

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

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Teoría](#)

[Configurar](#)

[con el nexo 1000v o VMware DV](#)

[Configuración UCS con VMware DV](#)

[Configuración usando el nexo 1000v con el puerto promiscuo en la conexión en sentido ascendente N5k](#)

[Resolución de problemas](#)

[Configuración usando el nexo 1000v con el puerto promiscuo en el Puerto-perfil del uplink N1K](#)

[Configuración UCS](#)

[Configuración de los dispositivos ascendentes](#)

[Configuración de N1K](#)

[Resolución de problemas](#)

Introducción

Este documento describe el soporte del VLAN privado (PVLAN) en el Cisco Unified Computing System (UCS) en la versión 2.2.(2C) y posterior

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- UCS
- Nexo de Cisco 1000 V (N1K) o VMware DV
- VMware
- Transferencia de la capa 2 (L2)

Componentes Utilizados

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

Teoría

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 del soporte, que se utilizan para crear la estructura PVLAN.

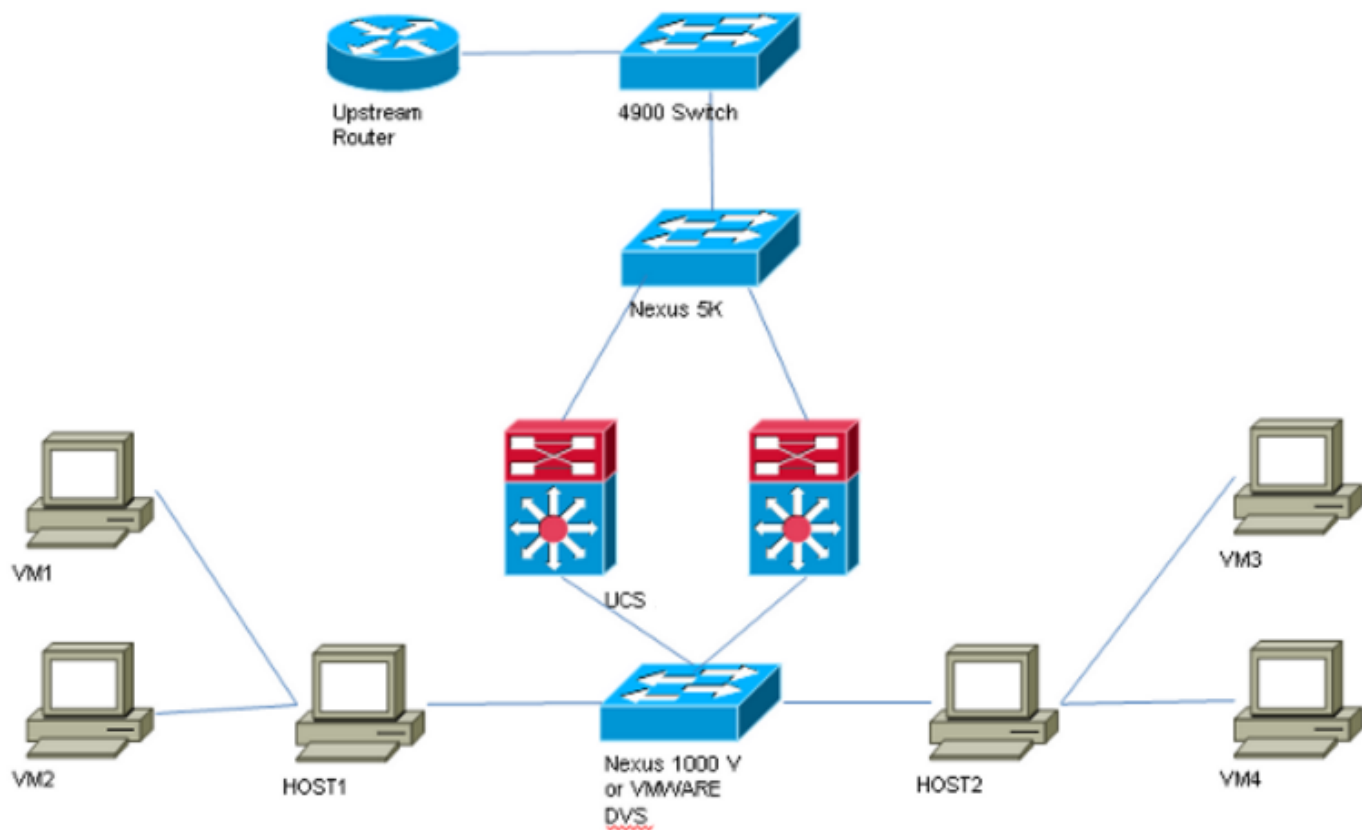
Hay tres tipos de puertos PVLAN:

- **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 (broadcasts incluyendo) 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. Los broadcasts 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 scalable en un entorno multicliente](#) para entender la teoría, la operación, y los conceptos de PVLAN.

Configurar

con el nexa 1000v o Vmware DV



Nota: Este ejemplo utiliza 1750 vlan como el primario, 1785 según lo aislado y 1786 como comunidad vlan

Configuración UCS con VMware DV

1. Para crear el VLAN principal, haga clic **primario** como el tipo de distribución, y ingrese un **VLAN ID** de 1750:

Properties

Name: **1750** VLAN ID:
 Native VLAN: **No** Fabric ID: **Dual**
 Network Type: **Lan** If Type: **Virtual**
 Locale: **External** Transport Type: **Ether**
 Owner: **Local**

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

Sharing Type: None Primary Isolated Community

Secondary VLANs

Filter | Export | Print

Name	ID	Type	Transport	Native	VLAN Sharing	Multicast Poli	
1785	1785	Lan	Ether	No	Isolated		^
1786	1786	Lan	Ether	No	Community		

< ||| >

2. Cree por consiguiente aislado y de la comunidad vlans como abajo. Ningunos de éstos tienen que ser un VLAN nativo

Properties

Name: **1785** VLAN ID:
 Native VLAN: **No** Fabric ID: **Dual**
 Network Type: **Lan** If Type: **Virtual**
 Locale: **External** Transport Type: **Ether**
 Owner: **Local**

Sharing Type: None Primary Isolated Community Primary VLAN:

Primary VLAN Properties

Name: **1750** VLAN ID: **1750**
 Native VLAN: **No** Fabric ID: **Dual**
 Network Type: **Lan** If Type: **Virtual**
 Locale: **External** Transport Type: **Ether**
 Owner: **Local**

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

Properties

Name: **1786** VLAN ID: **1786**
 Native VLAN: **No** Fabric ID: **Dual**
 Network Type: **Lan** If Type: **Virtual**
 Locale: **External** Transport Type: **Ether**
 Owner: **Local**

Sharing Type: None Primary Isolated Community Primary VLAN: **VLAN 1750 (1750)**

Primary VLAN Properties

Name: **1750** VLAN ID: **1750**
 Native VLAN: **No** Fabric ID: **Dual**
 Network Type: **Lan** If Type: **Virtual**
 Locale: **External** Transport Type: **Ether**
 Owner: **Local**

Multicast Policy Name: **<not set>** Create Multicast Policy
 Multicast Policy Instance: [org-root/mc-policy-default](#)

3. vnic en el servicio-perfil está llevando el vlans así como los pvlans regulares

VLAN	VLAN ID	Oper VLAN	Native VLAN
1750	1750	fabric/lan/net-1750	<input type="radio"/>
1785	1785	fabric/lan/net-1785	<input type="radio"/>
1786	1786	fabric/lan/net-1786	<input type="radio"/>
default	1	fabric/lan/net-default	<input type="radio"/>
qam-121	121	fabric/lan/net-qam-121	<input type="radio"/>
qam-221	221	fabric/lan/net-qam-221	<input type="radio"/>

4.

El canal del puerto del uplink en el UCS está llevando el vlans así como los pvlans regulares

```

interfaz port-channel1
descripción U: Uplink
switchport mode trunk
fijación de la frontera
switchport trunk no prohibido 1,121,221,321,1750,1785-1786 vlan
velocidad 10000

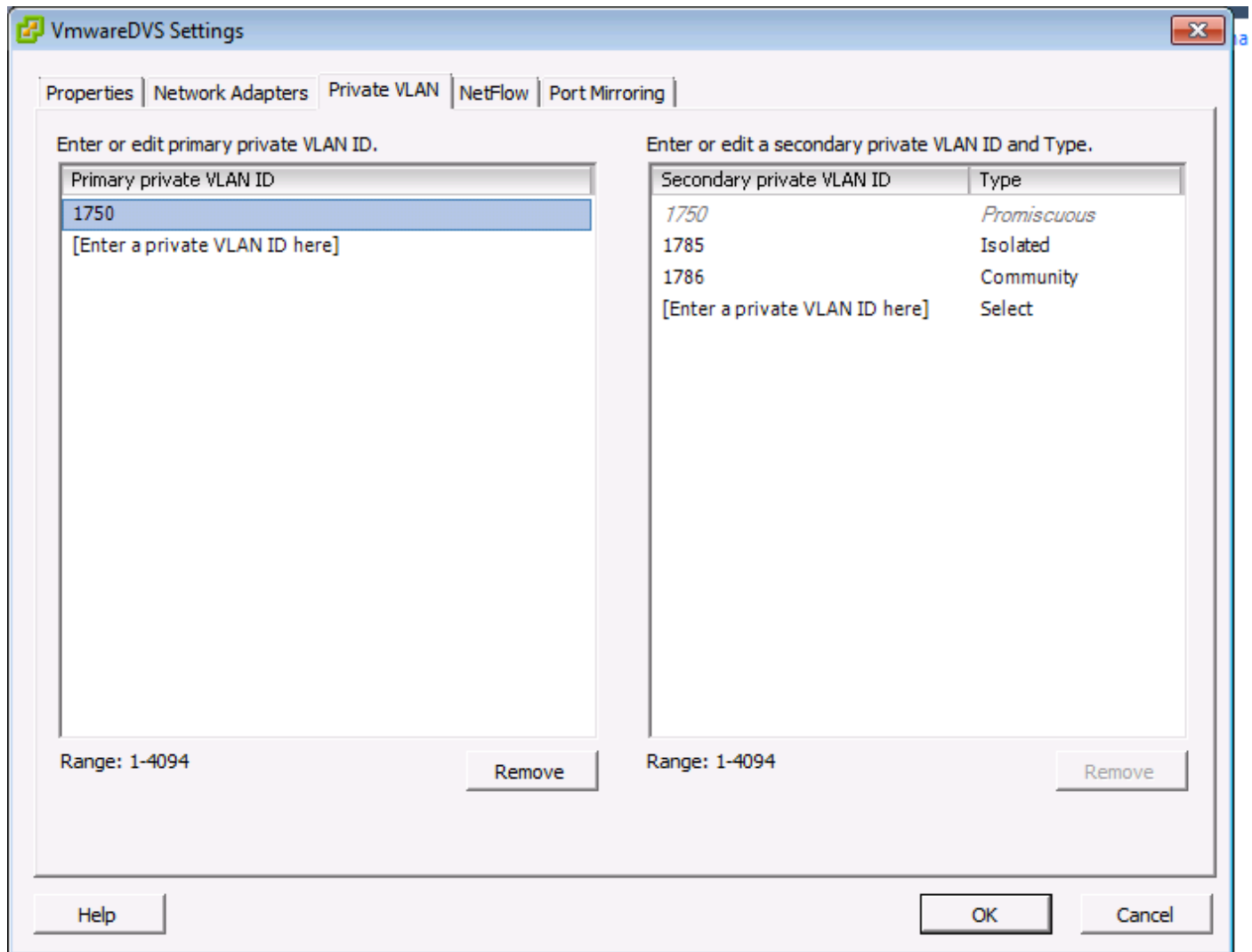
```

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

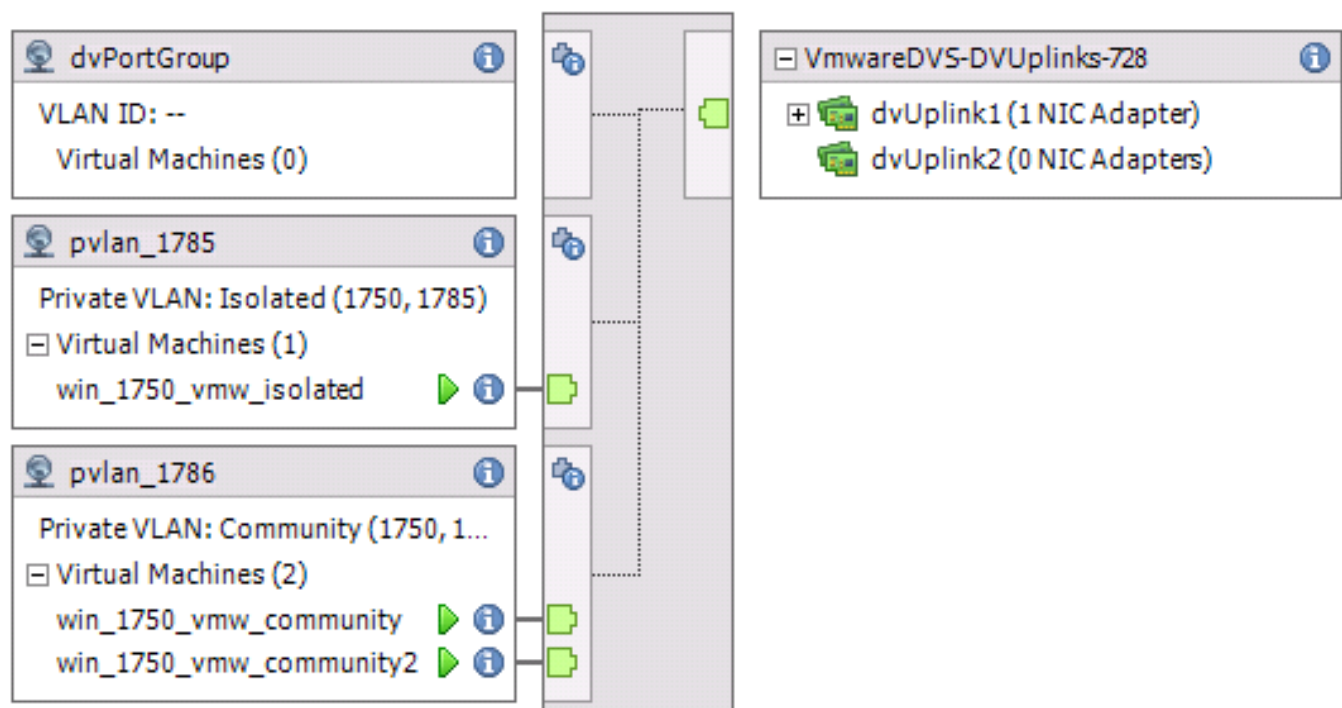
Demostración soldado-VLAN vlan F240-01-09-UCS4-A(nxos)#
 Primary Secondary Type Ports

1750 1785 aislados
 comunidad 1750 1786

Configuración en VMware DV



VMwareDVS ⓘ



Configuración del Switch de la conexión en sentido ascendente N5k

característica soldado-VLAN

1750 vlan
soldado-VLAN primario
asociación 1785-1786 de soldado-VLAN

1785 vlan
soldado-VLAN aisló

1786 vlan
comunidad de soldado-VLAN

interfaz Vlan1750

IP Address 10.10.175.252/24
private-vlan mapping 1785-1786

ningún apague

interconecte port-channel114

Descripción al UCS

switchport mode trunk
switchport trunk no prohibido 1,121,154,169,221,269,321,369,1750,1785-1786 vlan
borde del tipo del puerto de árbol de expansión
permiso del bpduguard del atravesar-árbol
permiso del bpdufilter del atravesar-árbol
el <=== del vpc 114 si hay un par 5k en configuración del vPC entonces agrega solamente esta línea a ambos N5k

Configuración del 4900 Switch por aguas arriba

En el 4900 Switch, tome estas medidas, y configure 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 nexa 5K.
3. Cree el puerto promiscuo en el puerto de egreso 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 una subinterfaz para el VLA N 1750 solamente. A este nivel, los requisitos dependen de la configuración de red que usted está utilizando:

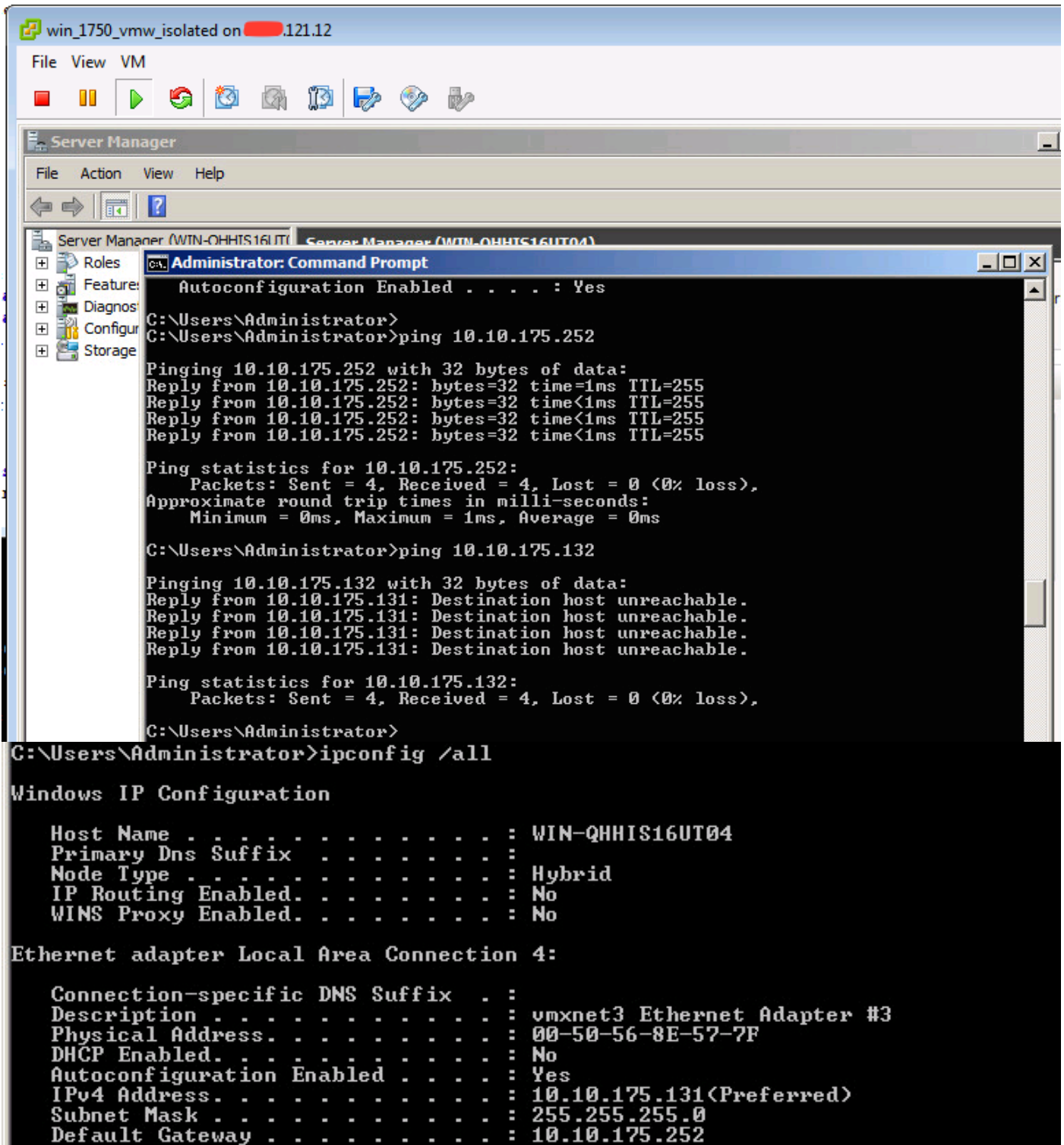
1. interfaz GigabitEthernet0/1.1
2. dot1q 1750 de la encapsulación

3. IP address 10.10.175.254/24

Resolución de problemas

Este procedimiento describe cómo probar la configuración para los dvs del vmware usando pvlan.

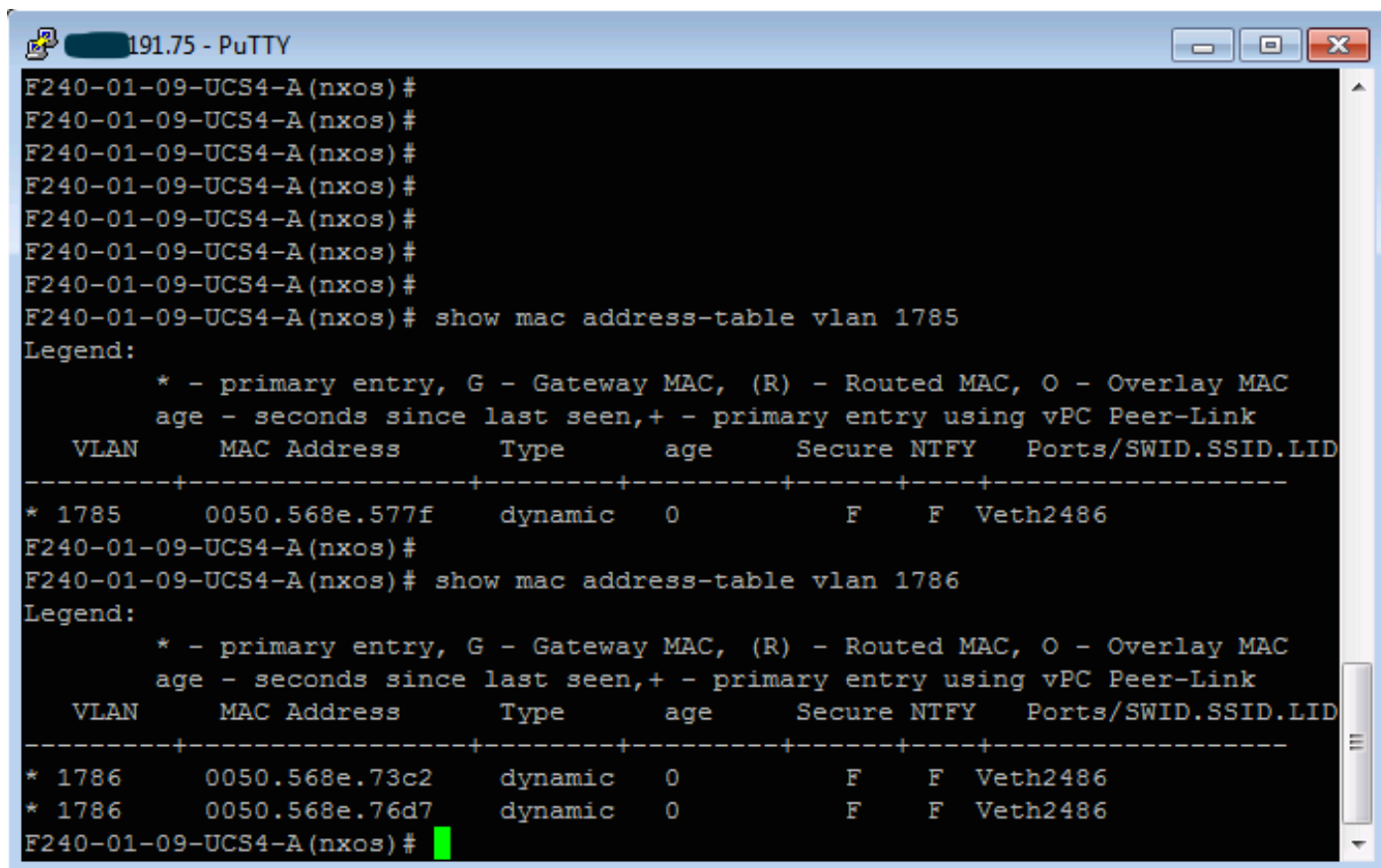
1. Funcione con los ping a otros sistemas configurados en el grupo de puertos así como el router o el otro dispositivo en el puerto promiscuo. Los ping al dispositivo más allá del puerto promiscuo deben trabajar, mientras que éstos a los otros dispositivos en el VLAN aislado deben fallar.



Marque 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 Switch con el puerto promiscuo.

En el Switch promiscuo el MAC debe estar en el VLAN principal.

2. UCS



```
F240-01-09-UCS4-A(nxos)#
F240-01-09-UCS4-A(nxos)#
F240-01-09-UCS4-A(nxos)#
F240-01-09-UCS4-A(nxos)#
F240-01-09-UCS4-A(nxos)#
F240-01-09-UCS4-A(nxos)#
F240-01-09-UCS4-A(nxos)#
F240-01-09-UCS4-A(nxos)# show mac address-table vlan 1785
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/SWID.SSID.LID
-----+-----+-----+-----+-----+-----
* 1785      0050.568e.577f    dynamic   0         F      F  Veth2486
F240-01-09-UCS4-A(nxos)#
F240-01-09-UCS4-A(nxos)# show mac address-table vlan 1786
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/SWID.SSID.LID
-----+-----+-----+-----+-----+-----
* 1786      0050.568e.73c2    dynamic   0         F      F  Veth2486
* 1786      0050.568e.76d7    dynamic   0         F      F  Veth2486
F240-01-09-UCS4-A(nxos)#
```

3. compruebe la conexión en sentido ascendente n5k para el mismo mac, salida similar a la salida antedicha debe estar presente en n5k

```
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 usando el nexa 1000v con el puerto promiscuo en la conexión en sentido ascendente N5k

Configuración UCS

La configuración UCS (config vnic including del servicio-perfil) permanecerá lo mismo según el ejemplo antedicho con el vmware DV

Configuración N1k

característica soldado-VLAN

1750 vlan
soldado-VLAN primario
asociación 1785-1786 de soldado-VLAN

1785 vlan
soldado-VLAN aisló

1786 vlan
comunidad de soldado-VLAN

el mismo puerto-perfil del uplink se está utilizando para el vlans y los pvlans regulares. En este ejemplo 121 y 221 vlan es el vlans regular pero usted puede cambiarlos por consiguiente

PVLAN-uplink-ninguno-baile de fin de curso de los Ethernetes del tipo del puerto-perfil
switchport mode trunk
MTU 9000
switchport trunk no prohibido 121,221,1750,1785-1786 vlan
modo automático del canal-grupo en la mac-fijación

sistema 121 vlan
ningún apague
estado habilitado
grupo de puertos del vmware

vethernet pvlan_1785 del tipo del puerto-perfil
host de soldado-VLAN del modo del switchport
host-asociación 1750 1785 de soldado-VLAN del switchport
VLAN de acceso al puerto del switch 1785
ningún apague
estado habilitado
grupo de puertos del vmware

vethernet pvlan_1786 del tipo del puerto-perfil
host de soldado-VLAN del modo del switchport
VLAN de acceso al puerto del switch 1786
host-asociación 1750 1786 de soldado-VLAN del switchport
ningún apague
estado habilitado
grupo de puertos del vmware

Resolución de problemas

Este procedimiento describe cómo probar la configuración.

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