Configurazione di VLAN private e UCS con VMware DVS o Cisco Nexus 1000v

Sommario

Introduzione

Questo documento descrive il supporto di VLAN private (PVLAN) per Cisco Unified Computing System (UCS) nella versione 2.2(2c) e successive.

> **Attenzione:** Il comportamento cambia a partire dalla versione 3.1(3a) del firmware UCS, come descritto nella sezione **Modifica del comportamento con UCS versione 3.1(3) e successive**.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- UCS

- Cisco Nexus 1000V (N1K) o VMware Distributed Virtual Switch (DVS)
- VMware
- Switching Layer 2 (L2)

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Una VLAN privata è una VLAN configurata per l'isolamento L2 da altre porte nell'ambito della stessa VLAN privata. Le porte che appartengono a una PVLAN sono associate a un set comune di VLAN di supporto, che vengono utilizzate per creare la struttura della PVLAN.

Sono disponibili tre tipi di porte PVLAN:

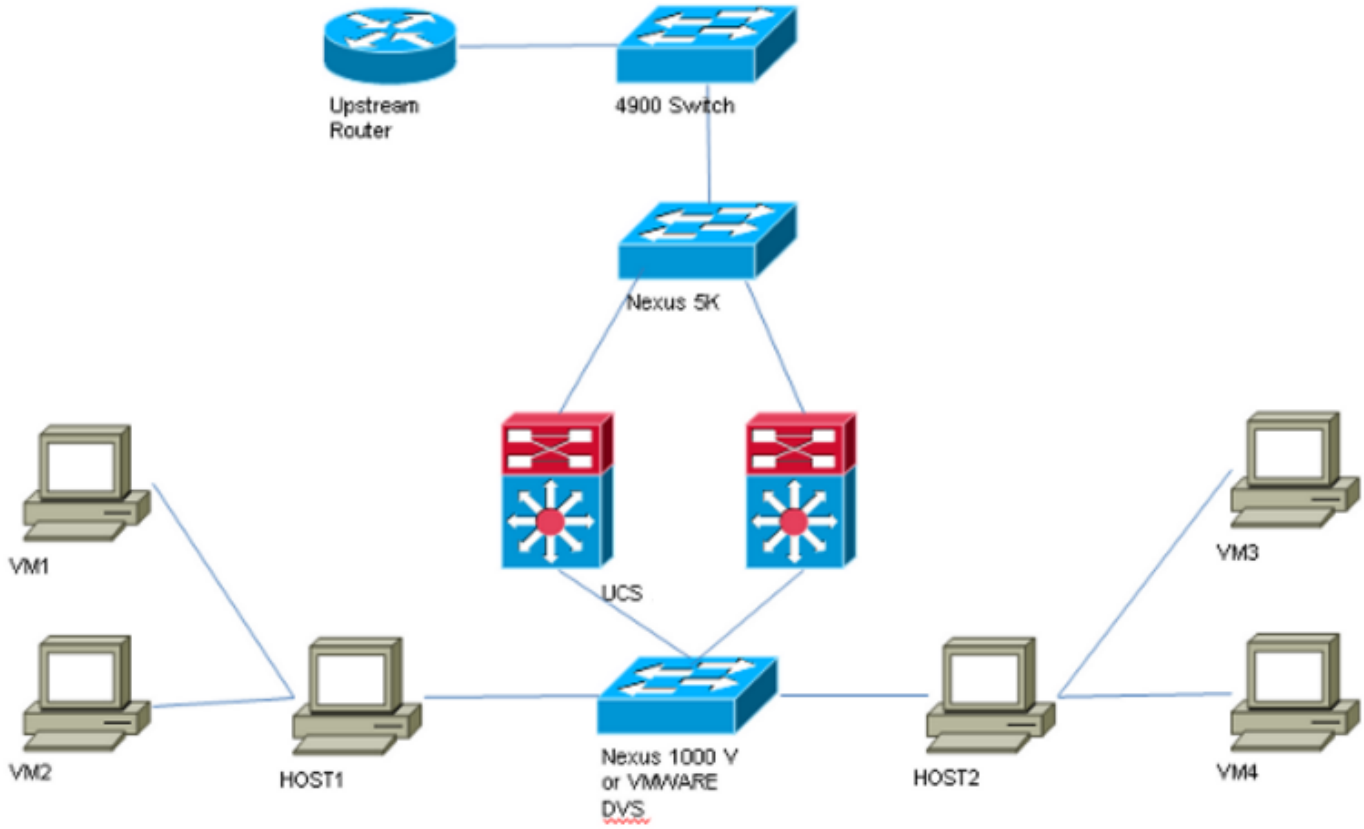
- Una porta promiscua comunica con tutte le altre porte PVLAN e è la porta utilizzata per comunicare con i dispositivi esterni alla PVLAN.
- Una porta isolata ha una separazione L2 completa (che include i broadcast) da altre porte nell'ambito della stessa PVLAN, ad eccezione della porta promiscua.
- Una porta della community può comunicare con altre porte della stessa PVLAN e della porta promiscua. Le porte della community sono isolate sull'L2 dalle porte di altre community o dalle porte PVLAN isolate. Le trasmissioni vengono propagate solo ad altri porti della comunità e alla porta promiscua.

Per ulteriori informazioni, fare riferimento alla RFC 5517 - VLAN private di Cisco Systems: Sicurezza scalabile in un ambiente multi-client per comprendere la teoria, il funzionamento e i concetti delle PVLAN.

Configurazione

Esempio di rete

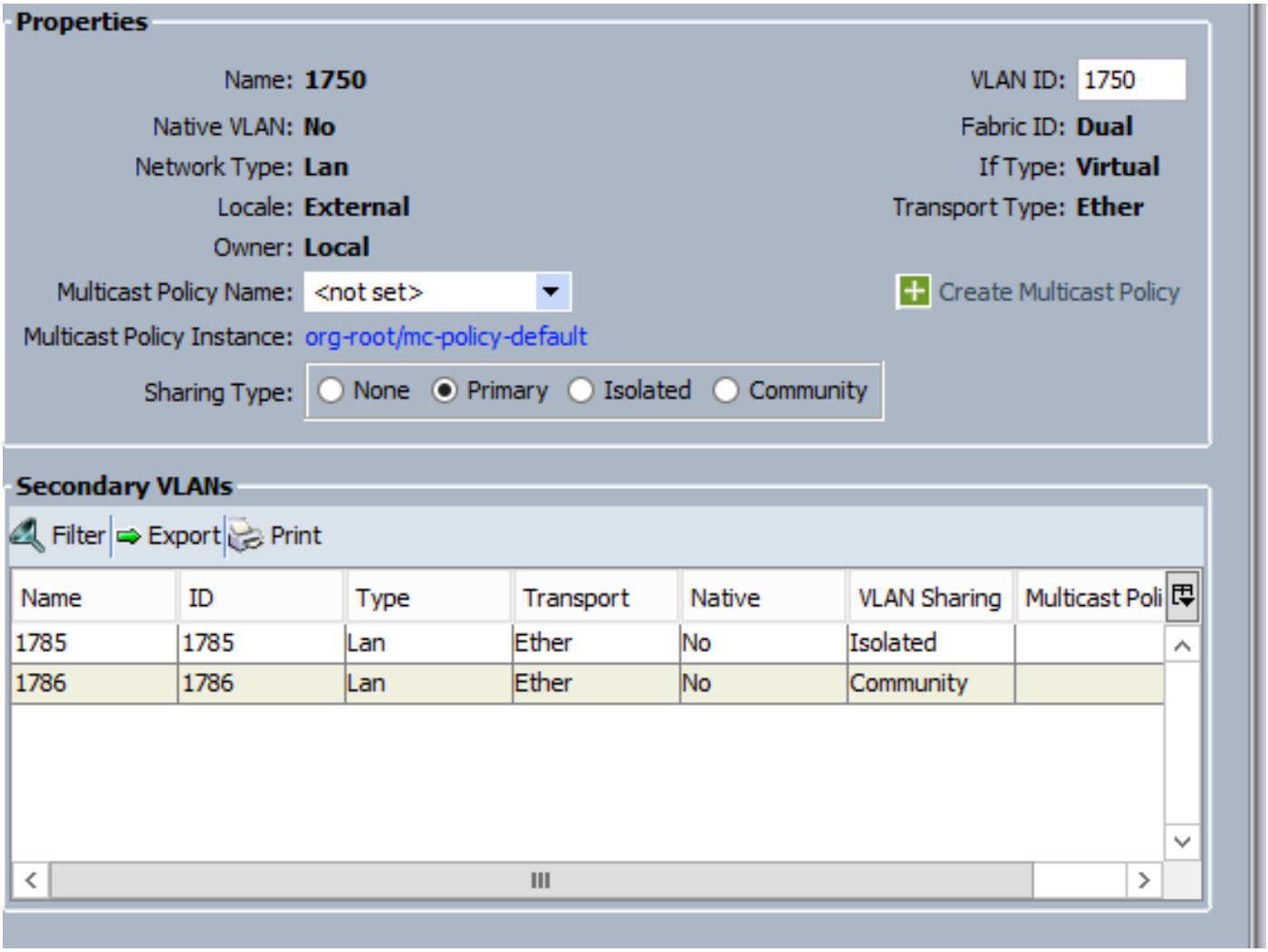
Con Nexus 1000v o VMware DVS



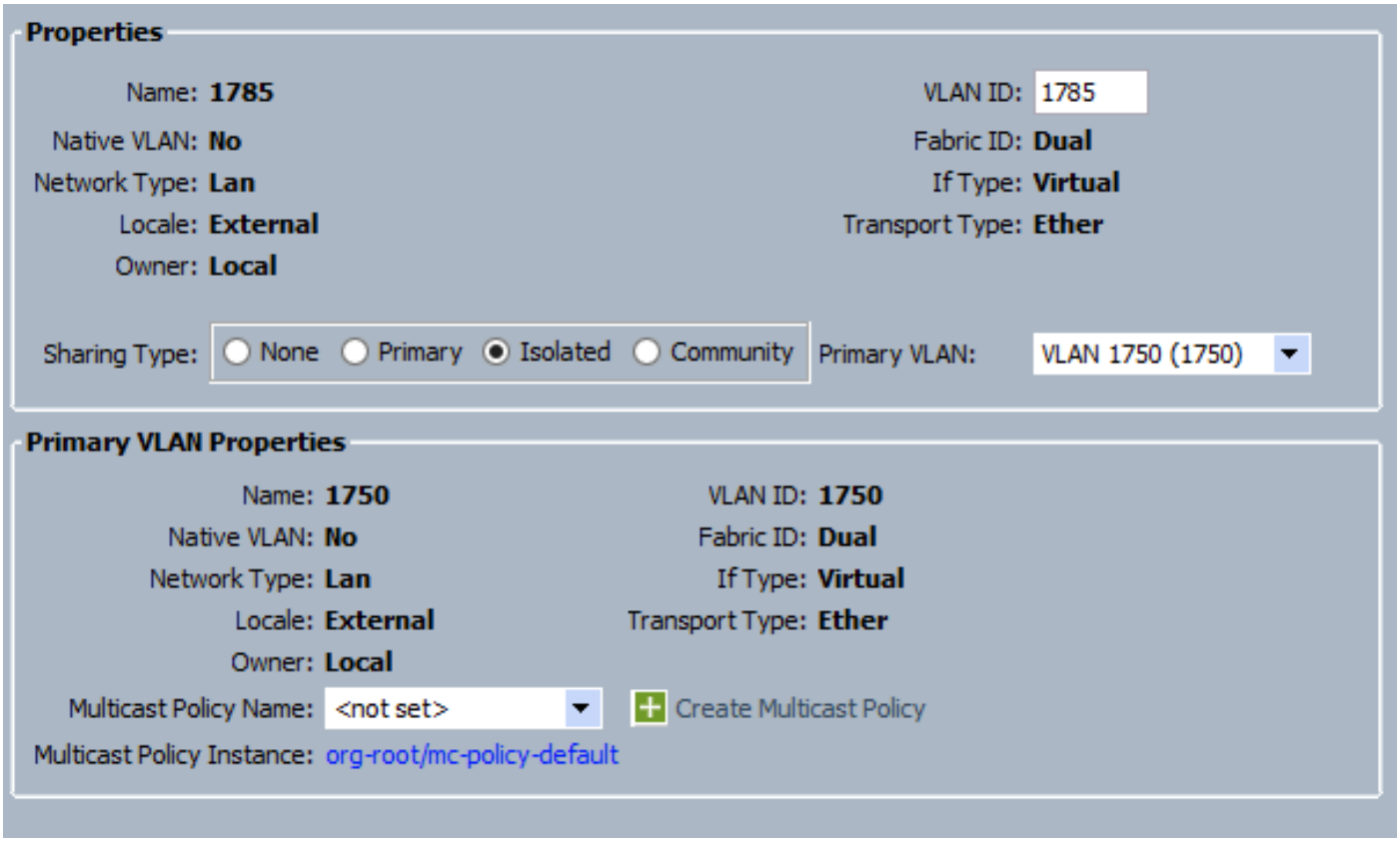
Nota: In questo esempio viene usata la VLAN 1750 come principale, la VLAN 1785 come isolata e la VLAN 1786 come comunità.

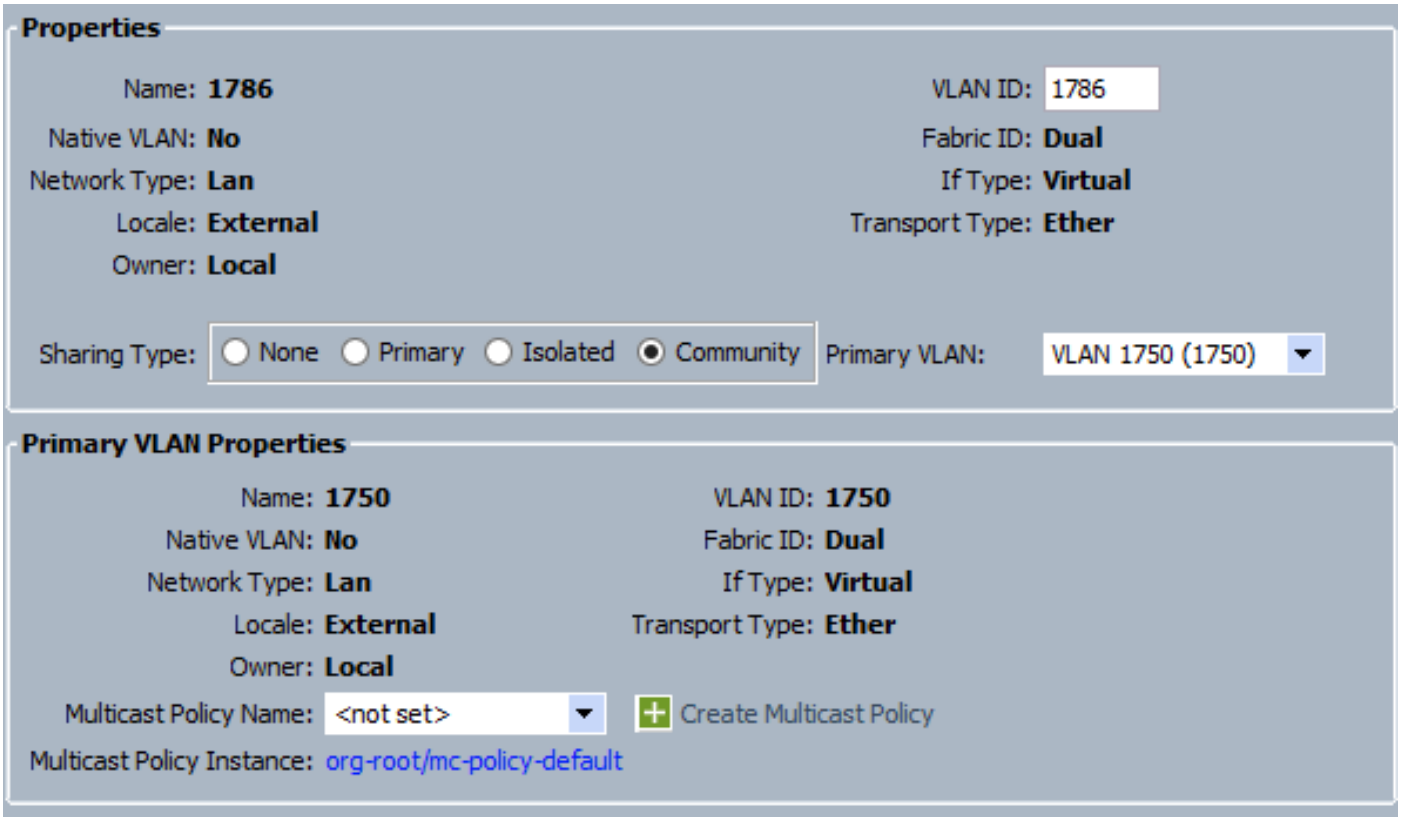
UCS con VMware DVS

1. Per creare la VLAN primaria, fare clic sul pulsante di opzione **Primary** (Principale) come tipo di condivisione, quindi immettere un **ID VLAN** di 1750, come mostrato nell'immagine.

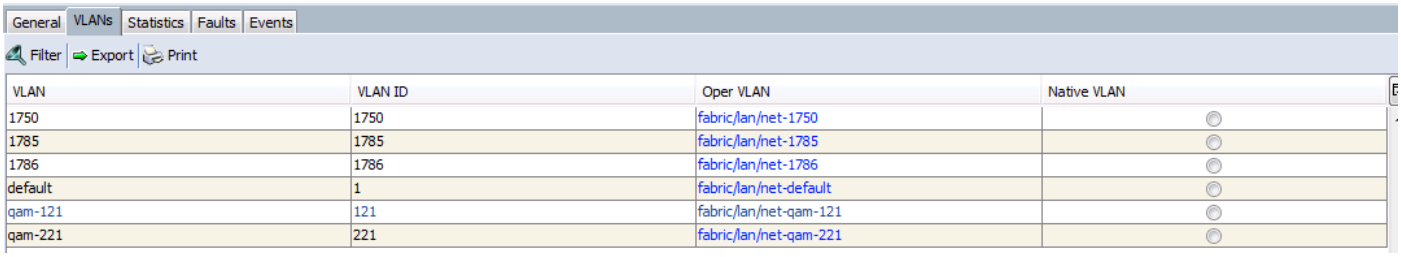


2. Creare VLAN **isolate** e **comunitarie** come mostrato nelle immagini. Nessuna di queste reti deve essere una VLAN nativa.





3. La scheda di interfaccia di rete virtuale (vNIC) sul profilo del servizio porta VLAN regolari e PVLAN, come mostrato nell'immagine.

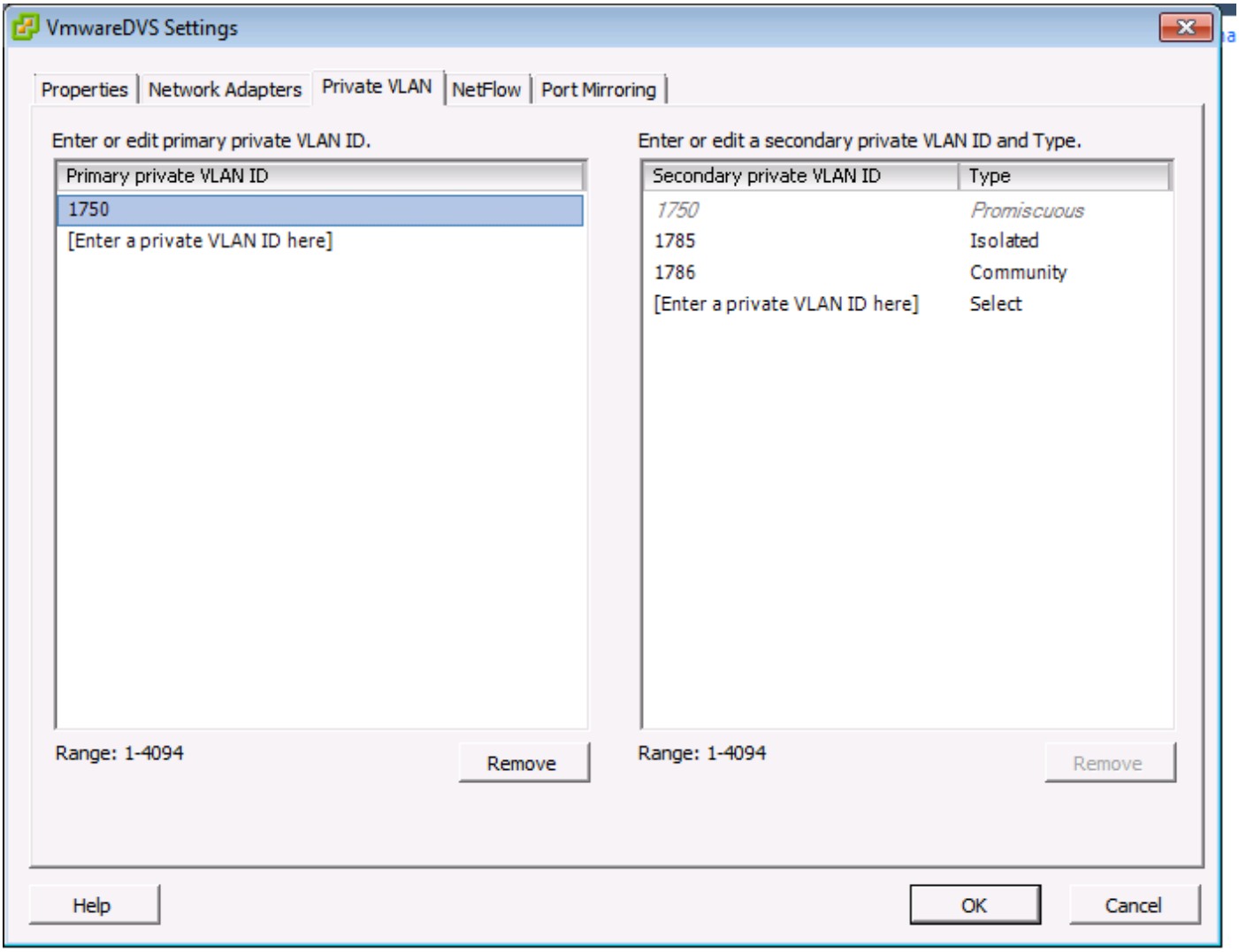


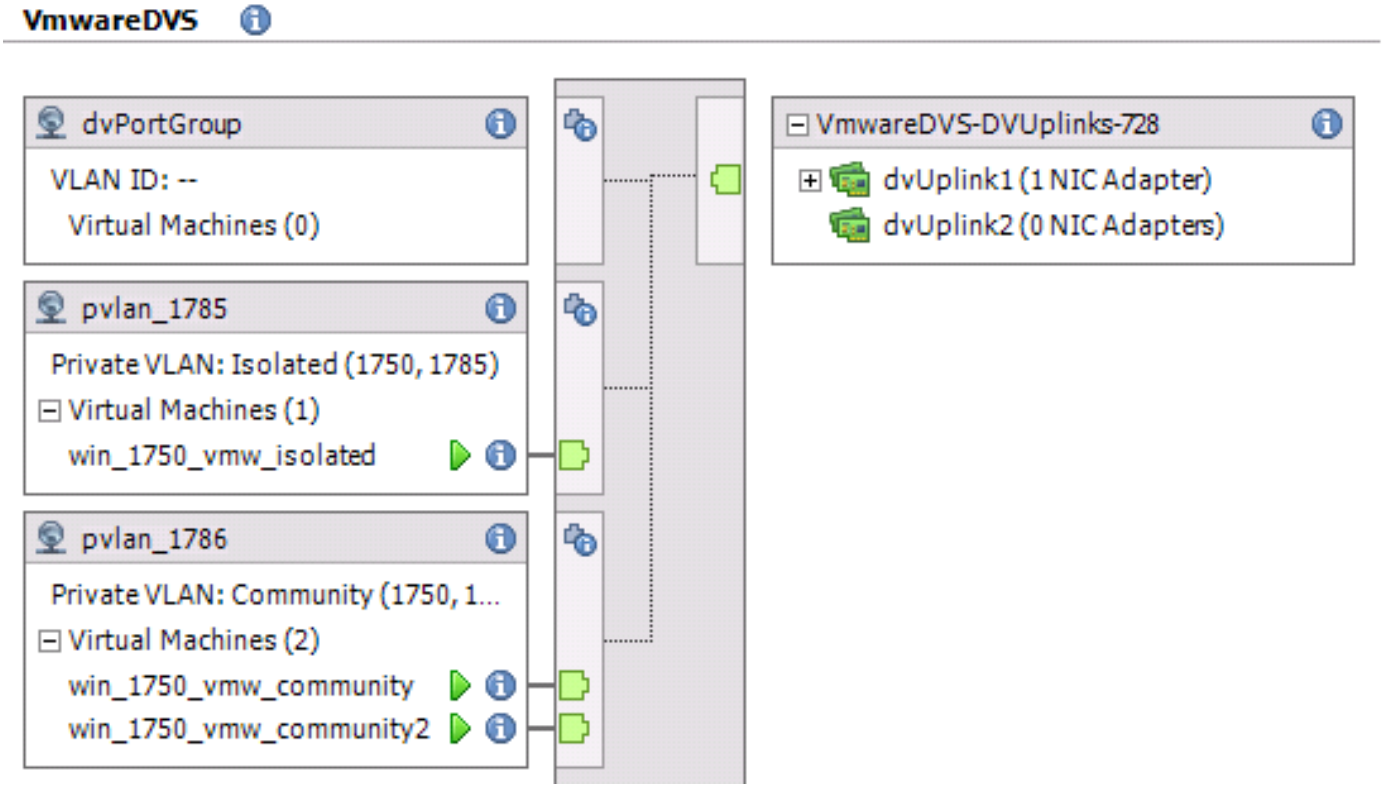
VLAN	VLAN ID	Oper VLAN	Native VLAN
1750	1750	fabric/lan/net-1750	
1785	1785	fabric/lan/net-1785	
1786	1786	fabric/lan/net-1786	
default	1	fabric/lan/net-default	
qam-121	121	fabric/lan/net-qam-121	
qam-221	221	fabric/lan/net-qam-221	

4. Il canale della porta uplink sull'UCS contiene VLAN regolari e 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 VMware





Switch Upstream 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
```

Modifica del comportamento con UCS versione 3.1(3)

Prima della versione 3.1(3) di UCS, è possibile fare in modo che una VM nella VLAN della community comunichi con una VM nella VLAN primaria su VMware DVS in cui la VLAN primaria risiede all'interno dell'UCS. Questo comportamento non è corretto in quanto la macchina virtuale primaria deve sempre essere in direzione nord o esterna a UCS. Questo comportamento è documentato tramite l'ID difetto CSCvh87378 .

A partire dalla versione UCS 2.2(2), a causa di un errore nel codice, la VLAN della community è stata in grado di comunicare con la VLAN primaria presente dietro l'interfaccia. Ma Isolato non potrebbe mai comunicare con il primario dietro la FI. Sia le VM (isolate e di comunità) sono ancora in grado di comunicare con le principali al di fuori dell'infrastruttura.

A partire dalla versione 3.1(3), questo difetto consente alla community di comunicare con il server principale dietro al server di infrastruttura, è stato corretto e quindi le VM della community non saranno in grado di comunicare con una VM nella VLAN principale che risiede all'interno di UCS.

Per risolvere questa situazione, la macchina virtuale primaria deve essere spostata (in direzione nord) al di fuori di UCS. Se questa opzione non è disponibile, la VM principale deve essere spostata su un'altra VLAN normale e non su una VLAN privata.

Ad esempio, prima del firmware 3.1(3), una VM nella VLAN 1786 della community può comunicare con una VM nella VLAN 1750 principale che risiede all'interno di UCS; tuttavia, questa comunicazione si interromperebbe con il firmware 3.1(3) e versioni successive, come mostrato

nell'immagine.

NOTA:

—

La tecnologia CSCvh87378 è stata trattata nelle versioni 3.2(3l) e 4.0.4e e successive, quindi possiamo avere una Vlan primaria dietro UCS. Tuttavia, si tenga presente che le vlan isolate all'interno di UCS non saranno in grado di comunicare con la vlan primaria all'interno di UCS. Solo le vlan di comunità e le vlan primarie possono comunicare tra loro quando entrambe sono dietro l'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 Upstream 4900

> **Nota:** Nell'esempio, 4900 è un'interfaccia L3 con una rete esterna. Se la topologia per L3 è diversa, apportare le modifiche necessarie

Sullo switch 4900, eseguire queste operazioni e configurare la porta promiscua. La PVLAN termina sulla porta promiscua.

1. Se necessario, attivare la funzione PVLAN.
2. Creare e associare le VLAN secondo le istruzioni del Nexus 5K.
3. Creare la porta promiscua sulla porta di uscita dello switch 4900. Da questo momento in poi, i pacchetti delle VLAN 1785 e 1786 vengono visualizzati sulla VLAN 1750.

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

Sul router upstream, creare una sottointerfaccia solo per la VLAN 1750. A questo livello, i requisiti dipendono dalla configurazione di rete utilizzata:

```
interface GigabitEthernet0/1.1

encapsulation dot1Q 1750

IP address10.10.175.254/24
```

Verifica

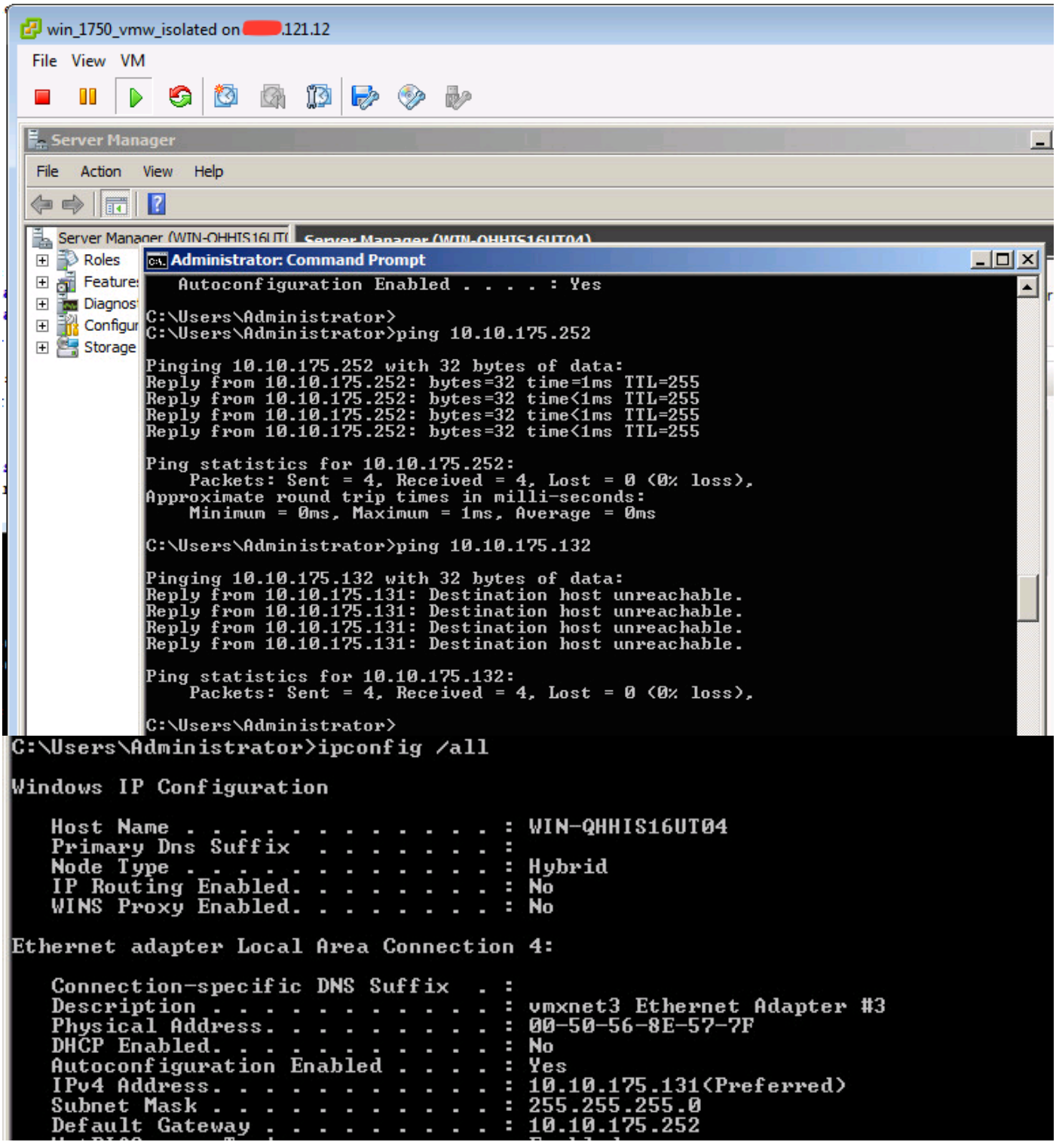
Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

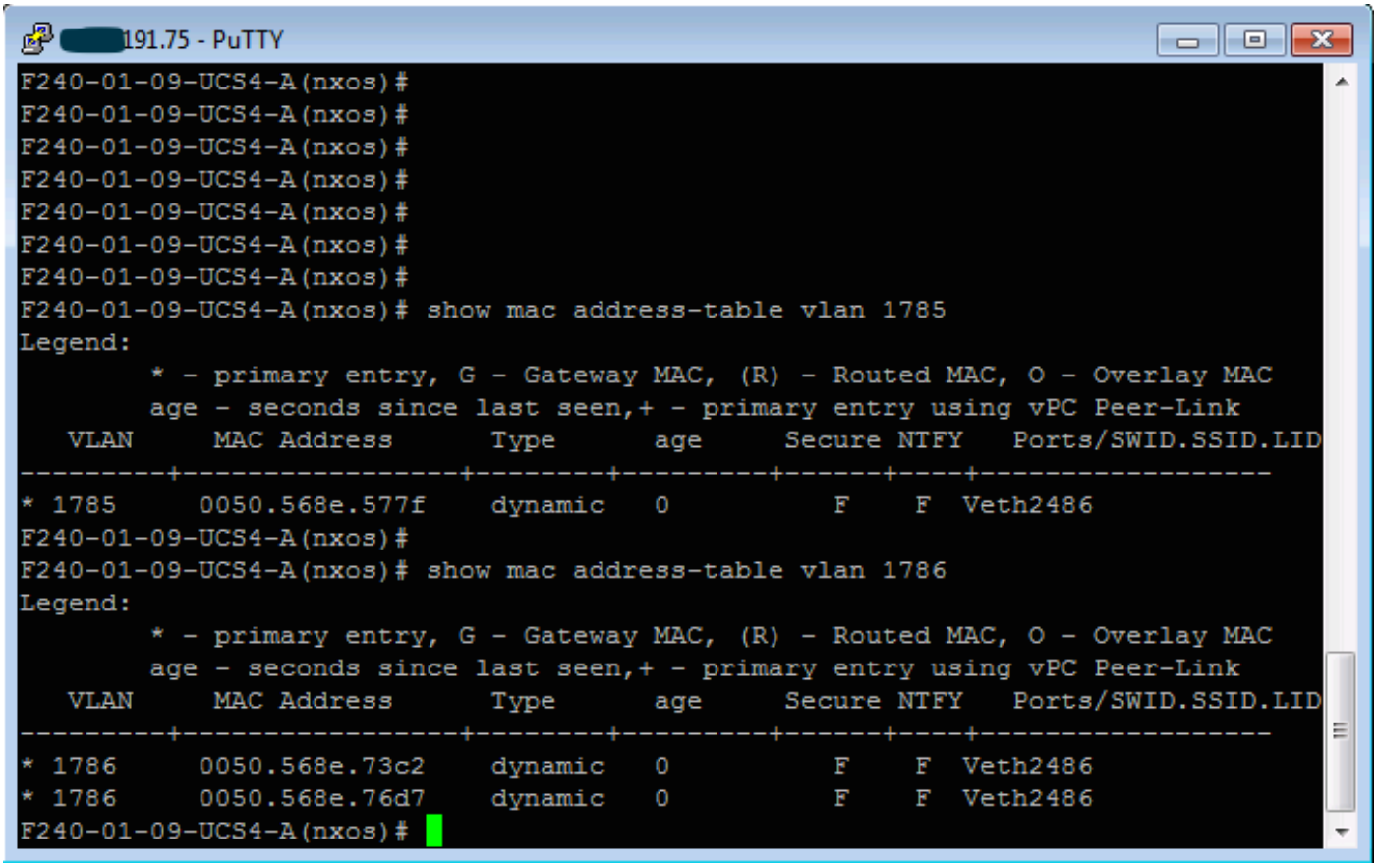
In questa procedura viene descritto come eseguire il test della configurazione per VMware DVS con l'utilizzo di PVLAN.

1. Eseguire i ping su altri sistemi configurati nel gruppo di porte e sul router o su un altro dispositivo della porta promiscua. I ping verso il dispositivo oltre la porta promiscua devono funzionare, mentre quelli verso altri dispositivi nella VLAN isolata devono avere esito negativo, come mostrato nelle immagini.



Controllare le tabelle degli indirizzi MAC per verificare dove viene appreso l'indirizzo MAC. Su tutti gli switch, l'indirizzo MAC deve essere nella VLAN isolata ad eccezione dello switch con la porta promiscua. Sullo switch promiscuo, l'indirizzo MAC deve essere nella VLAN primaria.

2. UCS come mostrato nell'immagine.



3. Controllare a monte n5k per lo stesso MAC, l'output simile a quello precedente deve essere presente su n5k e come mostrato nell'immagine.

```
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#
```

Configurazione con Nexus 1000v con porta promiscua su Upstream N5k

Configurazione UCS

La configurazione UCS (che include la configurazione vNIC del profilo del servizio) rimane la stessa dell'esempio di VMware DVS.

Configurazione 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
```

In questa procedura viene descritto come eseguire il test della configurazione.

1. Eseguire i ping su altri sistemi configurati nel gruppo di porte e sul router o su un altro dispositivo della porta promiscua. Il ping verso il dispositivo oltre la porta promiscua deve funzionare, mentre il ping verso gli altri dispositivi della VLAN isolata deve avere esito negativo, come mostrato nella sezione precedente e nelle immagini.