Configurez le VLAN privé et l'UCS avec le VMware DVS ou Cisco Nexus 1000v

Contenu

Introduction

Ce document décrit le soutien du VLAN privé (PVLAN) du Système d'informatique unifiée Cisco (UCS) dans 2.2(2c) la release et plus tard.

> **Attention** : Il y a un changement du comportement commençant par la version 3.1(3a) de micrologiciels UCS comme décrit dans la **modification de comportement avec la** section de **version 3.1(3) et ultérieures UCS**.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- UCS
- Cisco Nexus 1000V (N1K) ou VMware a distribué le commutateur virtuel (DVS)
- VMware
- Commutation de la couche 2 (L2)

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Un VLAN privé est un VLAN configuré pour l'isolation L2 d'autres ports dans le même VLAN privé. Des ports qui appartiennent à un PVLAN sont associés avec un ensemble commun de support VLAN, qui est utilisé afin de créer la structure PVLAN.

Il y a trois types de ports PVLAN :

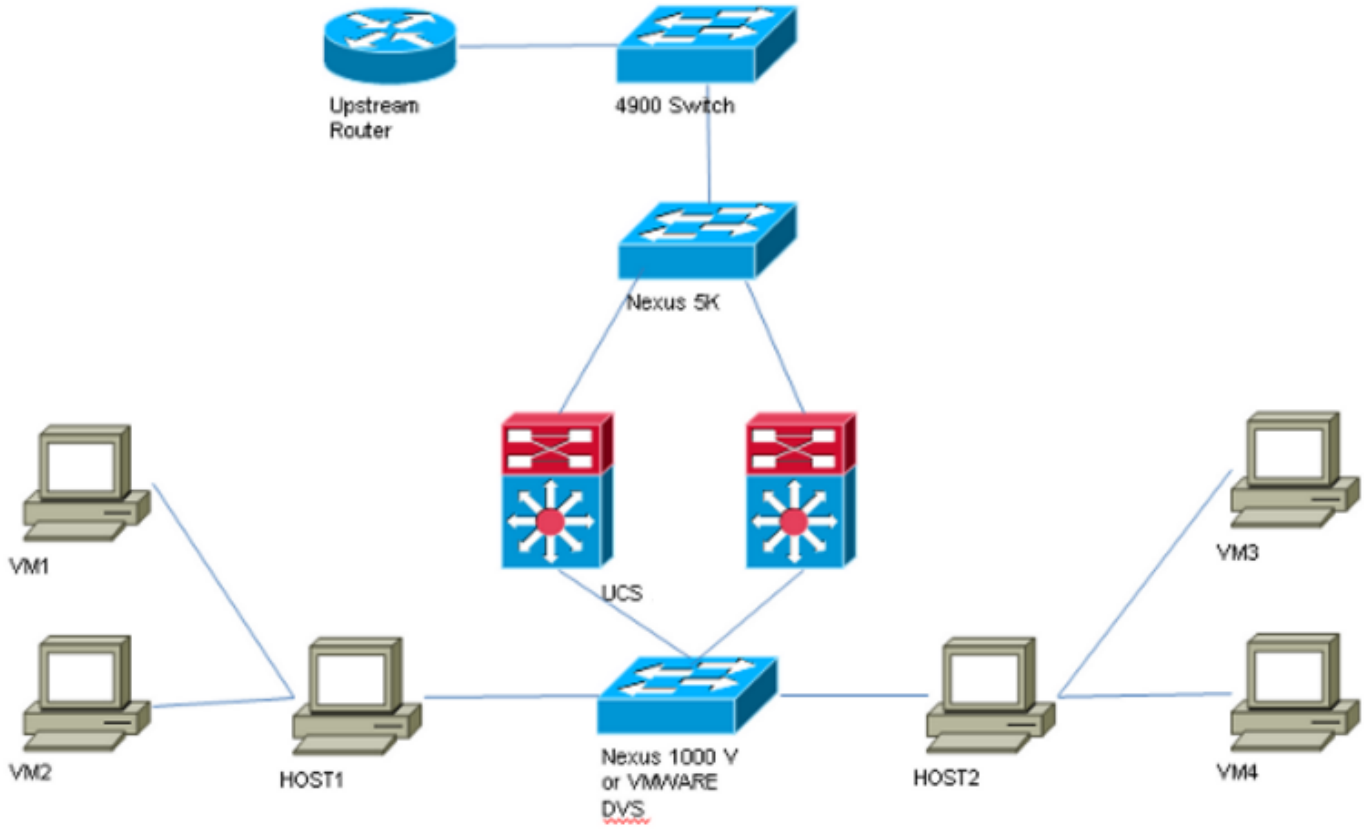
- Un port proche communique avec tous autres ports PVLAN et est le port utilisé afin de communiquer avec des périphériques en dehors de du PVLAN.
- Un port d'isolement a la séparation L2 complète (qui inclut des émissions) d'autres ports dans le même PVLAN excepté le port proche.
- Un port de la communauté peut communiquer avec d'autres ports dans le même PVLAN aussi bien que le port proche. Des ports de la Communauté sont isolés à L2 des ports dans d'autres communautés ou ports d'isolement PVLAN. Des émissions sont seulement propagées à d'autres ports dans la communauté et le port proche.

Référez-vous à RFC 5517, les VLAN privés des Cisco Systems : Sécurité extensible dans un environnement de Multi-client afin de comprendre la théorie, l'exécution, et les concepts de PVLANs.

Configurez

Diagramme du réseau

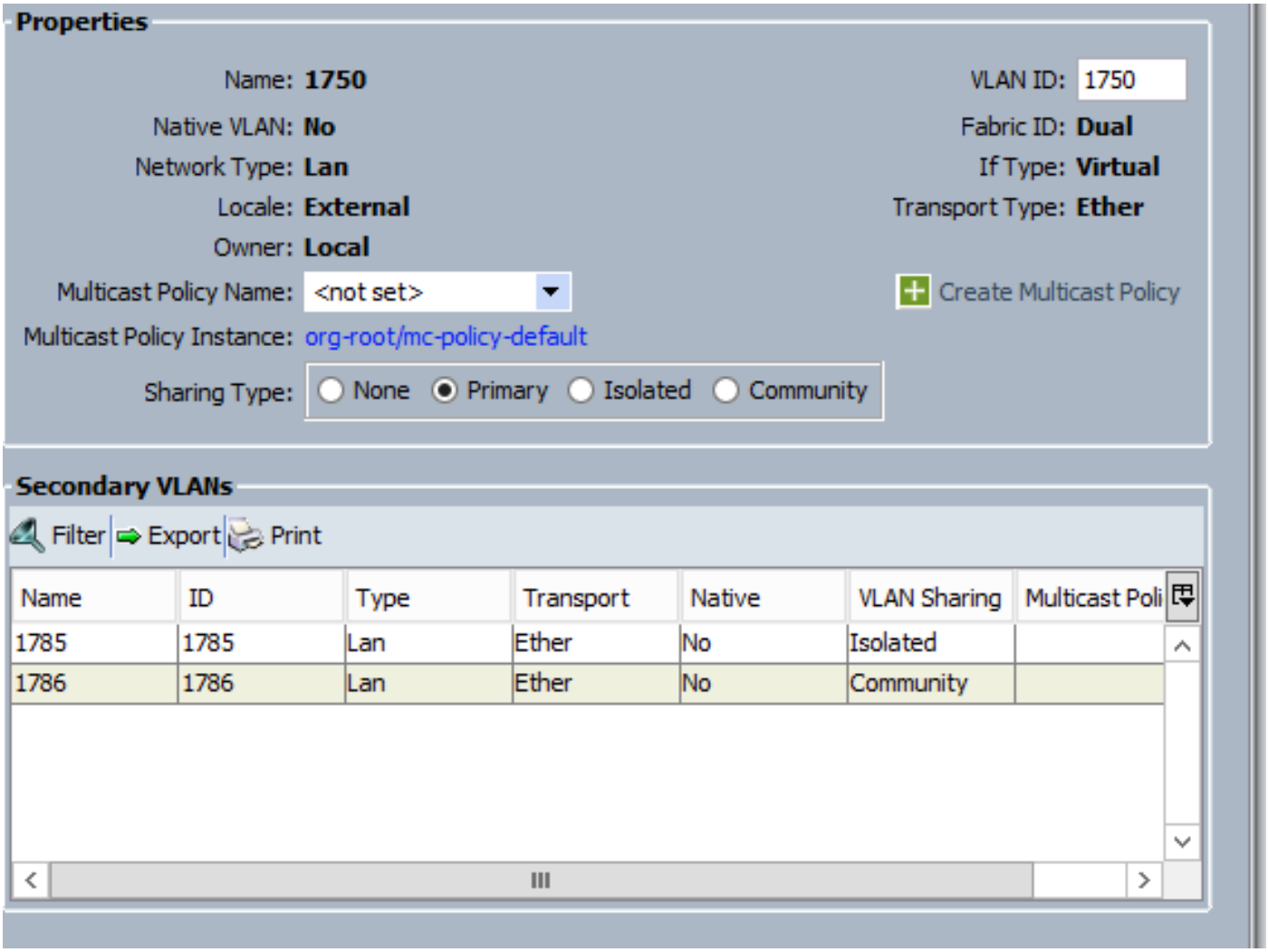
Avec le Nexus 1000v ou le VMware DVS



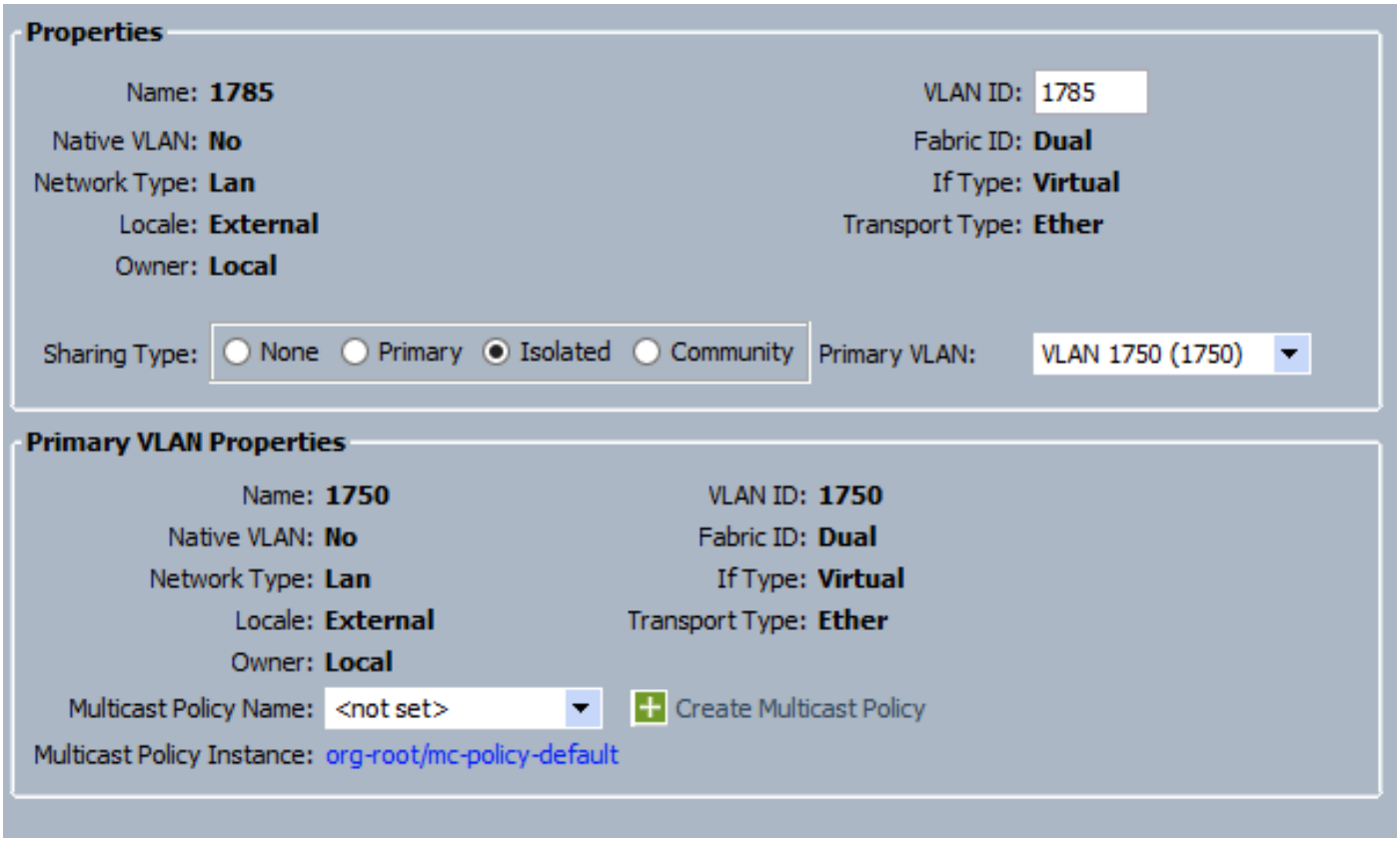
Note: Cet exemple utilise VLAN 1750 en tant que primaire, 1785 comme d'isolement et 1786 comme VLAN communautaire.

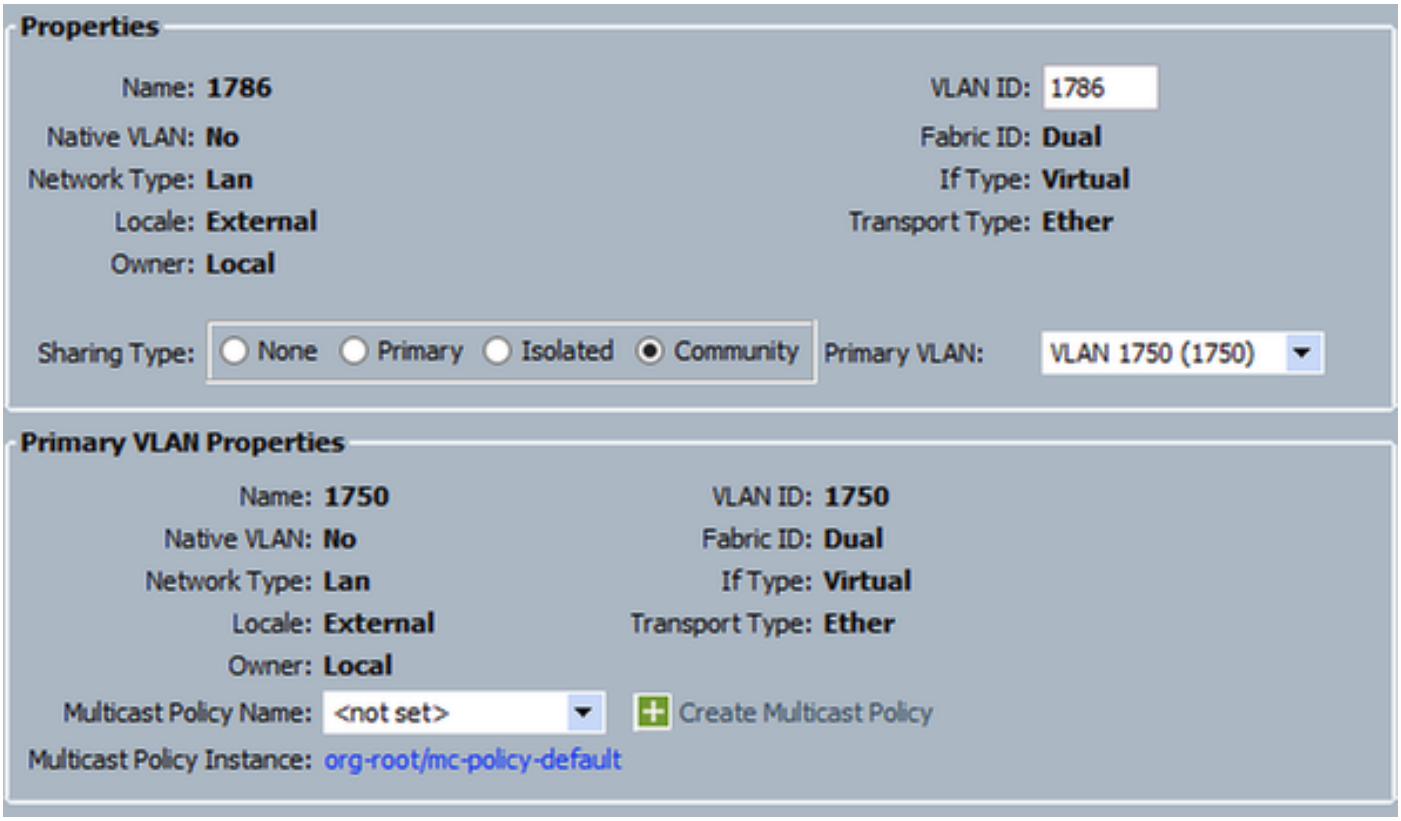
UCS avec le VMware DVS

1. Afin de créer le VLAN primaire, cliquez sur la case d'option **primaire** comme type partageant, et écrivez un **ID DE VLAN de** 1750 suivant les indications de l'image.

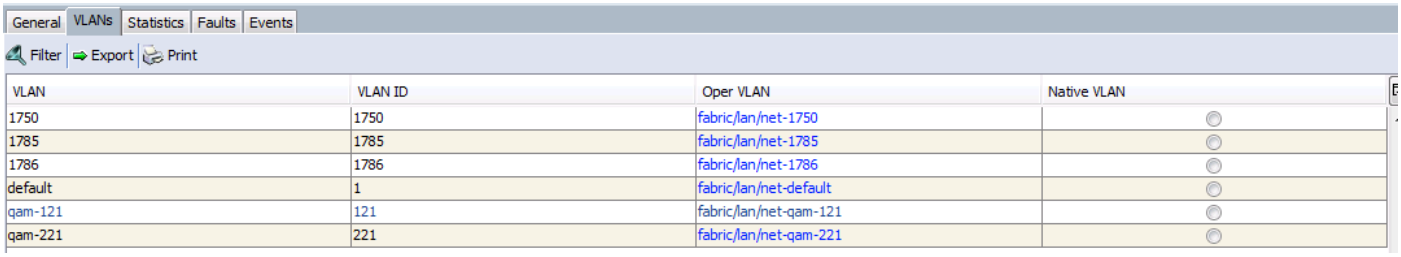


2. Créez **d'isolement** et la **Communauté** VLAN en conséquence suivant les indications des images. Aucune de ces derniers ne doit être un VLAN indigène.





3. Le network interface card virtuel (vNIC) sur le service profile porte le militaire de carrière VLAN aussi bien que PVLANs, comme vu dans l'image.

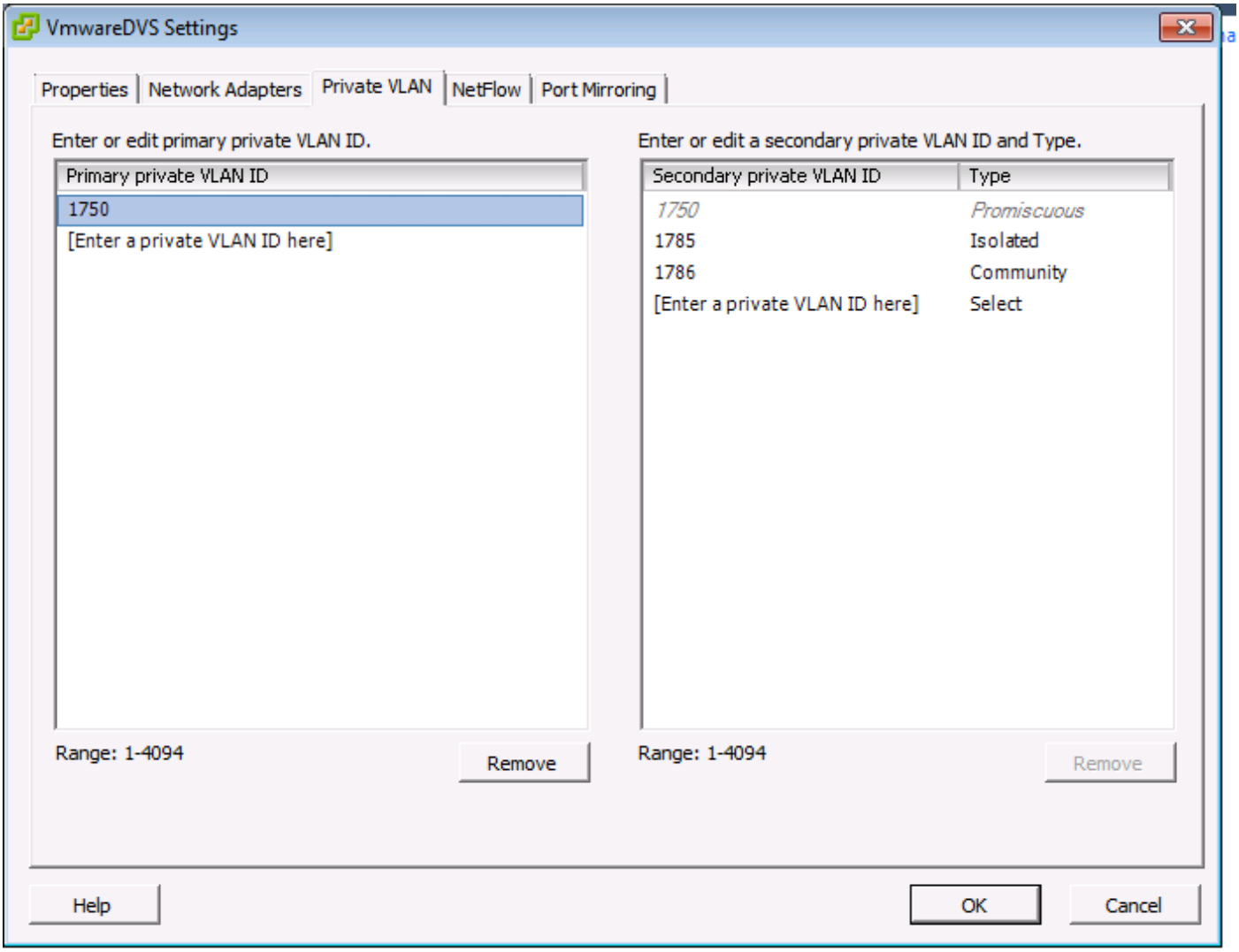


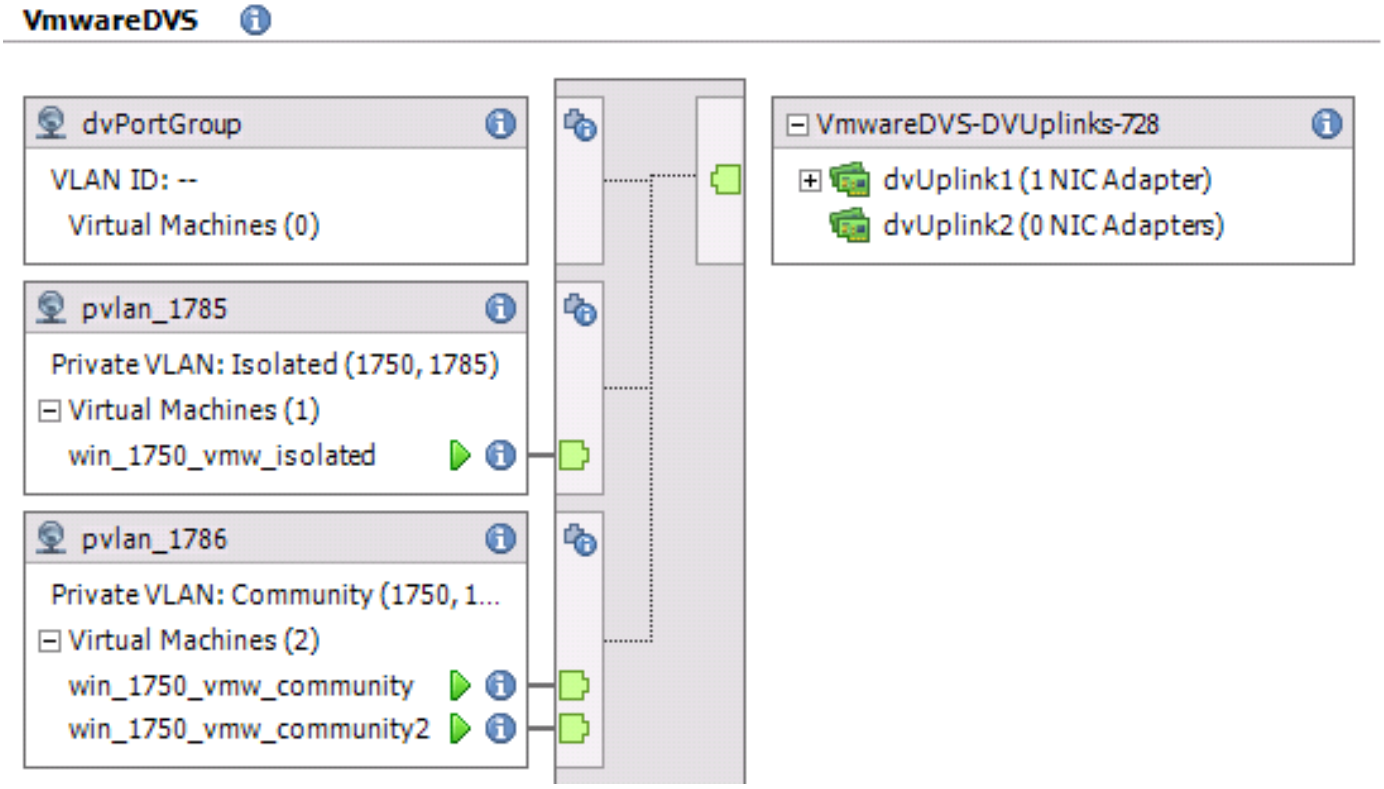
VLAN	VLAN ID	Oper VLAN	Native VLAN
1750	1750	fabric/lan/net-1750	
1785	1785	fabric/lan/net-1785	
1786	1786	fabric/lan/net-1786	
default	1	fabric/lan/net-default	
qam-121	121	fabric/lan/net-qam-121	
qam-221	221	fabric/lan/net-qam-221	

4. Le Port canalisé de liaison ascendante sur l'UCS porte le militaire de carrière VLAN aussi bien que PVLANs :

```
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





Commutateur en amont 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
```

Modification de comportement avec la version 3.1(3) et ultérieures UCS

Avant la version 3.1(3) UCS, vous pourriez faire communiquer une VM dans le VLAN communautaire avec une VM dans le VLAN primaire sur VMware DVS où la VM de VLAN primaire réside à l'intérieur de l'UCS. Ce comportement était tout incorrecte que la VM primaire doit toujours être allante vers le nord ou extérieure de l'UCS. Ce comportement est documenté par l'intermédiaire de l'ID CSCvh87378 de défaut .

De la version 2.2(2) UCS en avant, en raison d'un défaut dans le code, le VLAN communautaire pouvait communiquer avec le VLAN primaire qui était présent derrière le fi. Mais d'isolement a pu ne jamais communiquer avec le primaire derrière le fi. Les deux (d'isolement et la communauté) VMs peuvent encore communiquer avec le primaire en dehors du fi.

Àcompter de 3.1(3), ce défaut permet à la communauté pour communiquer avec primaire derrière le fi, a été rectifié et les VMs de la communauté ne pourront pas ainsi communiquer avec une VM dans le VLAN primaire qui réside dans l'UCS.

Afin de résoudre cette situation, la VM primaire l'un ou l'autre de besoin d'être déplacé (allant vers le nord) en dehors de l'UCS. Si ce n'est pas une option, alors la VM primaire devrait être entrée dans un autre VLAN qui est un militaire de carrière VLAN et pas un VLAN privé.

Par exemple, avant le micrologiciel 3.1(3), une VM dans le VLAN communautaire 1786 pourrait communiquer à une VM dans le VLAN primaire 1750 qui réside dans l'UCS, cependant, cette transmission enfoncerait le micrologiciel 3.1(3) et plus tard, suivant les indications de l'image.

```
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)#
```

Commutateur de l'en amont 4900

> **Note**: Dans cet exemple, 4900 est l'interface L3 au réseau extérieur. Si votre topologie pour L3 est différente, alors apportez des modifications avec bonté en conséquence

Sur le commutateur 4900, prenez ces mesures, et installez le port proche. Le PVLAN finit au port proche.

1. Activez la caractéristique PVLAN s'il y a lieu.
2. Créez et associez les VLAN comme fait sur le Nexus 5K.
3. Créez le port proche sur le port de sortie du commutateur 4900. À partir de là, les paquets de VLAN 1785 et 1786 sont vus sur VLAN 1750 dans ce cas.

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

Sur le routeur en amont, créez une sous-interface pour le VLAN 1750 seulement. À ce niveau, les conditions requises dépendent de la configuration réseau que vous utilisez :

```
interface GigabitEthernet0/1.1

encapsulation dot1Q 1750

IP address10.10.175.254/24
```

Vérifiez

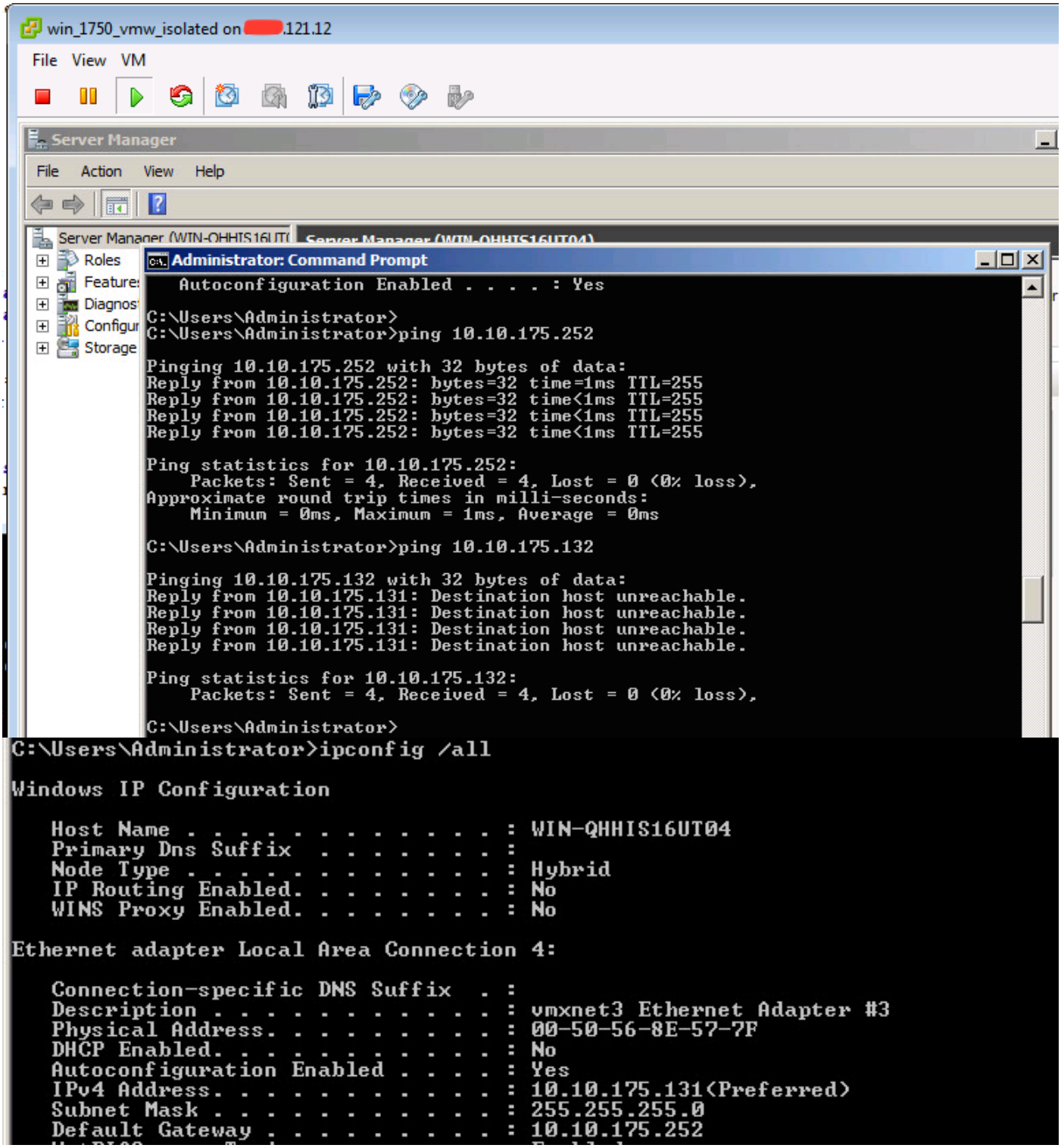
Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

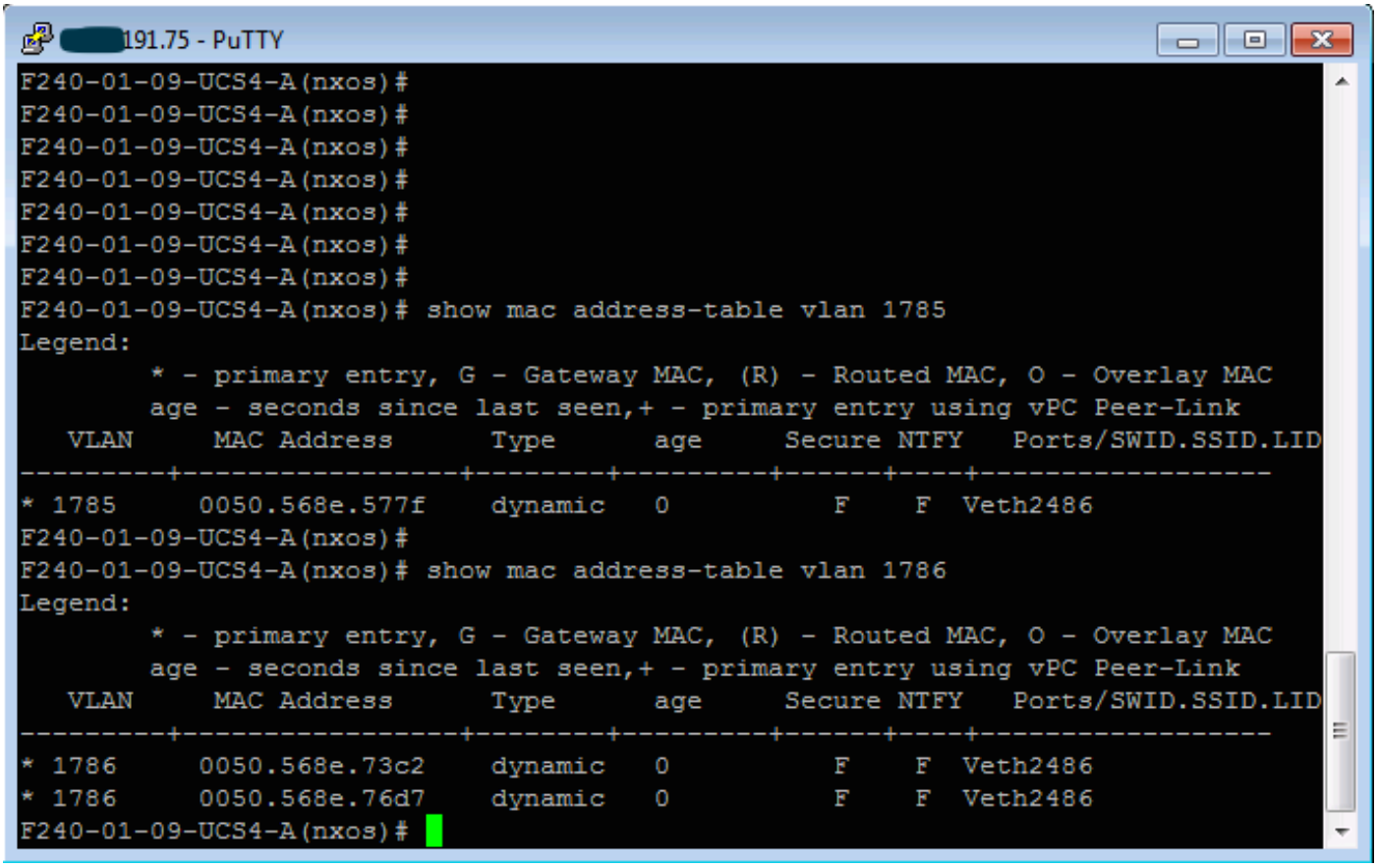
Cette procédure décrit comment tester la configuration pour le VMware DVS avec l'utilisation de PVLAN.

1. Exécutez les pings à d'autres systèmes configurés dans le port-groupe aussi bien que le routeur ou tout autre périphérique au port proche. Les pings au périphérique après le port proche doivent fonctionner, alors que ceux à d'autres périphériques dans le VLAN d'isolement doivent échouer suivant les indications des images.



Vérifiez les tables d'adresse MAC afin de voir où votre MAC est appris. Sur tous les Commutateurs, le MAC doit être dans le VLAN d'isolement excepté sur le commutateur avec le port proche. Sur le commutateur promiscueux, le MAC doit être dans le VLAN primaire.

2. UCS suivant les indications de l'image.



3. Vérifiez l'en amont n5k pour le même MAC, la sortie semblable pour sortir plus tôt doit être présente sur n5k et suivant les indications de l'image.

```
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#
```

Configuration avec le Nexus 1000v avec le port proche sur l'en amont N5k

Configuration UCS

La configuration UCS (qui inclut la configuration de vNIC de service profile) reste la même chose selon l'exemple avec le VMware DVS.

Configuration 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
```

Cette procédure décrit comment tester la configuration.

1. Exécutez les pings à d'autres systèmes configurés dans le port-groupe aussi bien que le routeur ou tout autre périphérique au port proche. Les pings au périphérique après le port proche doivent fonctionner, alors que ceux à d'autres périphériques dans le VLAN d'isolement doivent échouer, suivant les indications de la section précédente et dans les images.