Configuration de VLAN privé et UCS avec VMware DVS ou Cisco Nexus 1000v

Contenu

Introduction

Ce document décrit la prise en charge des VLAN privés (PVLAN) pour Cisco Unified Computing System (UCS) dans la version 2.2(2c) et les versions ultérieures.

> **Attention** : Il y a un changement de comportement à partir de la version 3.1(3a) du micrologiciel UCS, comme décrit dans la section **Changement de comportement avec UCS version 3.1(3) et ultérieure**.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- UCS
- Commutateur virtuel distribué (DVS) Cisco Nexus 1000V (N1K) ou VMware
- VMware
- Commutation de couche 2 (L2)

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Un VLAN privé est un VLAN configuré pour l'isolation de couche 2 par rapport aux autres ports du même VLAN privé. Les ports qui appartiennent à un PVLAN sont associés à un ensemble commun de VLAN de support, qui sont utilisés pour créer la structure PVLAN.

Il y a trois types de ports PVLAN :

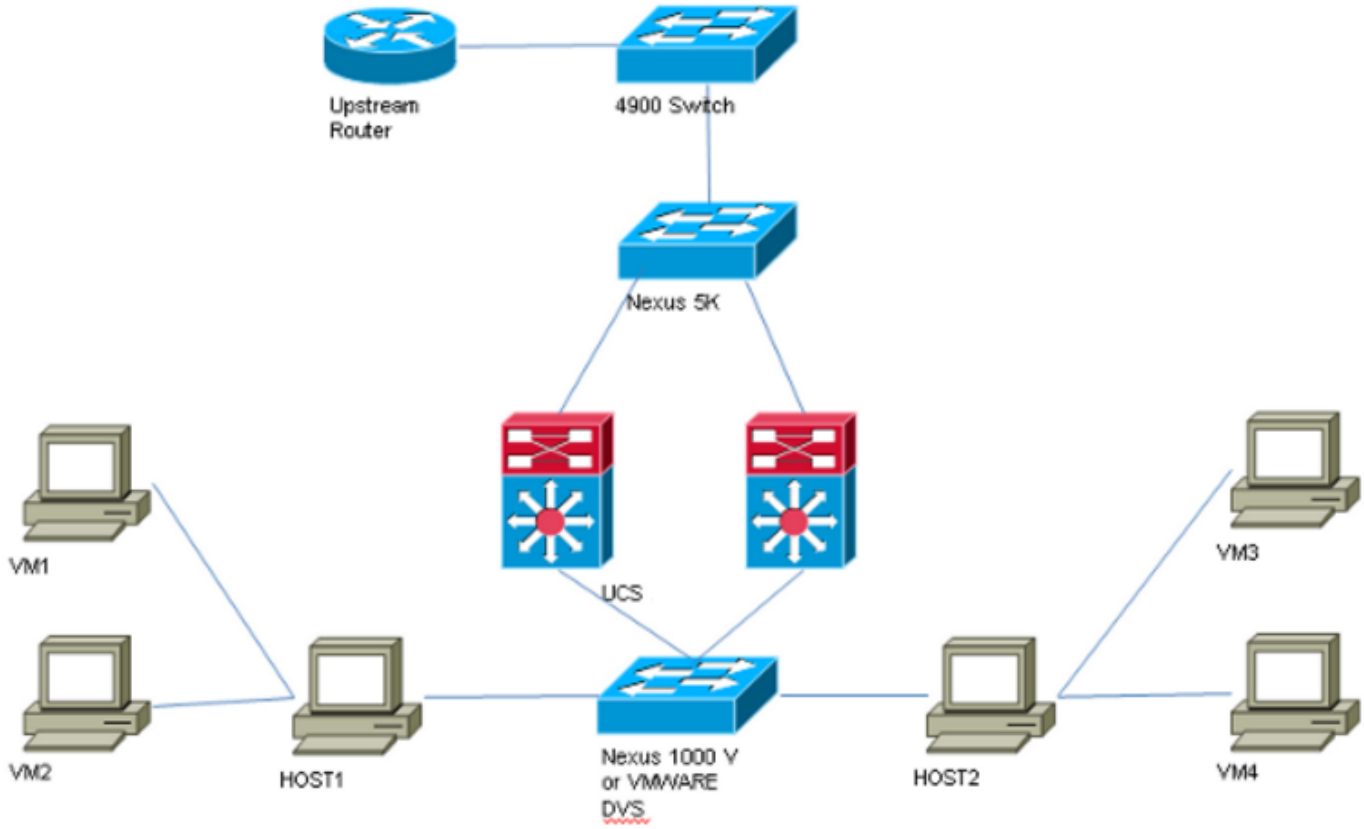
- Un port proche communique avec tous les autres ports PVLAN et est le port utilisé pour communiquer avec des périphériques situés en dehors du PVLAN.
- Un port isolé a une séparation L2 complète (qui inclut les diffusions) des autres ports du même PVLAN, à l'exception du port proche.
- Un port de communauté peut communiquer avec d'autres ports du même PVLAN ainsi qu'avec le port proche. Les ports communautaires sont isolés au niveau de L2 à partir de ports d'autres communautés ou de ports PVLAN isolés. Les diffusions ne sont propagées qu'à d'autres ports de la communauté et du port proche.

Référez-vous à RFC 5517, VLAN privés de Cisco Systems : Sécurité évolutive dans un environnement multiclient afin de comprendre la théorie, le fonctionnement et les concepts des PVLAN.

Configuration

Diagramme du réseau

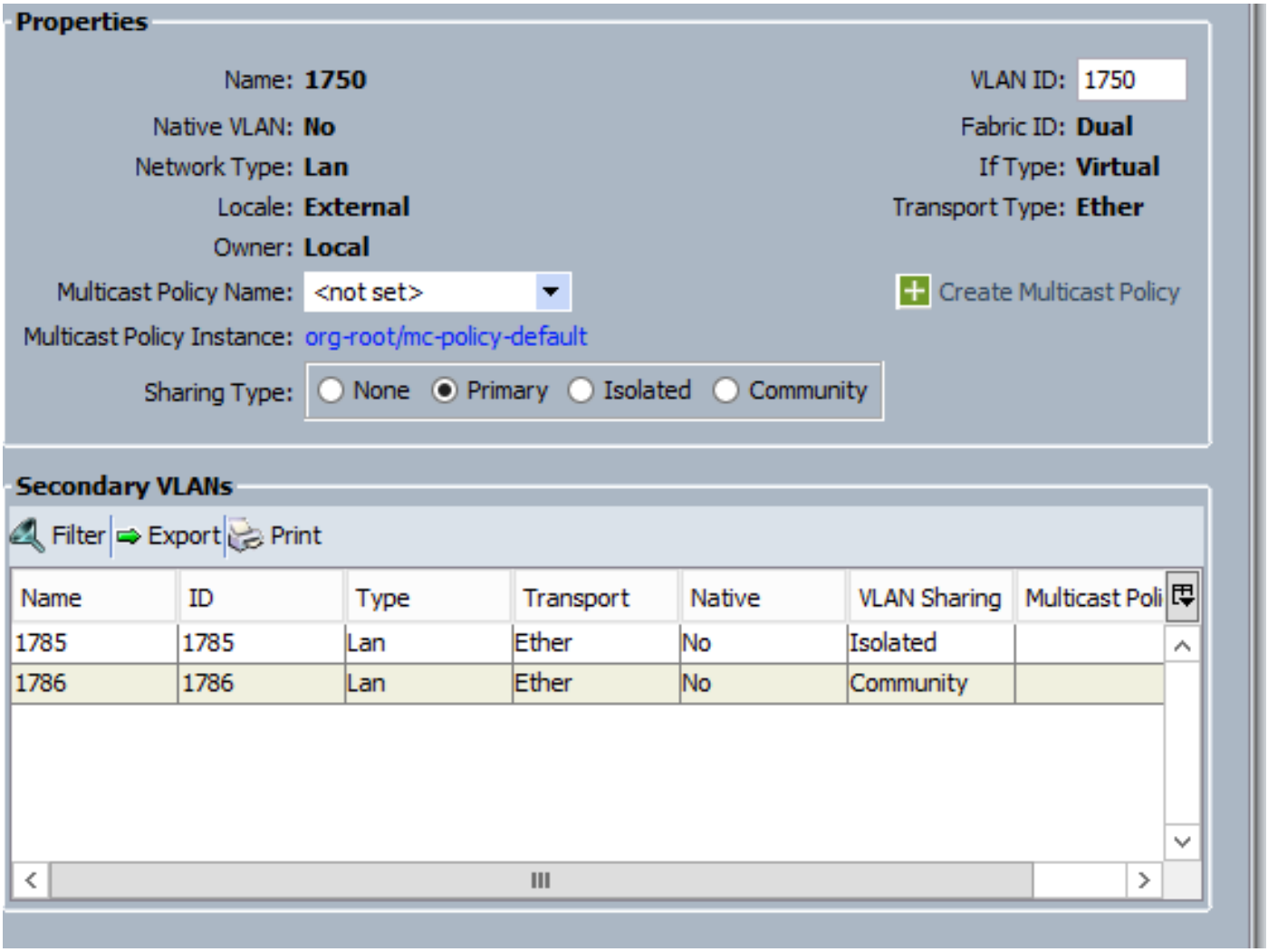
Avec Nexus 1000v ou VMware DVS



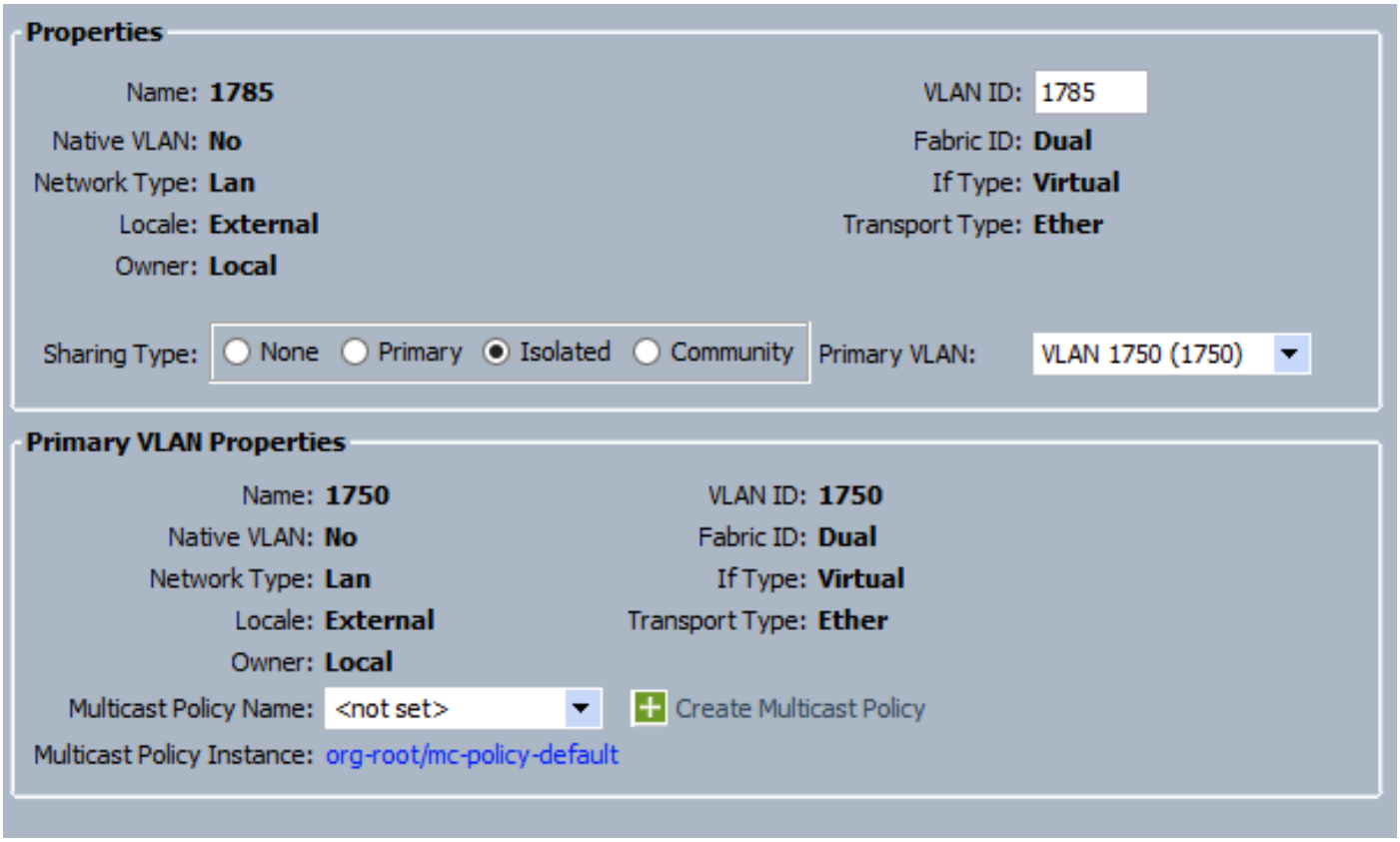
Note: Cet exemple utilise le VLAN 1750 comme principal, 1785 comme isolé et 1786 comme VLAN de communauté.

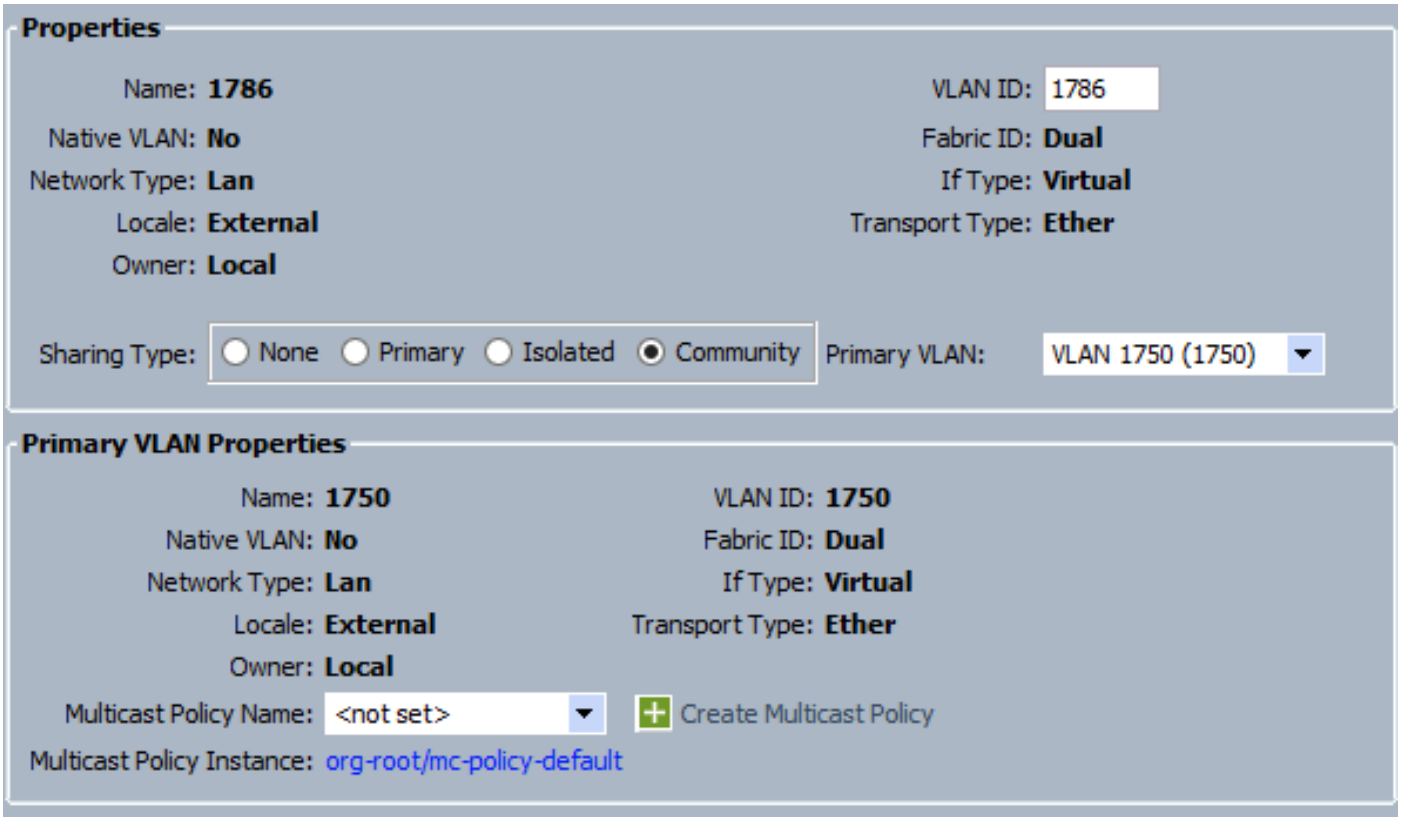
UCS avec VMware DVS

1. Afin de créer le VLAN principal, cliquez sur la case d'option **Principal** en tant que Type de partage, et entrez un **ID** de **VLAN** de 1750 comme indiqué dans l'image.

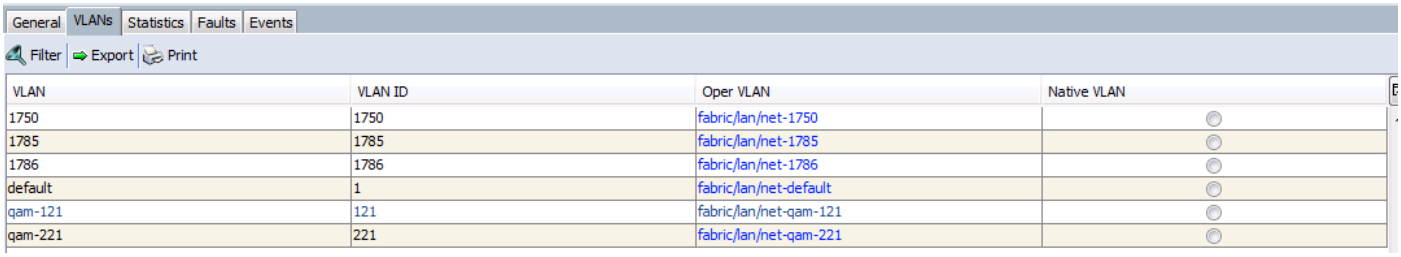


2. Créez des VLAN **isolés** et **communautaires** en conséquence, comme indiqué dans les images. Aucun de ces VLAN ne doit être un VLAN natif.





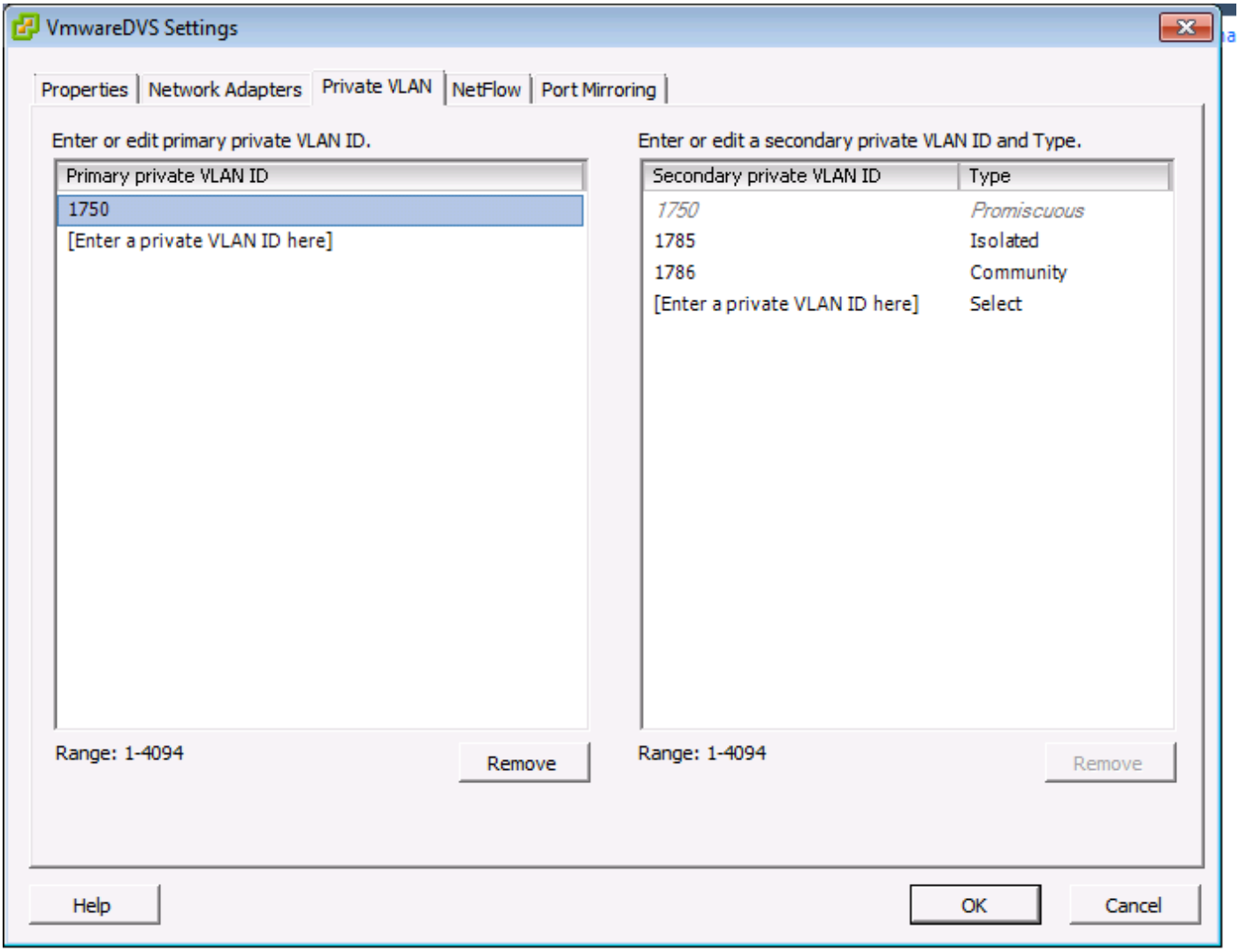
3. La carte d'interface réseau virtuelle (vNIC) sur le profil de service transporte des VLAN ordinaires ainsi que des PVLAN, comme le montre l'image.

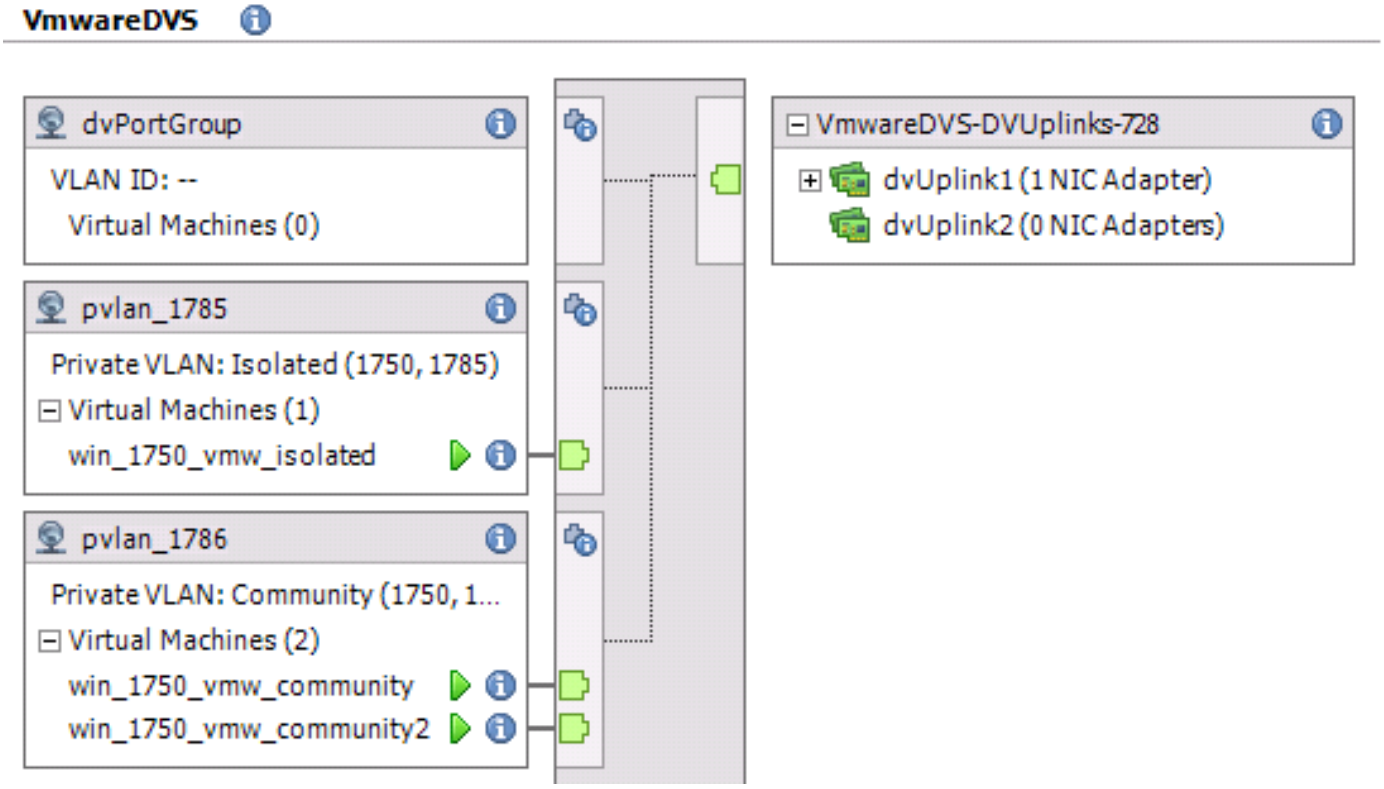


4. Le canal de port de liaison ascendante sur UCS transporte des VLAN ordinaires ainsi que des PVLAN :

```
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





Commutateur N5k ascendant

```
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
```

Changement de comportement avec UCS version 3.1(3)

Avant UCS version 3.1(3), une machine virtuelle dans le VLAN de communauté peut communiquer avec une machine virtuelle dans le VLAN principal sur le DVS VMware, où la machine virtuelle du VLAN principal réside à l'intérieur de l'UCS. Ce comportement était incorrect, car la machine virtuelle principale doit toujours être orientée vers le nord ou en dehors d'UCS. Ce comportement est documenté via l'ID de défaut CSCvh87378 .

Àpartir de la version 2.2(2) d'UCS, en raison d'un défaut dans le code, le VLAN de communauté a pu communiquer avec le VLAN principal qui était présent derrière l'IF. Mais Isolated ne pouvait jamais communiquer avec le principal derrière l'IF. Les machines virtuelles (isolées et communautaires) sont toujours en mesure de communiquer avec le principal à l'extérieur de l'IF.

Àpartir de la version 3.1(3), ce défaut permet à la communauté de communiquer avec le principal derrière l'FI, a été corrigé et par conséquent les machines virtuelles communautaires ne pourront pas communiquer avec une machine virtuelle dans le VLAN principal qui réside dans UCS.

Pour résoudre cette situation, la machine virtuelle principale doit être déplacée (vers le nord) en dehors d'UCS. Si ce n'est pas possible, la machine virtuelle principale doit être déplacée vers un autre VLAN qui est un VLAN normal et non un VLAN privé.

Par exemple, avant le microprogramme 3.1(3), une machine virtuelle du VLAN 1786 de la communauté pouvait communiquer à une machine virtuelle du VLAN 1750 principal qui réside dans UCS, mais cette communication romprait le microprogramme 3.1(3) et ultérieur, comme

l'illustre l'image.

NOTE:

—

CSCvh87378 a été traité dans les versions 3.2(3l) et 4.0.4e et ultérieures pour que nous puissions avoir un Vlan principal derrière UCS. Cependant, notez que le VLAN isolé dans UCS ne pourra pas parler au VLAN principal dans UCS. Seul le VLAN de communauté et le VLAN principal peuvent communiquer entre eux lorsque les deux sont derrière 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)#
```

Commutateur en amont 4900

> **Note**: Dans cet exemple, 4900 est une interface de couche 3 vers un réseau externe. Si votre topologie pour L3 est différente, apportez les modifications nécessaires

Sur le commutateur 4900, procédez comme suit et configurez le port de promiscuité. Le PVLAN se termine par le port proche.

1. Activez la fonction PVLAN si nécessaire.
2. Créez et associez les VLAN comme sur le Nexus 5K.
3. Créez le port proche sur le port de sortie du commutateur 4900. À partir de ce point, les paquets des 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 uniquement. À ce niveau, les exigences dépendent de la configuration réseau que vous utilisez :

```
interface GigabitEthernet0/1.1

encapsulation dot1Q 1750

IP address10.10.175.254/24
```

Vérification

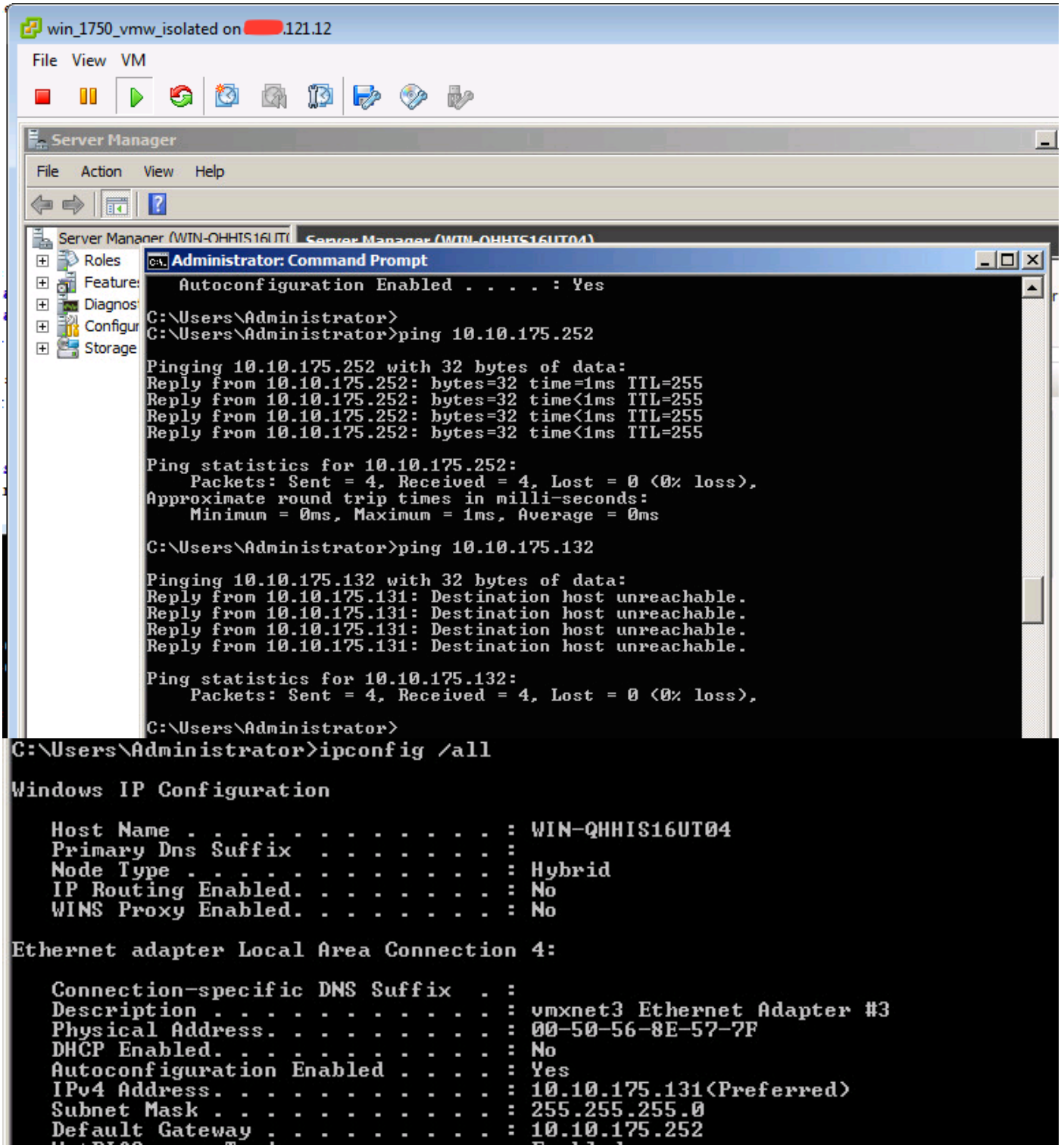
Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

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

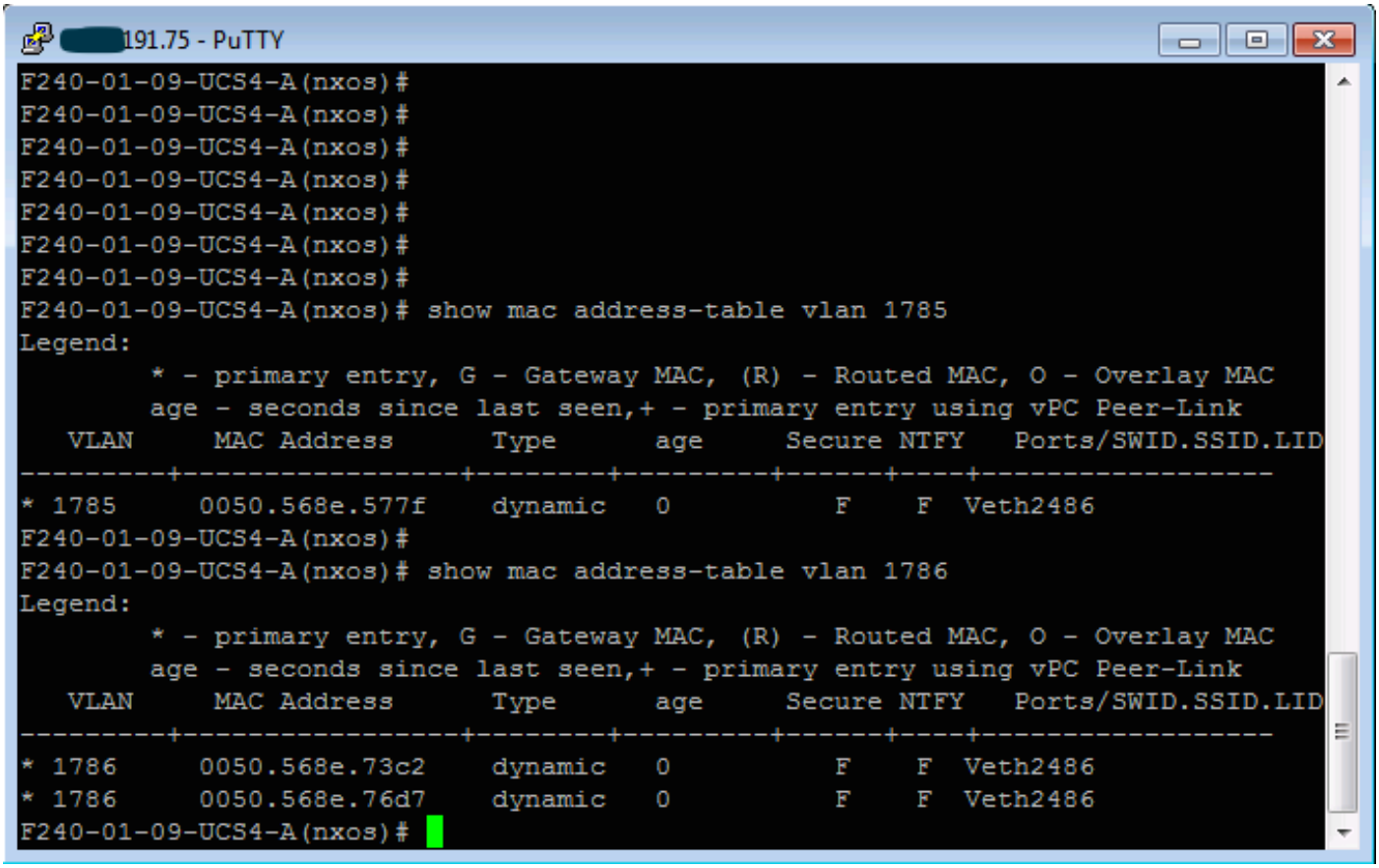
Cette procédure décrit comment tester la configuration de VMware DVS avec l'utilisation de PVLAN.

1. Exécutez des requêtes ping vers d'autres systèmes configurés dans le groupe de ports, ainsi que vers le routeur ou un autre périphérique au niveau du port proche. Les requêtes ping envoyées au périphérique au-delà du port proche doivent fonctionner, tandis que celles envoyées aux autres périphériques du VLAN isolé doivent échouer, comme le montrent les images.



Vérifiez les tables d'adresses MAC afin de voir où votre adresse MAC est apprise. Sur tous les commutateurs, l'adresse MAC doit se trouver dans le VLAN isolé, sauf sur le commutateur avec le port proche. Sur le commutateur proche, l'adresse MAC doit se trouver dans le VLAN principal.

2. UCS comme l'illustre l'image.



3. Vérifiez que la sortie n5k en amont est identique à celle de la sortie précédente sur n5k et comme le montre 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 Nexus 1000v avec port de promiscuité en amont N5k

Configuration UCS

La configuration UCS (qui inclut la configuration vNIC du profil de service) reste la même que dans l'exemple de 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 des requêtes ping vers d’autres systèmes configurés dans le groupe de ports, ainsi que vers le routeur ou un autre périphérique au niveau du port proche. Les requêtes ping envoyées au périphérique au-delà du port proche doivent fonctionner, tandis que celles envoyées aux autres périphériques du VLAN isolé doivent échouer, comme indiqué dans la section précédente et dans les images.