Configuración de VLAN privada y UCS con VMware DVS o Cisco Nexus 1000v

Contenido

Introducción

Este documento describe el soporte de VLAN privada (PVLAN) para Cisco Unified Computing System (UCS) en la versión 2.2(2c) y posteriores.

> **Precaución:** Hay un cambio en el comportamiento que comienza con la versión 3.1(3a) del firmware de UCS, como se describe en la sección **Cambio de comportamiento con la versión 3.1(3) y posteriores de UCS**.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- UCS
- Switch virtual distribuido (DVS) Cisco Nexus 1000V (N1K) o VMware
- 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

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:

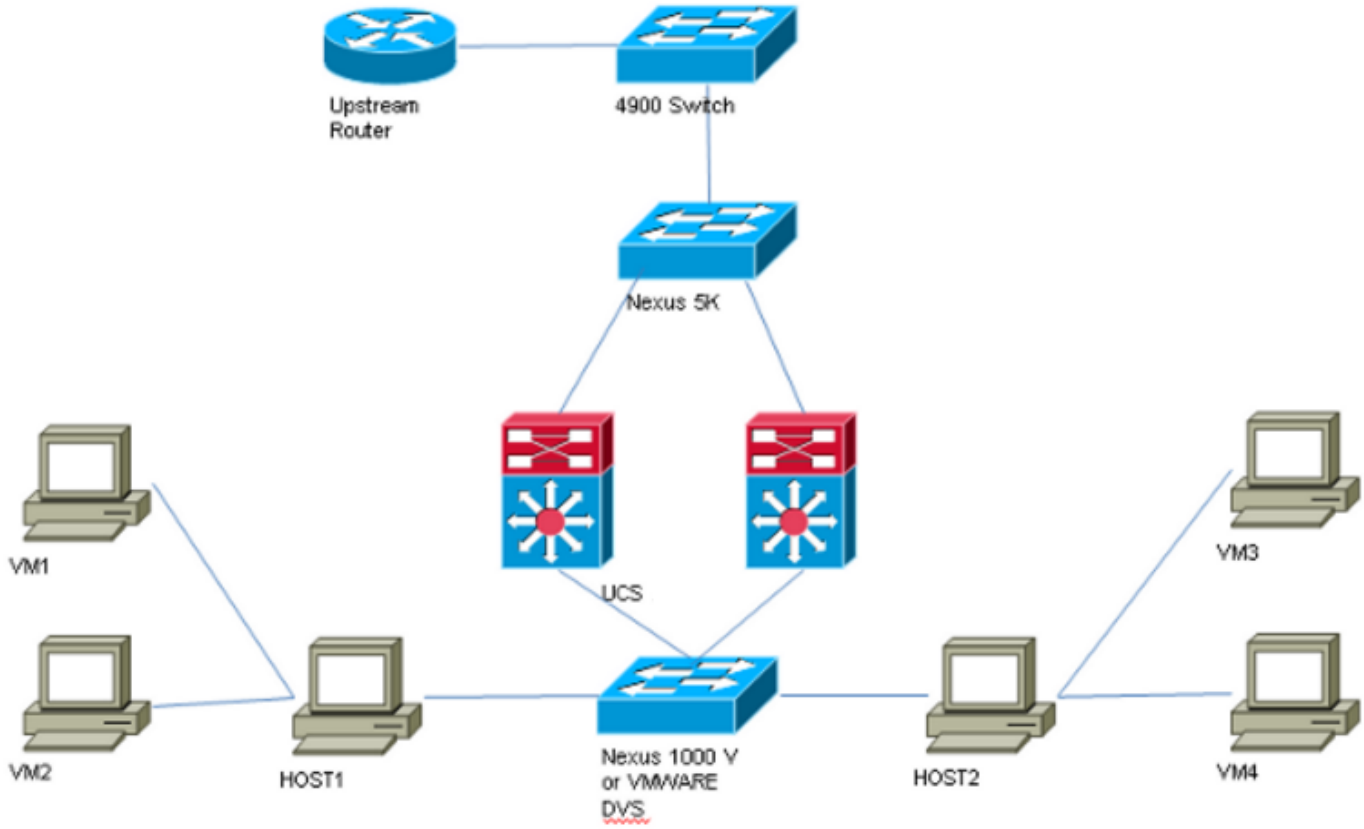
- Un puerto promiscuo se comunica con todos los demás puertos PVLAN y es el puerto utilizado para comunicarse con los dispositivos fuera de la PVLAN.
- Un puerto aislado tiene separación L2 completa (que incluye broadcasts) de otros puertos dentro de la misma PVLAN, con la excepción del puerto promiscuo.
- 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.

Configurar

Diagrama de la red

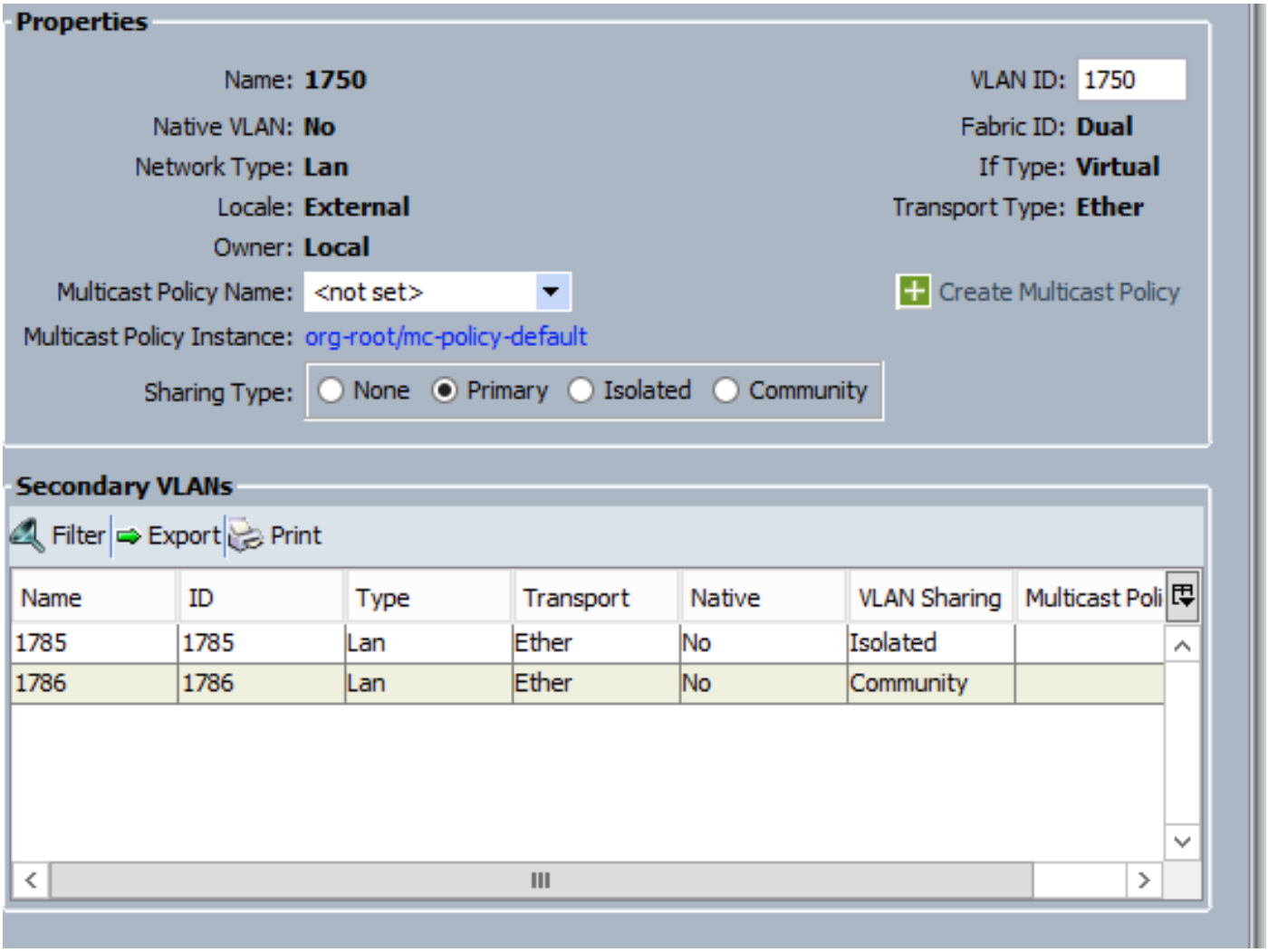
Con Nexus 1000v o DVS de VMware



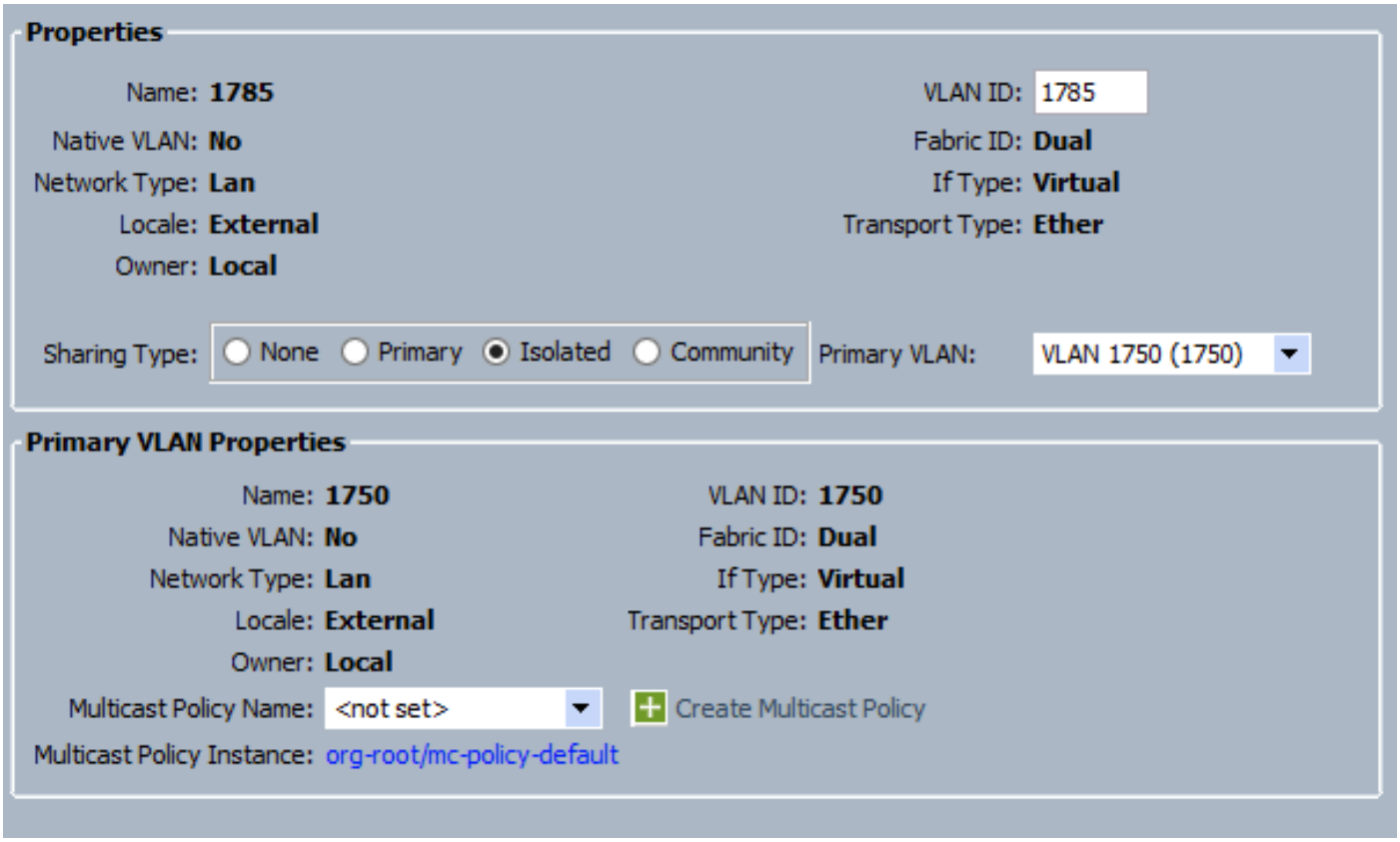
Nota: Este ejemplo utiliza VLAN 1750 como la principal, 1785 como aislada y 1786 como VLAN de comunidad.

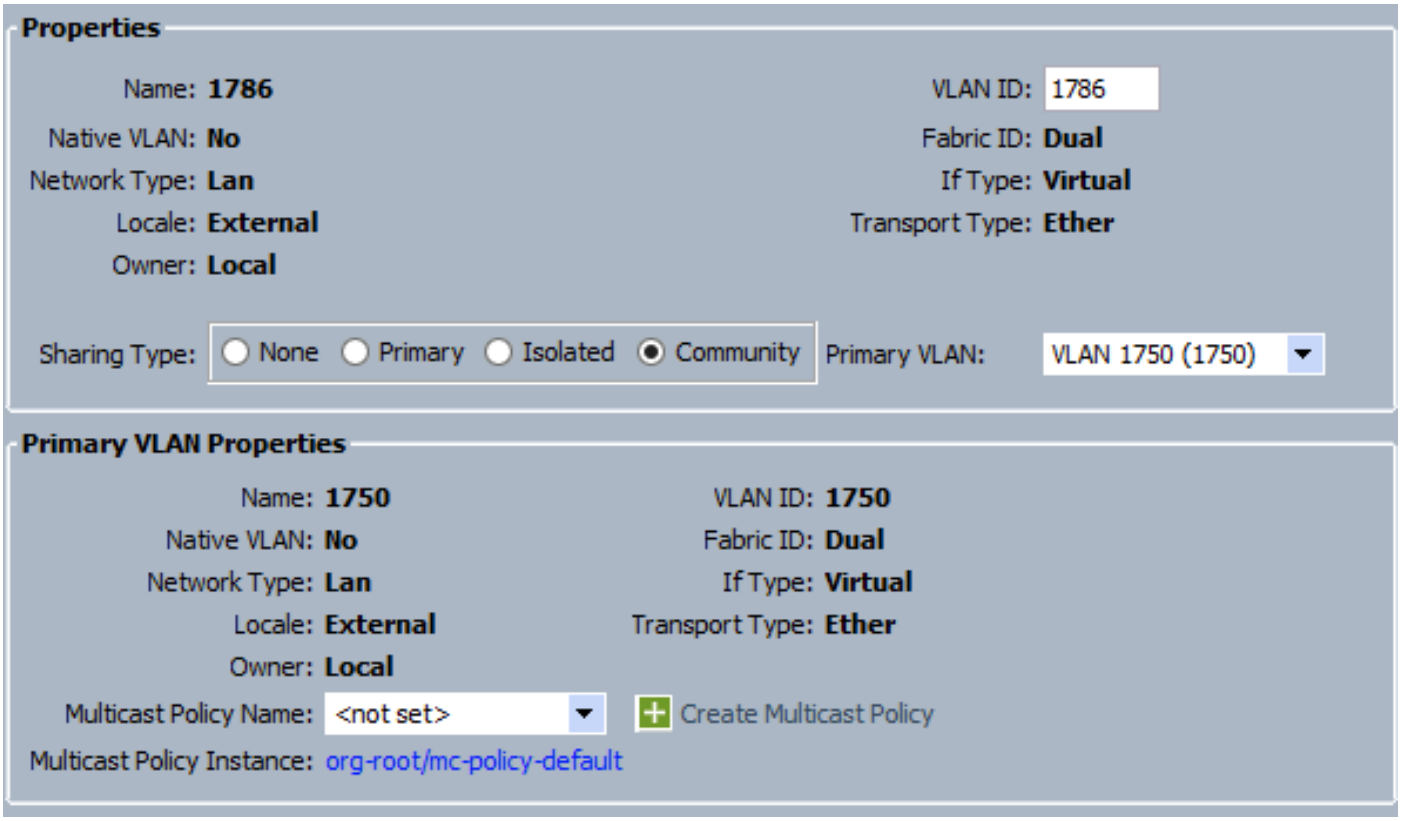
UCS con DVS de VMware

1. Para crear la VLAN principal, haga clic en el botón de radio **Primary** como el Tipo de uso compartido, e ingrese un **ID de VLAN** de 1750 como se muestra en la imagen.

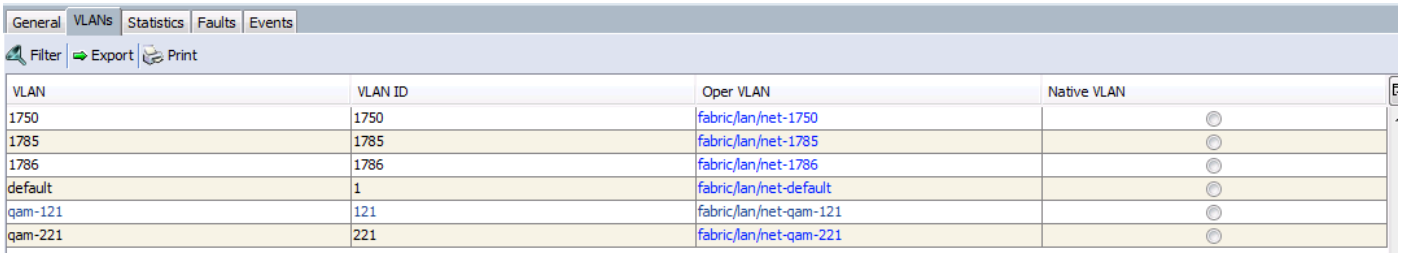


2. Cree las VLAN **Aisladas** y **comunitarias** en consecuencia como se muestra en las imágenes. Ninguno de estos debe ser una VLAN nativa.





3. La tarjeta de interfaz de red virtual (vNIC) en el perfil de servicio lleva VLAN regulares y PVLAN, como se ve en la imagen.

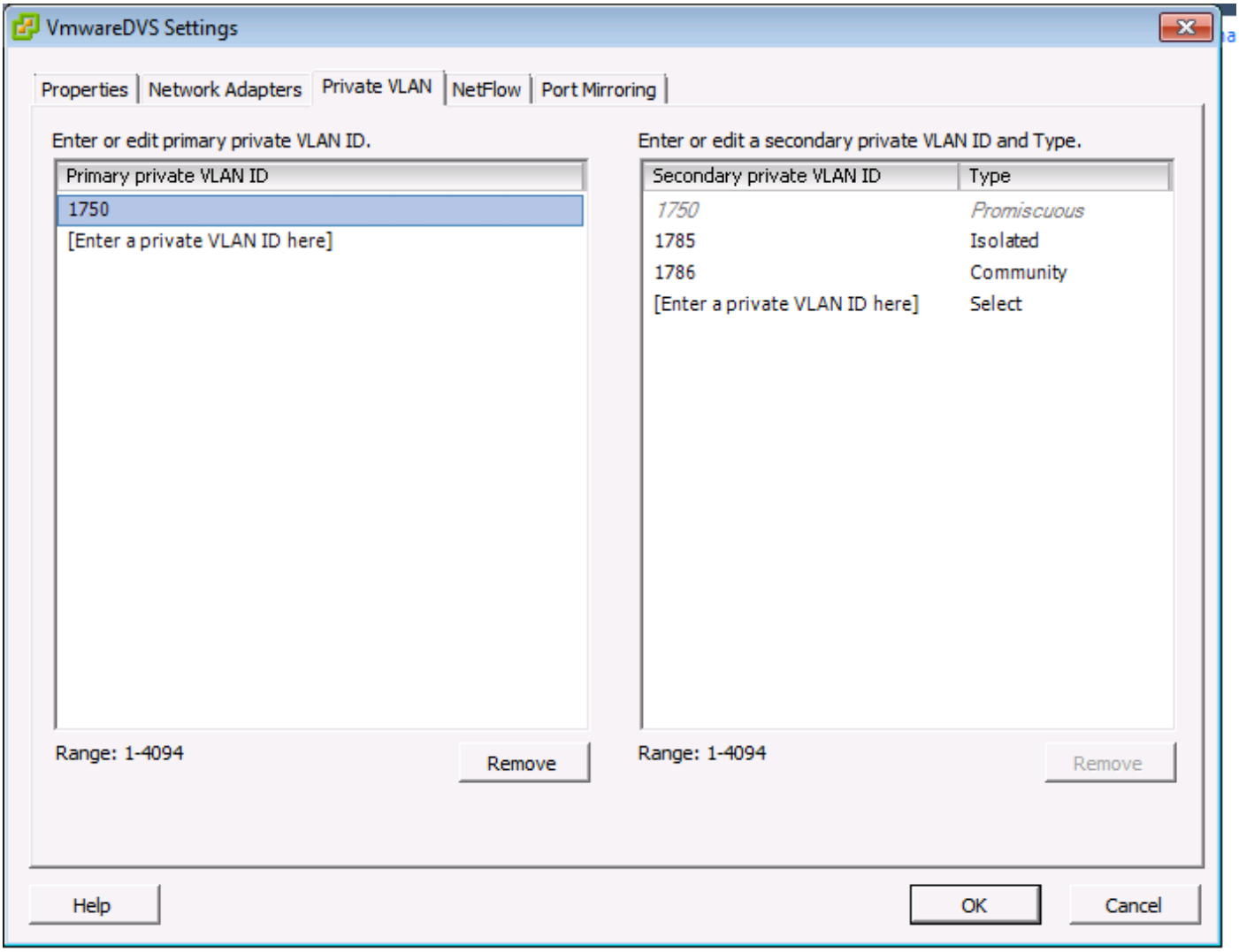


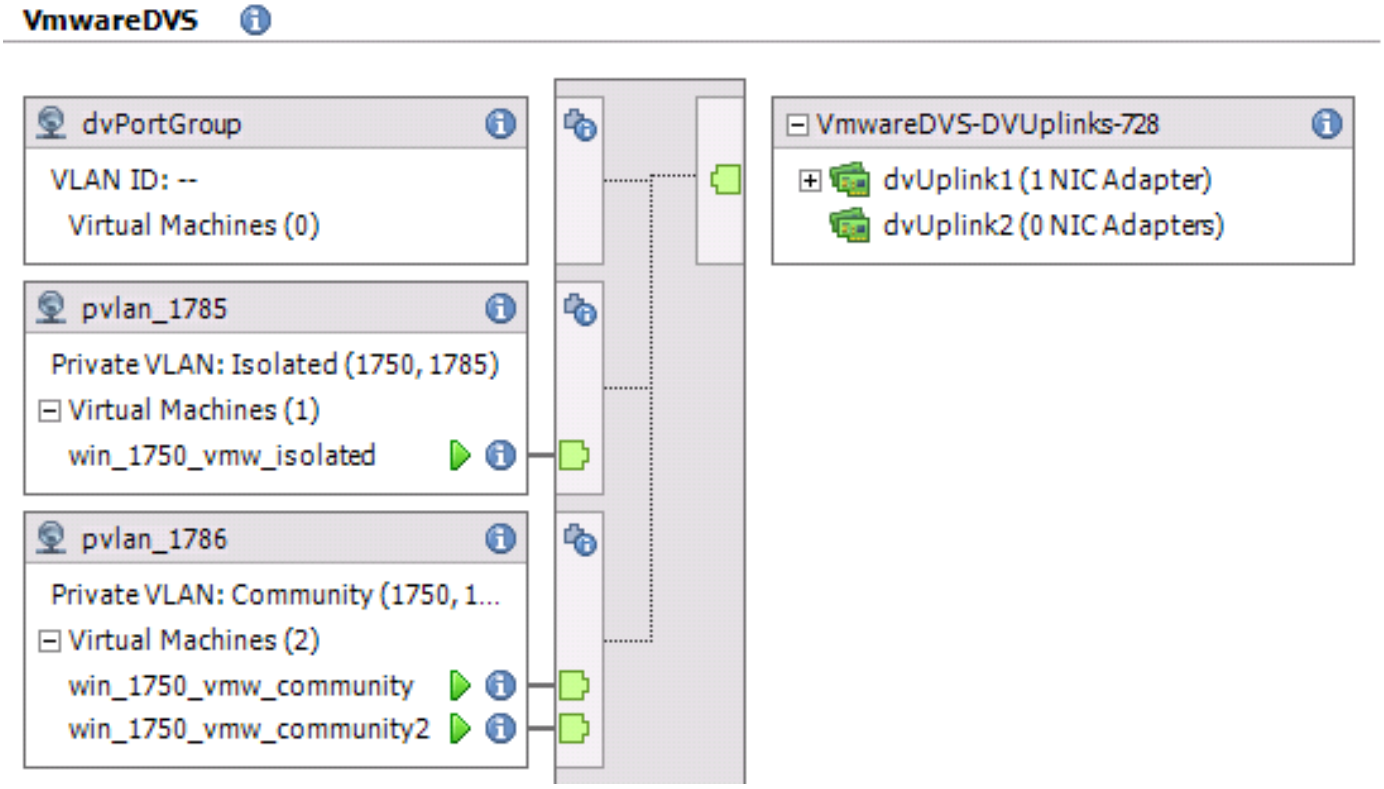
VLAN	VLAN ID	Oper VLAN	Native VLAN
1750	1750	fabric/lan/net-1750	
1785	1785	fabric/lan/net-1785	
1786	1786	fabric/lan/net-1786	
default	1	fabric/lan/net-default	
qam-121	121	fabric/lan/net-qam-121	
qam-221	221	fabric/lan/net-qam-221	

4. El canal de puerto de enlace ascendente en UCS transporta VLAN regulares así como PVLAN:

```
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
```

DVS de VMware





Switch ascendente 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 de comportamiento con UCS versión 3.1(3)

Antes de la versión 3.1(3) de UCS, podría tener una VM en una VLAN comunitaria para comunicarse con una VM en la VLAN principal en VMware DVS donde reside la VM de VLAN principal dentro de UCS. Este comportamiento era incorrecto, ya que la VM principal siempre debe estar en sentido ascendente o fuera de UCS. Este comportamiento se documenta a través del ID de defecto CSCvh87378 .

A partir de la versión 2.2(2) de UCS en adelante, debido a un defecto en el código, la VLAN de la comunidad pudo comunicarse con la VLAN principal que estaba presente detrás de la FI. Pero Aislado nunca pudo comunicarse con el primario detrás de la FI. Tanto las VM (aisladas como las comunitarias) todavía pueden comunicarse con el primario fuera de la FI.

A partir de 3.1(3), este defecto permite a la comunidad comunicarse con el primario detrás de la FI, se rectificó y, por lo tanto, las VM comunitarias no podrán comunicarse con una VM en la VLAN principal que reside dentro de UCS.

Para resolver esta situación, la VM principal tendría que moverse (hacia el norte) fuera de UCS. Si no es una opción, la VM principal tendría que moverse a otra VLAN que sea una VLAN normal y no una VLAN privada.

Por ejemplo, antes del firmware 3.1(3), una VM en la VLAN 1786 de la comunidad podría comunicarse con una VM en la VLAN 1750 principal que reside dentro de UCS; sin embargo, esta comunicación se interrumpiría en el firmware 3.1(3) y posterior, como se muestra en la imagen.

NOTE:

—

CSCvh87378 se ha abordado en 3.2(3l) y 4.0.4e y superiores para que podamos tener la Vlan principal detrás de UCS. Sin embargo, tenga en cuenta que la vlan aislada dentro de UCS no podrá comunicarse con la vlan principal dentro de UCS. Solo la vlan de comunidad y la vlan principal pueden comunicarse entre sí cuando ambos están detrás de UCS.

```
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)#
```

Switch ascendente 4900

> **Nota:** En este ejemplo, 4900 es la interfaz L3 a la red externa. Si su topología para L3 es diferente, haga los cambios correspondientes

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 1785 y 1786 se ven en VLAN 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 una subinterfaz sólo para la VLAN 1750. En este nivel, los requisitos dependen de la configuración de red que utilice:

```
interface GigabitEthernet0/1.1

encapsulation dot1Q 1750

IP address10.10.175.254/24
```

Verificación

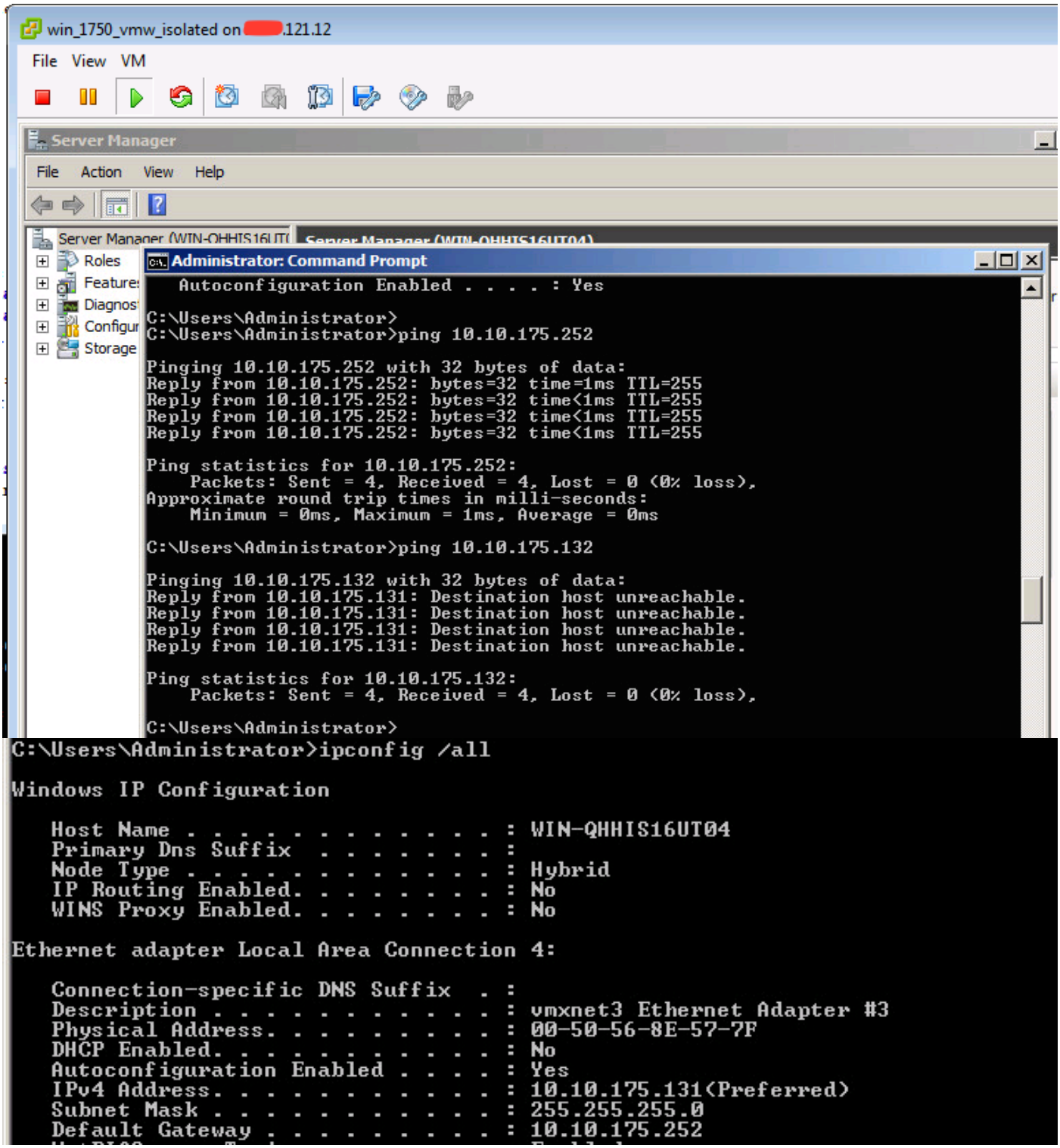
Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

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

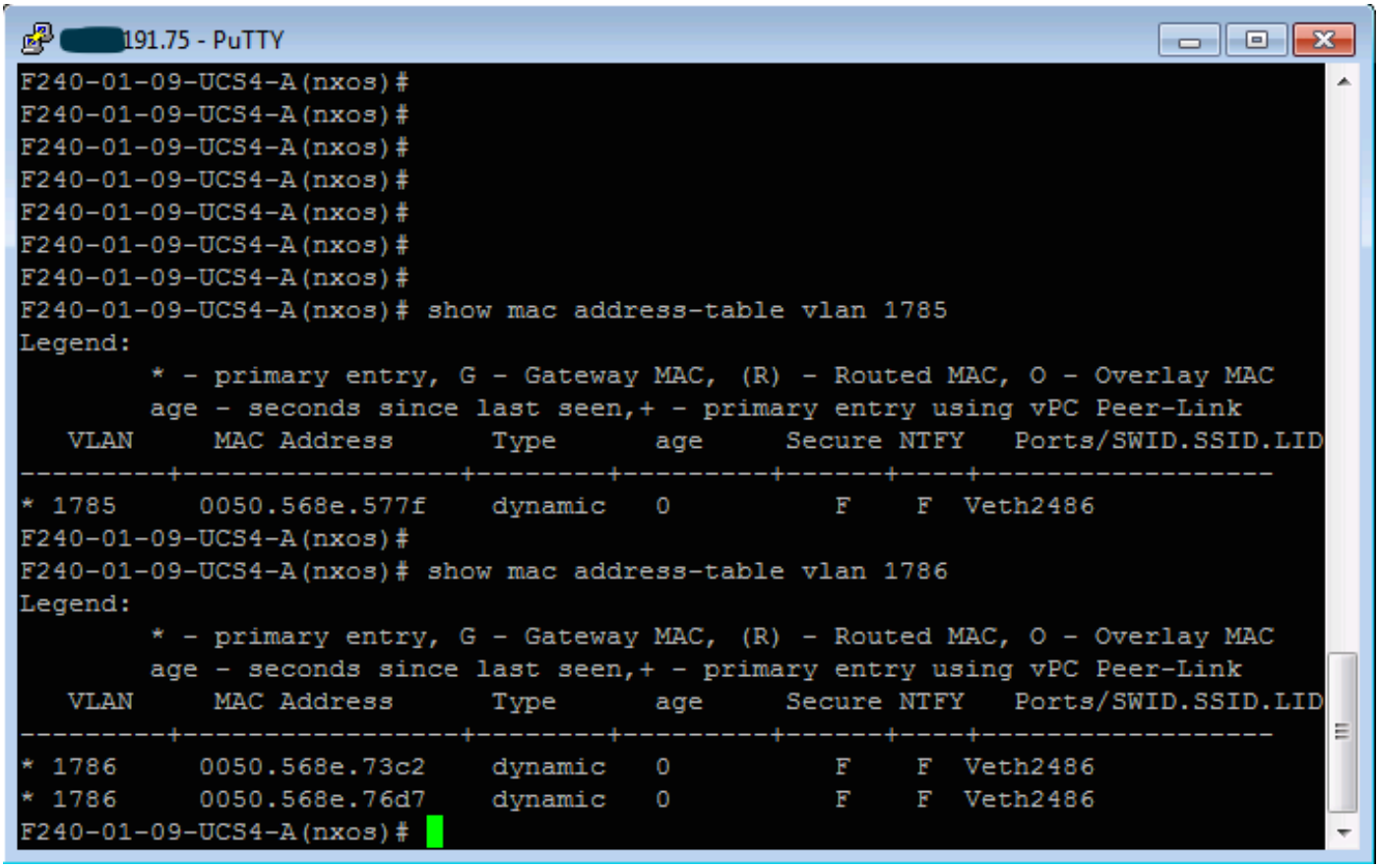
1. Ejecute pings a otros sistemas configurados en el grupo de puertos, así como al router u otro dispositivo en el puerto promiscuo. Los ping al dispositivo que pasa por el puerto promiscuo deben funcionar, mientras que aquellos a otros dispositivos en la VLAN aislada deben fallar como se muestra en las imágenes.



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, el MAC debe estar en la VLAN principal.

2. UCS como se muestra en la imagen.



3. Verifique en el flujo ascendente n5k el mismo MAC, la salida similar a la anterior debe estar presente en n5k y como se muestra en 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 Nexus 1000v con puerto promiscuo en N5k ascendente

Configuración de UCS

La configuración de UCS (que incluye la configuración vNIC de perfil de servicio) permanece igual que en el ejemplo con VMware DVS.

Configuración de 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. 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 pasa por el puerto promiscuo deben funcionar, mientras que aquellos a otros dispositivos en la VLAN aislada deben fallar, como se muestra en la sección anterior y en las imágenes.