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

Contenu

Introduction

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

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- UCS
- Cisco Nexus 1000 V (N1K) ou Vmware DVS
- VMware
- Commutation de la couche 2 (L2)

Composants utilisés

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

Théorie

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.

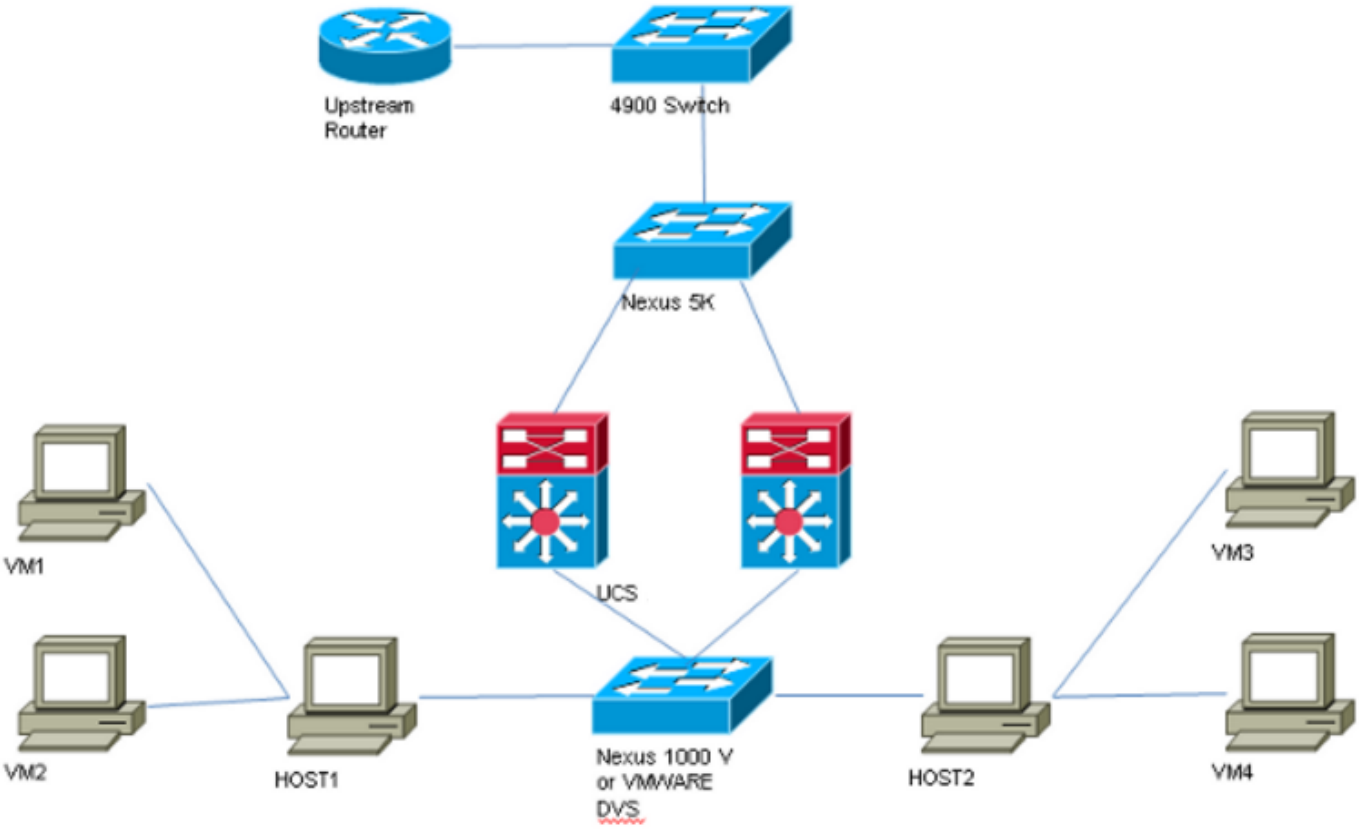
Il y a trois types de ports PVLAN :

- **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 (émissions y compris) 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

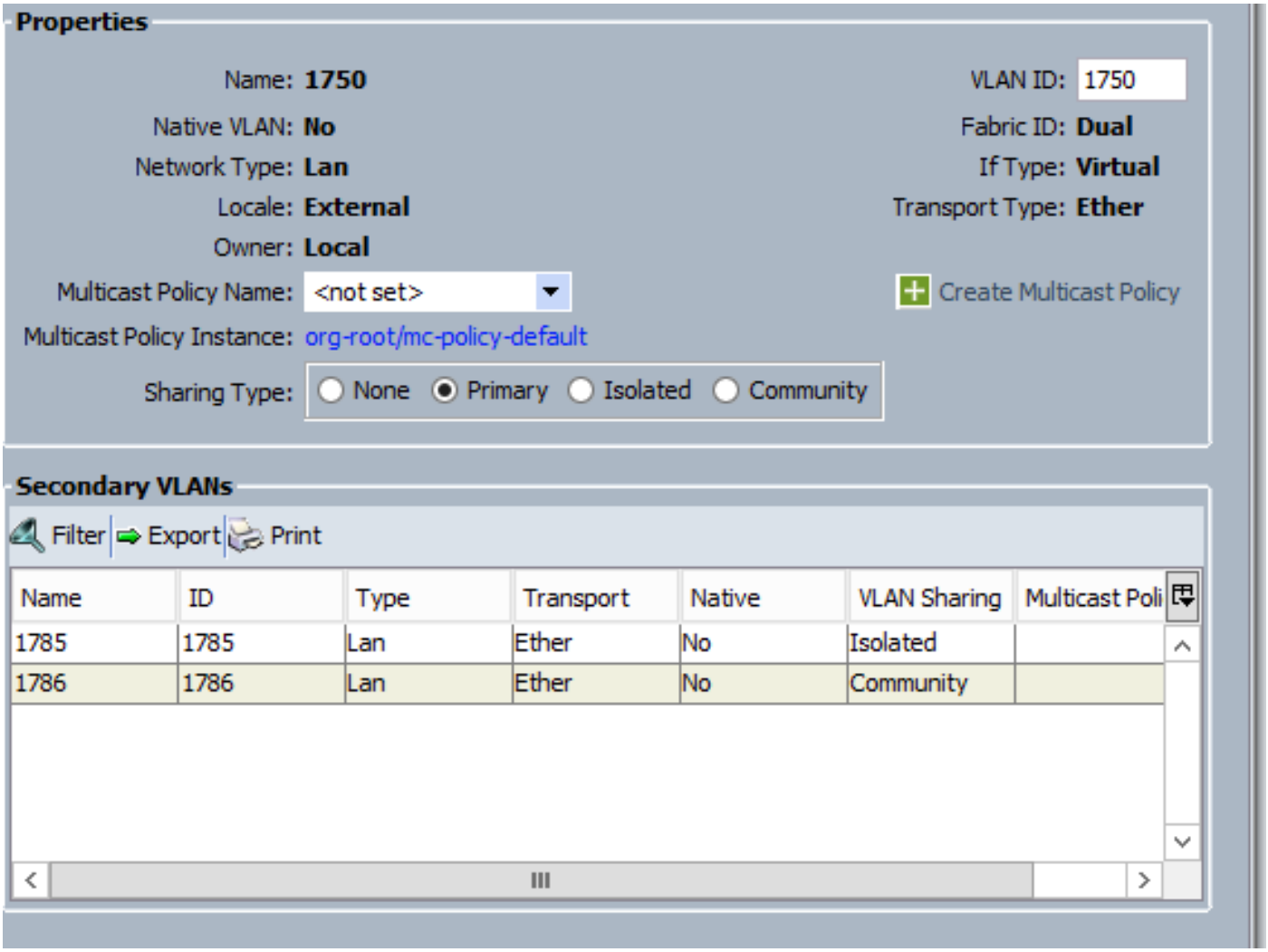
avec le Nexus 1000v ou Vmware DVS



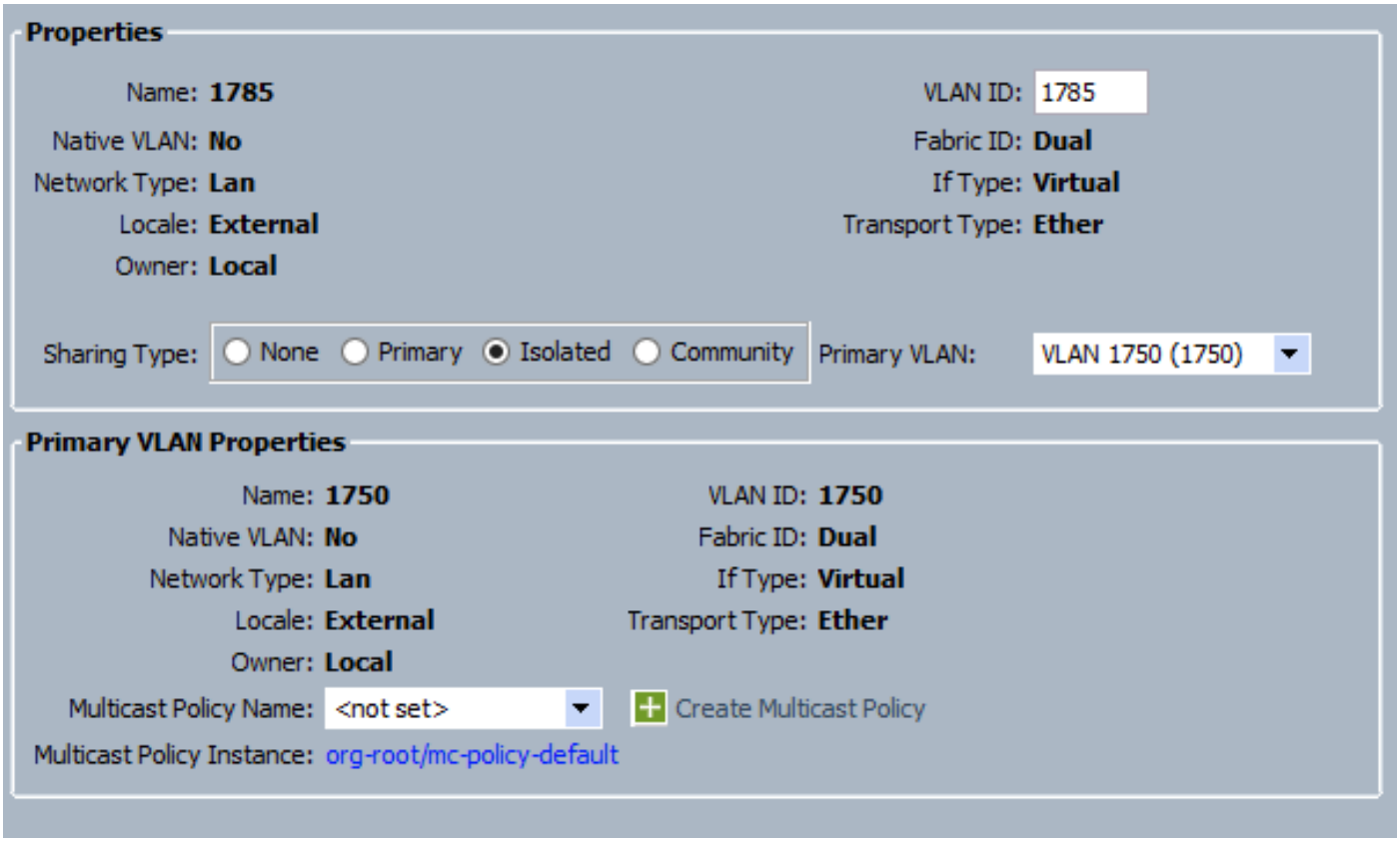
Remarque: Cet exemple utilise le VLAN 1750 en tant que primaire, 1785 comme d'isolement et 1786 comme VLAN de la communauté

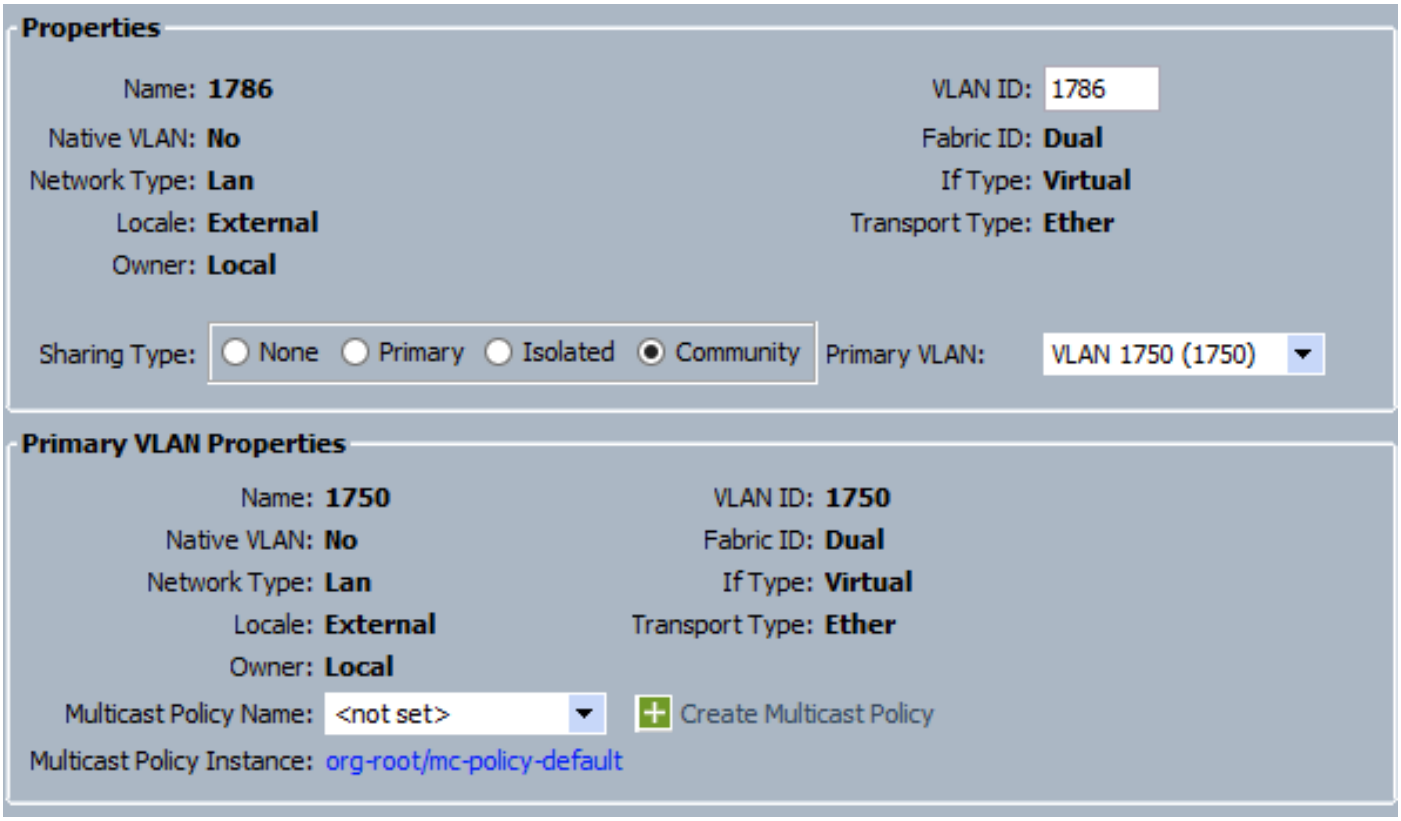
Configuration UCS avec le VMware DVS

1. Afin de créer le VLAN primaire, cliquez sur **primaire** comme type partageant, et écrivez un **ID DE VLAN de** 1750 :

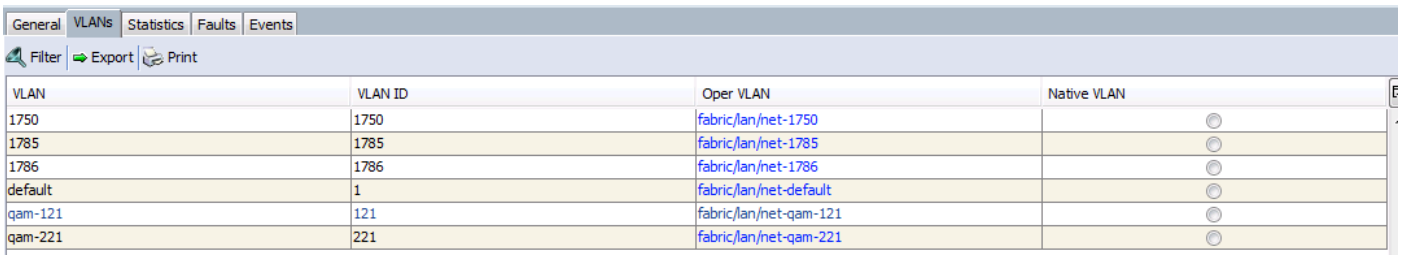


2. Créez en conséquence isolé et de la Communauté des VLAN en tant que ci-dessous. Aucune de ces derniers ne doit être un VLAN indigène





3. vnic sur le service profile porte des VLAN réguliers aussi bien que des pvlans



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 des VLAN réguliers aussi bien que des pvlans

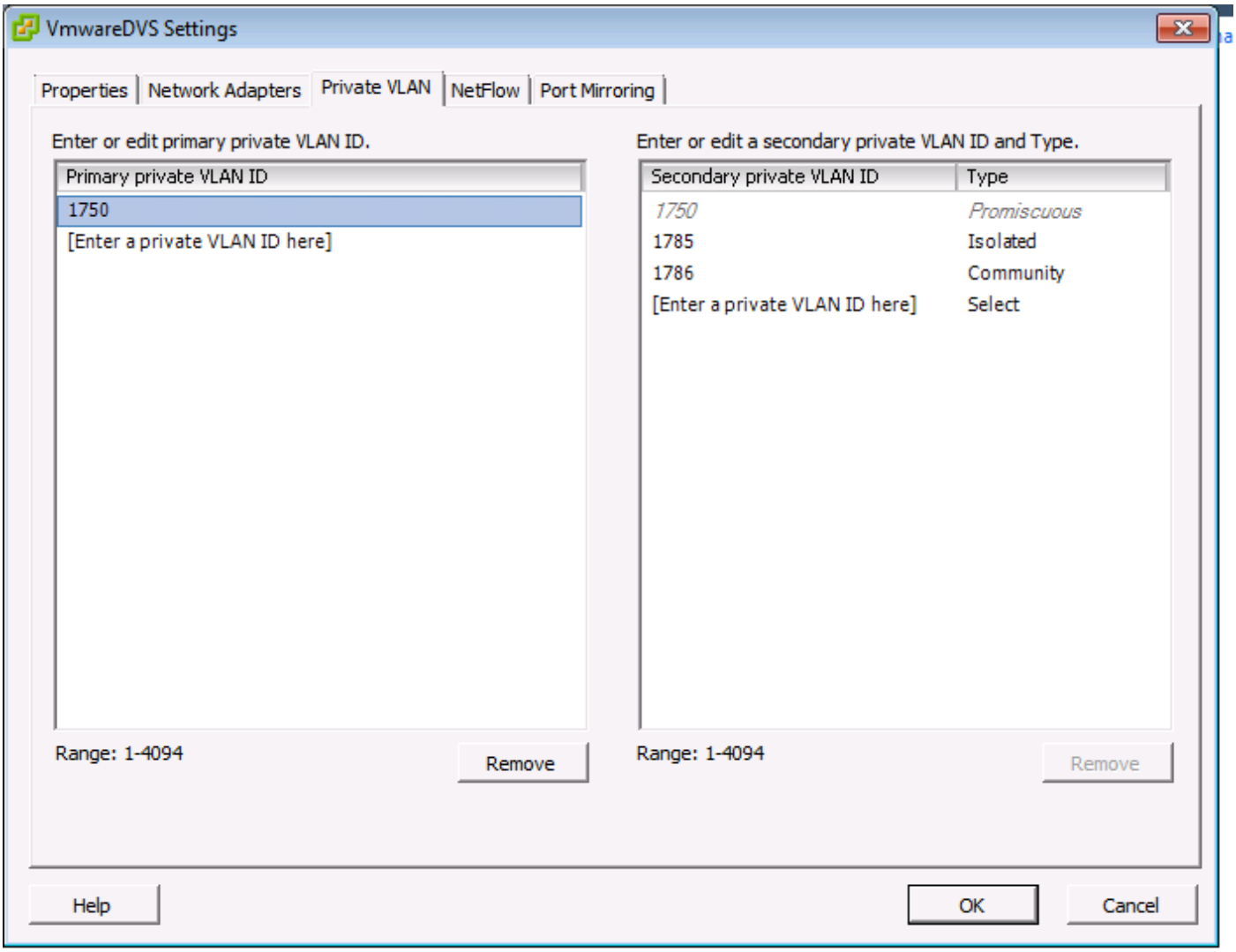
interface port-channel1
description U : Liaison ascendante
switchport mode trunk
goupiller le cadre
switchport trunk allowed vlan 1,121,221,321,1750,1785-1786
vitesse 10000

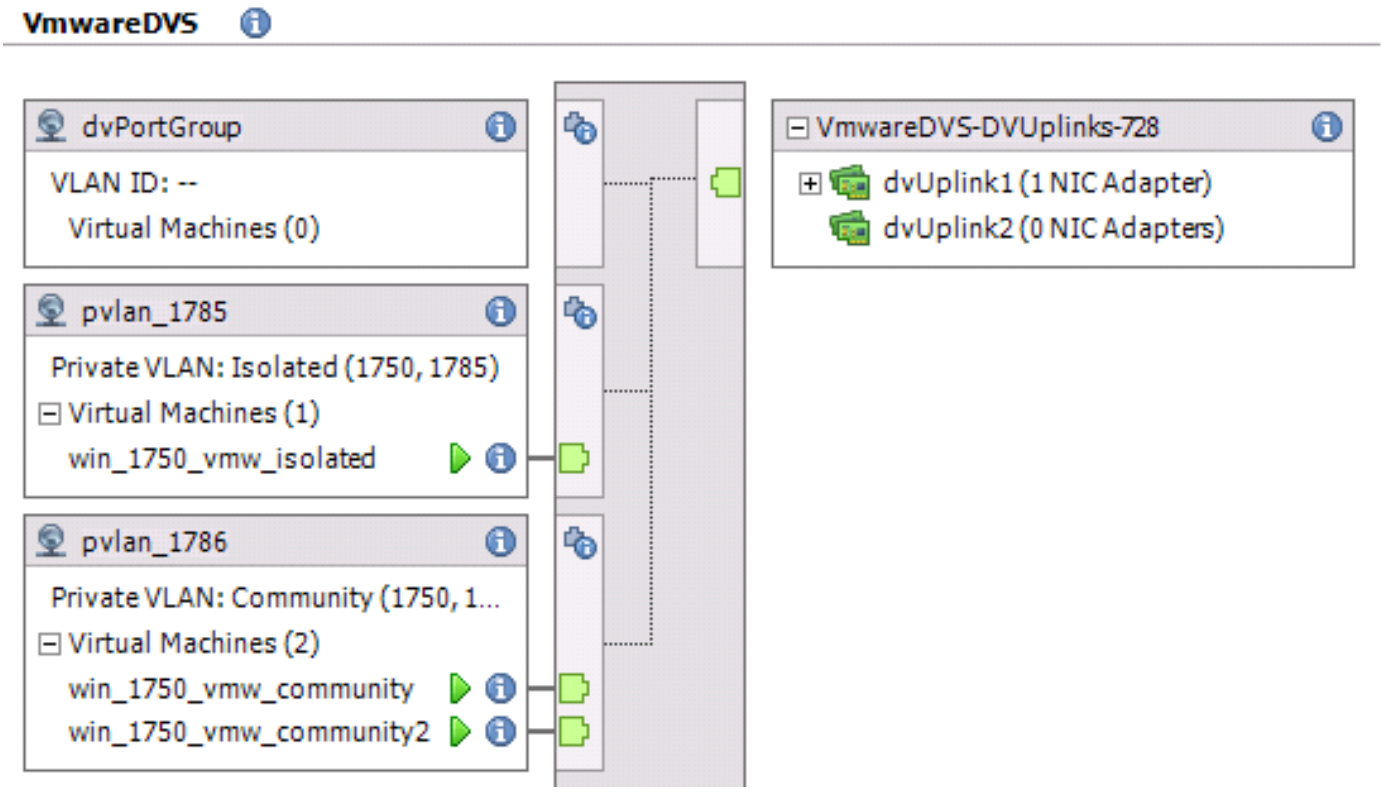
F240-01-09-UCS4-A(nxos)#

Show vlan private-vlan F240-01-09-UCS4-A(nxos)#
Ports secondaires primaires de type
------- --------- --------------- ----------

1750 1785 d'isolement
la communauté 1750 1786

Configuration sur le VMware DVS





Configuration de commutateur en amont N5k

feature private-vlan

VLAN 1750
private-vlan primaire
private-vlan association 1785-1786

VLAN 1785
private-vlan d'isolement

VLAN 1786
la communauté de private-vlan

interface Vlan1750

IP address 10.10.175.252/24
private-vlan mapping 1785-1786

aucun arrêt

interface port-channel114

Description à l'UCS
switchport mode trunk
switchport trunk allowed vlan 1,121,154,169,221,269,321,369,1750,1785-1786
spanning-tree port type edge
enable de spanning-tree bpduguard
enable de spanning-tree bpdufilter
le <=== du vpc 114 s'il y a une paire 5k dans la configuration de vpc ajoutent seulement alors cette ligne aux deux N5k

Configuration de commutateur de l'en amont 4900

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 :

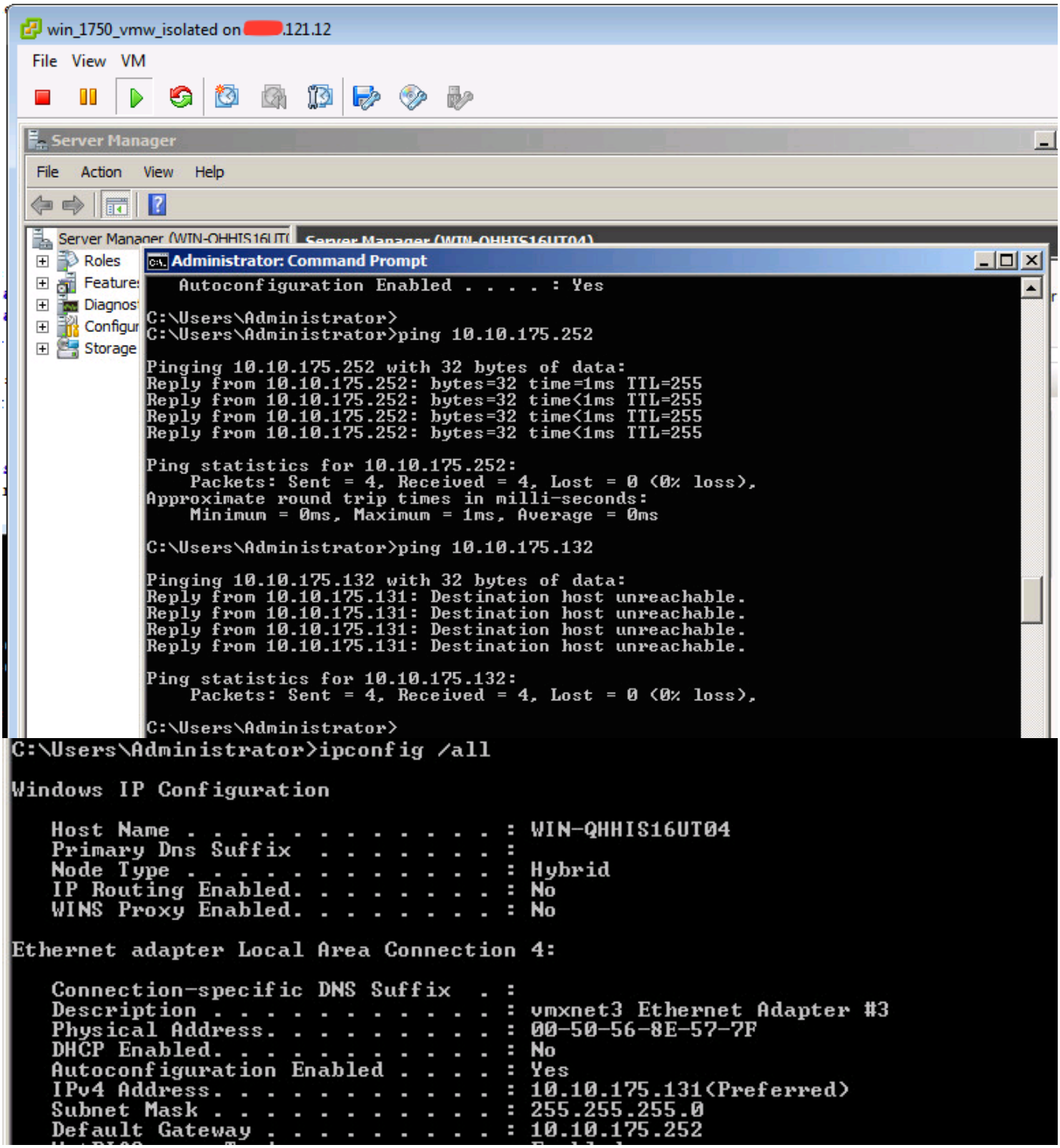
1. interface GigabitEthernet0/1.1
2. encapsulation dot1Q 1750

3. IP address10.10.175.254/24

Dépannage

Cette procédure décrit comment tester la configuration pour des dvs de vmware utilisant pvlan.

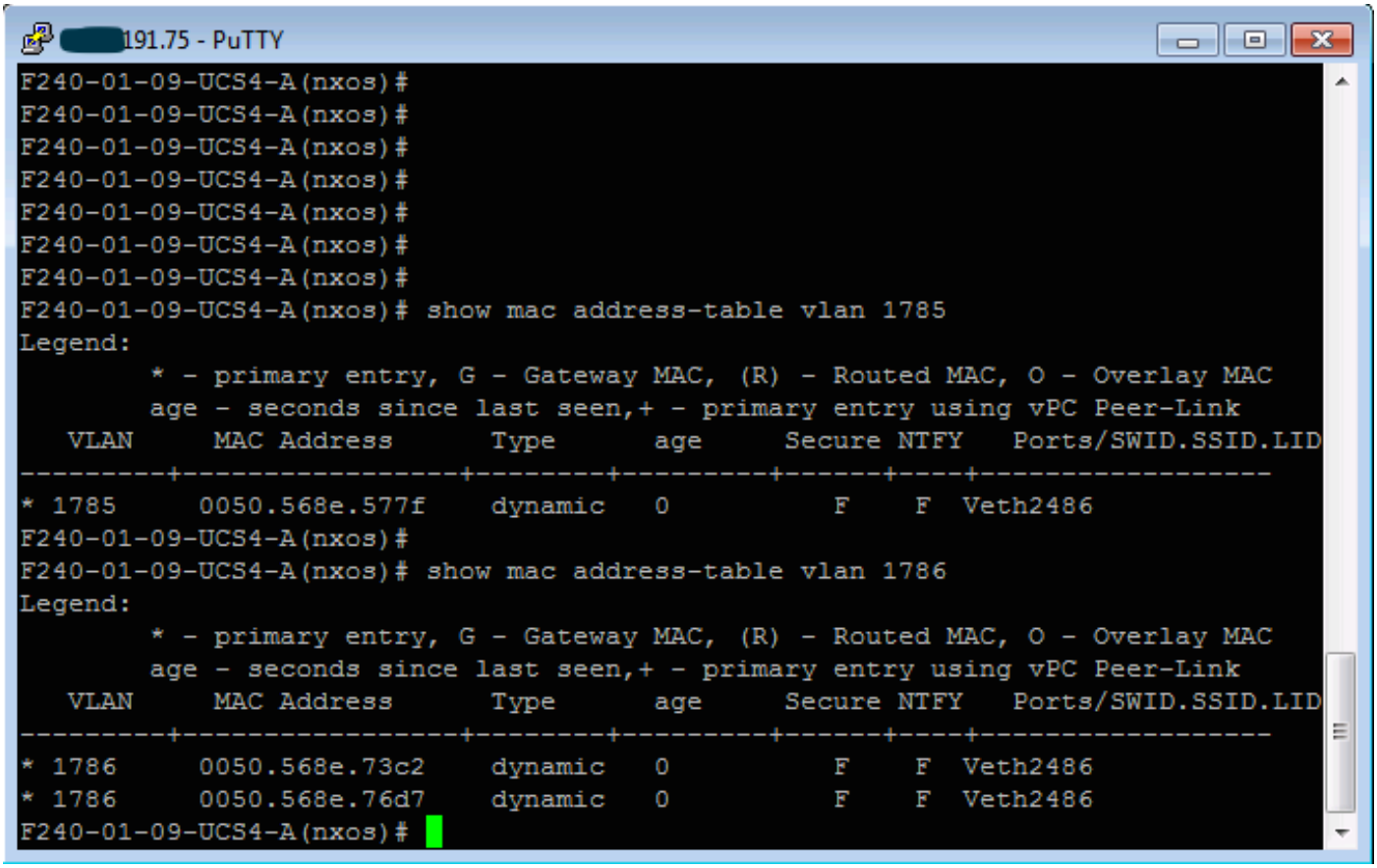
1. Exécutez les pings à d'autres systèmes configurés dans le port-groupe aussi bien que le routeur ou tout autre périphérique au port proche. Les pings au périphérique après le port proche devraient fonctionner, alors que ceux à d'autres périphériques dans le VLAN d'isolement devraient échouer.



Vérifiez les tables d'adresse MAC afin de voir où votre MAC est appris. Sur tous les

Commutateurs, le MAC devrait être dans le VLAN d'isolement excepté sur le commutateur avec le port proche. Sur le commutateur promiscueux le MAC devrait être dans le VLAN primaire.

2. UCS



3. vérifiez l'en amont n5k pour le même MAC, sortie semblable à la sortie ci-dessus devrait être présent sur n5k

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

Configuration UCS

La configuration UCS (config vnic inclusing de service profile) restera la même chose selon l'exemple ci-dessus avec le vmware DVS

Configuration N1k

feature private-vlan

VLAN 1750
private-vlan primaire
private-vlan association 1785-1786

VLAN 1785
private-vlan d'isolement

VLAN 1786
la communauté de private-vlan

le même port-profil de liaison ascendante est utilisé pour des VLAN réguliers et des pvlans. Dans ce VLAN 121 et 221 d'exemple sont les VLAN réguliers mais vous pouvez les changer en conséquence

pvlan-liaison ascendante-aucun-bal d'étudiants d'Ethernets de type de port-profil
switchport mode trunk
mtu 9000
switchport trunk allowed vlan 121,221,1750,1785-1786
mode automatique de channel-group sur MAC-goupiller

VLAN 121 de système
aucun arrêt
état activé
port-groupe de vmware

vethernet pvlan_1785 de type de port-profil
switchport mode private-vlan host
switchport private-vlan host-association 1750 1785
switchport access vlan 1785
aucun arrêt
état activé
port-groupe de vmware

vethernet pvlan_1786 de type de port-profil
switchport mode private-vlan host
switchport access vlan 1786
switchport private-vlan host-association 1750 1786
aucun arrêt
état activé
port-groupe de vmware

Dépannage

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 devraient fonctionner, alors que ceux à d'autres périphériques dans le VLAN d'isolement devraient échouer, suivant les indications de la section précédente