使用VMware DVS或Cisco Nexus 1000v配置專用VLAN和UCS

目錄

簡介

本檔案介紹2.2(2c)版本及更新版本中思科整合運算系統(UCS)的私人VLAN(PVLAN)支援。

> **注意**：從UCS韌體版本3.1(3a)開始，行為會發生更改，如**UCS版本3.1(3)及更高版本中的行為更改**一節所述。

必要條件

需求

思科建議您瞭解以下主題：

- UCS
- Cisco Nexus 1000V(N1K)或VMware分散式虛擬交換機(DVS)
- VMware

- 第2層(L2)交換

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

專用VLAN是配置為從同一個專用VLAN中的其他埠隔離第2層的VLAN。屬於PVLAN的連線埠與一組常見的支援VLAN關聯，用於建立PVLAN架構。

PVLAN埠有三種型別：

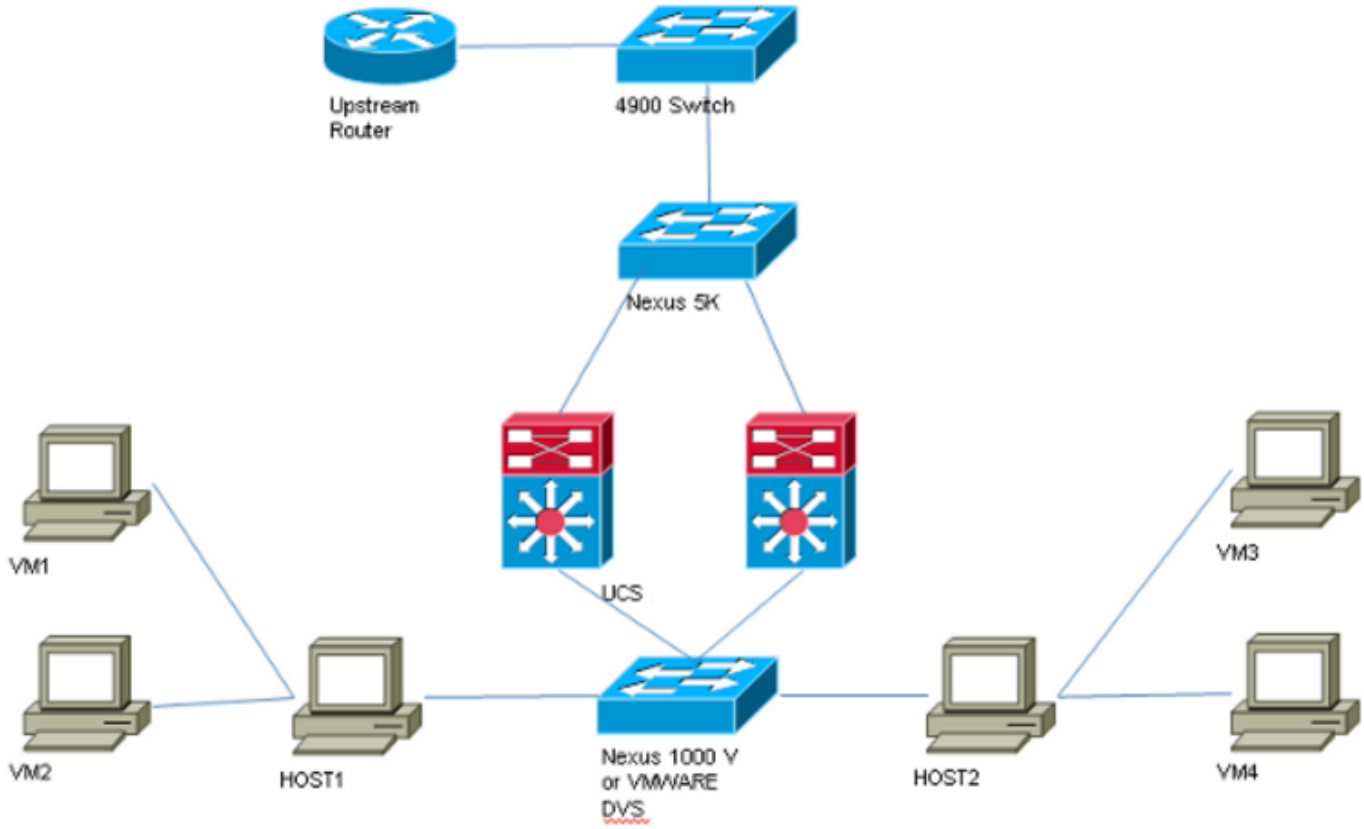
- 混雜埠與所有其他PVLAN埠通訊，並且是用來與PVLAN外部裝置通訊的埠。
- 隔離連線埠與相同PVLAN中除了混雜連線埠以外的其他連線埠完全分離L2（包括廣播）。
- 社群連線埠可與相同PVLAN中的其他連線埠以及混雜連線埠通訊。在L2中，團體埠與其他團體中的埠或隔離的PVLAN埠隔離。廣播只會傳播到團體中的其他連線埠和混雜連線埠。

請參閱RFC 5517,Cisco Systems的私人VLAN:在多客戶端環境中實現可擴展的安全性，以便瞭解PVLAN的理論、操作和概念。

設定

網路圖表

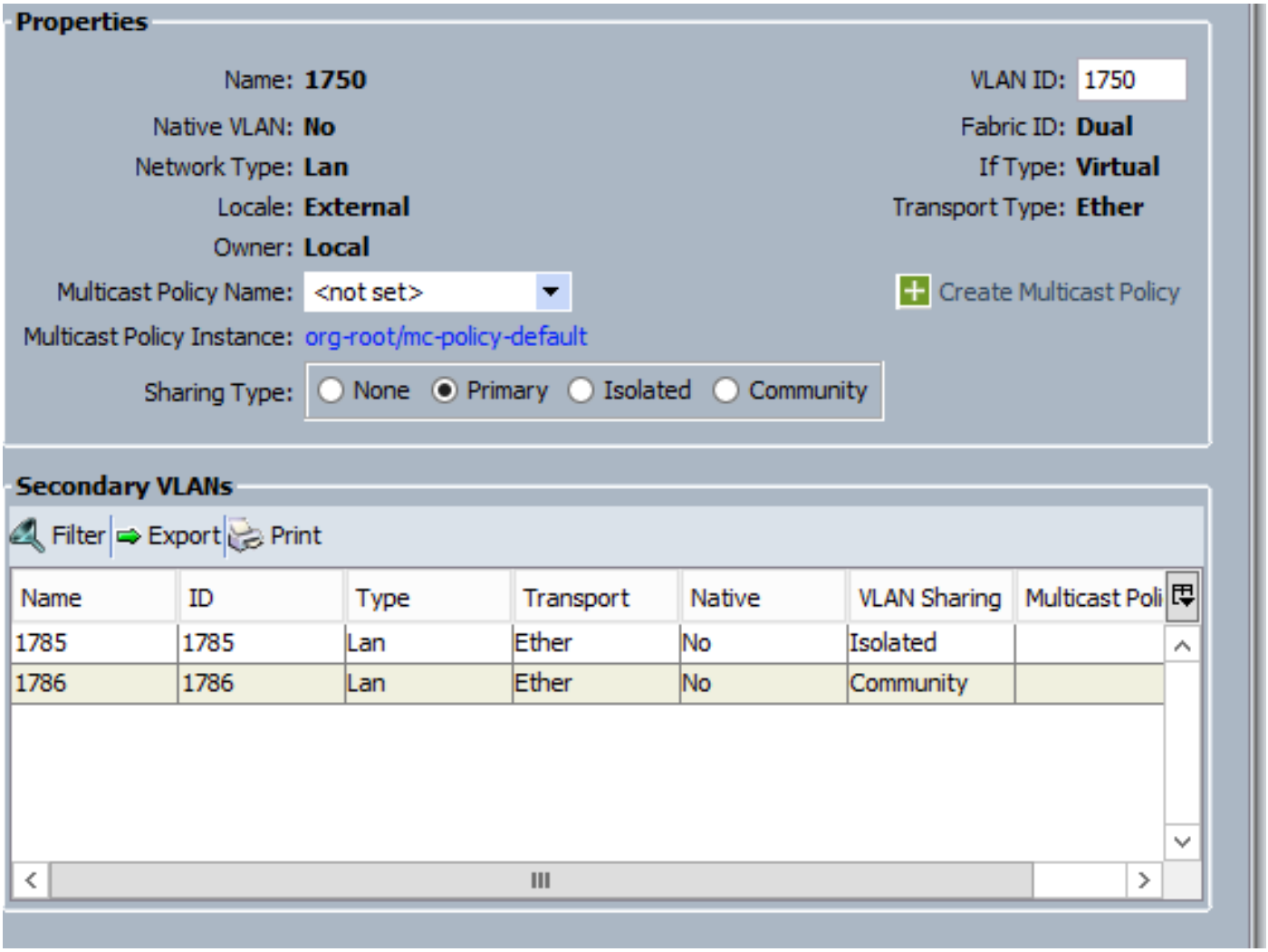
使用Nexus 1000v或VMware DVS



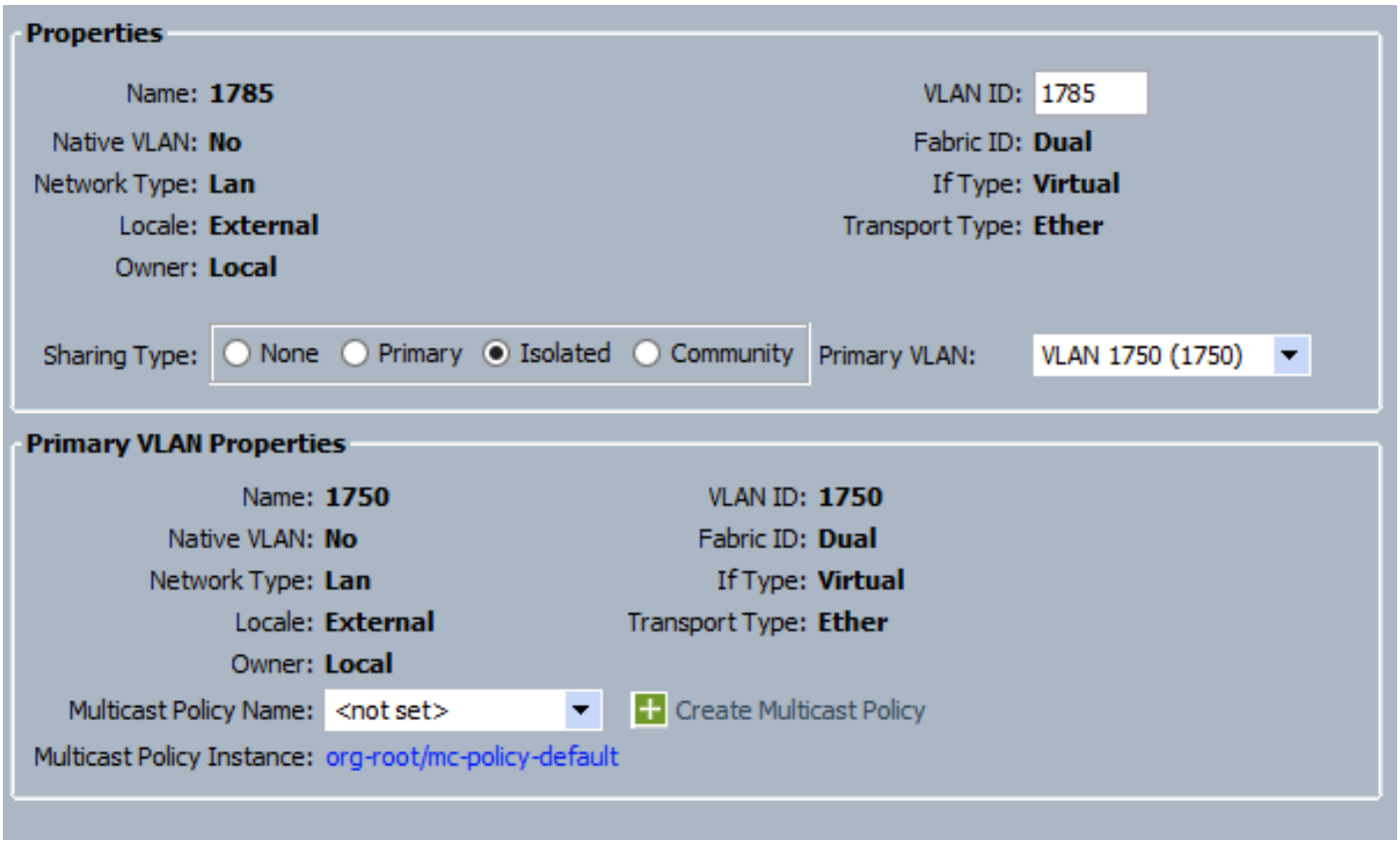
附註：本示例使用VLAN 1750作為主要，1785作為隔離，1786作為社群VLAN。

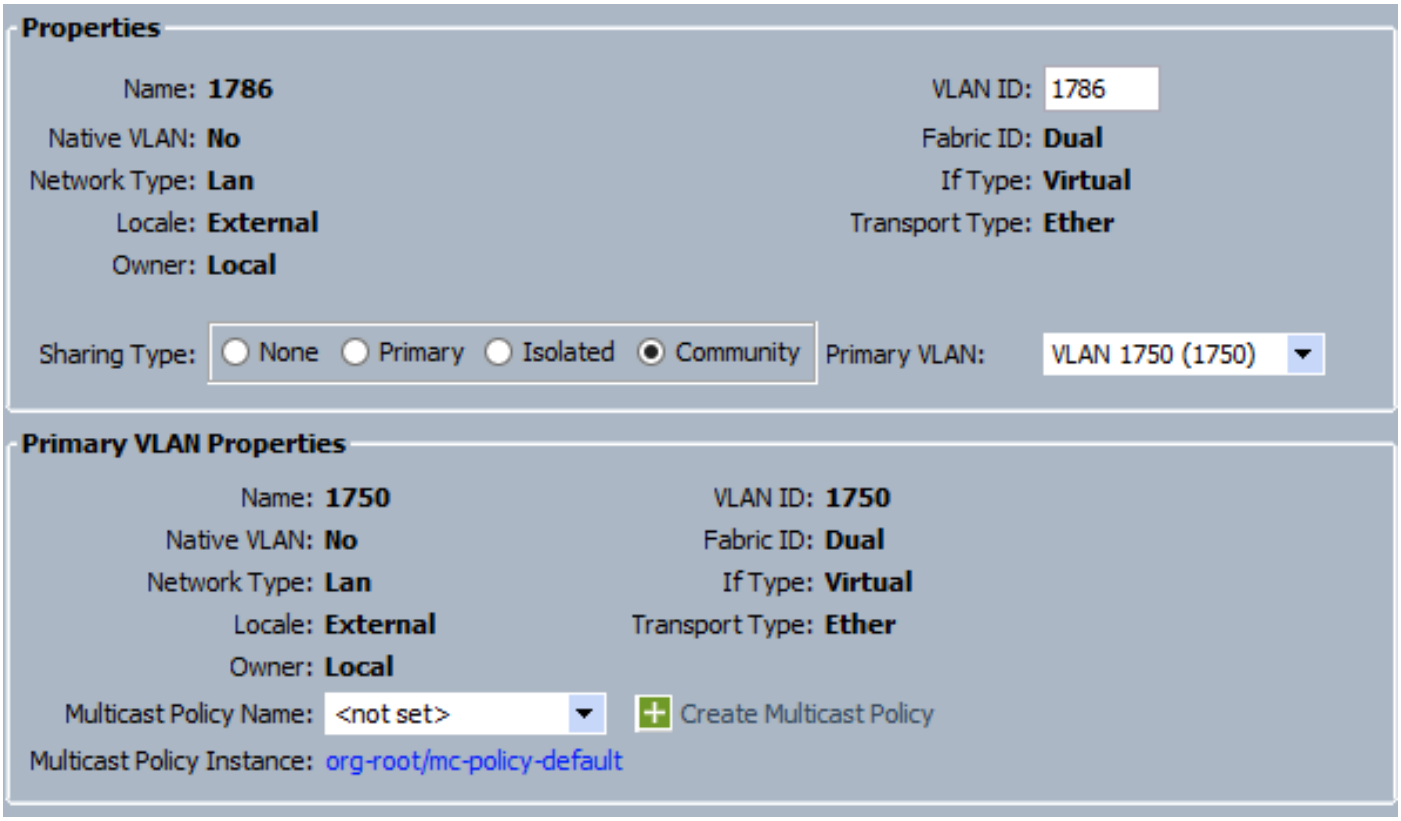
採用VMware DVS的UCS

1. 要建立主VLAN，請按一下**主**單選按鈕作為共用型別，然後輸入**VLAN ID** 1750，如下圖所示。

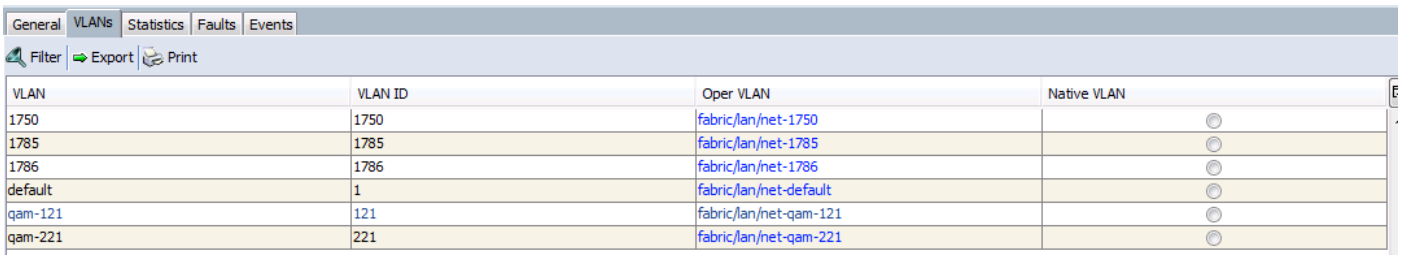


2.相應地建立**隔離**和**社群** VLAN，如下圖所示。這些都不必須是本徵VLAN。





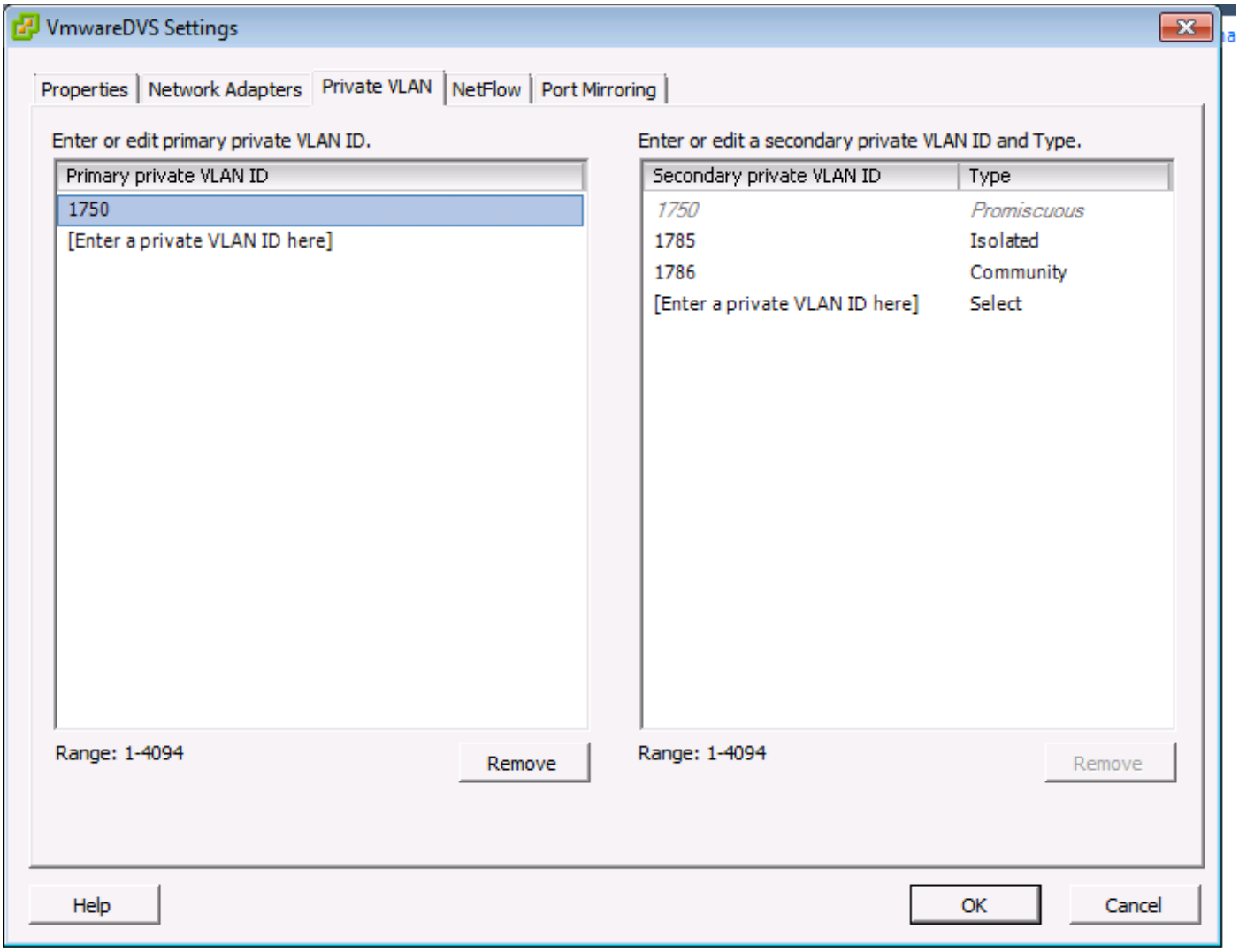
3. service-profile上的虛擬網路介面卡(vNIC)傳輸常規VLAN以及PVLAN，如圖所示。

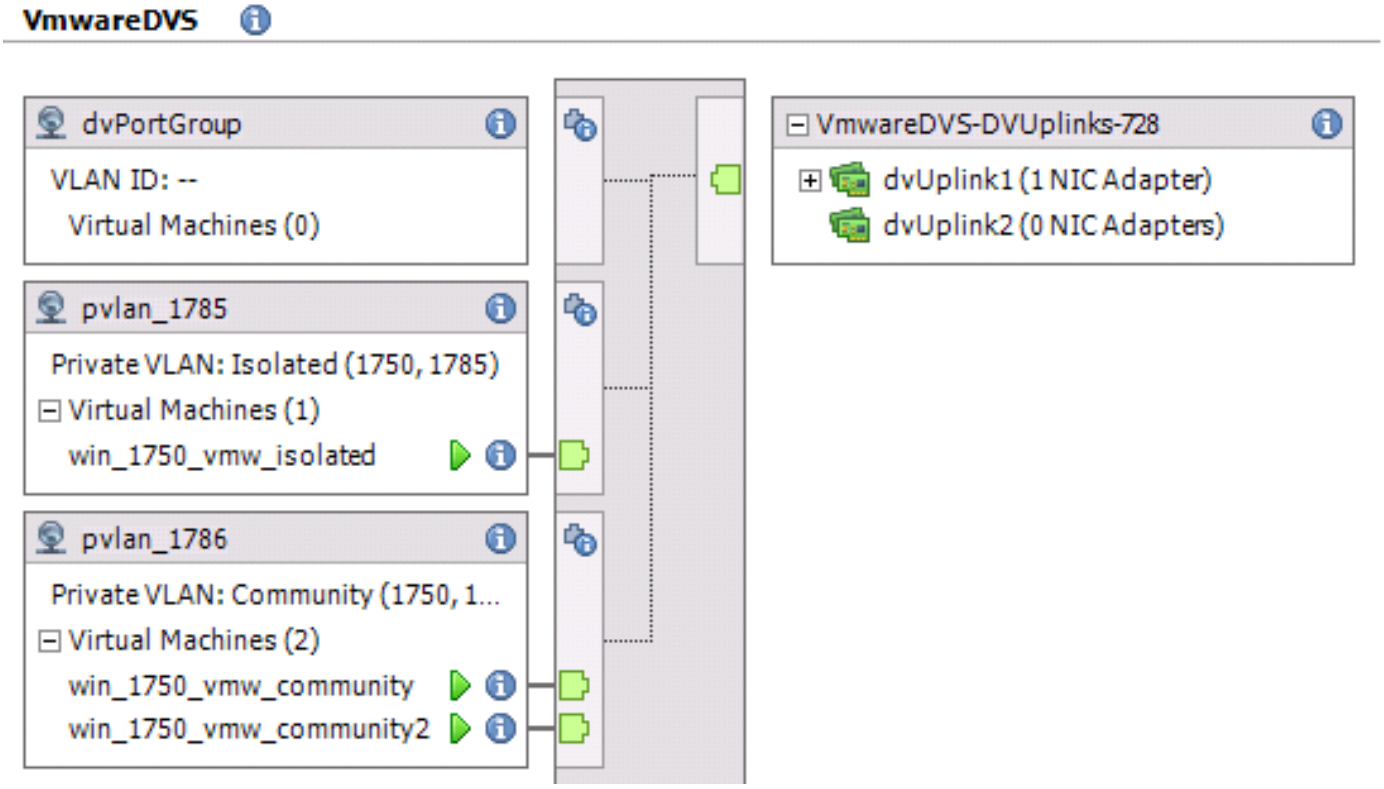


4. UCS上的上行鏈路埠通道傳輸常規VLAN以及PVLAN:

```
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
```

VMware DVS


VmwareDVS Settings
Properties
Network Adapters
Private VLAN
NetFlow
Port Mirroring
Enter or edit primary private VLAN ID.
Primary private VLAN ID
1750
[Enter a private VLAN ID here]
Range: 1-4094
Remove
Enter or edit a secondary private VLAN ID and Type.
Secondary private VLAN ID
Type
1750
Promiscuous
1785
Isolated
1786
Community
[Enter a private VLAN ID here]
Select
Range: 1-4094
Remove
Help
OK
Cancel


VmwareDVS
dvPortGroup
VLAN ID: --
Virtual Machines (0)
pvlan_1785
Private VLAN: Isolated (1750, 1785)
Virtual Machines (1)
win_1750_vmw_isolated
pvlan_1786
Private VLAN: Community (1750, 1...
Virtual Machines (2)
win_1750_vmw_community
win_1750_vmw_community2
VmwareDVS-DVUplinks-728
dvUplink1 (1 NIC Adapter)
dvUplink2 (0 NIC Adapters)

上游N5k交換機

```
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
```

UCS版本3.1(3)的行為更改

在UCS版本3.1(3)之前，社群VLAN中的虛擬機器可以與VMware DVS上的主VLAN中的虛擬機器通訊，主VLAN虛擬機器位於UCS中。此行為不正確，因為主VM必須始終北向或UCS外部。此行為通過缺陷ID CSCvh87378記錄 .

從UCS版本2.2(2)開始，由於代碼中的缺陷，社群VLAN能夠與FI後方的主VLAN通訊。但是Isolated無法與FI背後的主節點通訊。兩個（隔離的和社群）VM仍能夠與FI外部的主虛擬機器通訊。

從3.1(3)開始，此缺陷允許團體與位於FI後面的主虛擬機器通訊，已修復，因此社群VM將無法與位於UCS內的主VLAN中的VM通訊。

為了解決這種情況，主VM或者需要移出（北向）UCS。如果不可行，則需要將主VM移至另一個屬於常規VLAN而非專用VLAN的VLAN。

例如，在韌體3.1(3)之前，社群VLAN 1786中的VM可以與駐留在UCS中的主VLAN 1750中的VM通訊，但此通訊在韌體3.1(3)及更高版本中會中斷，如圖所示。

附註：

CSCvh87378已在3.2(3l)和4.0.4e及更高版本中進行了定址，因此在UCS後面可以有主Vlan。但是

請注意，UCS內的隔離VLAN將無法與UCS內的主VLAN通訊。只有社群VLAN和主VLAN才能在UCS落後時相互通訊。

```
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)#
```

上游4900交換器

附註：在本例中，4900是到外部網路的L3介面。如果您的L3拓撲不同，請進行相應的更改

在4900交換機上，執行這些步驟，並設定混雜埠。PVLAN在混雜埠結束。

1. 如果需要，開啟PVLAN功能。
2. 按照在Nexus 5K上的步驟建立和關聯VLAN。
3. 在4900交換器的輸出連線埠上建立混雜連線埠。從此以後，在VLAN 1750上會看到來自VLAN 1785和1786的資料包，本例中如此。

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

在上游路由器上，只為VLAN 1750建立子介面。在此級別，要求取決於您使用的網路配置：

```
interface GigabitEthernet0/1.1

encapsulation dot1Q 1750

IP address10.10.175.254/24
```

驗證

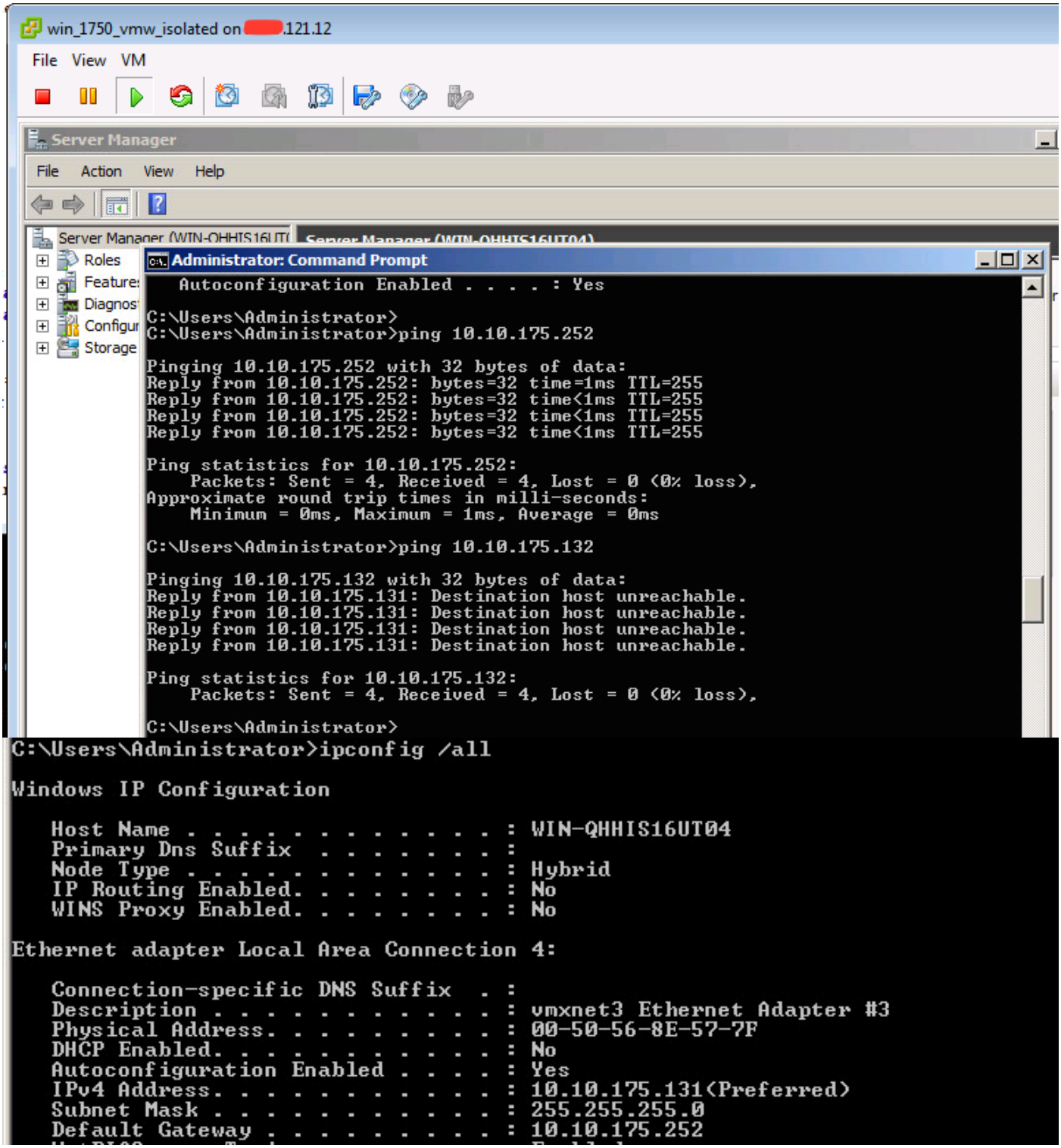
目前沒有適用於此組態的驗證程序。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

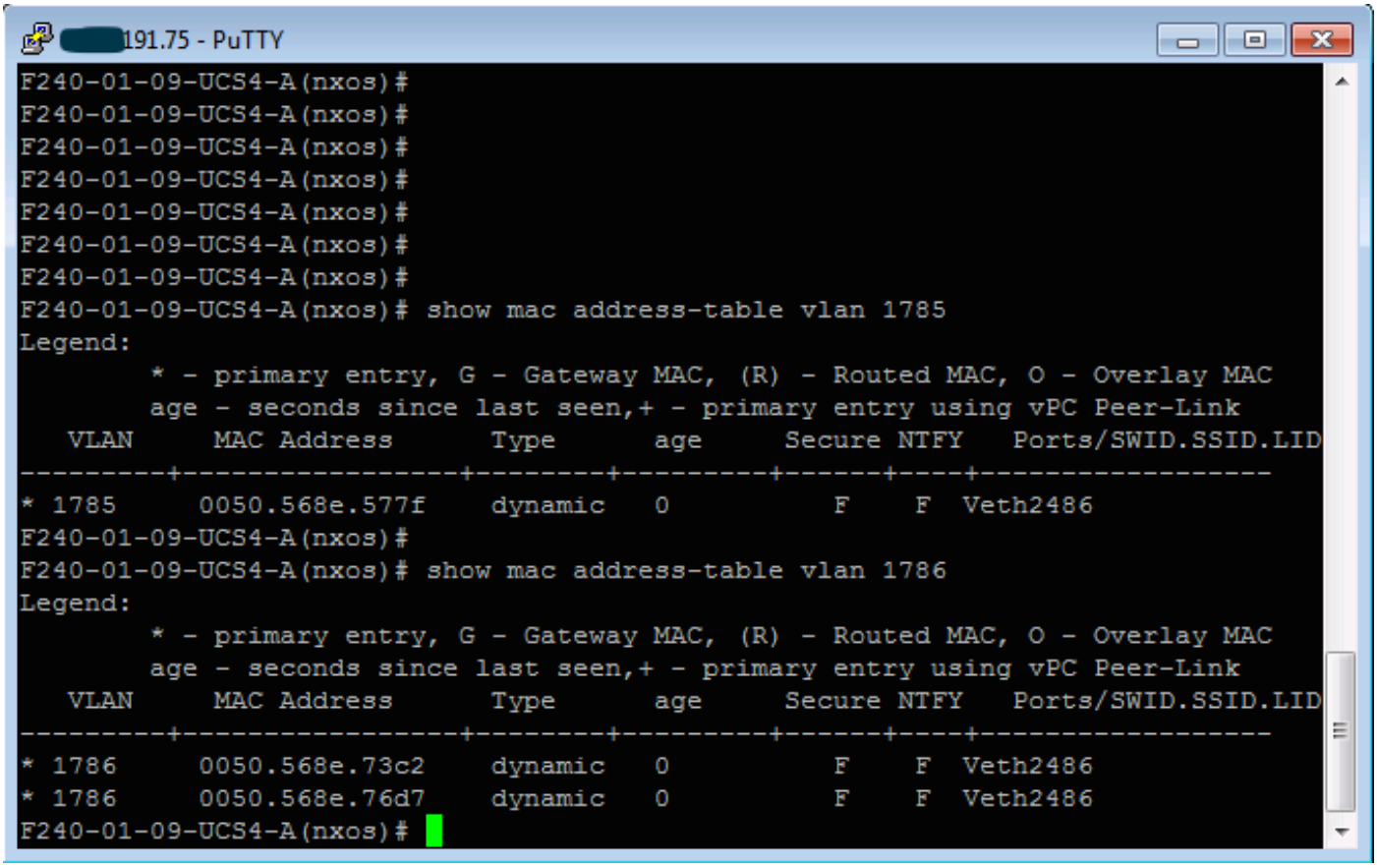
此過程介紹如何使用PVLAN測試VMware DVS的配置。

1.對埠組中配置的其他系統以及混雜埠上的路由器或其他裝置運行ping。對通過混雜埠的裝置執行Ping操作必須有效，而對隔離VLAN中的其他裝置執行的Ping操作必須失敗，如圖所示。



檢查MAC地址表，檢視您的MAC被獲取的位置。在所有交換機上，MAC必須位於隔離VLAN中，具有混雜埠的交換機除外。在混雜交換器上，MAC必須在主VLAN中。

2. UCS，如圖所示。



3.檢查同一MAC的上游n5k，n5k上必須存在與早期輸出類似的輸出，如下圖所示。

```
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#
```

在上游N5k上配置帶有混雜埠的Nexus 1000v

UCS配置

根據VMware DVS的示例，UCS配置（包括服務配置檔案vNIC配置）保持不變。

N1k配置

```
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
```

此程式介紹如何測試配置。

1.對埠組中配置的其他系統以及混雜埠上的路由器或其他裝置運行ping。通過混雜埠對裝置執行的Ping操作必須有效，而通過隔離VLAN中的其他裝置的ping操作必須失敗，如上一節和圖中所示。