

Configuración de VLAN privada y Cisco UCS anterior a 2.2(2C)

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Teoría](#)

[Implementación de PVLAN en UCS](#)

[Objetivo](#)

[Configurar](#)

[Diagramas de la Red](#)

[PVLAN en vSwitch: PVLAN aislada con puerto promiscuo en un dispositivo ascendente](#)

[Configuración en UCS](#)

[Configuración de dispositivos ascendentes](#)

[Resolución de problemas](#)

[PVLAN aislada en N1K con puerto promiscuo en un dispositivo ascendente](#)

[Configuración en UCS](#)

[Configuración de dispositivos ascendentes](#)

[Configuración de N1K](#)

[Resolución de problemas](#)

[PVLAN aislada en N1K con puerto promiscuo en el perfil de puerto de enlace ascendente N1K](#)

[Configuración en UCS](#)

[Configuración de dispositivos ascendentes](#)

[Configuración de N1K](#)

[Resolución de problemas](#)

[PVLAN de comunidad en N1K con puerto promiscuo en el perfil de puerto de enlace ascendente N1K](#)

[N1K](#)

[Resolución de problemas](#)

[PVLAN aislada y PVLAN de comunidad en el puerto promiscuo VMware DVS en el DVS](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe la compatibilidad con VLAN privada (PVLAN) en Cisco Unified Computing System (UCS), una función introducida en la versión 1.4 de Cisco UCS Manager (UCSM). También detalla las funciones, las advertencias y la configuración cuando se utilizan PVLAN en un entorno UCS.

ESTE DOCUMENTO SE UTILIZA CON LA VERSIÓN 2.2(2C) DE UCSM Y VERSIONES

ANTERIORES. En las versiones posteriores a la versión 2.2(2C), se han realizado cambios en UCSM y se admite el DVS de ESXi. También hay cambios en cómo funciona el etiquetado para la NIC PVLAN.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- UCS
- Cisco Nexus 1000 V (N1K)
- VMware
- Switching de capa 2 (L2)

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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.

Antecedentes

Teoría

Una VLAN privada es una VLAN configurada para el aislamiento de L2 de otros puertos dentro de la misma VLAN privada. Los puertos que pertenecen a una PVLAN están asociados con un conjunto común de VLAN de soporte, que se utilizan para crear la estructura PVLAN.

Hay tres tipos de puertos PVLAN:

- Un **puerto promiscuo** se comunica con todos los demás puertos PVLAN y es el puerto utilizado para comunicarse con los dispositivos fuera de la PVLAN.
- Un **puerto aislado** tiene separación L2 completa (incluyendo broadcasts) de otros puertos dentro de la misma PVLAN con la excepción del puerto promiscuo.
- Un **puerto de comunidad** puede comunicarse con otros puertos en la misma PVLAN así como con el puerto promiscuo. Los puertos comunitarios se aíslan en L2 de los puertos de otras comunidades o de los puertos PVLAN aislados. Las transmisiones sólo se propagan a otros puertos de la comunidad y al puerto promiscuo.

Consulte [RFC 5517, VLAN privadas de Cisco Systems: Seguridad escalable en un entorno de varios clientes](#) para comprender la teoría, el funcionamiento y los conceptos de las PVLAN.

Implementación de PVLAN en UCS

UCS se asemeja mucho a la arquitectura de Nexus 5000/2000, en la que Nexus 5000 es similar a UCS 6100 y Nexus 2000 a los Fabric Extenders UCS 2104.

Muchas limitaciones de la funcionalidad de PVLAN en UCS se deben a las limitaciones encontradas en la implementación de Nexus 5000/2000.

Los puntos importantes que hay que recordar son:

- UCS sólo admite puertos aislados. Con el N1K incorporado, puede utilizar VLAN de comunidad, pero el puerto promiscuo también debe estar en el N1K.
- No hay soporte para puertos/troncales promiscuos, puertos/troncales de comunidad o troncales aislados.
- Los puertos promiscuos deben estar fuera del dominio UCS, como un switch/router ascendente o un N1K descendente.

Objetivo

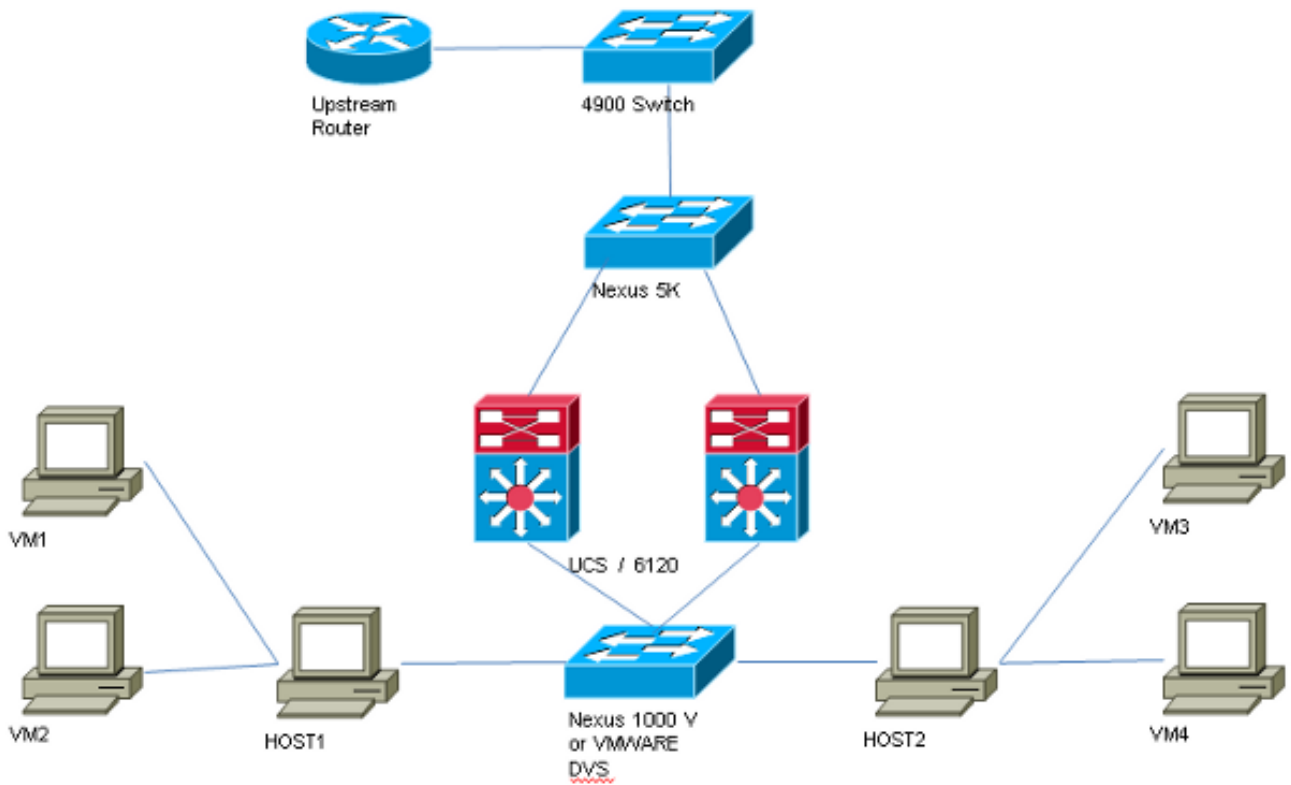
Este documento abarca varias configuraciones diferentes disponibles para PVLAN con UCS:

1. PVLAN aislada con puerto promiscuo en un dispositivo ascendente.
2. PVLAN aislada en N1K con puerto promiscuo en un dispositivo ascendente.
3. PVLAN aislada en N1K con puerto promiscuo en el perfil de puerto de enlace ascendente N1K
4. PVLAN de comunidad en N1K con puerto promiscuo en el perfil de puerto de link ascendente N1K.
5. PVLAN aislada en el puerto promiscuo VMware Distributed Virtual Switch (DVS) en el DVS.
6. PVLAN de comunidad en el puerto promiscuo del switch DVS de VMware en el DVS.

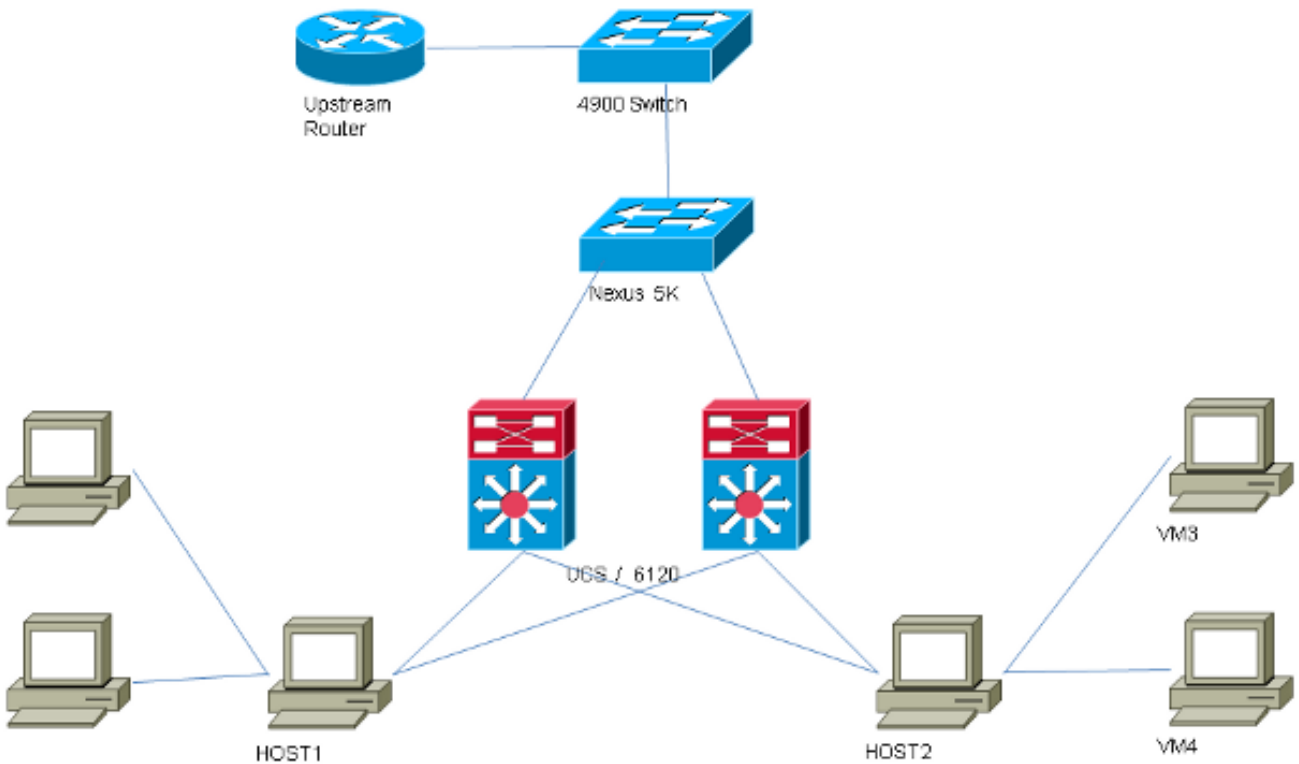
Configurar

Diagramas de la Red

La topología para todos los ejemplos con un switch distribuido es:



La topología para todos los ejemplos sin switch distribuido es:



PVLAN en vSwitch: PVLAN aislada con puerto promiscuo en un dispositivo ascendente

En esta configuración, está pasando el tráfico PVLAN a través de UCS a un puerto promiscuo que

está en flujo ascendente. Debido a que no puede enviar VLAN primarias y secundarias en el mismo vNIC, necesita un vNIC para cada blade para cada PVLAN, para llevar el tráfico PVLAN.

Configuración en UCS

Este procedimiento describe cómo crear las VLAN principales y las que se encuentran aisladas.

Nota: Este ejemplo utiliza 266 como primario y 166 como aislado; el sitio determinará los ID de VLAN.

1. Para crear la VLAN principal, haga clic en **Primary** como el Tipo de uso compartido e ingrese un **ID de VLAN** de 266:

The screenshot displays the configuration interface for a VLAN. The 'Properties' section is at the top, and the 'Secondary VLANs' section is below it.

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

Filter | Export | Print

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

2. Para crear la VLAN aislada, haga clic en **Aislado** como tipo de uso compartido, ingrese un **ID de VLAN** de 166 y elija **VLAN 266 (266)** como VLAN principal:

Properties

Name: **166** VLAN ID: **166**

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

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

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

Sharing Type: None Primary Isolated Primary VLAN: **VLAN 266 (266)**

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: **<not set>**

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

3. Para agregar la VLAN a la vNIC, haga clic en la casilla de verificación **Select** para VLAN 166 y haga clic en el botón de radio asociado **Native VLAN**.

Modify VLANs

Modify VLANs

VLANs

| Select | Name | Native VLAN |
|-------------------------------------|--------------|----------------------------------|
| <input type="checkbox"/> | default | <input type="radio"/> |
| <input type="checkbox"/> | 1233 | <input type="radio"/> |
| <input type="checkbox"/> | 1234 | <input type="radio"/> |
| <input type="checkbox"/> | 124 | <input type="radio"/> |
| <input type="checkbox"/> | 126 | <input type="radio"/> |
| <input checked="" type="checkbox"/> | 166 | <input checked="" type="radio"/> |
| <input type="checkbox"/> | 266 | <input type="radio"/> |
| <input type="checkbox"/> | 777 | <input type="radio"/> |
| <input type="checkbox"/> | Tbeaudre_177 | <input type="radio"/> |
| <input type="checkbox"/> | Tbeaudre_277 | <input type="radio"/> |
| <input type="checkbox"/> | Tbeaudre_377 | <input type="radio"/> |
| <input type="checkbox"/> | vlan_51 | <input type="radio"/> |

OK Cancel

Sólo se agrega la VLAN aislada, se debe establecer como primaria y sólo puede haber una para cada vNIC. Debido a que la VLAN nativa se define aquí, no configure el etiquetado de VLAN en los grupos de puertos VMware.

Configuración de dispositivos ascendentes

Estos procedimientos describen cómo configurar un Nexus 5K para pasar la PVLAN a un switch ascendente 4900 donde está el puerto promiscuo. Aunque esto puede no ser necesario en todos los entornos, utilice esta configuración en el caso de que deba pasar la PVLAN a través de otro switch.

En Nexus 5K, ingrese estos comandos y verifique la configuración del link ascendente:

1. Active la función PVLAN:

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

2. Agregue las VLAN como principales y aisladas:

```
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. Asocie VLAN 266 con la VLAN 166 aislada:

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

4. Asegúrese de que todos los uplinks estén configurados para hacer un trunk de las VLAN:

```
interfaz Ethernet1/1description Connection to 4900switchport mode trunkspeed
1000interface Ethernet1/3descripción Conexión al puerto FIB 5switchport mode trunkspeed
1000interface Ethernet1/4descripción Conexión al puerto FIA 5switchport mode trunkspeed
1000
```

En el switch 4900, tome estos pasos y configure el puerto promiscuo. La PVLAN termina en el puerto promiscuo.

1. Active la función PVLAN si es necesario.
2. Cree y asocie las VLAN tal como se hace en Nexus 5K.
3. Cree el puerto promiscuo en el puerto de salida del switch 4900. A partir de este punto, los paquetes de VLAN 166 se ven en VLAN 266 en este caso.

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

En el router ascendente, cree una subinterfaz sólo para la VLAN 266. En este nivel, los requisitos dependen de la configuración de red que esté utilizando:

1. interface GigabitEthernet0/1.1

2. encapsulation dot1Q 266
3. IP address 209.165.200.225 255.255.255.224

Resolución de problemas

Este procedimiento describe cómo probar la configuración.

1. Configure la interfaz virtual del switch (SVI) en cada switch, lo que le permite hacer ping a la SVI desde la 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. Verifique las tablas de direcciones MAC para ver dónde se está aprendiendo su MAC. En todos los switches, el MAC debe estar en la VLAN aislada excepto en el switch con el puerto promiscuo. En el switch promiscuo, observe que el MAC está en la VLAN principal.

En Fabric Interconnect, la dirección MAC 0050.56bd.7bef se aprende en Veth1491:

```
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.29d2.495a    dynamic   80       F      F      Veth1491
* 166      0025.b581.991e    static    0        F      F      Veth1491
* 166      0050.56bd.7bef    dynamic   20       F      F      Veth1491
* 266      0025.b581.9a9d    static    0        F      F      Veth1475
* 266      0050.56bd.53b6    dynamic   170      F      F      Veth1475
* 177      000c.29d2.4950    dynamic   10       F      F      Veth1480
* 177      0025.b581.9a3f    dynamic   10       F      F      Veth1402
* 177      0025.b581.9a4d    dynamic   10       F      F      Veth1480
* 177      0025.b585.100a    dynamic   980     F      F      Veth1424
* 177      0050.566b.01ad    dynamic   980     F      F      Veth1402
* 177      0050.566c.d835    dynamic   10       F      F      Veth1472
* 126      0025.b581.999e    static    0        F      F      Veth1392
* 124      0023.04c6.dbe2    dynamic   10       F      F      Veth1404
* 124      0023.04c6.dbe3    static    0        F      F      Veth1404
* 4044     0024.971f.6bc2    dynamic   0        F      F      Eth2/1/9
* 4044     0026.5108.0b2c    dynamic   0        F      F      Eth1/1/9
* 4044     0026.5108.cac2    dynamic   0        F      F      Eth1/1/9
--More--
```

En el Nexus 5K, la dirección MAC 0050.56bd.7bef se aprende en 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#

```

En el switch 4900, la dirección MAC 0050.56bd.7bef se aprende en 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.cccc   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--

```

En esta configuración, los sistemas en esta VLAN aislada no pueden comunicarse entre sí, pero pueden comunicarse con otros sistemas a través del puerto promiscuo en el switch 4900. Un problema es cómo configurar los dispositivos de descarga. En este caso, está utilizando VMware y dos hosts.

Recuerde que debe utilizar un vNIC para cada PVLAN. Estos vNIC se presentan a VMware vSphere ESXi y, a continuación, puede crear grupos de puertos y tener invitados a estos grupos

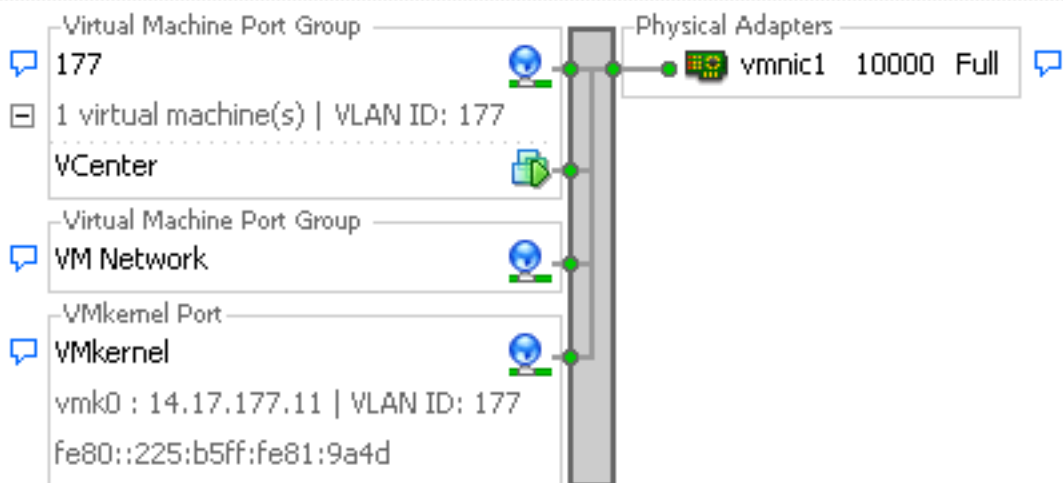
de puertos.

Si se agregan dos sistemas al mismo grupo de puertos en el mismo switch, pueden comunicarse entre sí porque sus comunicaciones se conmutan localmente en el vSwitch. En este sistema, hay dos blades con dos hosts cada uno.

En el primer sistema, se han creado dos grupos de puertos diferentes: uno llamado 166 y otro llamado 166A. Cada uno se conecta a una sola NIC, que se configura en la VLAN aislada en UCS. Actualmente, sólo hay un invitado para cada grupo de puertos. En este caso, debido a que se separan en ESXi, no pueden comunicarse entre sí.

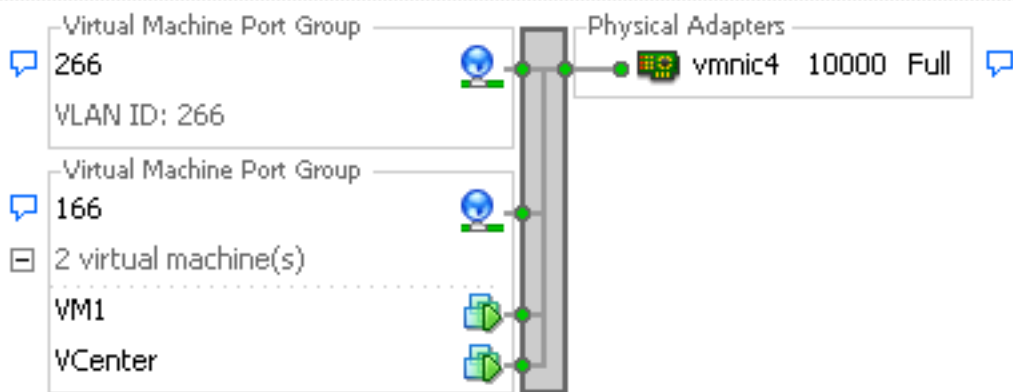
Standard Switch: vSwitch0

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



Standard Switch: vSwitch1

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



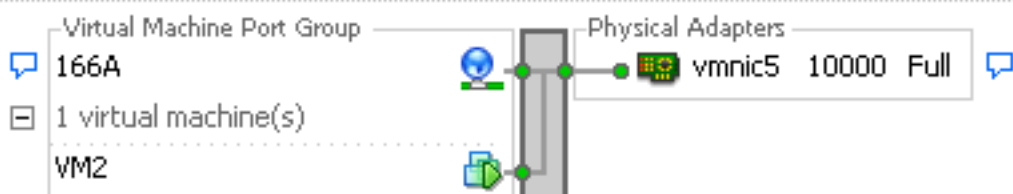
Standard Switch: vSwitch2

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



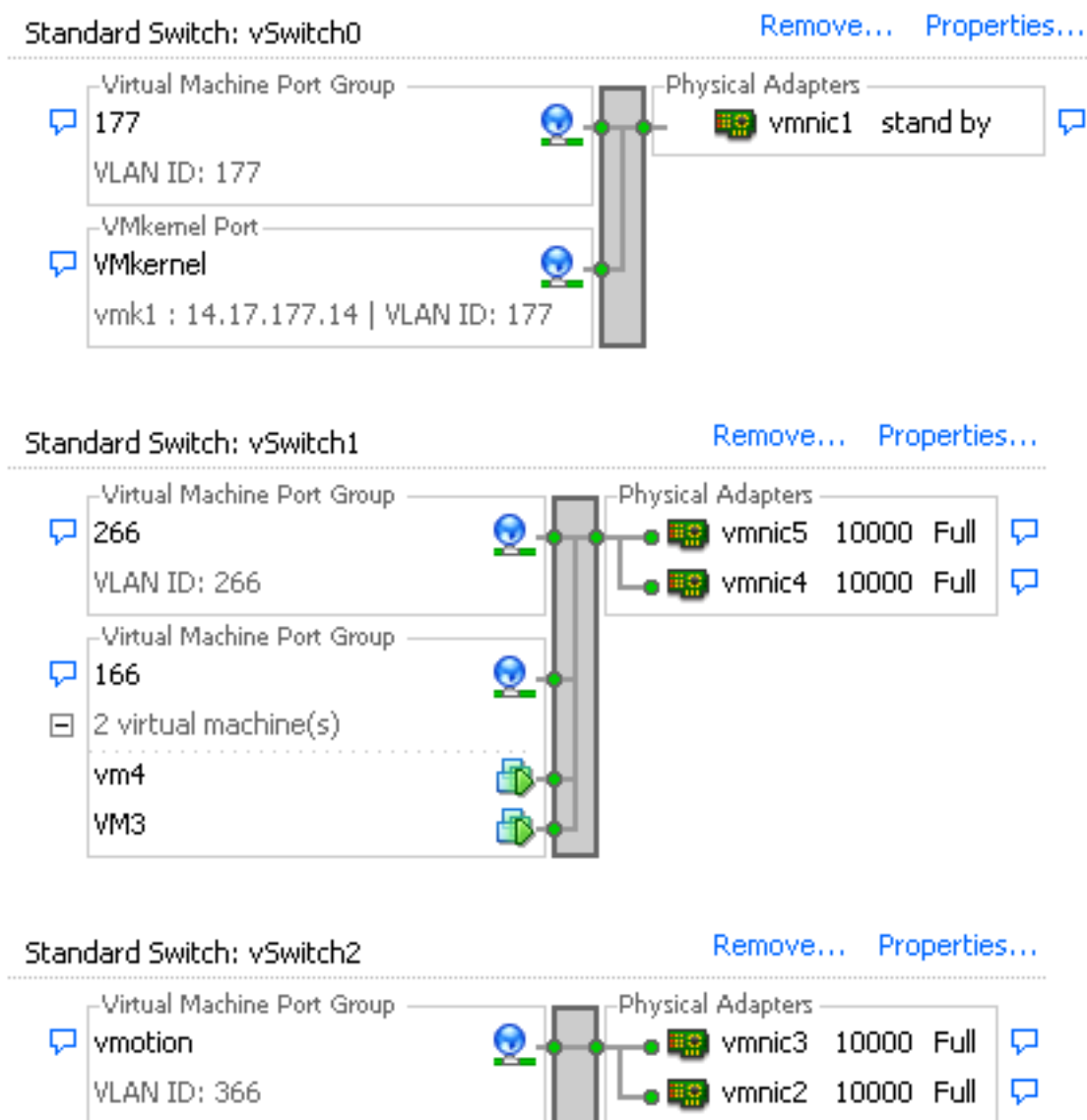
Standard Switch: vSwitch3

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



En el segundo sistema, hay sólo un grupo de puertos llamado 166. Hay dos invitados en este grupo de puertos. En esta configuración, VM3 y VM4 pueden comunicarse entre sí aunque no desee que esto suceda. Para corregir esto, debe configurar una única NIC para cada máquina virtual (VM) que se encuentre en la VLAN aislada y, a continuación, crear un grupo de puertos conectado a esa vNIC. Una vez configurado, coloque sólo un invitado en el grupo de puertos.

Este no es un problema con una instalación de Windows sin software específico porque no tiene estos vSwitches subyacentes.



PVLAN aislada en N1K con puerto promiscuo en un dispositivo ascendente

En esta configuración, está pasando el tráfico PVLAN a través de un N1K y luego el UCS a un puerto promiscuo ascendente. Debido a que no puede enviar VLAN primarias y secundarias en el mismo vNIC, necesita un vNIC para cada link ascendente PVLAN para llevar el tráfico PVLAN.

Configuración en UCS

Este procedimiento describe cómo crear las VLAN principales y las que se encuentran aisladas.

Nota: Este ejemplo utiliza 266 como primario y 166 como aislado; el sitio determinará los ID de VLAN.

1. Para crear la VLAN principal, haga clic en **Primary** como el Tipo de uso compartido:

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 | <input type="button" value="↑"/> |

2. Para crear la VLAN aislada, haga clic en **Aislado** como Tipo de uso compartido:

Properties

| | |
|--------------------------|---|
| Name: 166 | VLAN ID: <input type="text" value="166"/> |
| Native VLAN: No | Fabric ID: Dual |
| Network Type: Lan | If Type: Virtual |
| Locale: External | Transport Type: Ether |

Sharing Type: None Primary Isolated Primary VLAN:

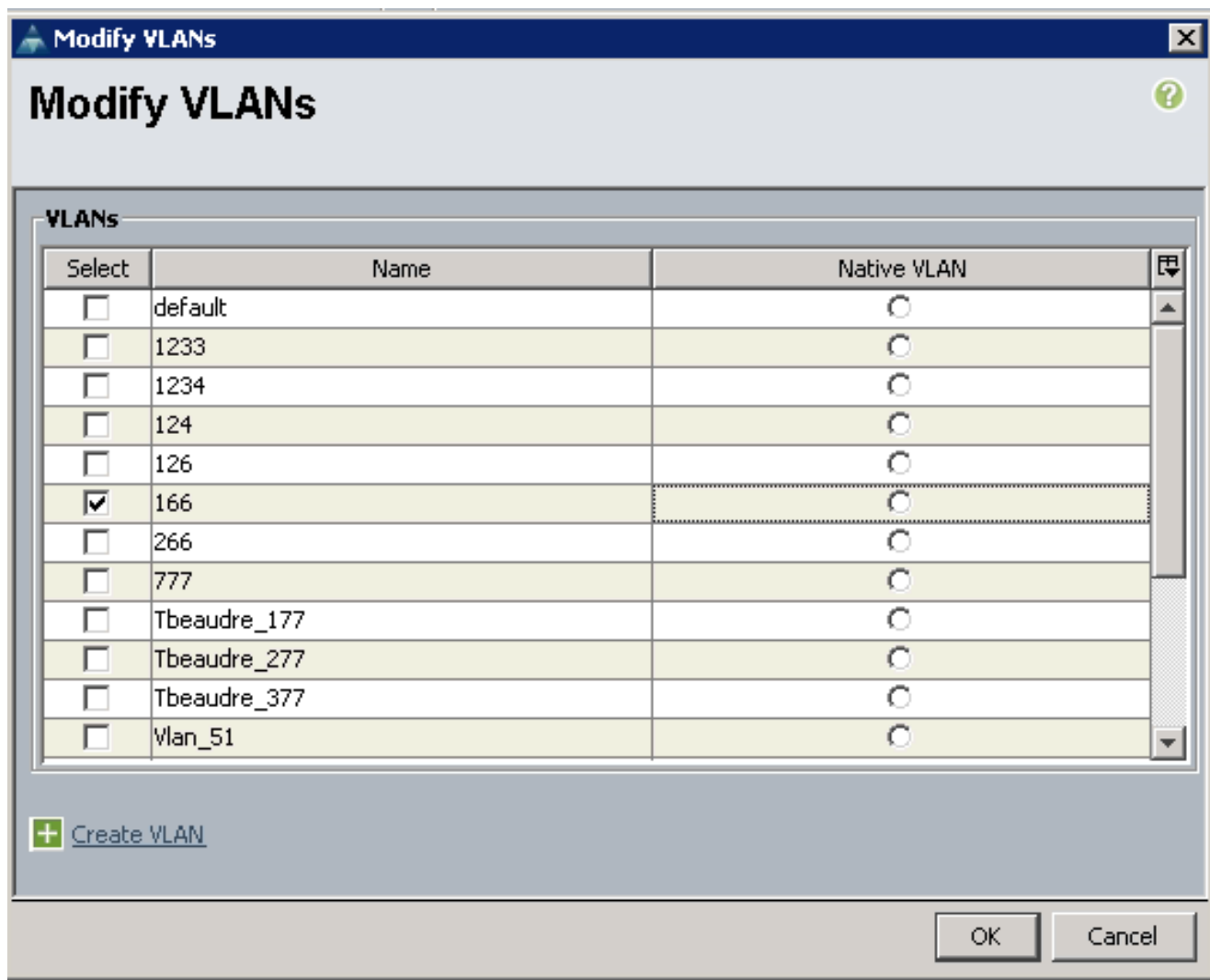
Primary VLAN Properties

| | |
|--------------------------|------------------------------|
| 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. Para agregar la VLAN a la vNIC, haga clic en la casilla **Select** para VLAN 166. La VLAN 166 no tiene la VLAN nativa seleccionada.



Sólo se agrega la VLAN aislada, no se debe establecer como nativa y sólo puede haber una para cada vNIC. Debido a que la VLAN nativa no se define aquí, etiquete la VLAN nativa en el N1K. La opción para etiquetar una VLAN nativa no está disponible en el DVS de VMware, por lo que no se admite en el DVS.

Configuración de dispositivos ascendentes

Estos procedimientos describen cómo configurar un Nexus 5K para pasar la PVLAN a un switch ascendente 4900 donde está el puerto promiscuo. Aunque esto puede no ser necesario en todos los entornos, utilice esta configuración en el caso de que deba pasar la PVLAN a través de otro switch.

En Nexus 5K, ingrese estos comandos y verifique la configuración del link ascendente:

1. Active la función PVLAN:

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

2. Agregue las VLAN como principales y aisladas:

```
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. Asocie VLAN 266 con la VLAN 166 aislada:

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

4. Asegúrese de que todos los uplinks estén configurados para hacer un trunk de las VLAN:

```
interfaz Ethernet1/1description Connection to 4900switchport mode trunkspeed
1000interface Ethernet1/3descripción Conexión al puerto FIB 5switchport mode trunkspeed
1000interface Ethernet1/4descripción Conexión al puerto FIA 5switchport mode trunkspeed
1000
```

En el switch 4900, tome estos pasos y configure el puerto promiscuo. La PVLAN termina en el puerto promiscuo.

1. Active la función PVLAN si es necesario.
2. Cree y asocie las VLAN tal como se hace en Nexus 5K.
3. Cree el puerto promiscuo en el puerto de salida del switch 4900. A partir de este punto, los paquetes de VLAN 166 se ven en VLAN 266 en este caso.

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

En el router ascendente, cree una subinterfaz sólo para la VLAN 266. En este nivel, los requisitos dependen de la configuración de red que utilice:

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

Configuración de N1K

Este procedimiento describe cómo configurar el N1K como un trunk estándar, no un trunk PVLAN.

1. Cree y asocie las VLAN tal como se hace en Nexus 5K. Refiérase a la sección [Configuración de Dispositivos Ascendentes](#) para obtener más información.
2. Cree un perfil de puerto de enlace ascendente para el tráfico PVLAN:

```
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. Cree el grupo de puertos para la VLAN aislada; cree un puerto de host PVLAN con la asociación de host para las VLAN principales y aisladas:


```

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

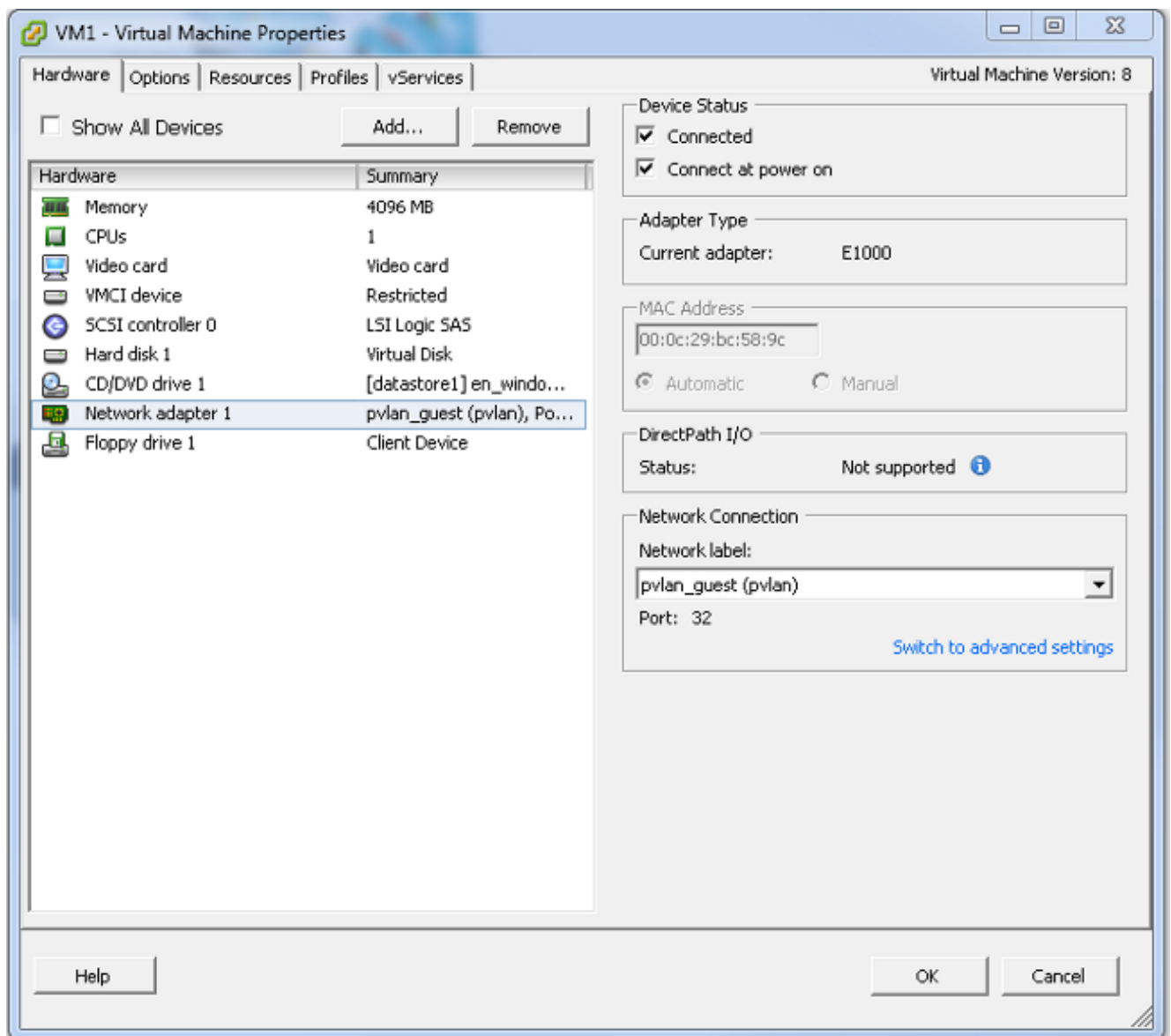
```

- En el vCenter, agregue el vNIC adecuado al enlace ascendente PVLAN. Ésta es la vNIC a la que agregó la VLAN aislada en la configuración en UCS.

| | | | | | |
|-------------------------------------|---|--------|-------|---------------------------------|-----------------------------|
| <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... |

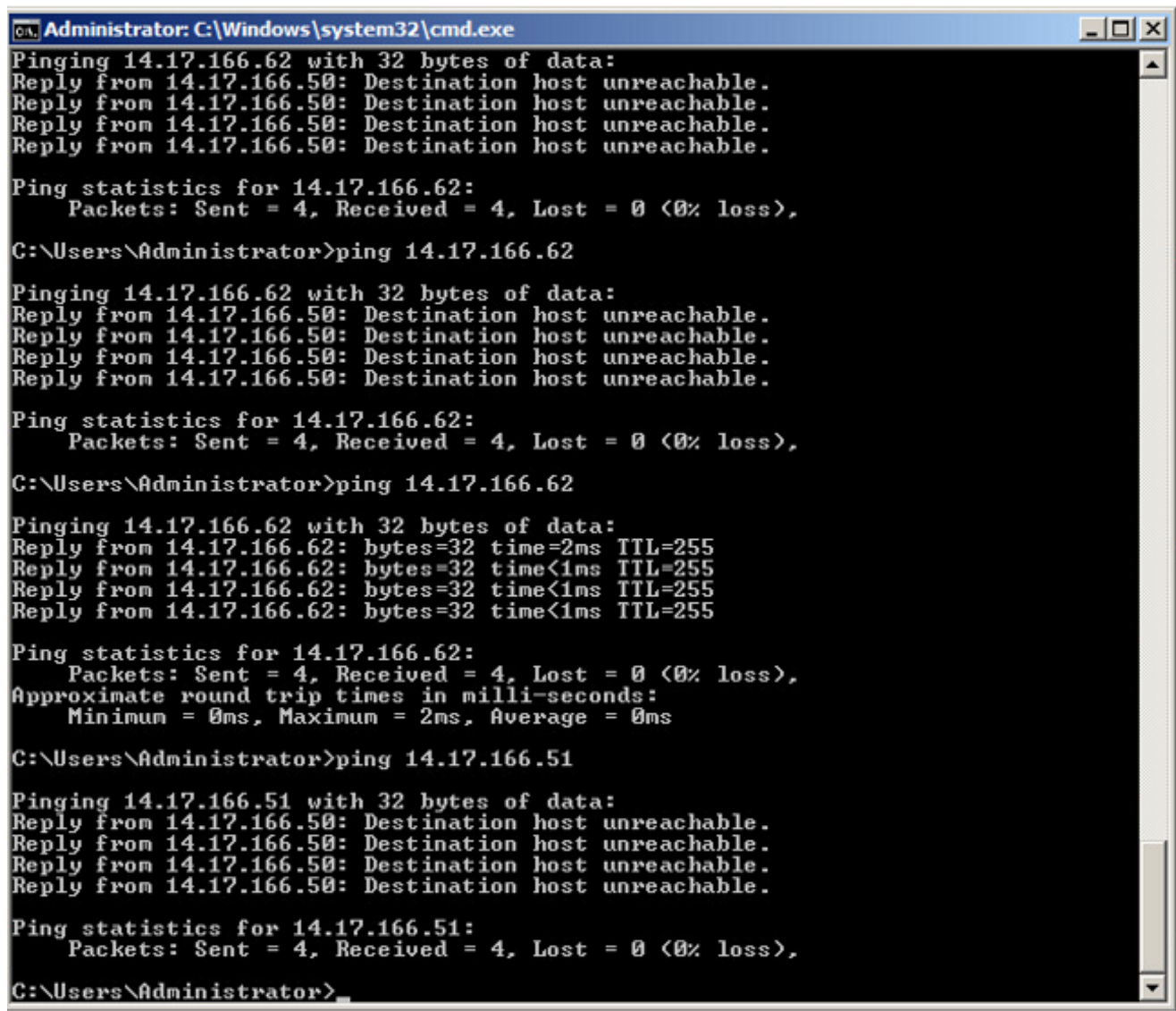
- Agregue la VM al grupo de puertos correcto:

En la ficha Hardware, haga clic en **Network adapter 1**. Elija **pvlan_guest (pvlan)** para la etiqueta Red en Conexión de Red:



Este procedimiento describe cómo probar la configuración.

1. Ejecute pings a otros sistemas configurados en el grupo de puertos, así como al router u otro dispositivo en el puerto promiscuo. Los ping al dispositivo que se encuentra más allá del puerto promiscuo deben funcionar, mientras que los que se dirigen a otros dispositivos en la VLAN aislada deben fallar.



```
Administrator: C:\Windows\system32\cmd.exe
Pinging 14.17.166.62 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 14.17.166.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Administrator>ping 14.17.166.62

Pinging 14.17.166.62 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 14.17.166.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Administrator>ping 14.17.166.62

Pinging 14.17.166.62 with 32 bytes of data:
Reply from 14.17.166.62: bytes=32 time=2ms TTL=255
Reply from 14.17.166.62: bytes=32 time<1ms TTL=255
Reply from 14.17.166.62: bytes=32 time<1ms TTL=255
Reply from 14.17.166.62: bytes=32 time<1ms TTL=255

Ping statistics for 14.17.166.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\Administrator>ping 14.17.166.51

Pinging 14.17.166.51 with 32 bytes of data:
Reply from 14.17.166.50: 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. En el N1K, las VM se enumeran en la VLAN principal; esto ocurre porque está en los puertos de host PVLAN que están asociados a la PVLAN. Debido a cómo se aprenden las VM, asegúrese de no configurar la PVLAN como nativa en el sistema UCS. Tenga en cuenta también que aprende el dispositivo ascendente del canal de puerto y que el dispositivo ascendente también se aprende en la VLAN principal. Esto se debe aprender en este método, que es el motivo por el cual tiene la VLAN principal como la VLAN nativa en el link ascendente PVLAN.

En esta captura de pantalla, los dos dispositivos en Veth3 y Veth 4 son las VM. El dispositivo en Po1 es el router ascendente que está más allá del puerto promiscuo.

```

pvlan# show mac address-table
VLAN      MAC Address      Type      Age      Port
-----+-----+-----+-----+-----+-----+
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   3        Po3                      3
177      000c.29c2.d1ba   dynamic   15       Po3                      3
177      0050.5686.3bc0   dynamic   56       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      0012.8032.86a9   dynamic   214     Po1                      3
Total MAC Addresses: 17
pvlan#

```

3. En el sistema UCS, debería estar aprendiendo todas las MAC, para esta comunicación, en la VLAN aislada. No debería ver el flujo ascendente aquí:

```

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

```

4. En Nexus 5K, las dos VM están en la VLAN aislada, mientras que el dispositivo ascendente está en la VLAN principal:

```

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

```

5. En el switch 4900, donde se encuentra el puerto promiscuo, todo está en la VLAN principal:

| 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.cccc | system | Gi1/1 |
| 1 | ffff.ffff.ffff | system | Gi1/1 |
| 266 | ffff.ffff.ffff | system | Gi1/1,Gi1/2 |

PVLAN aislada en N1K con puerto promiscuo en el perfil de puerto de enlace ascendente N1K

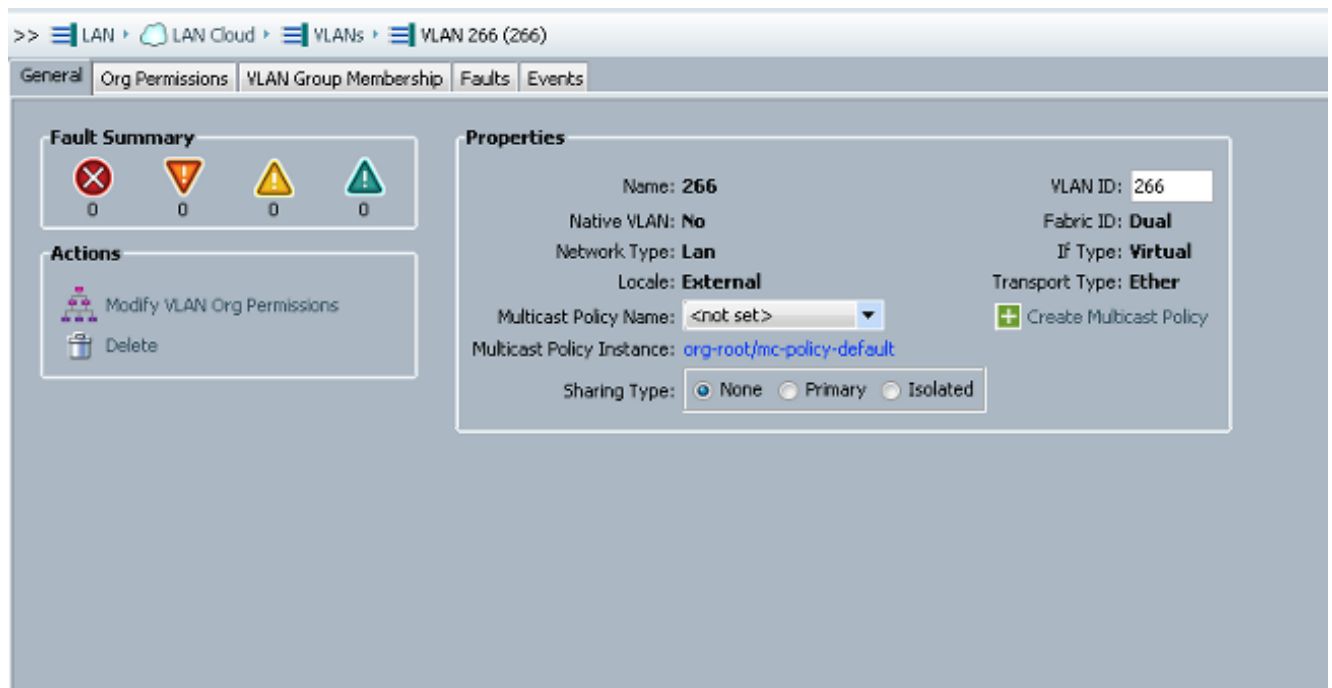
En esta configuración, usted contiene el tráfico PVLAN al N1K con sólo la VLAN principal utilizada ascendente.

Configuración en UCS

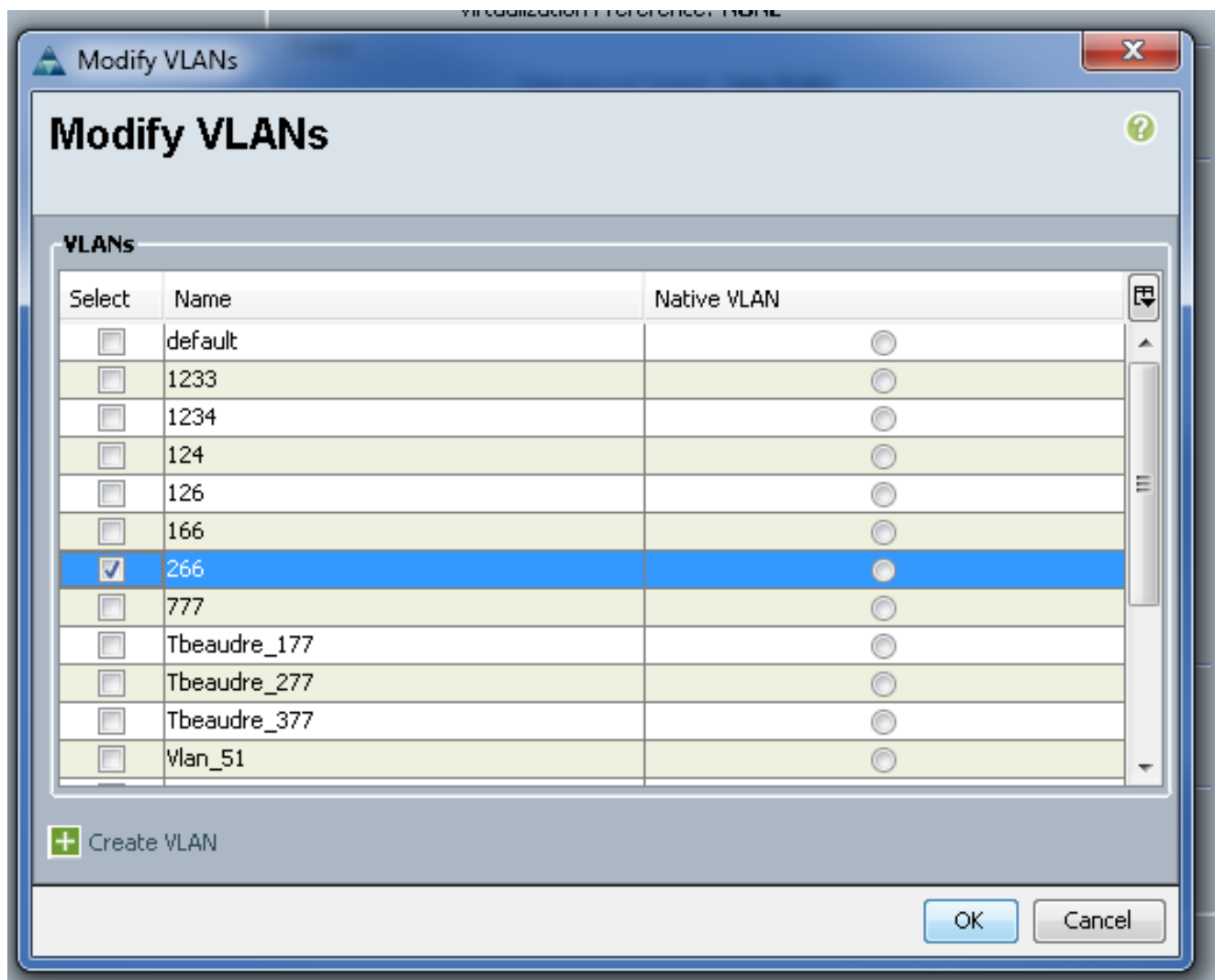
Este procedimiento describe cómo agregar la VLAN principal al vNIC. No se necesita configuración de PVLAN porque sólo necesita la VLAN principal.

Nota: Este ejemplo utiliza 266 como primario y 166 como aislado; el sitio determinará los ID de VLAN.

1. Tenga en cuenta que el tipo de uso compartido es **Ninguno**.



2. Haga clic en la casilla de verificación **Select** para VLAN 266 para agregar la VLAN principal al vNIC. No lo establezca como Nativo.



Configuración de dispositivos ascendentes

Estos procedimientos describen cómo configurar los dispositivos ascendentes. En este caso, los switches ascendentes sólo necesitan puertos troncales, y sólo necesitan una VLAN 266 troncal porque es la única VLAN que ven los switches ascendentes.

En Nexus 5K, ingrese estos comandos y verifique la configuración del link ascendente:

1. Agregue la VLAN como principal:

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

2. Asegúrese de que todos los uplinks estén configurados para hacer un trunk de las VLAN:

```
interfaz Ethernet1/1description Connection to 4900switchport mode trunkspeed
1000interface Ethernet1/3descripción Conexión al puerto FIB 5switchport mode trunkspeed
1000interface Ethernet1/4descripción Conexión al puerto FIA 5switchport mode trunkspeed
1000
```

En el switch 4900, siga estos pasos:

1. Cree las VLAN utilizadas como principales en el N1K.
2. Realice un enlace troncal de todas las interfaces hacia y desde el switch 4900 para que se pase la VLAN.

En el router ascendente, cree una subinterfaz sólo para la VLAN 266. En este nivel, los requisitos dependen de la configuración de red que utilice.

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

Configuración de N1K

Este procedimiento describe cómo configurar el N1K.

1. Cree y asocie las VLAN:

```
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. Cree un perfil de puerto de enlace ascendente para el tráfico PVLAN con el puerto promiscuo anotado:

```
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. Cree el grupo de puertos para la VLAN aislada; cree un puerto de host PVLAN con la asociación de host para las VLAN principales y aisladas:

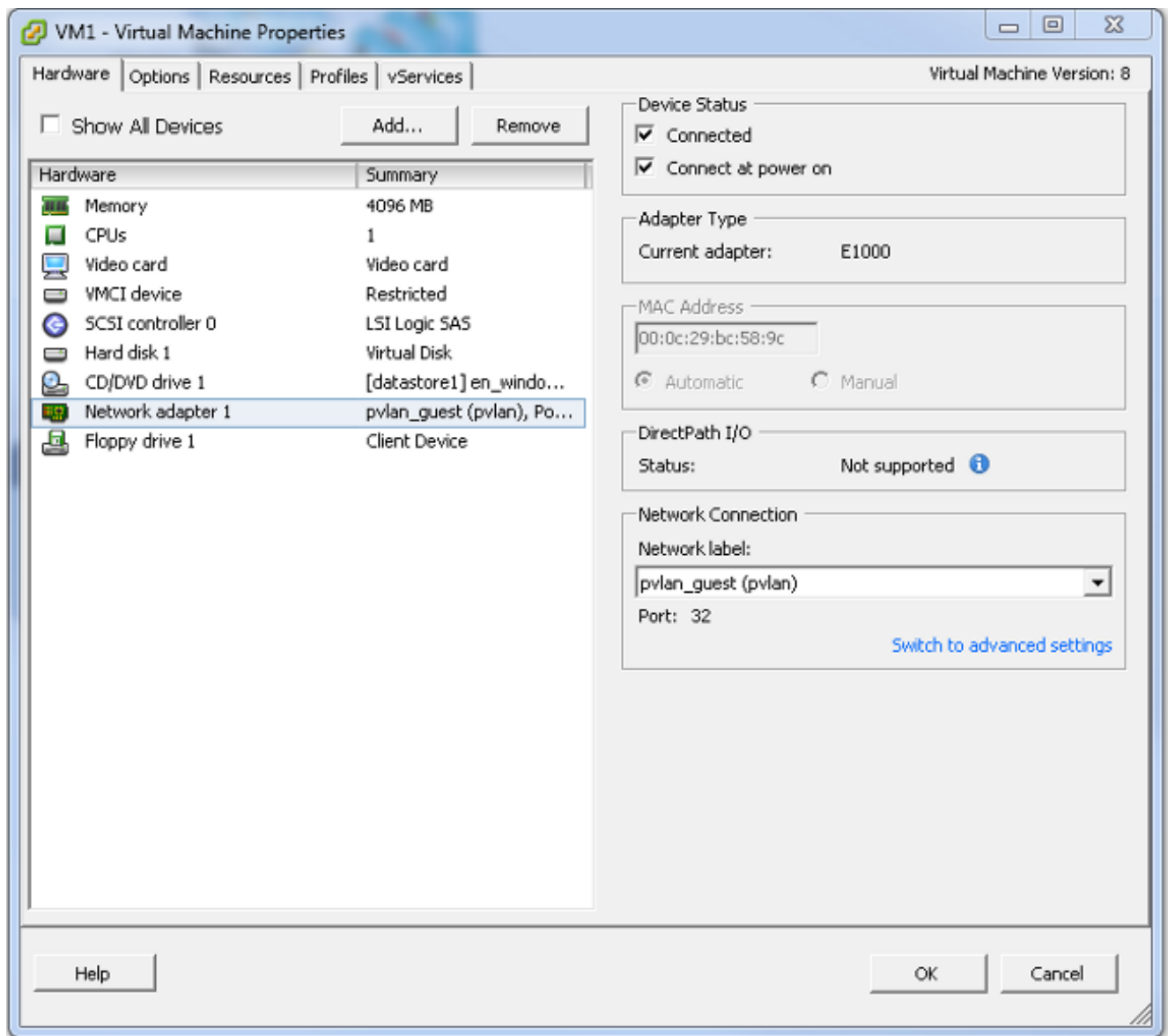
```
Switch(config)# port-profile type vethernet pvlan_guest
Switch(config-port-prof)# vmware port-group
Switch(config-port-prof)# switchport mode private-vlan host
Switch(config-port-prof)# switchport private-vlan host-association 266 166
Switch(config-port-prof)# no shut
Switch(config-port-prof)# state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

4. En el vCenter, agregue el vNIC adecuado al enlace ascendente PVLAN. Ésta es la vNIC a la que agregó la VLAN aislada en la configuración en UCS.

| | | | | |
|-------------------------------------|--|-------|---------------------------------|-----------------------------|
| <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. Agregue la VM al grupo de puertos correcto.

En la ficha Hardware, haga clic en **Network adapter 1**. Elija **pvlan_guest (pvlan)** para la etiqueta de red en Conexión de red.



Resolución de problemas

Este procedimiento describe cómo probar la configuración.

1. Ejecute pings a otros sistemas configurados en el grupo de puertos, así como al router u otro dispositivo en el puerto promiscuo. Los ping al dispositivo que se encuentra más allá del puerto promiscuo deben funcionar, mientras que los que se dirigen a otros dispositivos en la VLAN aislada deben fallar.

```

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>_

```

- En el N1K, las VM se enumeran en la VLAN principal; esto ocurre porque está en los puertos de host PVLAN que están asociados a la PVLAN. Tenga en cuenta también que aprende el dispositivo ascendente del canal de puerto y que el dispositivo ascendente también se aprende en la VLAN principal.

En esta captura de pantalla, los dos dispositivos en Veth3 y Veth 4 son las VM. El dispositivo en Po1 es el dispositivo ascendente que está más allá del puerto promiscuo.

```

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)#

```

- En el sistema UCS, debería estar aprendiendo todas las MAC, para esta comunicación, en la VLAN principal que utiliza en el N1K. No debería estar aprendiendo el flujo ascendente aquí:


```
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. En el Nexus 5K, todas las MAC se encuentran en la VLAN principal que seleccionó:

```
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. En el switch 4900, todo está en la VLAN principal que ha seleccionado:

```
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#
```

PVLAN de comunidad en N1K con puerto promiscuo en el perfil de puerto de enlace ascendente N1K

Esta es la única configuración admitida para la VLAN de comunidad con UCS.

Esta configuración es la misma que la configurada en la [PVLAN Aislada en N1K con Puerto Promiscuo en la sección Perfil de Puerto de Enlace Ascendente N1K](#). La única diferencia entre comunidad y aislado es la configuración de la PVLAN.

Para configurar el N1K, cree y asocie las VLAN como hizo en el 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
```

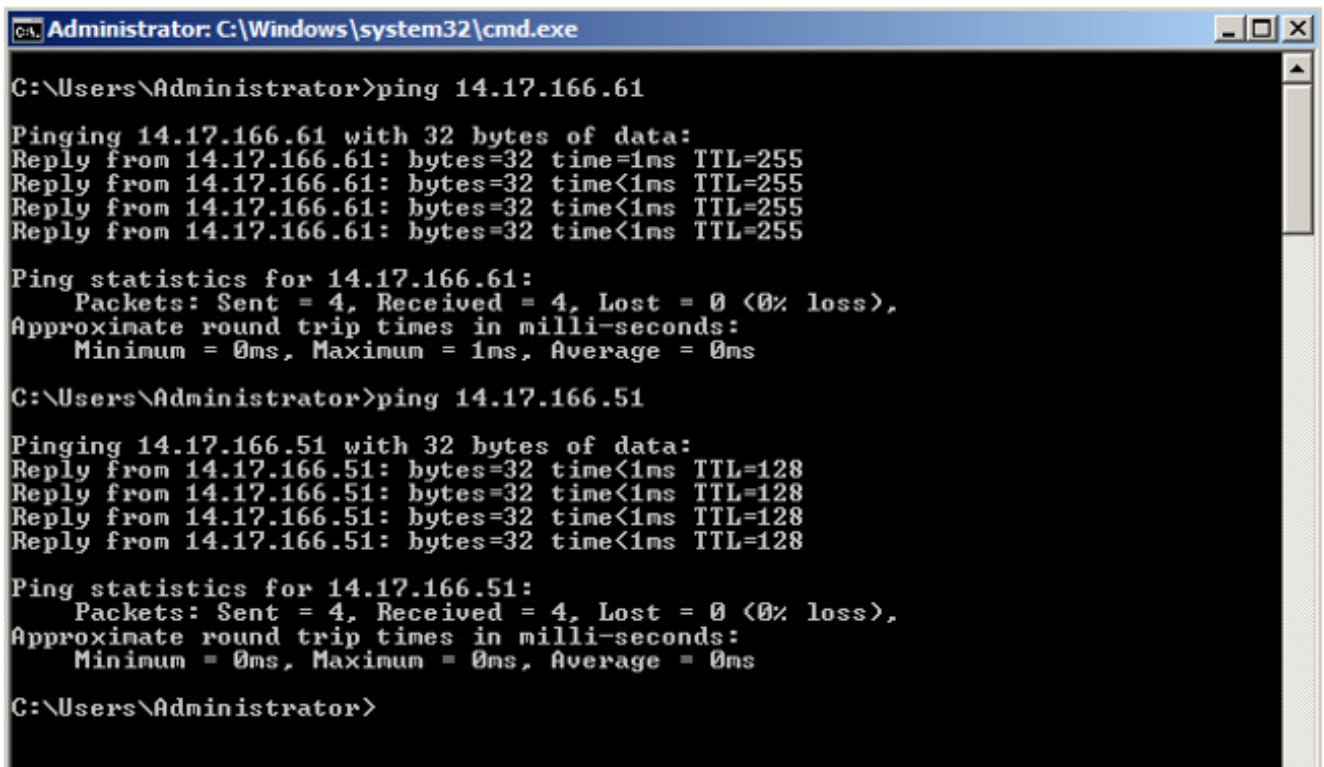
El resto de la configuración es la misma que la PVLAN aislada en N1K con puerto promiscuo en el perfil de puerto de link ascendente N1K.

Una vez configurado, puede comunicarse con todas las VM conectadas al perfil de puerto vEthernet utilizado para su PVLAN.

Resolución de problemas

Este procedimiento describe cómo probar la configuración.

1. Ejecute pings a otros sistemas configurados en el grupo de puertos, así como al router u otro dispositivo en el puerto promiscuo. Los ping más allá del puerto promiscuo y a otros sistemas de la comunidad deberían funcionar.



```
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. El resto de troubleshooting es el mismo que el [PVLAN aislado](#).

PVLAN aislada y PVLAN de comunidad en el puerto promiscuo VMware DVS en el DVS

Debido a los problemas de configuración tanto en el DVS como en el sistema UCS, las PVLAN con DVS y UCS no son compatibles antes de la versión 2.2(2c).

Verificación

Actualmente no hay procedimientos de verificación disponibles para estas configuraciones.

Troubleshoot

Las secciones anteriores proporcionaban información que puede utilizar para resolver problemas de sus configuraciones.

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver un análisis de información de salida del comando show.