Configure el VLAN privado y el UCS con VMware DV o el nexo 1000v de Cisco

Contenido

Introducción

Este documento describe la ayuda del VLAN privado (PVLAN) para el Cisco Unified Computing System (UCS) en 2.2(2c) la versión y más adelante.

> **Caution**: Hay un cambio en el comportamiento que comienza con la versión de firmware UCS 3.1(3a) según lo descrito en el **cambio del comportamiento con la** sección de la **versión 3.1(3) y posterior UCS**.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- UCS

- El nexo 1000V (N1K) o VMware de Cisco distribuyó el switch virtual (los DV)
- VMware
- Transferencia de la capa 2 (L2)

Componentes usados

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Un VLAN privado es un VLA N configurado para el aislamiento L2 de otros puertos dentro del mismo VLAN privado. Los puertos que pertenecen a un PVLAN se asocian a un conjunto común de VLA N de la ayuda, que se utilizan para crear la estructura PVLAN.

Hay tres tipos de puertos PVLAN:

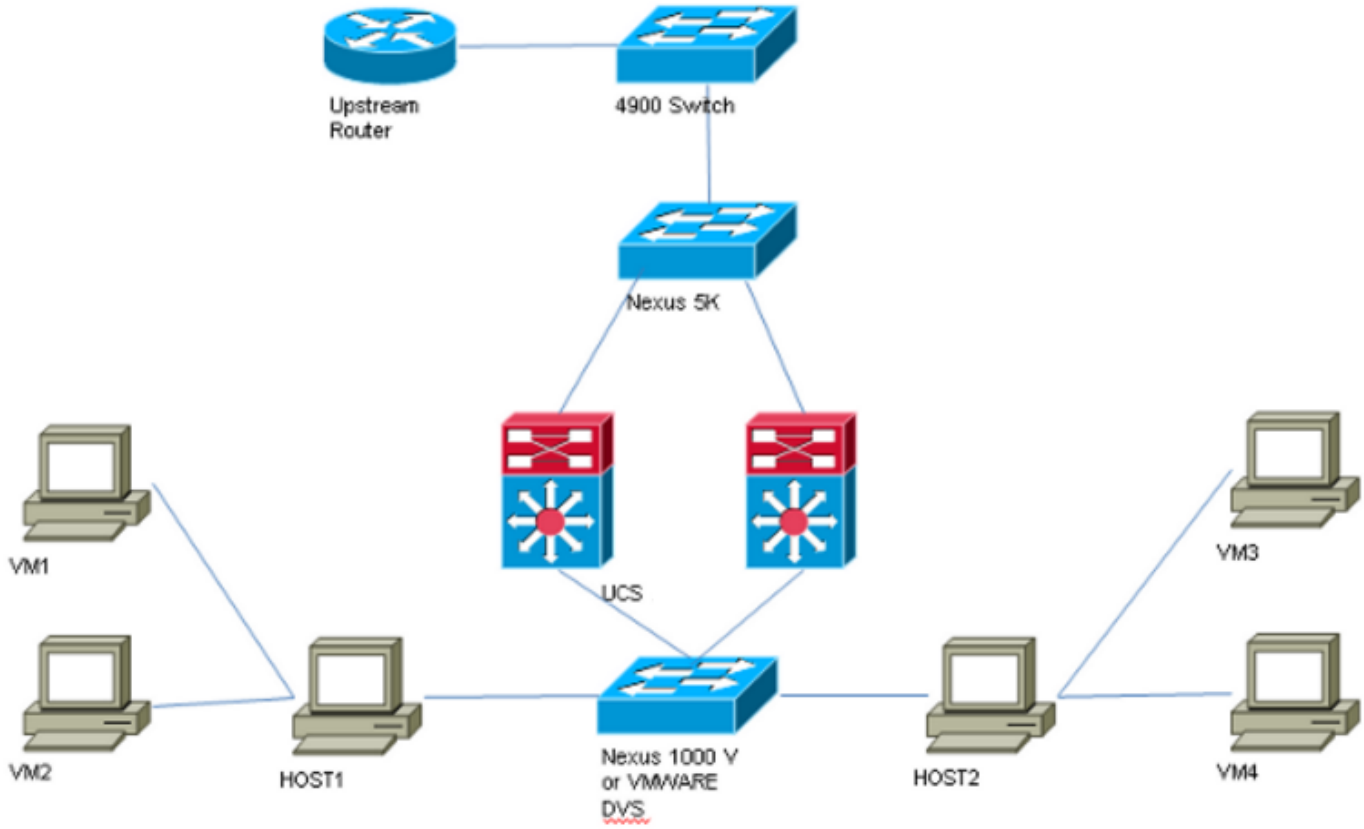
- Un puerto promiscuo comunica con el resto de los puertos PVLAN y es el puerto usado para comunicar con los dispositivos fuera del PVLAN.
- Un puerto aislado tiene separación completa L2 (que incluya las difusiones) de otros puertos dentro del mismo PVLAN a excepción del puerto promiscuo.
- Un puerto de la comunidad puede comunicar con otros puertos en el mismo PVLAN así como el puerto promiscuo. Los puertos de la comunidad se aíslan en el L2 de los puertos en otras comunidades o puertos aislados PVLAN. Las difusiones se propagan solamente a otros puertos en la comunidad y el puerto promiscuo.

Refiera al RFC 5517, los VLAN privados de los Cisco Systems: Seguridad escalable en un entorno multicliente para entender la teoría, la operación, y los conceptos de PVLANs.

Configurar

Diagrama de la red

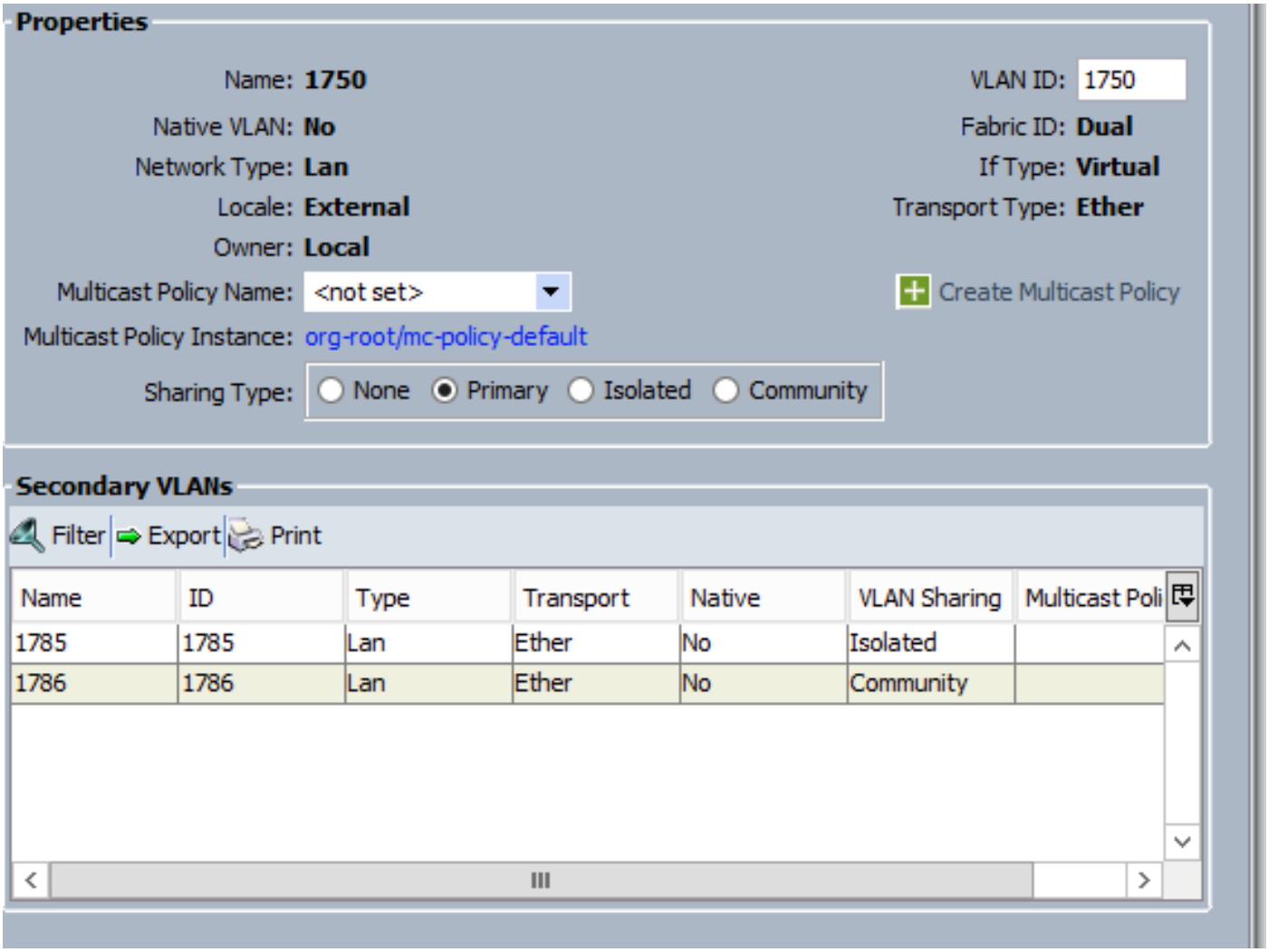
Con el nexo 1000v o VMware DV



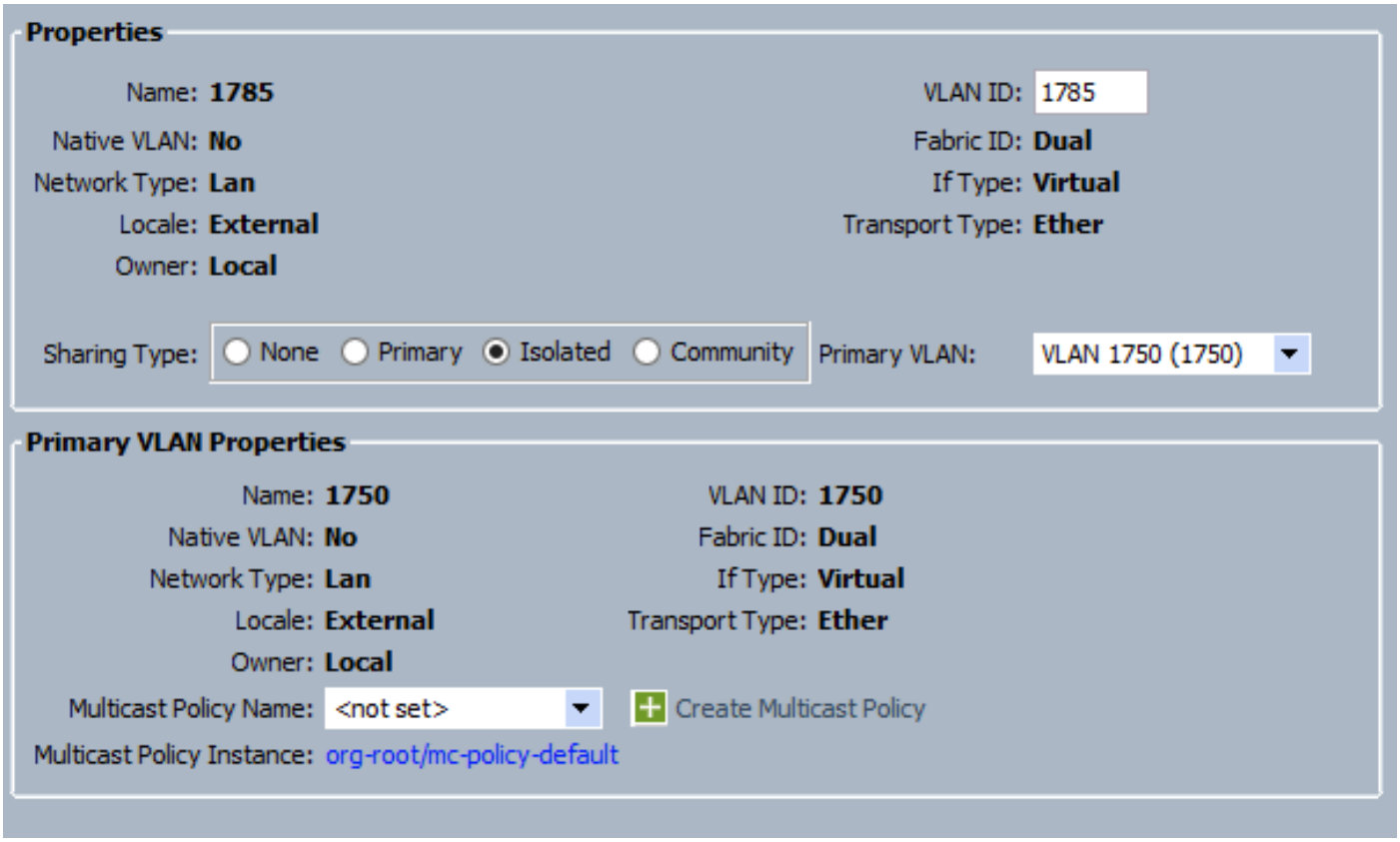
Note: Este ejemplo utiliza el VLA N 1750 como el primario, 1785 según lo aislado y 1786 como VLA N de la comunidad.

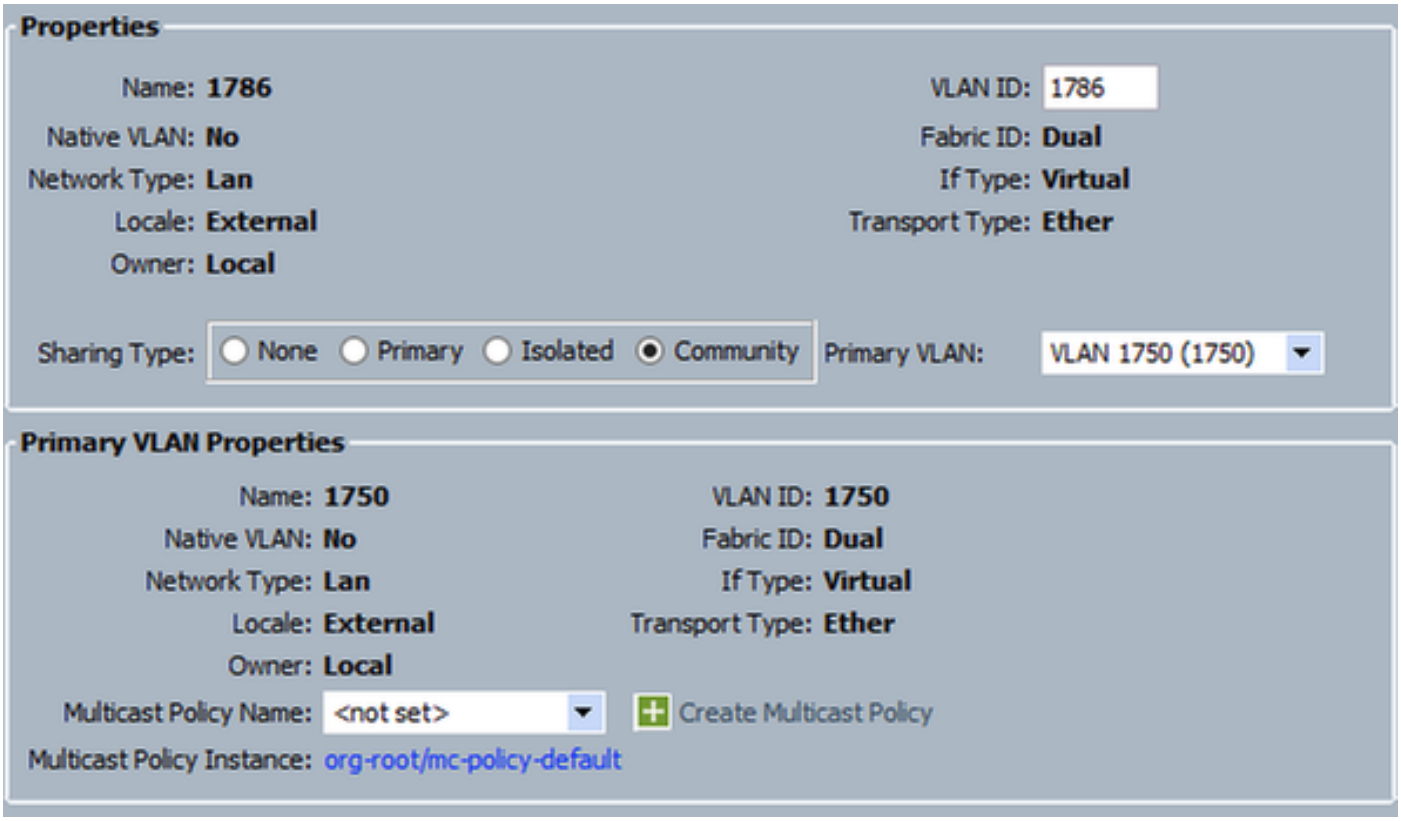
UCS con VMware DV

1. Para crear el VLAN principal, haga clic el botón de radio **primario** como el tipo de distribución, y ingrese una **identificación del VLA N** de 1750 tal y como se muestra en de la imagen.

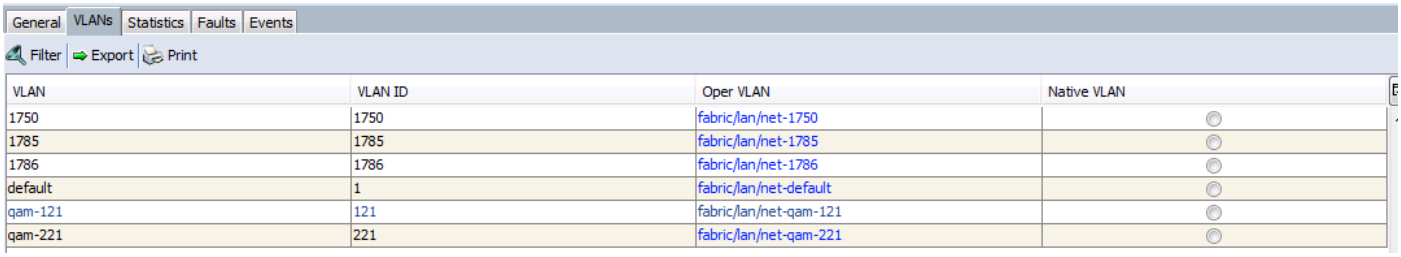


2. Cree por consiguiente **aislado** y de la **comunidad los** VLA N tal y como se muestra en de las imágenes. Ningunos de éstos tienen que ser un VLA N nativo.





3. El indicador luminoso LED amarillo de la placa muestra gravedad menor de interfaz de red virtual (vNIC) en el servicio-perfil lleva los VLA N así como PVLANs regulares, como se ve en la imagen.

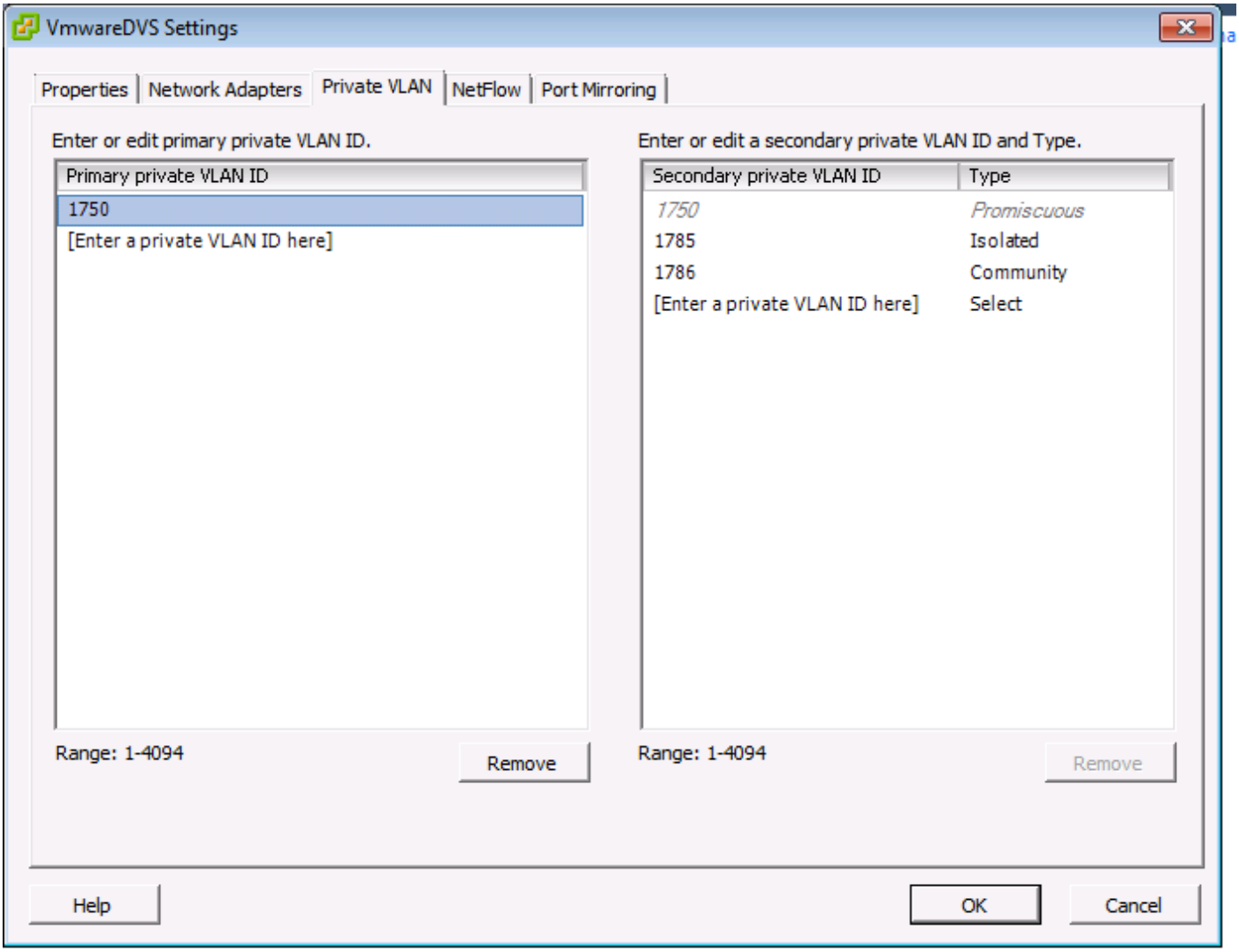


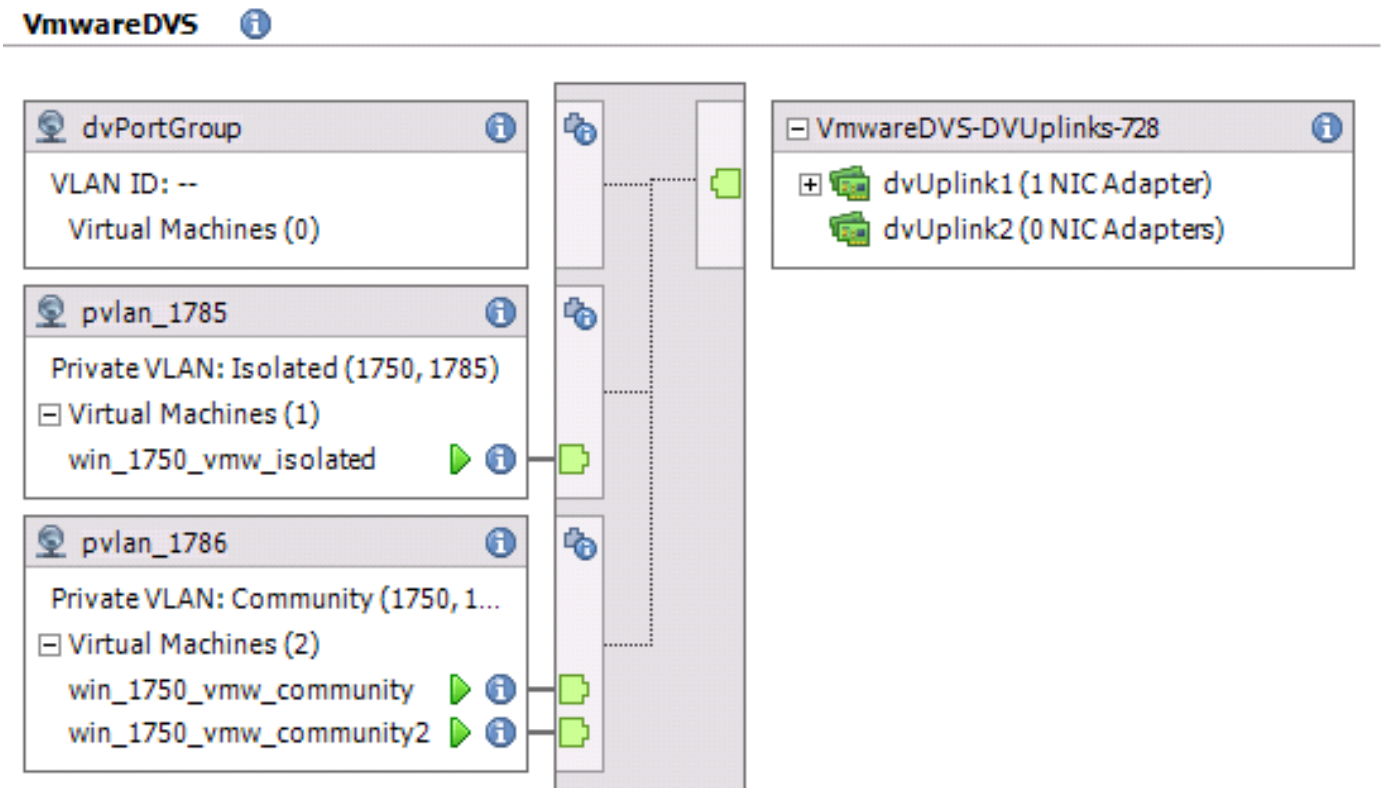
VLAN	VLAN ID	Oper VLAN	Native VLAN
1750	1750	fabric/lan/net-1750	
1785	1785	fabric/lan/net-1785	
1786	1786	fabric/lan/net-1786	
default	1	fabric/lan/net-default	
qam-121	121	fabric/lan/net-qam-121	
qam-221	221	fabric/lan/net-qam-221	

4. Uplink el Canal de puerto en el UCS lleva los VLA N así como PVLANs regulares:

```
interface port-channel1
description U: Uplink
switchport mode trunk
pinning border
switchport trunk allowed vlan 1,121,221,321,1750,1785-1786
speed 10000

F240-01-09-UCS4-A(nxos)#


F240-01-09-UCS4-A(nxos)# show vlan private-vlan
Primary Secondary Type Ports
------- --------- --------------- ----------------------------------------

1750     1785          isolated
1750     1786          community
```

VMware DV





Conmutador por aguas arriba N5k

```
feature private-vlan


vlan 1750 private-vlan primary private-vlan association 1785-1786


vlan 1785 private-vlan isolated

vlan 1786 private-vlan community




interface Vlan1750

ip address 10.10.175.252/24 private-vlan mapping 1785-1786

no shutdown


interface port-channel114

Description To UCS
switchport mode trunk
switchport trunk allowed vlan 1,121,154,169,221,269,321,369,1750,1785-1786
spanning-tree port type edge
spanning-tree bpduguard enable
spanning-tree bpdufilter enable
vpc 114 <=== if there is a 5k pair in vPC configuration only then add this line to both N5k
```

Cambio del comportamiento con la versión 3.1(3) y posterior UCS

Antes de la versión 3.1(3) UCS, usted podría hacer que una VM en el VLA N de la comunidad comunique con una VM en el VLAN principal en VMware DV donde el VLAN principal VM reside dentro del UCS. Este comportamiento era tan incorrecta que la VM primaria debe siempre ser en dirección del norte o exterior del UCS. Este comportamiento se documenta vía el ID del defecto CSCvh87378 .

De la versión 2.2(2) UCS hacia adelante, debido a un defecto en el código, el VLA N de la comunidad podía comunicar con el VLAN principal que estaba presente detrás del FI. Pero aislado podía nunca comunicar con el primario detrás del FI. Ambas (aislado y comunidad) VM pueden todavía comunicar con el primario fuera del FI.

A partir de la 3.1(3) hacia adelante, este defecto permite que la comunidad comunique con primario detrás del FI, fue rectificado y la comunidad VM no podrá así comunicar con una VM en el VLAN principal que reside dentro del UCS.

Para resolver esta situación, la VM primaria cualquier necesidad de ser movido (en dirección del norte) fuera del UCS. Si eso no es una opción, después la VM primaria necesitaría ser trasladada a otro VLA N que es un VLA N regular y no un VLAN privado.

Por ejemplo, antes de los firmwares 3.1(3), una VM en el VLA N 1786 de la comunidad podría comunicar a una VM en el VLAN principal 1750 que reside dentro del UCS, sin embargo, esta comunicación adaptaría los firmwares 3.1(3) y más adelante, tal y como se muestra en de la

imagen.

```
F240-01-09-UCS4-A(nxos)# show mac address-table | inc 76d7
* 1786      0050.568e.76d7    dynamic   440         F    F  Veth3148
F240-01-09-UCS4-A(nxos)#
```

```
   VLAN     MAC Address      Type      age     Secure NTFY   Ports/SWID.SSID.LID
---------+----------------+--------+---------+------+----+------------------
* 1750     0050.568e.476f    dynamic   0          F    F  Veth3240
F240-01-09-UCS4-B(nxos)#
```

4900 Switch por aguas arriba

> **Note**: En este ejemplo, 4900 es el interfaz L3 a la red externa. Si su topología para el L3 es diferente, después realice amablemente los cambios por consiguiente

En el 4900 Switch, tome estas medidas, y ponga el puerto promiscuo. Los extremos PVLAN en el puerto promiscuo.

1. Gire la función PVLAN si procede.
2. Cree y asocie los VLA N según lo hecho en el nexo 5K.
3. Cree el puerto promiscuo en el puerto de la salida del 4900 Switch. Desde aquí, los paquetes del VLA N 1785 y 1786 se ven en el VLA N 1750 en este caso.

```
Switch(config-if)#switchport mode trunk
switchport private-vlan mapping 1785-1786
switchport mode private-vlan promiscuous
```

En el router ascendente, cree un subinterface para el VLA N 1750 solamente. A este nivel, los requisitos dependen de la configuración de red que usted utiliza:

```
interface GigabitEthernet0/1.1

encapsulation dot1Q 1750

IP address10.10.175.254/24
```

Verifique

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

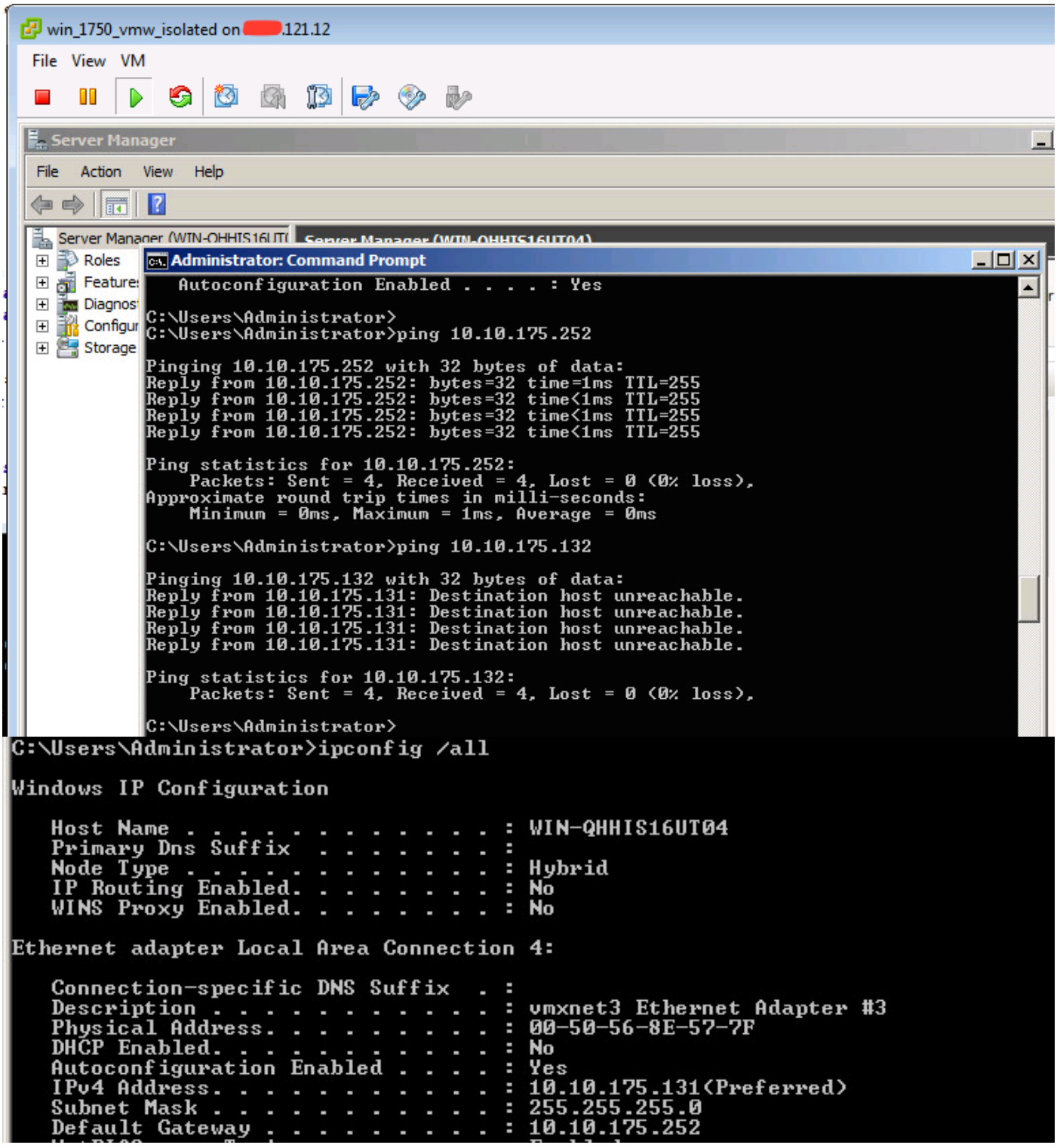
Troubleshooting

Esta sección proporciona a la información que usted puede utilizar para resolver problemas su configuración.

Este procedimiento describe cómo probar la configuración para VMware DV con el uso de PVLAN.

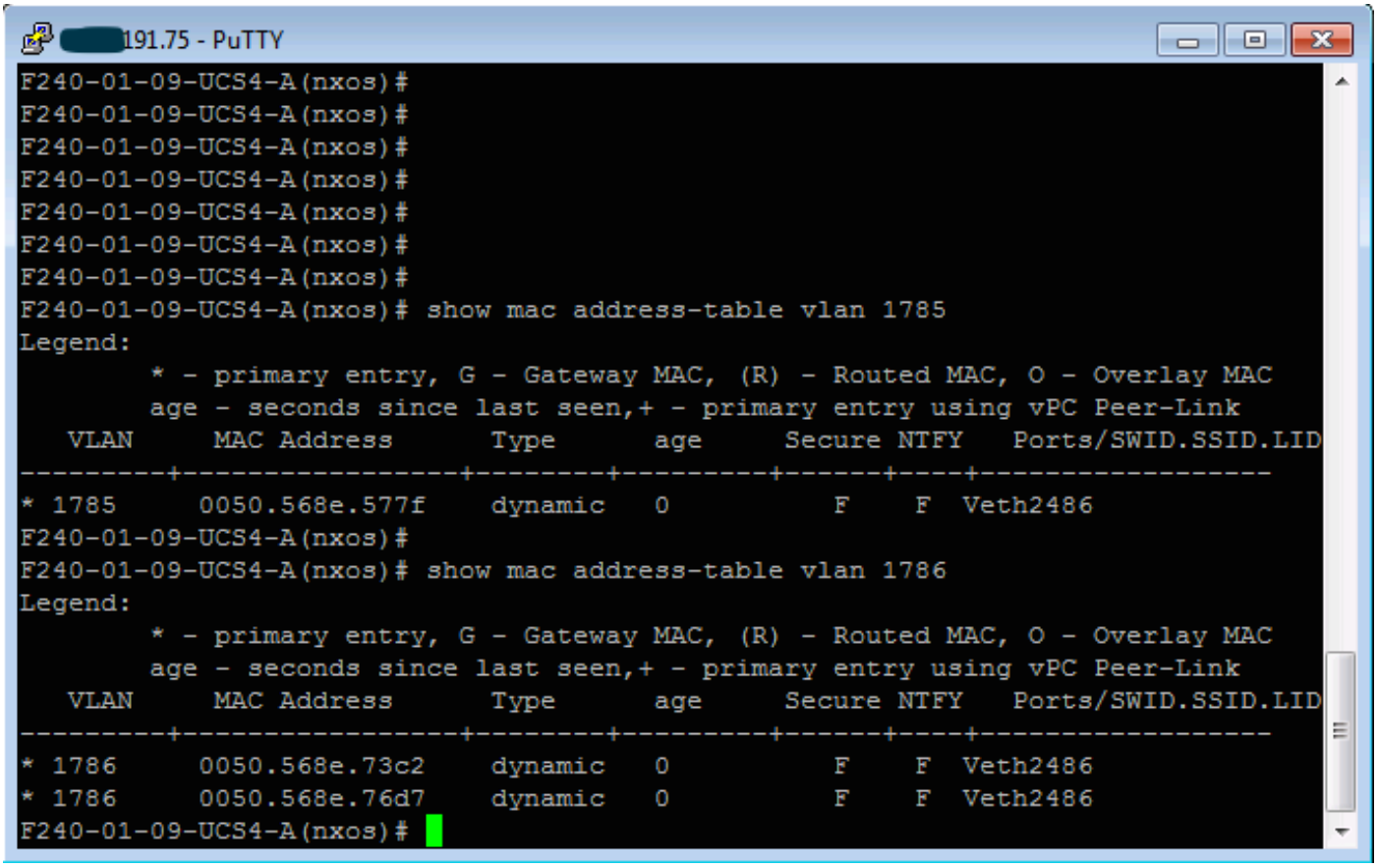
1. Funcione con los pings a otros sistemas configurados en el grupo de puertos así como el router

o el otro dispositivo en el puerto promiscuo. Los pings al dispositivo más allá del puerto promiscuo deben trabajar, mientras que ésos a los otros dispositivos en el VLAN aislado deben fallar tal y como se muestra en de las imágenes.



Controle las tablas de la dirección MAC para ver donde está estando docto su MAC. En todo el Switches, el MAC debe estar en el VLAN aislado excepto en el conmutador con el puerto promiscuo. En el conmutador promiscuo, el MAC debe estar en el VLAN principal.

2. UCS tal y como se muestra en de la imagen.



3. Compruebe n5k por aguas arriba para el mismo MAC, salida similar para hacer salir anterior debe estar presente en n5k y tal y como se muestra en de la imagen.

```
f241-01-08-5596-a# show mac address-table | inc 577f
* 1785      0050.568e.577f    dynamic   170         F     F  Po114
f241-01-08-5596-a#
f241-01-08-5596-a# show mac address-table | inc 73c2
* 1786      0050.568e.73c2    dynamic   10          F     F  Po114
f241-01-08-5596-a# show mac address-table | inc 76d7
* 1786      0050.568e.76d7    dynamic   30          F     F  Po114
f241-01-08-5596-a#
```

Configuración con el nexo 1000v con el puerto promiscuo en N5k por aguas arriba

Configuración UCS

La configuración UCS (que incluye la configuración del vNIC del servicio-perfil) permanece lo mismo según el ejemplo con VMware DV.

Configuración N1k

```
feature private-vlan


vlan 1750 private-vlan primary private-vlan association 1785-1786
```

```
vlan 1785 private-vlan isolated

vlan 1786 private-vlan community


same uplink port-profile is being used for regular vlans & pvlans. In this example vlan 121 &
221 are regular vlans but you can change them accordingly

port-profile type ethernet pvlan-uplink-no-prom
switchport mode trunk
mtu 9000
switchport trunk allowed vlan 121,221,1750,1785-1786
channel-group auto mode on mac-pinning

system vlan 121 no shutdown state enabled vmware port-group

port-profile type vethernet pvlan_1785
switchport mode private-vlan host
switchport private-vlan host-association 1750 1785
switchport access vlan 1785
no shutdown
state enabled
vmware port-group

port-profile type vethernet pvlan_1786 switchport mode private-vlan host switchport access vlan
1786 switchport private-vlan host-association 1750 1786 no shutdown state enabled vmware port-
group
```

Este procedimiento describe cómo probar la configuración.

1. Funcione con los pings a otros sistemas configurados en el grupo de puertos así como el router o el otro dispositivo en el puerto promiscuo. Los pings al dispositivo más allá del puerto promiscuo deben trabajar, mientras que ésos a los otros dispositivos en el VLAN aislado deben fallar, tal y como se muestra en de la sección anterior y en las imágenes.