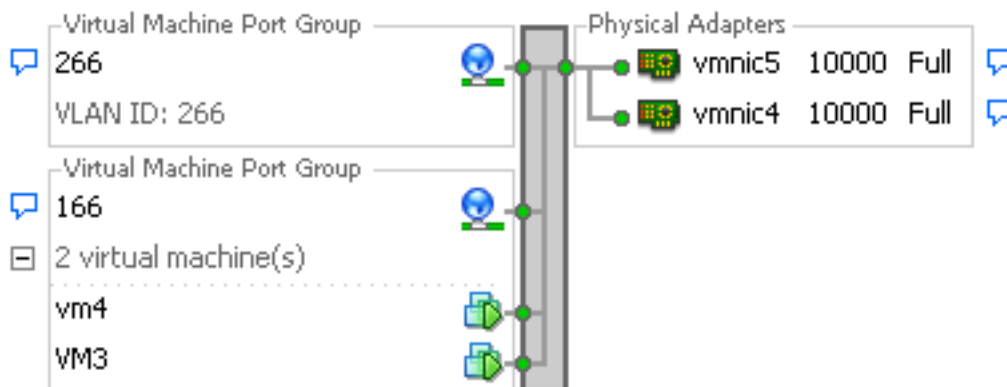
Standard Switch: vSwitch0

[Remove...](#) [Properties...](#)



Standard Switch: vSwitch1

[Remove...](#) [Properties...](#)



Standard Switch: vSwitch2

[Remove...](#) [Properties...](#)



Isolated PVLAN on N1K with Promiscuous Port on an Upstream Device

In this configuration, you are passing PVLAN traffic through an N1K then the UCS to a promiscuous port that is upstream. Because you cannot send both primary and secondary VLANs on the same vNIC, you need one vNIC for each PVLAN uplink in order to carry the PVLAN traffic.

Configuration in UCS

This procedure describes how to create both the primary and any isolated VLANs.

Note: This example uses 266 as the primary and 166 as the isolated; the VLAN IDs will be determined by the site.

1. In order to create the primary VLAN, click **Primary** as the Sharing Type:

Properties

Name: **266** VLAN ID:

Native VLAN: **No** Fabric ID: **Dual**

Network Type: **Lan** If Type: **Virtual**

Locale: **External** Transport Type: **Ether**

Multicast Policy Name:

Multicast Policy Instance: [org-root/mc-policy-default](#)

Sharing Type: None Primary Isolated

Secondary VLANs

Name	ID	Type	Transport	Native	VLAN Sharing
166	166	Lan	Ether	No	Isolated

2. In order to create the isolated VLAN, click **Isolated** as the Sharing Type:

Properties

Name: **166** VLAN ID:

Native VLAN: **No** Fabric ID: **Dual**

Network Type: **Lan** If Type: **Virtual**

Locale: **External** Transport Type: **Ether**

Sharing Type: None Primary Isolated Primary VLAN:

Primary VLAN Properties

Name: **266** VLAN ID: **266**

Native VLAN: **No** Fabric ID: **Dual**

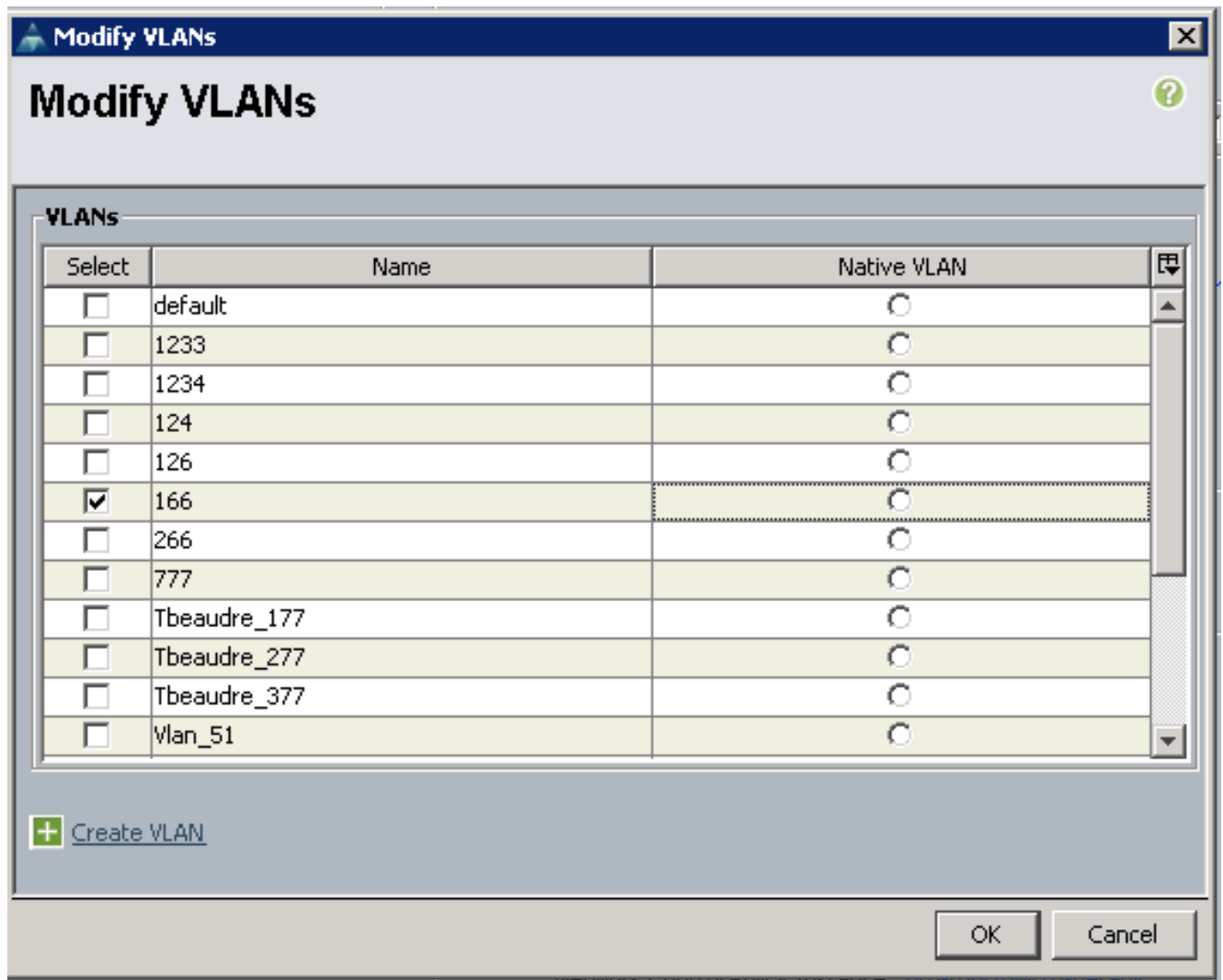
Network Type: **Lan** If Type: **Virtual**

Locale: **External** Transport Type: **Ether**

Multicast Policy Name:

Multicast Policy Instance: [org-root/mc-policy-default](#)

3. In order to add the VLAN to the vNIC, click the **Select** checkbox for VLAN 166. VLAN 166 does not have Native VLAN selected.



Only the isolated VLAN is added, it must not be set as native, and there can only be one for each vNIC. Because the Native VLAN is not defined here, tag the native VLAN on the N1K. The option to tag a Native VLAN is not available in the VMware DVS, so this is not supported on DVS.

Configuration of Upstream Devices

These procedures describe how to configure a Nexus 5K in order to pass the PVLAN through to an upstream 4900 switch where the promiscuous port is. While this might not be necessary in all environments, use this configuration in the event that you must pass the PVLAN through another switch.

On the Nexus 5K, enter these commands, and check uplink configuration:

1. Turn on the PVLAN feature:

```
Nexus5000-5(config)# feature private-vlan
```

2. Add the VLANs as primary and isolated:

```
Nexus5000-5(config)# vlan 166
Nexus5000-5(config-vlan)# private-vlan isolated
Nexus5000-5(config-vlan)# vlan 266
Nexus5000-5(config-vlan)# private-vlan primary
```

3. Associate VLAN 266 with the isolated VLAN 166:

```
Nexus5000-5(config-vlan)# private-vlan association 166
```

4. Make sure that all uplinks are configured in order to trunk the VLANs:

```
interface Ethernet1/1description Connection to 4900switchport mode trunkspeed
1000interface Ethernet1/3description Connection to FIB Port 5switchport mode trunkspeed
1000interface Ethernet1/4description Connection to FIA port 5switchport mode trunkspeed
1000
```

On the 4900 switch, take these steps, and set up the promiscuous port. The PVLAN ends at the promiscuous port.

1. Turn on PVLAN feature if required.
2. Create and associate the VLANs as done on the Nexus 5K.
3. Create the promiscuous port on the egress port of the 4900 switch. From this point on, the packets from VLAN 166 are seen on VLAN 266 in this case.

```
Switch(config-if)#switchport mode trunk
switchport private-vlan mapping 266 166
switchport mode private-vlan promiscuous
```

On the upstream router, create a subinterface for the VLAN 266 only. At this level, the requirements depend upon the network configuration that you use:

1. interface GigabitEthernet0/1.1
2. encapsulation dot1Q 266
3. IP address 209.165.200.225 255.255.255.224

Configuration of N1K

This procedure describes how to configure the N1K as a standard trunk, not a PVLAN trunk.

1. Create and associate the VLANs as done on the Nexus 5K. Refer to the [Configuration of Upstream Devices](#) section for more information.
2. Create an uplink port-profile for the PVLAN traffic:

```
Switch(config)#port-profile type ethernet pvlan_uplink
Switch(config-port-prof)# vmware port-group
Switch(config-port-prof)# switchport mode trunk
Switch(config-port-prof)# switchport trunk allowed vlan 166,266
Switch(config-port-prof)# switchport trunk native vlan 266 <-- This is necessary to handle
traffic coming back from the promiscuous port.
Switch(config-port-prof)# channel-group auto mode on mac-pinning
Switch(config-port-prof)# no shut
Switch(config-port-prof)# state enabled
```

3. Create the port-group for the isolated VLAN; create a PVLAN host port with the host association for the primary and isolated VLANs:

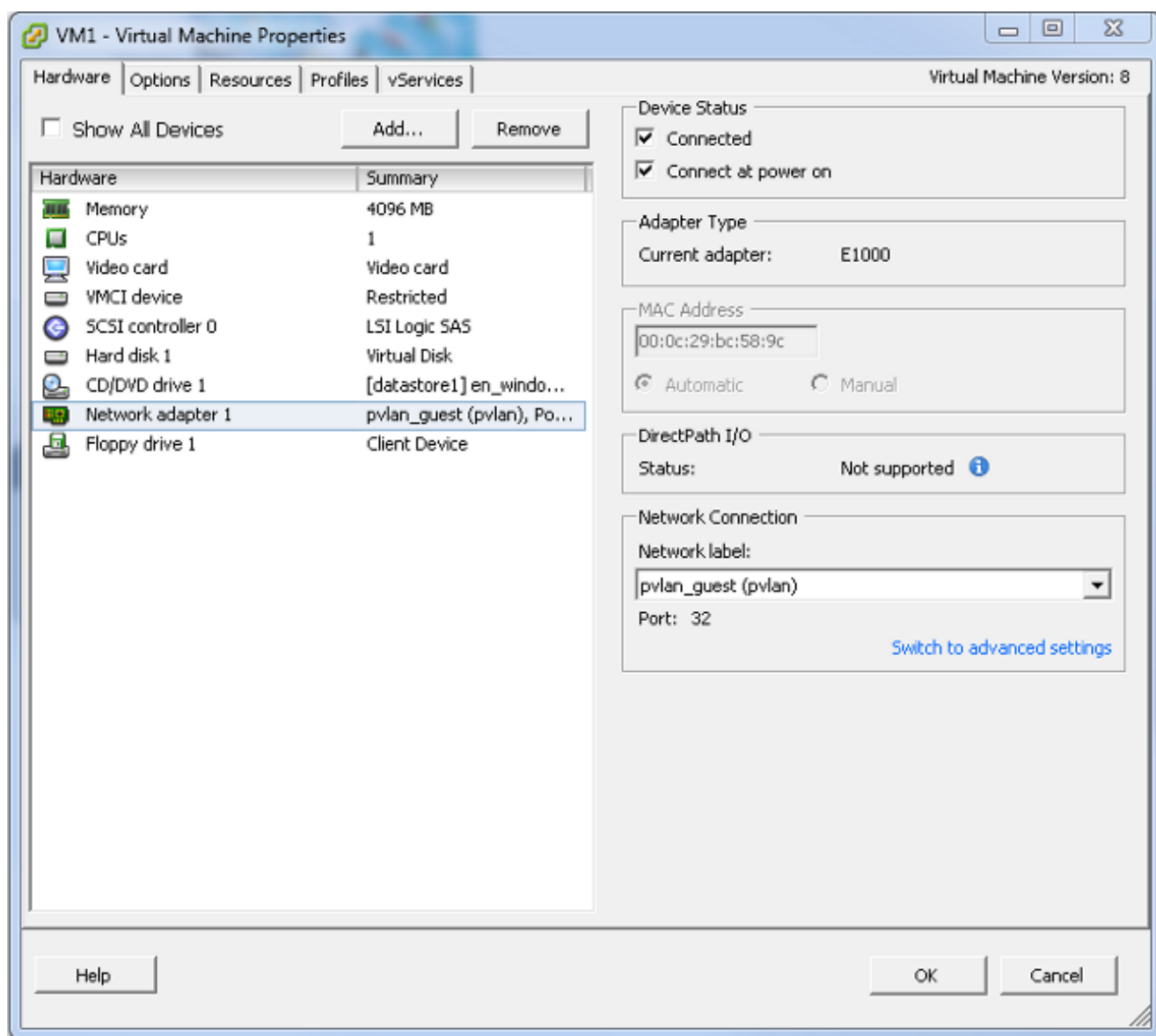
```
Switch(config)# port-profile type vethernet pvlan_guest
Switch(config-port-prof)# vmware port-group
Switch(config-port-prof)# switchport mode private-vlan host
Switch(config-port-prof)# switchport private-vlan host-association 266 166
Switch(config-port-prof)# no shut
Switch(config-port-prof)# state enabled
```

- In the vCenter, add the proper vNIC to the PVLAN uplink. This is the vNIC to which you added the Isolated VLAN under the Configuration in UCS settings.

<input type="checkbox"/>		vmnic3	--	View Details...	Select an uplink port gr...
<input checked="" type="checkbox"/>		vmnic4	pvlan	View Details...	pvlan_uplink
<input type="checkbox"/>		vmnic5	--	View Details...	Select an uplink port gr...

- Add the VM to the correct port-group:

In the Hardware tab, click **Network adapter 1**. Choose **pvlan_guest (pvlan)** for the Network label under Network Connection:



Troubleshooting

- On the UCS system, you should be learning all MACs, for this communication, in the isolated VLAN. You should not see the upstream here:

```
F340-31-9-1-B(nxos)# show mac address-table
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link
VLAN      MAC Address      Type      age      Secure NTFY      Ports
-----+-----+-----+-----+-----+-----
* 166     000c.2996.9a1d   dynamic   10       F      F      Veth1491
* 166     000c.29bc.589c   dynamic   270      F      F      Veth1491
* 166     0025.b581.991e   static    0        F      F      Veth1491
```

- On the Nexus 5K, the two VMs are on the isolated VLAN, while the upstream device is on the primary VLAN:

```
F340.11.13-Nexus5000-5# show mac address-table
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link
VLAN      MAC Address      Type      age      Secure NTFY      Ports
-----+-----+-----+-----+-----+-----
* 266     0012.8032.86a9   dynamic   0        F      F      Eth1/1
* 166     000c.2996.9a1d   dynamic   40       F      F      Eth1/4
* 166     000c.29bc.589c   dynamic   60       F      F      Eth1/4
```

- On the 4900 switch, where the promiscuous port is, everything is on the primary VLAN:

```
Unicast Entries
vlan      mac address      type      protocols      port
-----+-----+-----+-----+-----
266      000c.2996.9a1d   dynamic   ip,ipx,assigned,other GigabitEthernet1/1
266      000c.29bc.589c   dynamic   ip,ipx,assigned,other GigabitEthernet1/1
266      0012.8032.86a9   dynamic   ip,ipx,assigned,other GigabitEthernet1/2

Multicast Entries
vlan      mac address      type      ports
-----+-----+-----+-----
1         0100.0ccc.ccce   system   Gi1/1
1         ffff.ffff.ffff   system   Gi1/1
266      ffff.ffff.ffff   system   Gi1/1,Gi1/2
```

Isolated PVLAN on N1K with Promiscuous Port on the N1K Uplink Port-Profile

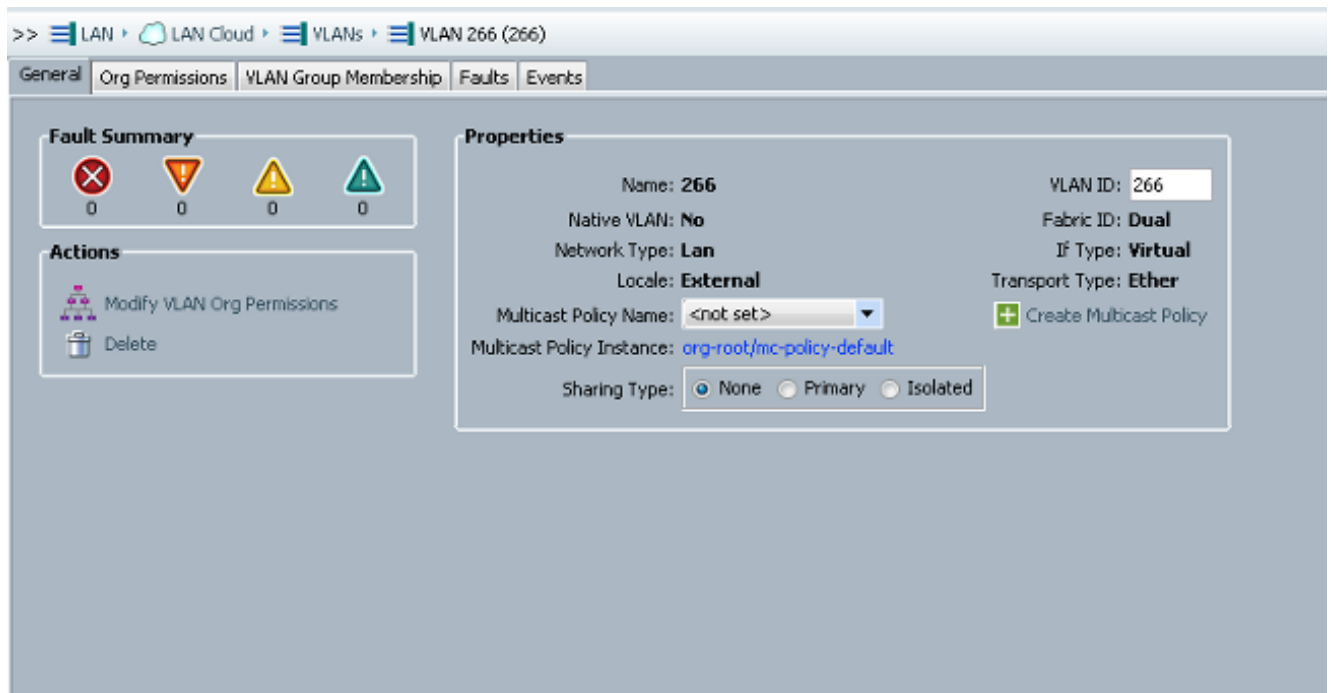
In this configuration, you contain PVLAN traffic to the N1K with only the primary VLAN used upstream.

Configuration in UCS

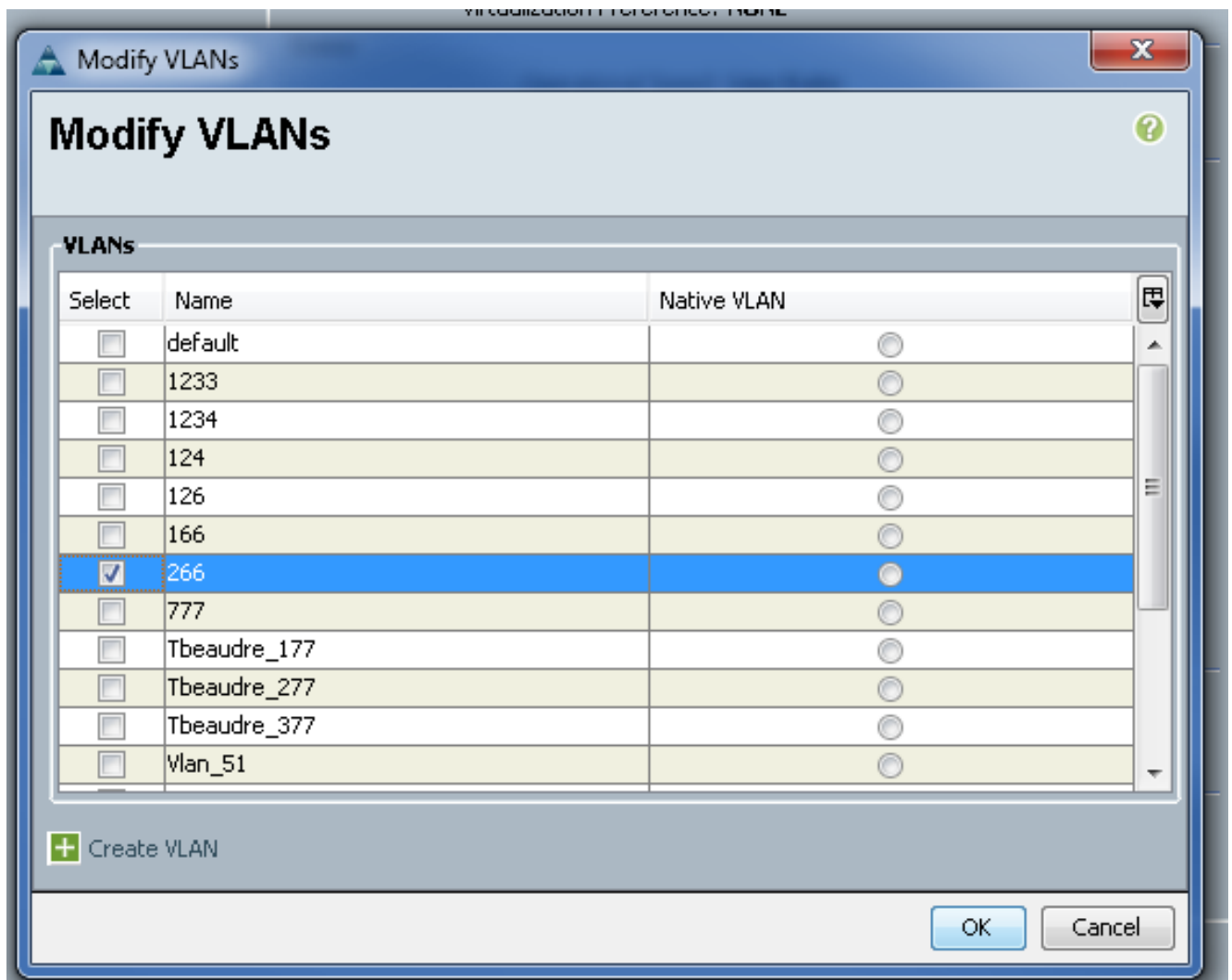
This procedure describes how to add the primary VLAN to the vNIC. There is no need for PVLAN configuration because you only need the primary VLAN.

Note: This example uses 266 as the primary and 166 as the isolated; the VLAN IDs will be determined by the site.

1. Note that the Sharing Type is **None**.



2. Click the **Select** checkbox for VLAN 266 in order to add the primary VLAN to the vNIC. Do not set it as Native.



Configuration of Upstream Devices

These procedures describe how to configure the upstream devices. In this case, the upstream switches only need trunk ports, and they only need to trunk VLAN 266 because it is the only VLAN the upstream switches see.

On the Nexus 5K, enter these commands, and check uplink configuration:

1. Add the VLAN as primary:

```
Nexus5000-5(config-vlan)# vlan 266
```

2. Make sure that all uplinks are configured in order to trunk the VLANs:

```
interface Ethernet1/1description Connection to 4900switchport mode trunkspeed 1000interface Ethernet1/3description Connection to FIB Port 5switchport mode trunkspeed 1000interface Ethernet1/4description Connection to FIA port 5switchport mode trunkspeed 1000
```

On the 4900 switch, take these steps:

1. Create the VLANs used as primary on the N1K.
2. Trunk all interfaces to and from the 4900 switch so that the VLAN is passed.

On the upstream router, create a subinterface for the VLAN 266 only. At this level, the requirements depend upon the network configuration that you use.

1. interface GigabitEthernet0/1.1
2. encapsulation dot1Q 266
3. IP address 209.165.200.225 255.255.255.224

Configuration of N1K

This procedure describes how to configure the N1K.

1. Create and associate the VLANs:

```
Switch(config)# vlan 166
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# vlan 266
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association 166
```

2. Create an uplink port-profile for the PVLAN traffic with the promiscuous port noted:

```
Switch(config)#port-profile type ethernet pvlan_uplink
Switch(config-port-prof)# vmware port-group
Switch(config-port-prof)# switchport mode private-vlan trunk promiscuous
Switch(config-port-prof)# switchport private-vlan trunk allowed vlan 266 <-- Only need to allow the primary VLAN
Switch(config-port-prof)# switchport private-vlan mapping trunk 266 166 <-- The VLANs must be mapped at this point
Switch(config-port-prof)# channel-group auto mode on mac-pinning
Switch(config-port-prof)# no shut
Switch(config-port-prof)# state enabled
```

3. Create the port-group for the isolated VLAN; create a PVLAN host port with the host

association for the primary and isolated VLANs:

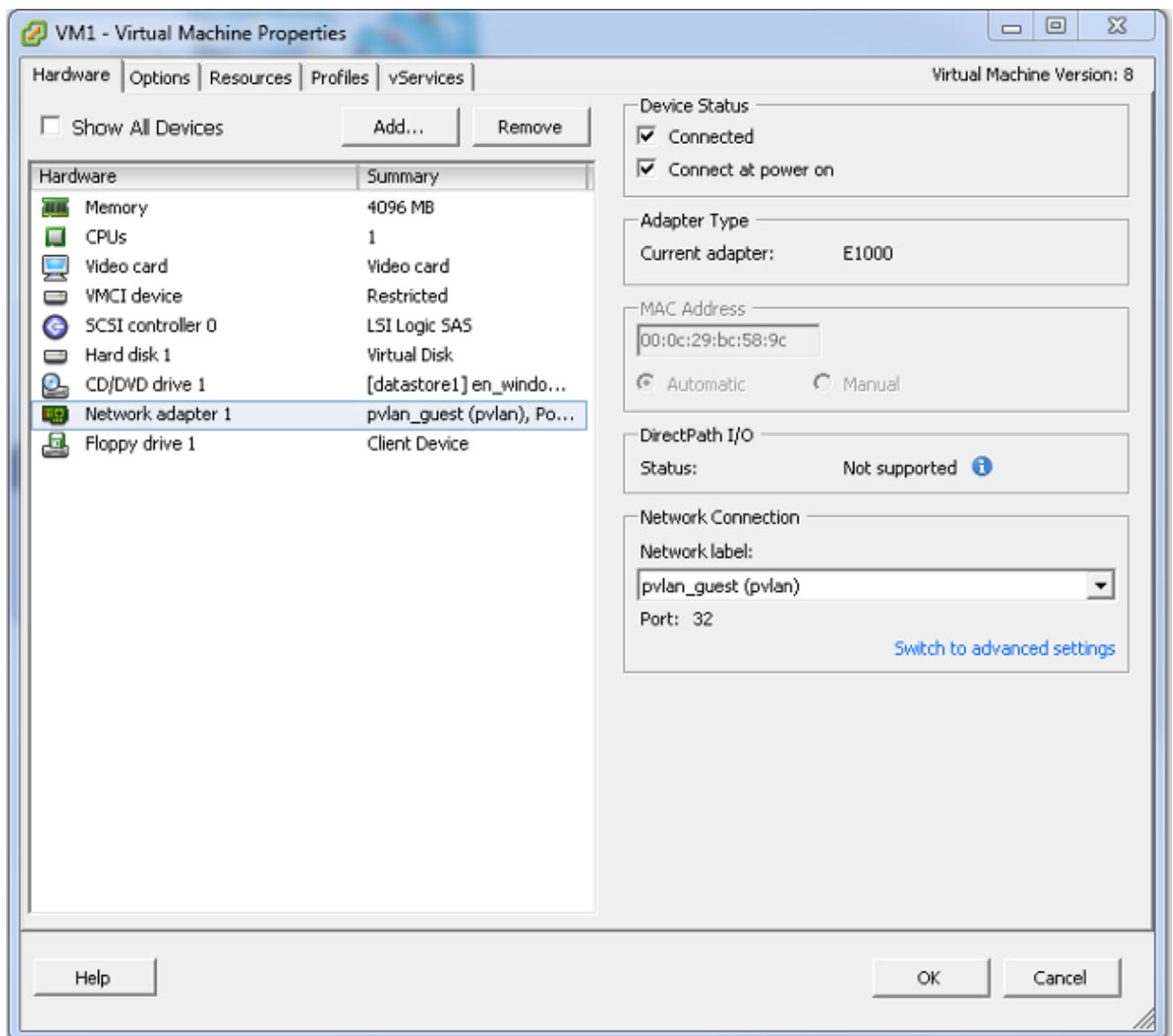
```
Switch(config)# port-profile type vethernet pvlan_guest
Switch(config-port-prof)# vmware port-group
Switch(config-port-prof)# switchport mode private-vlan host
Switch(config-port-prof)# switchport private-vlan host-association 266 166
Switch(config-port-prof)# no shut
Switch(config-port-prof)# state enabled
```

4. In the vCenter, add the proper vNIC to the PVLAN uplink. This is the vNIC to which you added the Isolated VLAN under the Configuration in UCS settings.

<input type="checkbox"/>		vmnic3	--	View Details...	Select an uplink port gr...
<input checked="" type="checkbox"/>		vmnic4	pvlan	View Details...	pvlan_uplink
<input type="checkbox"/>		vmnic5	--	View Details...	Select an uplink port gr...

5. Add the VM to the correct port-group.

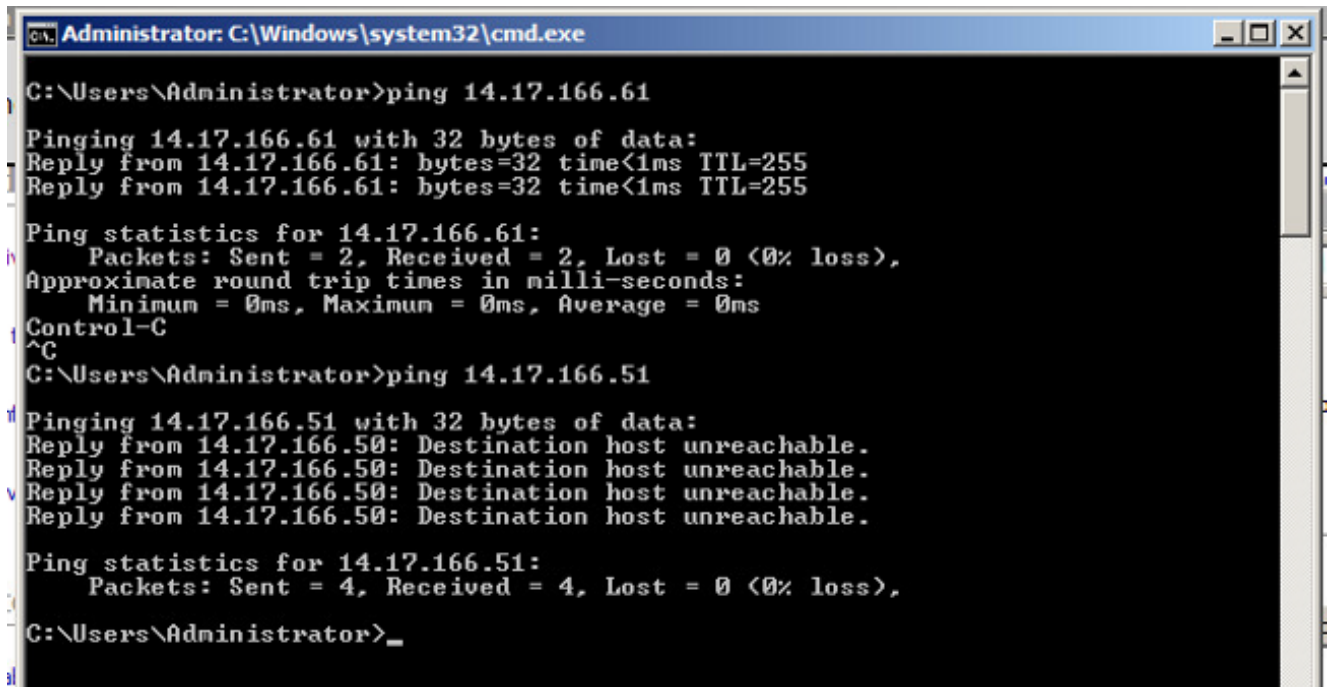
In the Hardware tab, click **Network adapter 1**. Choose **pvlan_guest (pvlan)** for the Network label under Network Connection.



Troubleshooting

This procedure describes how to test the configuration.

1. Run pings to other systems configured in the port-group as well as the router or other device at the promiscuous port. Pings to the device past the promiscuous port should work, while those to other devices in the isolated VLAN should fail.



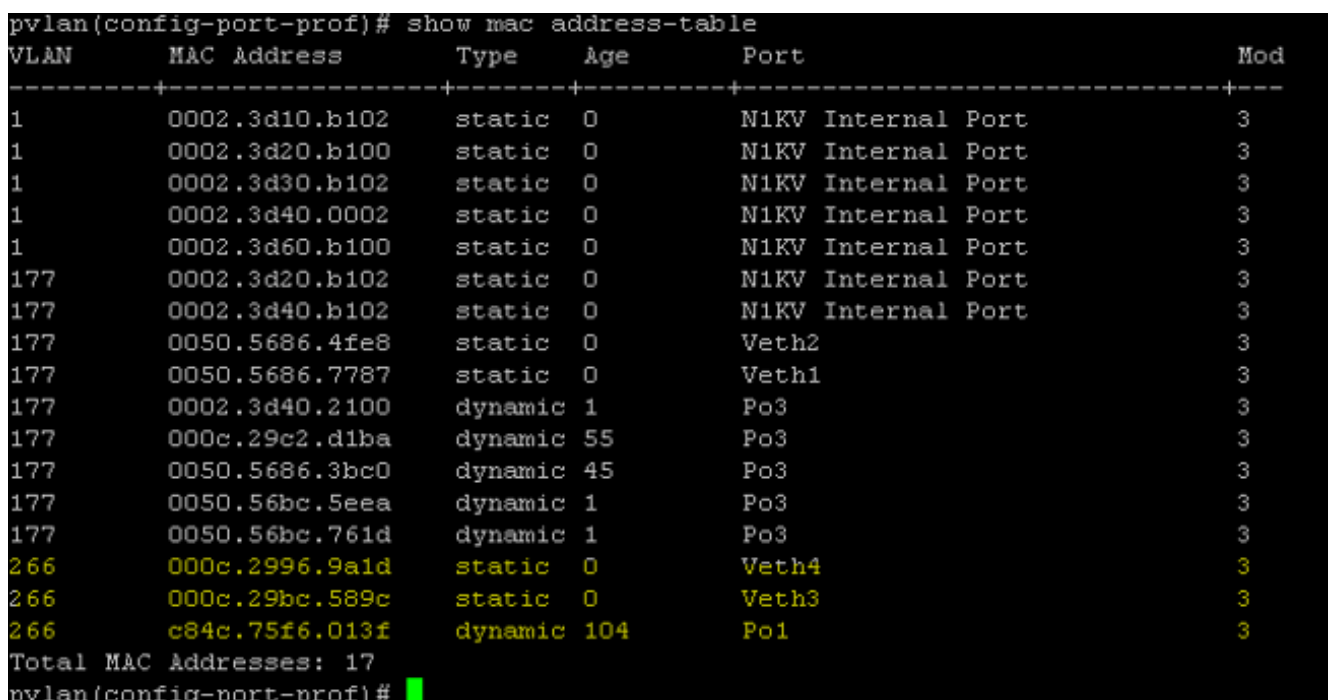
```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping 14.17.166.61
Pinging 14.17.166.61 with 32 bytes of data:
Reply from 14.17.166.61: bytes=32 time<1ms TTL=255
Reply from 14.17.166.61: bytes=32 time<1ms TTL=255

Ping statistics for 14.17.166.61:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\Administrator>ping 14.17.166.51
Pinging 14.17.166.51 with 32 bytes of data:
Reply from 14.17.166.50: Destination host unreachable.
Reply from 14.17.166.50: Destination host unreachable.
Reply from 14.17.166.50: Destination host unreachable.
Reply from 14.17.166.50: Destination host unreachable.

Ping statistics for 14.17.166.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
C:\Users\Administrator>_
```

2. On the N1K, the VMs are listed on the primary VLAN; this occurs because you are in PVLAN host ports that are associated to the PVLAN. Also note that you learn the upstream device from the port channel and that the upstream device is learned on the primary VLAN as well.

In this screen shot, the two devices on Veth3 and Veth 4 are the VMs. The device on Po1 is the upstream device that is past the promiscuous port.



```
pvlan(config-port-prof)# show mac address-table
VLAN      MAC Address      Type      Age      Port      Mod
-----+-----+-----+-----+-----+-----
1         0002.3d10.b102   static    0        N1KV Internal Port  3
1         0002.3d20.b100   static    0        N1KV Internal Port  3
1         0002.3d30.b102   static    0        N1KV Internal Port  3
1         0002.3d40.0002   static    0        N1KV Internal Port  3
1         0002.3d60.b100   static    0        N1KV Internal Port  3
177       0002.3d20.b102   static    0        N1KV Internal Port  3
177       0002.3d40.b102   static    0        N1KV Internal Port  3
177       0050.5686.4fe8   static    0        Veth2         3
177       0050.5686.7787   static    0        Veth1         3
177       0002.3d40.2100   dynamic   1        Po3           3
177       000c.29c2.d1ba   dynamic   55       Po3           3
177       0050.5686.3bc0   dynamic   45       Po3           3
177       0050.56bc.5eea   dynamic   1        Po3           3
177       0050.56bc.761d   dynamic   1        Po3           3
266       000c.2996.9a1d   static    0        Veth4         3
266       000c.29bc.589c   static    0        Veth3         3
266       c84c.75f6.013f   dynamic   104     Po1           3
Total MAC Addresses: 17
pvlan(config-port-prof)#
```

3. On the UCS system, you should be learning all MACs, for this communication, in the primary VLAN you use on the N1K. You should not be learning the upstream here:

```
F340-31-9-1-B(nxos)# show mac address-table
Legend:
    * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
    age - seconds since last seen,+ - primary entry using vPC Peer-Link
VLAN      MAC Address      Type      age      Secure NTFY      Ports
-----+-----+-----+-----+-----+-----
* 266     000c.2996.9a1d   dynamic   100      F      F      Veth1491
* 266     000c.29bc.589c   dynamic   180      F      F      Veth1491
* 177     0025.b581.9a3f   dynamic   0        F      F      Veth1402
* 177     0025.b585.100a   dynamic   350      F      F      Veth1424
* 177     0050.566b.01ad   dynamic   380      F      F      Veth1402
* 126     0025.b581.999e   static    0        F      F      Veth1392
* 124     0023.04c6.dbe2   dynamic   0        F      F      Veth1404
```

4. On the Nexus 5K, all MACs are in the primary VLAN you selected:

```
F340.11.13-Nexus5000-5# show mac address-table
Legend:
    * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
    age - seconds since last seen,+ - primary entry using vPC Peer-Link
VLAN      MAC Address      Type      age      Secure NTFY      Ports
-----+-----+-----+-----+-----+-----
* 266     000c.2996.9a1d   dynamic   90       F      F      Eth1/4
* 266     000c.29bc.589c   dynamic   20       F      F      Eth1/4
* 266     c84c.75f6.013f   dynamic   100      F      F      Eth1/1
F340.11.13-Nexus5000-5#
```

5. On the 4900 switch, everything is on the primary VLAN you have selected:

```
Switch#show mac address-table
Unicast Entries
vlan      mac address      type      protocols      port
-----+-----+-----+-----+-----+-----
266       000c.2996.9a1d   dynamic   ip,ipx,assigned,other GigabitEthernet1/1
266       000c.29bc.589c   dynamic   ip,ipx,assigned,other GigabitEthernet1/1
266       c84c.75f6.013f   static    ip,ipx,assigned,other Switch

Multicast Entries
vlan      mac address      type      ports
-----+-----+-----+-----+-----
1         0100.0ccc.ccce   system    Gi1/1
1         ffff.ffff.ffff   system    Gi1/1
166       ffff.ffff.ffff   system    Gi1/1
266       ffff.ffff.ffff   system    Gi1/1,Gi1/2,Switch
Switch#
```

Community PVLAN on N1K with Promiscuous Port on the N1K Uplink Port-Profile

This is the only supported configuration for community VLAN with UCS.

This configuration is the same as that set up in the [Isolated PVLAN on N1K with Promiscuous Port](#)

[on the N1K Uplink Port-Profile](#) section. The only difference between community and isolated is the configuration of the PVLAN.

In order to configure the N1K, create and associate the VLANs as you did on the Nexus 5K:

```
Switch(config)# vlan 166
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# vlan 266
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association 16
```

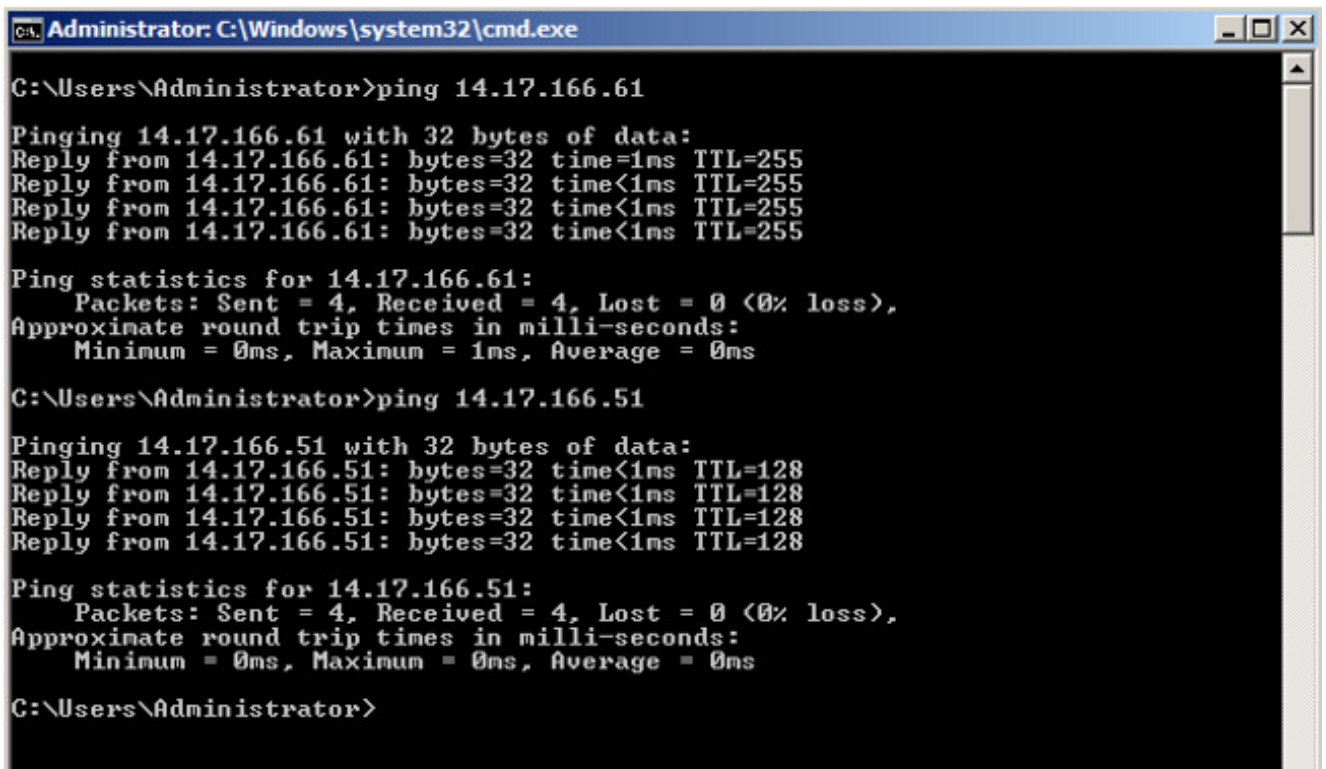
All other configuration is the same as the isolated PVLAN on N1K with promiscuous port on the N1K uplink port-profile.

Once this is configured, you can communicate with all VMs connected to the vEthernet port-profile used for your PVLAN.

Troubleshooting

This procedure describes how to test the configuration.

1. Run pings to other systems configured in the port-group as well as the router or other device at the promiscuous port. Pings past the promiscuous port and to other systems in the community should work.



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping 14.17.166.61
Pinging 14.17.166.61 with 32 bytes of data:
Reply from 14.17.166.61: bytes=32 time<1ms TTL=255
Reply from 14.17.166.61: bytes=32 time<1ms TTL=255
Reply from 14.17.166.61: bytes=32 time<1ms TTL=255
Reply from 14.17.166.61: bytes=32 time<1ms TTL=255

Ping statistics for 14.17.166.61:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>ping 14.17.166.51
Pinging 14.17.166.51 with 32 bytes of data:
Reply from 14.17.166.51: bytes=32 time<1ms TTL=128
Reply from 14.17.166.51: bytes=32 time<1ms TTL=128
Reply from 14.17.166.51: bytes=32 time<1ms TTL=128
Reply from 14.17.166.51: bytes=32 time<1ms TTL=128

Ping statistics for 14.17.166.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

2. All other troubleshooting is the same as the [isolated PVLAN](#).

Isolated PVLAN and Community PVLAN on VMware DVS Promiscuous Port on the DVS

Because of the configuration issues on both the DVS and the UCS system, PVLANS with DVS and UCS are not supported prior to Version 2.2(2c).

Verify

There are currently no verification procedures available for these configurations.

Troubleshoot

The previous sections provided information you can use in order to troubleshoot your configurations.

The [Output Interpreter Tool](#) ([registered](#) customers only) supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output.