Private VLAN en UCS configureren met VMware DVS of Cisco Nexus 1000v

Inhoud

Inleiding

Dit document beschrijft de ondersteuning van Private VLAN (PVLAN) voor Cisco Unified Computing System (UCS) in de release 2.2(2c) en hoger.

> **Voorzichtig:** Er is een gedragsverandering die begint met UCS firmware versie 3.1(3a) zoals beschreven in **Gedragsverandering met UCS versie 3.1(3) en Later** sectie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- UCS
- Cisco Nexus 1000V (N1K) voor VMware gedistribueerde virtuele switch (DVS)

- VMware
- Layer 2 (L2) switching

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Een privé VLAN is een VLAN dat voor L2 isolatie van andere poorten binnen hetzelfde privé VLAN wordt gevormd. PVLAN-poorten die tot een PVLAN behoren, worden gekoppeld aan een gemeenschappelijke reeks VLAN's voor ondersteuning, die worden gebruikt om de PVLAN-structuur te maken.

Er zijn drie typen PVLAN-poorten:

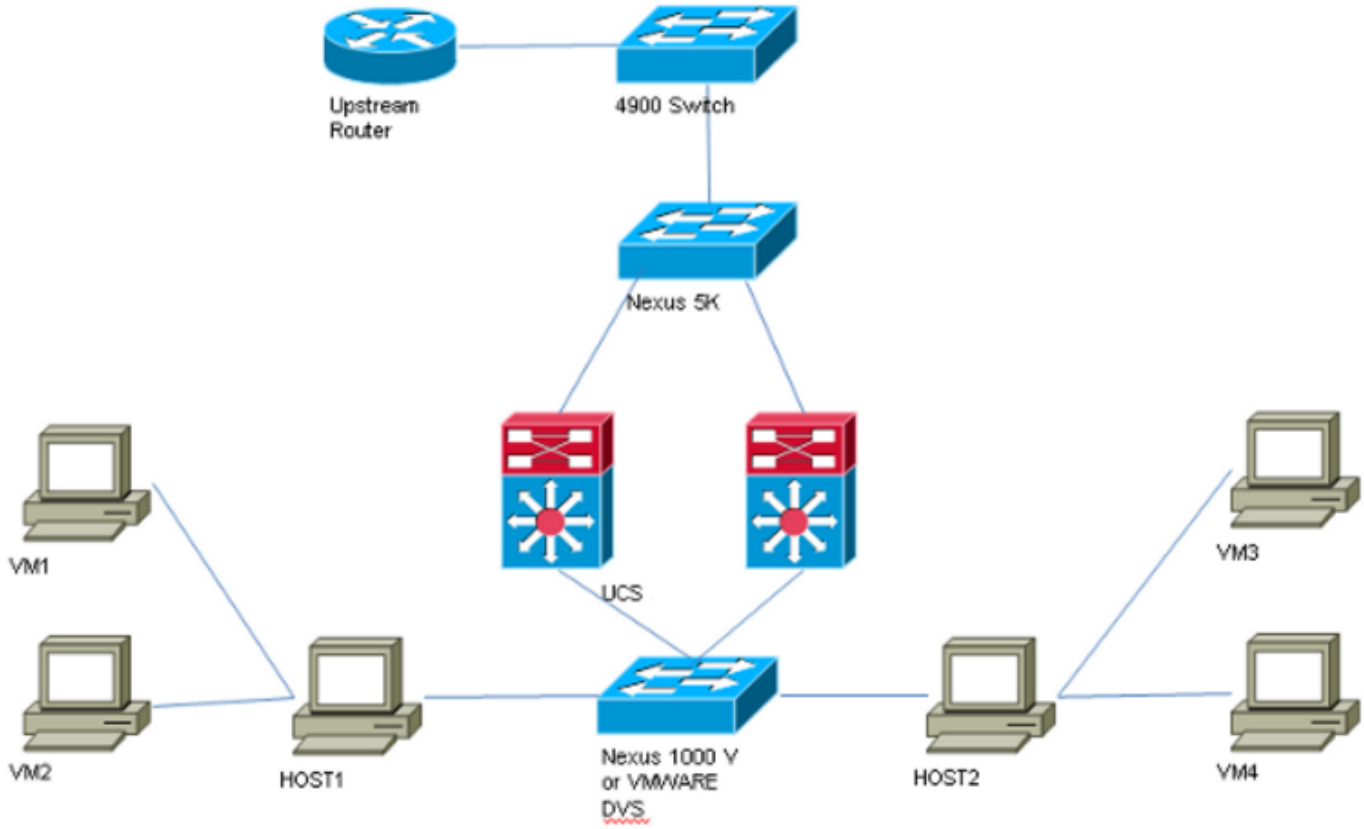
- Een veelbelovende poort communiceert met alle andere PVLAN-poorten en is de poort die wordt gebruikt om met apparaten buiten het PVLAN te communiceren.
- Een geïsoleerde haven heeft een volledige L2-scheiding (die uitzendingen omvat) van andere havens binnen hetzelfde PVLAN met uitzondering van de veelbelovende haven.
- Een community-poort kan met andere poorten in hetzelfde PVLAN communiceren evenals de veelbelovende poort. De havens van de Gemeenschap worden in L2 geïsoleerd van havens in andere gemeenschappen of geïsoleerde havens van PVLAN. De uitzendingen worden alleen verspreid naar andere havens in de gemeenschap en naar de veelbelovende haven.

Raadpleeg RFC 5517, Cisco Systems' Private VLAN's: Schaalbare beveiliging in een omgeving voor meerdere client om de theorie, werking en concepten van PVLAN's te begrijpen.

Configureren

Netwerkdiagram

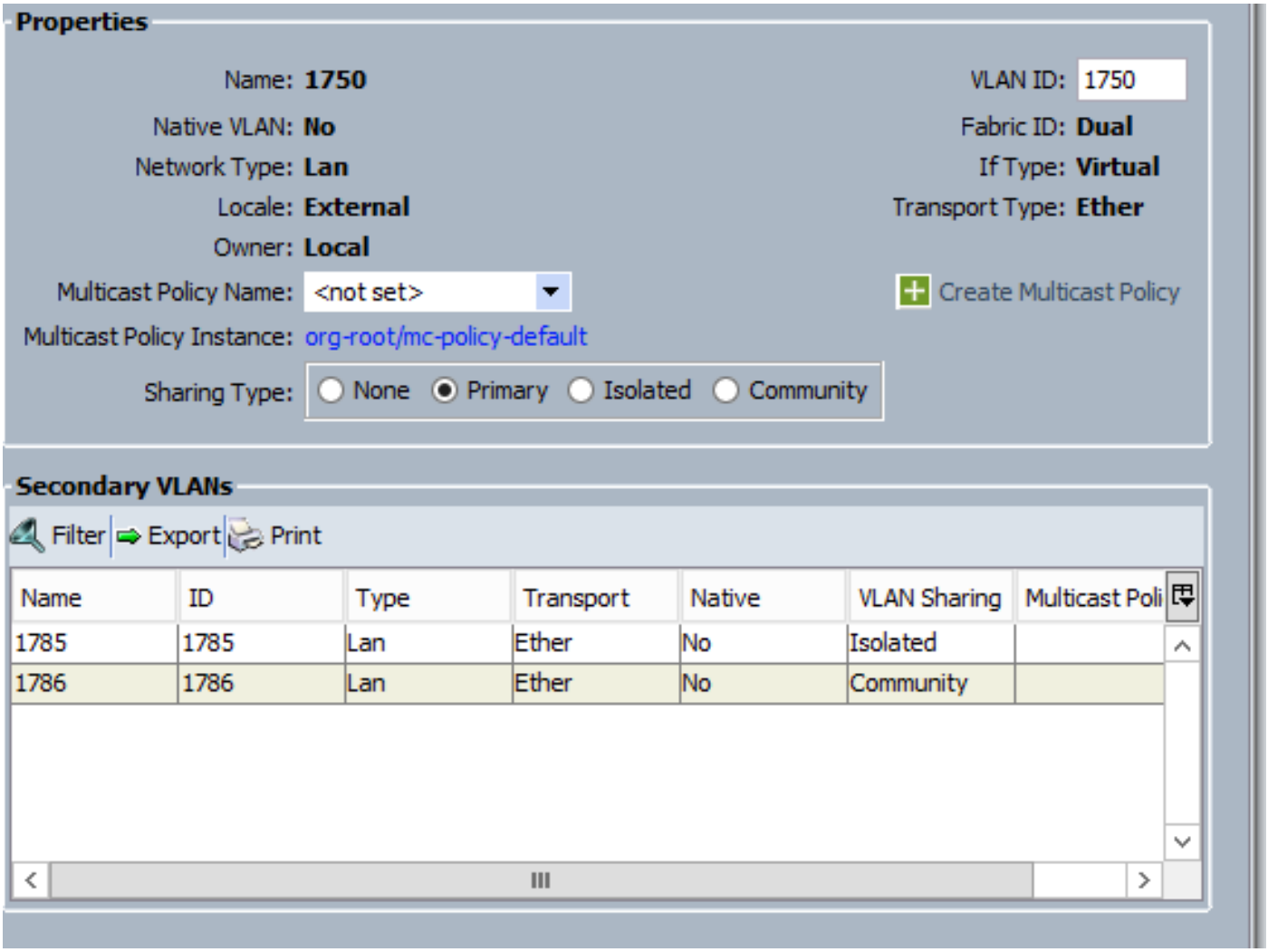
Met Nexus 1000v of VMware DVS



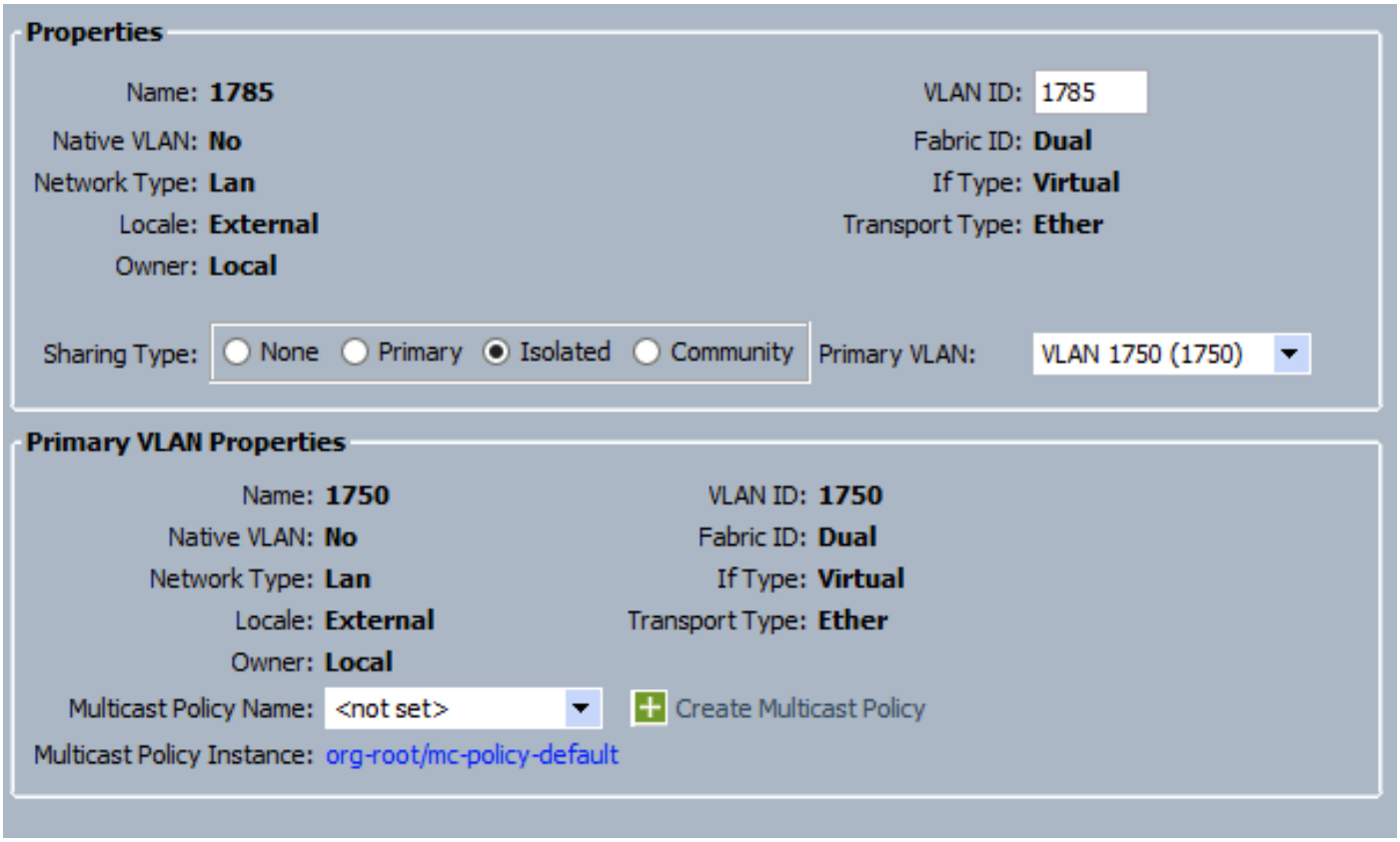
Opmerking: Dit voorbeeld gebruikt VLAN 1750 als primaire, 1785 als geïsoleerd en 1786 als gemeenschap VLAN.

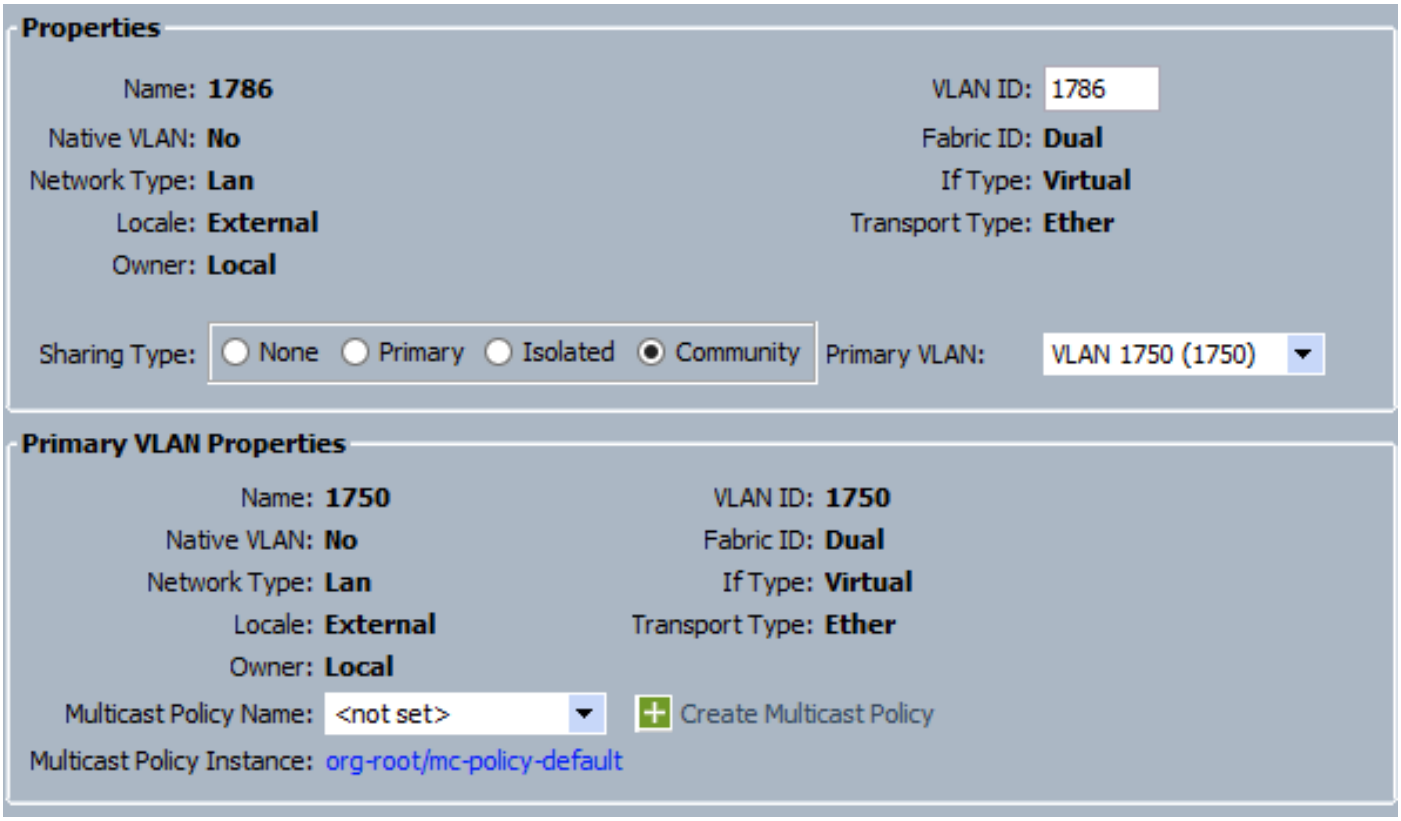
UCS met VMware DVS

1. Als u het primaire VLAN wilt maken, klikt u op de knop **Primaire** radio als het Type delen en vervolgens voert u een **VLAN-ID** van 1750 in zoals in de afbeelding.

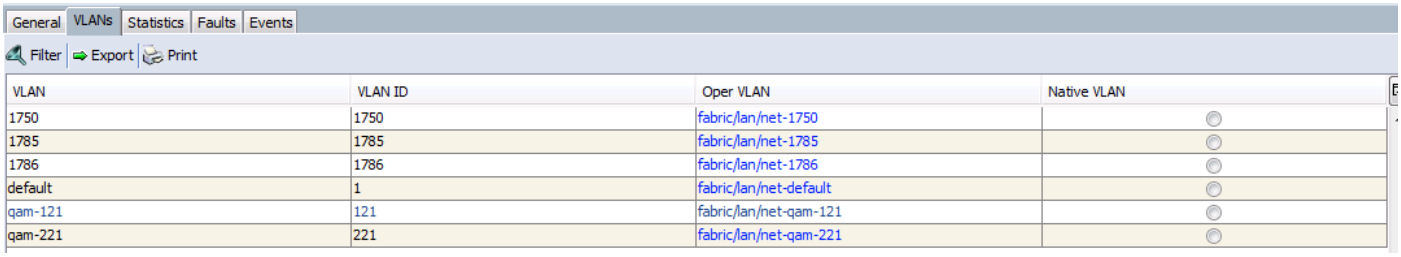


2. Maak dienovereenkomstig **geïsoleerde** en **communityVLAN**'s zoals in de afbeeldingen weergegeven. Geen van deze hoeft een Native VLAN te zijn.





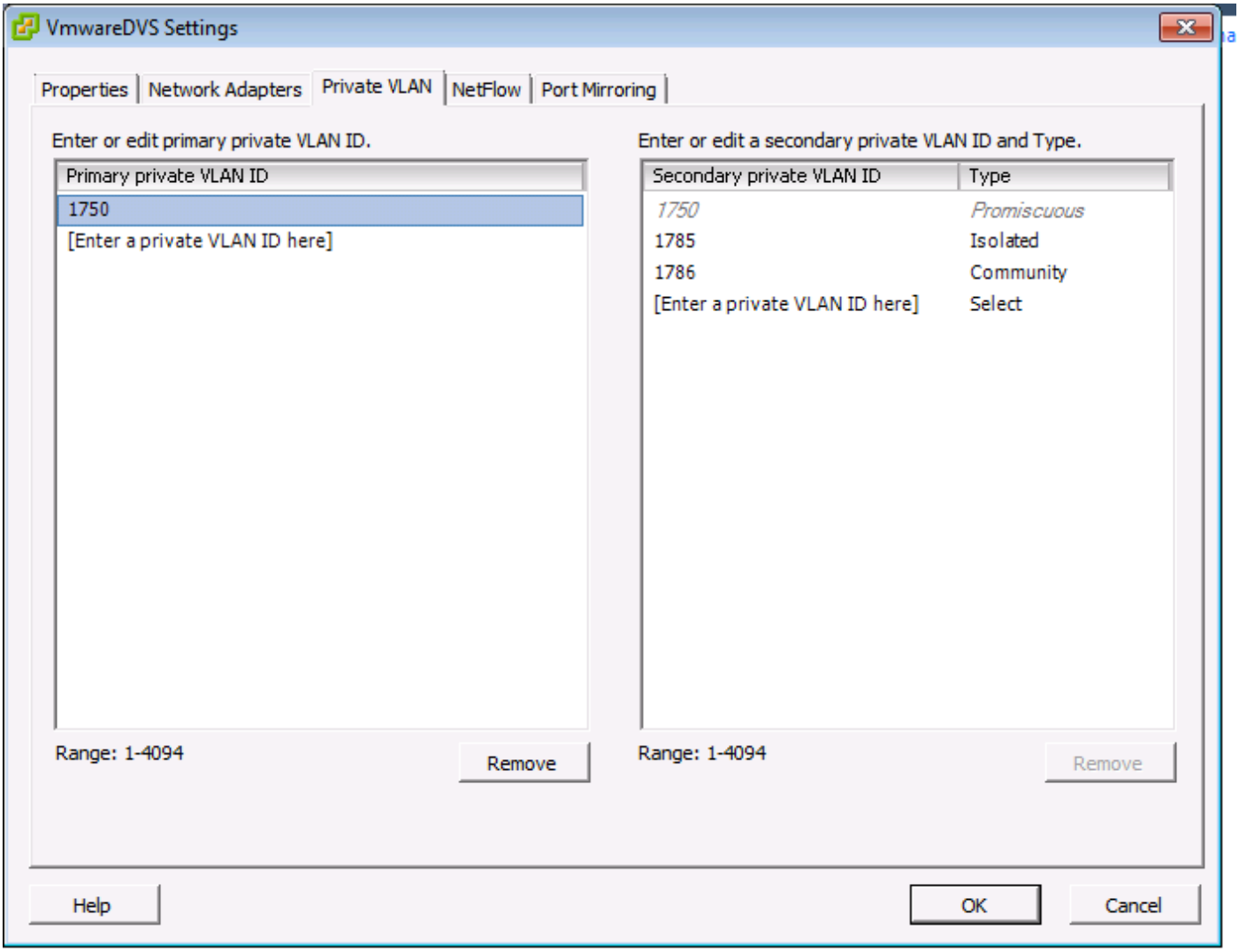
3. Virtual Network Interface Card (vNIC) op serviceprofiel bevat zowel regelmatige VLAN's als PVLAN's, zoals in de afbeelding gezien.

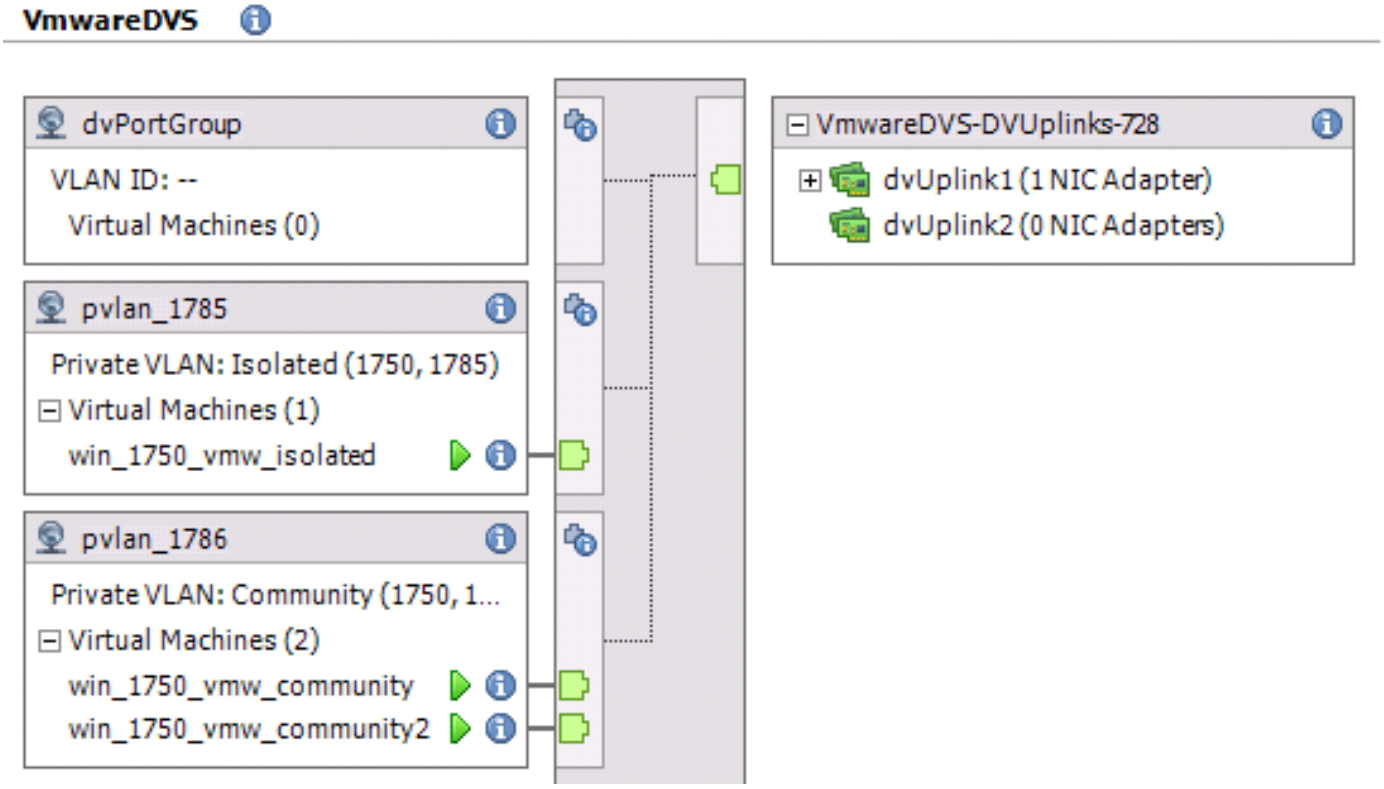


4. Uplink poort-kanaal op UCS draagt regelmatig VLAN's evenals PVLAN's:

```
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





Upstream N5K-switch

```
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
```

Gedragsverandering met UCS versie 3.1(3)

Vóór UCS versie 3.1(3) kunt u een VM in gemeenschapsVLAN laten communiceren met een VM in Primair VLAN op VMware DVS, waar de primaire VLAN-VM zich in de UCS bevindt. Dit gedrag was onjuist, aangezien de primaire VM altijd noordgebonden of buiten de UCS moet zijn. Dit gedrag is gedocumenteerd via defect ID CSCvh87378 .

Vanaf UCS versie 2.2(2), door een defect in de code, kon gemeenschap VLAN met primair VLAN communiceren dat achter de FI aanwezig was. Maar geïsoleerd kon nooit communiceren met de hoofdpersoon achter de FI. Zowel (geïsoleerde als lokale) VM's kunnen nog steeds communiceren met de primaire VM's buiten de FI.

Vanaf 3.1(3) biedt dit defect de gemeenschap de mogelijkheid om met primaire componenten achter de FI te communiceren, is gecorrigeerd, zodat VM's uit de gemeenschap niet met een VM in primair VLAN kunnen communiceren dat zich in UCS bevindt.

Om deze situatie op te lossen zou de primaire VM ofwel moeten worden verplaatst (naar het noorden gebonden) buiten UCS. Als dat geen optie is, moet de primaire VM worden verplaatst naar een ander VLAN dat een regelmatig VLAN is en geen privé VLAN.

Vóór firmware 3.1(3) kon een VM in gemeenschapsVLAN 1786 bijvoorbeeld communiceren met een VM in primair VLAN 1750 dat zich in UCS bevindt, maar deze communicatie zou in firmware 3.1(3) en later, zoals in de afbeelding wordt getoond, breken.

OPMERKING:

—

CSCvh87378 is behandeld in 3.2(3l) en 4.0.4e en hoger zodat we Primair VLAN achter UCS kunnen hebben. Houd er echter rekening mee dat geïsoleerd VLAN in UCS niet met primair VLAN in UCS kan praten. Alleen gemeenschapsvlan en primair VLAN kunnen met elkaar praten als ze allebei achter UCS zitten.

```
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)#
```

Upstream 4900 switch

> Opmerking: In dit voorbeeld is 4900 L3 interface naar buiten netwerk. Als uw topologie voor L3 anders is, dan stel uw veranderingen dienovereenkomstig aan

Doe deze stappen op de 4900-schakelaar en stel de veelbelovende poort in. PVLAN eindigt bij de veelbelovende poort.

1. Schakel de functie PVLAN in indien nodig.
2. Maak en associeer de VLAN's zoals uitgevoerd op Nexus 5K.
3. Maak de veelbelovende poort op de uitgang van de 4900-schakelaar. Vanaf dit punt op, worden de pakketten van VLAN 1785 & 1786 in dit geval op VLAN 1750 gezien.

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

Op de upstream router kunt u alleen een subinterface maken voor VLAN 1750. Op dit niveau zijn de eisen afhankelijk van de netwerkconfiguratie die u gebruikt:

```
interface GigabitEthernet0/1.1

encapsulation dot1Q 1750

IP address10.10.175.254/24
```

Verifiëren

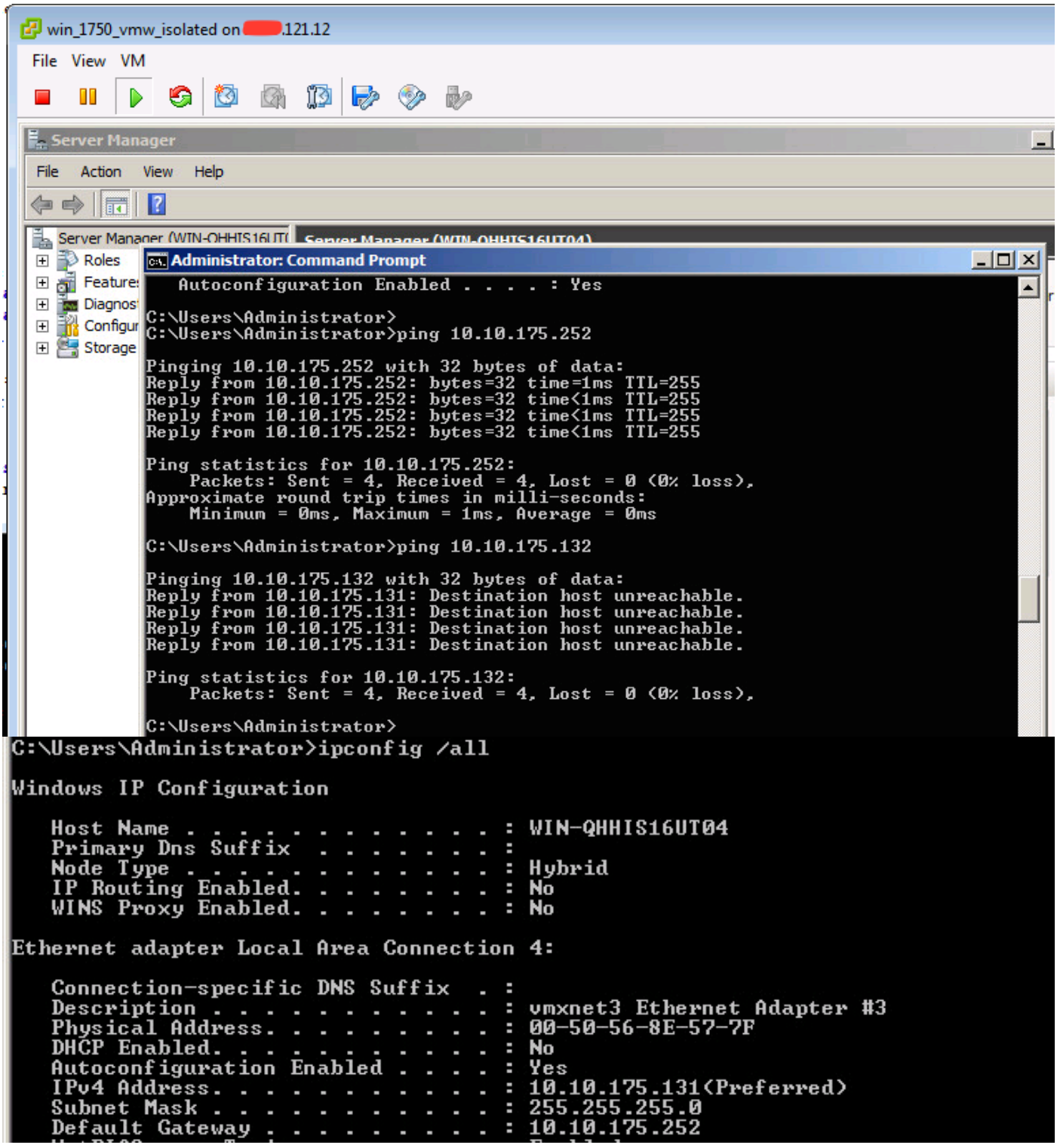
Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

In deze procedure wordt beschreven hoe de configuratie voor VMware DVS met het gebruik van PVLAN moet worden getest.

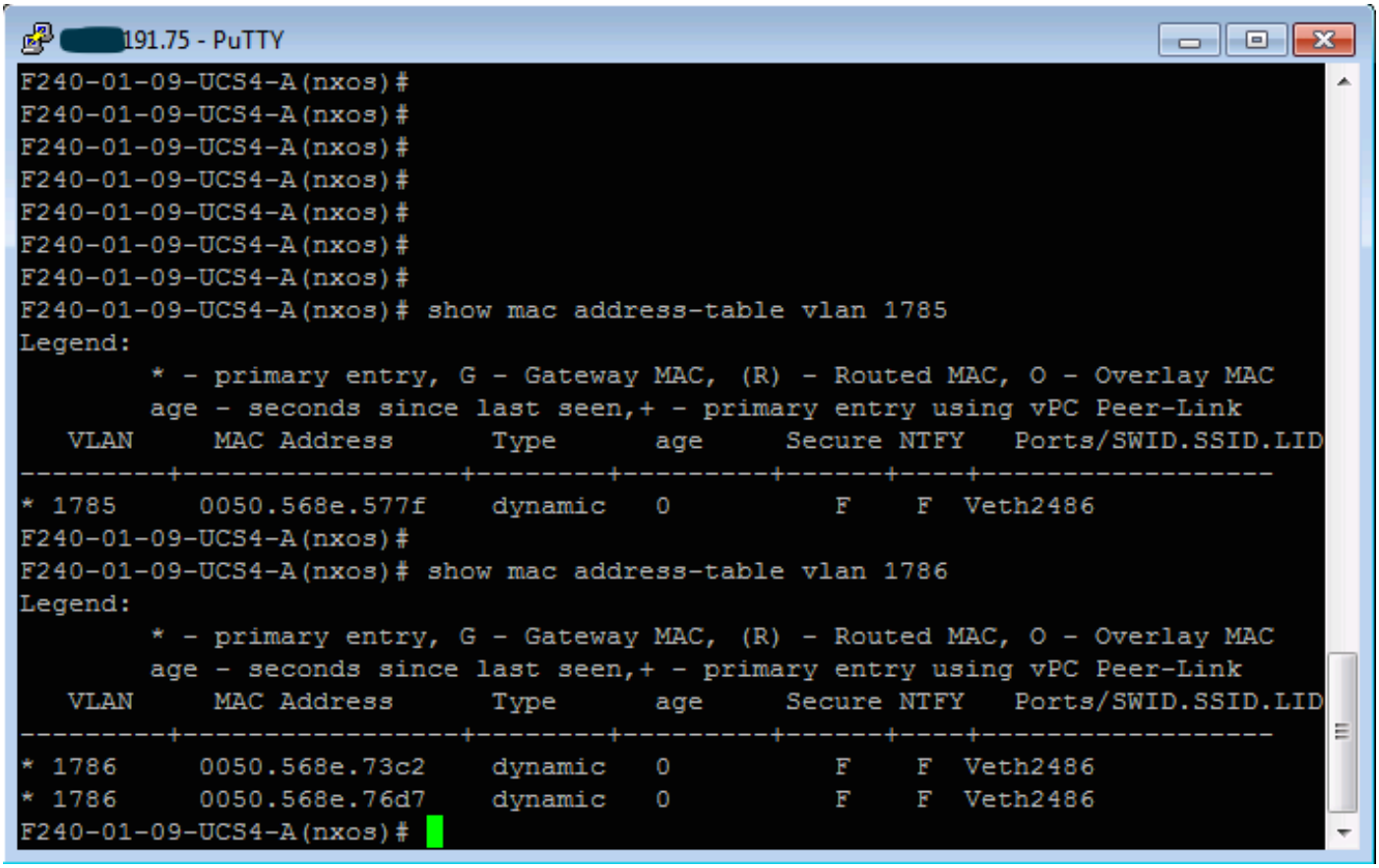
1. Start pings naar andere systemen die in de poortgroep zijn geconfigureerd, evenals de router of een ander apparaat in de veelbelovende poort. Pings aan het apparaat voorbij de promiscuous port moet werken, terwijl die aan andere apparaten in het geïsoleerde VLAN moeten falen zoals in de beelden wordt getoond.



Controleer de MAC-adrestabellen om te zien waar uw MAC wordt geleerd. Op alle switches moet de MAC in het geïsoleerde VLAN zijn behalve op de switch met de veelbelovende poort. Op de

veelbelovende schakelaar, moet de MAC in het primaire VLAN zijn.

2. UCS zoals in de afbeelding.



3. Controleer op stroomopwaarts n5k voor dezelfde MAC-uitvoer, uitvoer die vergelijkbaar is met eerdere uitvoer, moet aanwezig zijn op n5k en zoals in de afbeelding.

```
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#
```

Configuratie met Nexus 1000v met Promiscuous Port op Upstream N5k

UCS-configuratie

De UCS-configuratie (waaronder de configuratie van het serviceprofiel vNIC) blijft hetzelfde als bij het voorbeeld voor VMware DVS.

Configuratie 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 deze procedure wordt beschreven hoe de configuratie moet worden getest.

1. Start pings naar andere systemen die in de poortgroep zijn geconfigureerd, evenals de router of een ander apparaat in de veelbelovende poort. Pings aan het apparaat voorbij de promiscuous port moet werken, terwijl die aan andere apparaten in het geïsoleerde VLAN moeten falen, zoals in vorige sectie en in de beelden wordt getoond.