

Configurer la machine virtuelle sur le serveur lame UCS en tant que destination SPAN

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Machine virtuelle avec adresse IP](#)

[VM de renifleur sans adresse IP](#)

[Scénario d'échec](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit les étapes à suivre pour capturer un flux de trafic qui se trouve complètement en dehors de Cisco Unified Computing System (UCS) et le diriger vers une machine virtuelle exécutant un outil de renifleur à l'intérieur d'UCS. La source et la destination du trafic capturé se trouvent en dehors de l'UCS. La capture peut être initiée sur un commutateur physique directement connecté à UCS ou à quelques sauts de distance.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- UCS
- VMware ESX version 4.1 ou ultérieure
- Analyseur de port de commutateur distant encapsulé (ERSPAN)

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Catalyst 6503 exécutant 12.2(18)ZYA3c
- Gamme Cisco UCS B exécutant 2.2(3e)

- VMWare ESXi 5.5 build 1331820

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.

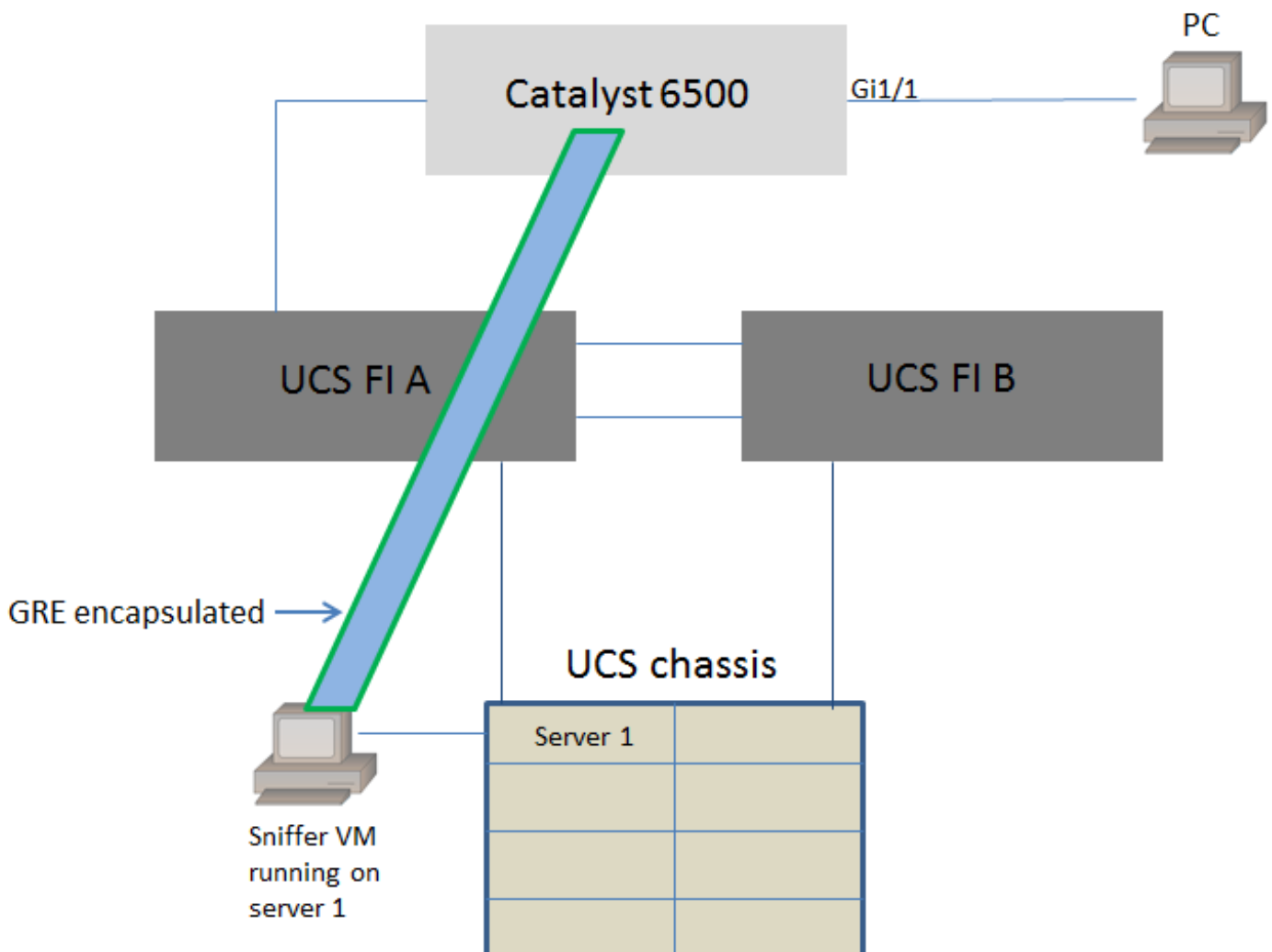
Informations générales

UCS ne dispose pas de la fonctionnalité Remote SPAN (RSPAN) pour recevoir le trafic SPAN d'un commutateur connecté et le diriger vers un port local. La seule façon d'y parvenir dans un environnement UCS est donc d'utiliser la fonctionnalité RSPAN encapsulée (ERSPAN) sur un commutateur physique et d'envoyer le trafic capturé à la machine virtuelle à l'aide d'IP. Dans certaines implémentations, la machine virtuelle exécutant l'outil de renifleur ne peut pas avoir d'adresse IP. Ce document explique la configuration requise lorsque la machine virtuelle du renifleur a une adresse IP, ainsi que le scénario sans adresse IP. La seule limite ici est que la machine virtuelle renifleur doit être capable de lire l'encapsulation GRE/ERSPAN à partir du trafic qui lui est envoyé.

Configuration

Diagramme du réseau

Cette topologie a été prise en compte dans ce document :



Le PC connecté à GigabitEthernet1/1 du Catalyst 6500 est surveillé. Le trafic sur GigabitEthernet1/1 est capturé et envoyé à la machine virtuelle du renifleur qui s'exécute à l'intérieur de Cisco UCS sur le serveur 1. La fonctionnalité ERSPAN du commutateur 6500 capture le trafic, l'encapsule à l'aide de GRE et l'envoie à l'adresse IP de la machine virtuelle de renifleur.

Machine virtuelle avec adresse IP

Note: Les étapes décrites dans cette section peuvent également être utilisées dans le scénario où le renifleur s'exécute dans un serveur sans système d'exploitation sur une lame UCS au lieu de s'exécuter sur une machine virtuelle.

Ces étapes sont requises lorsque la machine virtuelle du renifleur peut avoir une adresse IP :

- Configurer la machine virtuelle de renifleur dans l'environnement UCS avec une adresse IP accessible à partir du 6500
- Exécuter l'outil de renifleur à l'intérieur de la machine virtuelle
- Configurez une session source ERSPAN sur le 6500 et envoyez le trafic capturé directement à l'adresse IP de la machine virtuelle

Les étapes de configuration du commutateur 6500 :

```
CAT6K-01(config)#monitor session 1 type erspan-source
CAT6K-01(config-mon-erspan-src)#source interface gi1/1
CAT6K-01(config-mon-erspan-src)#destination
CAT6K-01(config-mon-erspan-src-dst)#ip address 192.0.2.2
CAT6K-01(config-mon-erspan-src-dst)#origin ip address 192.0.2.1
CAT6K-01(config-mon-erspan-src-dst)#erspan-id 1
CAT6K-01(config-mon-erspan-src-dst)#exit
CAT6K-01(config-mon-erspan-src)#no shut
CAT6K-01(config-mon-erspan-src)#end
```

Dans cet exemple, l'adresse IP de la machine virtuelle du renifleur est 192.0.2.2

VM de renifleur sans adresse IP

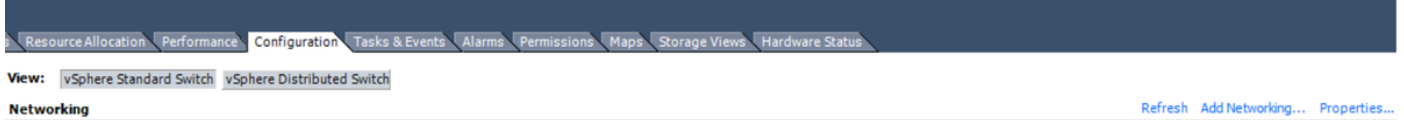
Ces étapes sont requises lorsque la machine virtuelle du renifleur ne peut pas avoir d'adresse IP :

- Configurer la machine virtuelle de renifleur dans l'environnement UCS
- Exécuter l'outil de renifleur à l'intérieur de la machine virtuelle
- Créez une deuxième machine virtuelle pouvant avoir une adresse IP dans le même hôte et configurez-la avec une adresse IP accessible à partir du 6500
- Configurez le groupe de ports sur le commutateur virtuel VMWare pour qu'il soit en mode proche
- Configurez une session source ERSPAN sur le 6500 et envoyez le trafic capturé à l'adresse IP de la deuxième machine virtuelle

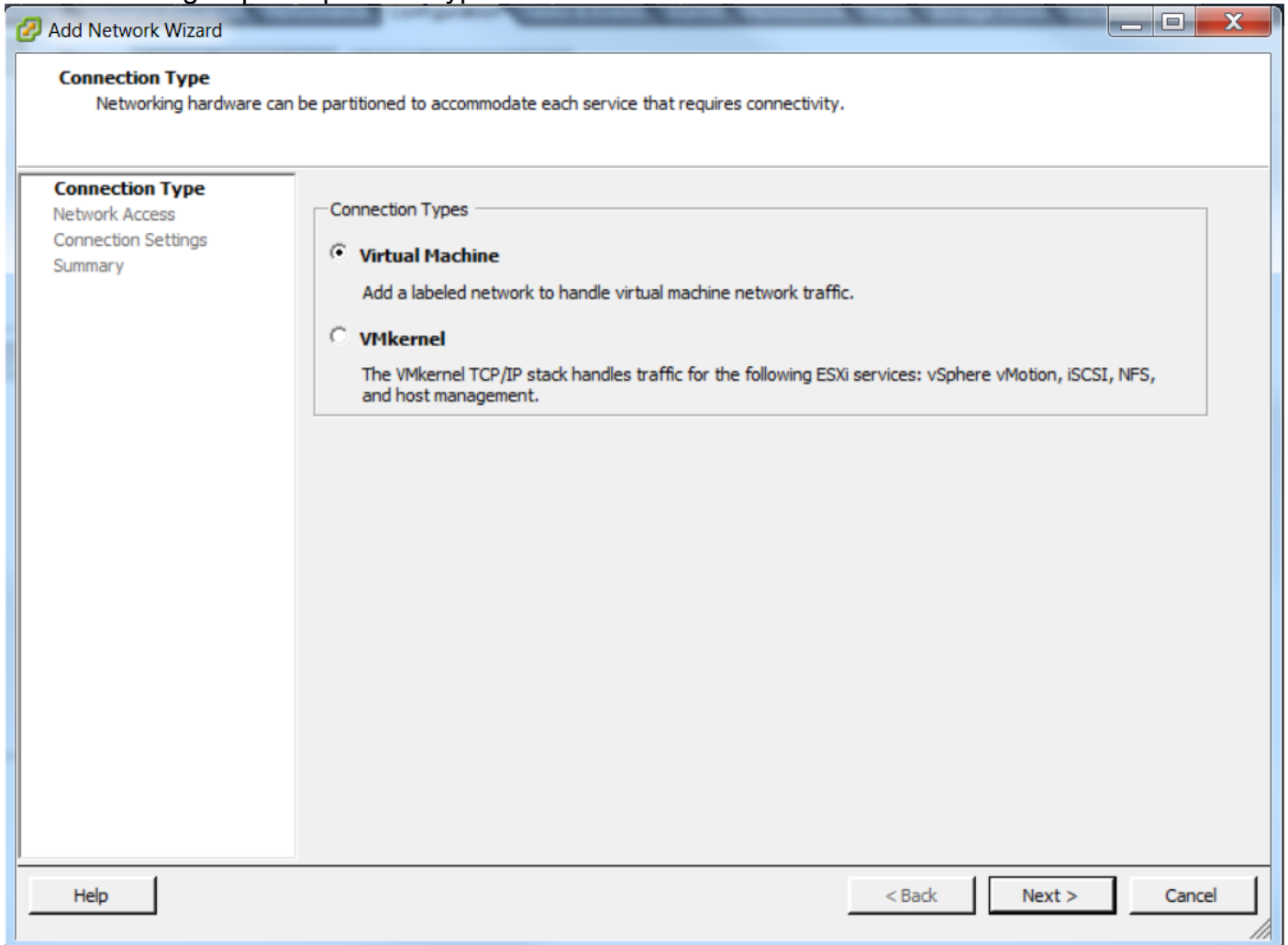
Ces étapes indiquent la configuration requise sur VMWare ESX : Accédez directement à l'étape 2 si un groupe de ports est déjà configuré.

1. Créer un groupe de ports de machine virtuelle et lui affecter les deux machines virtuelles

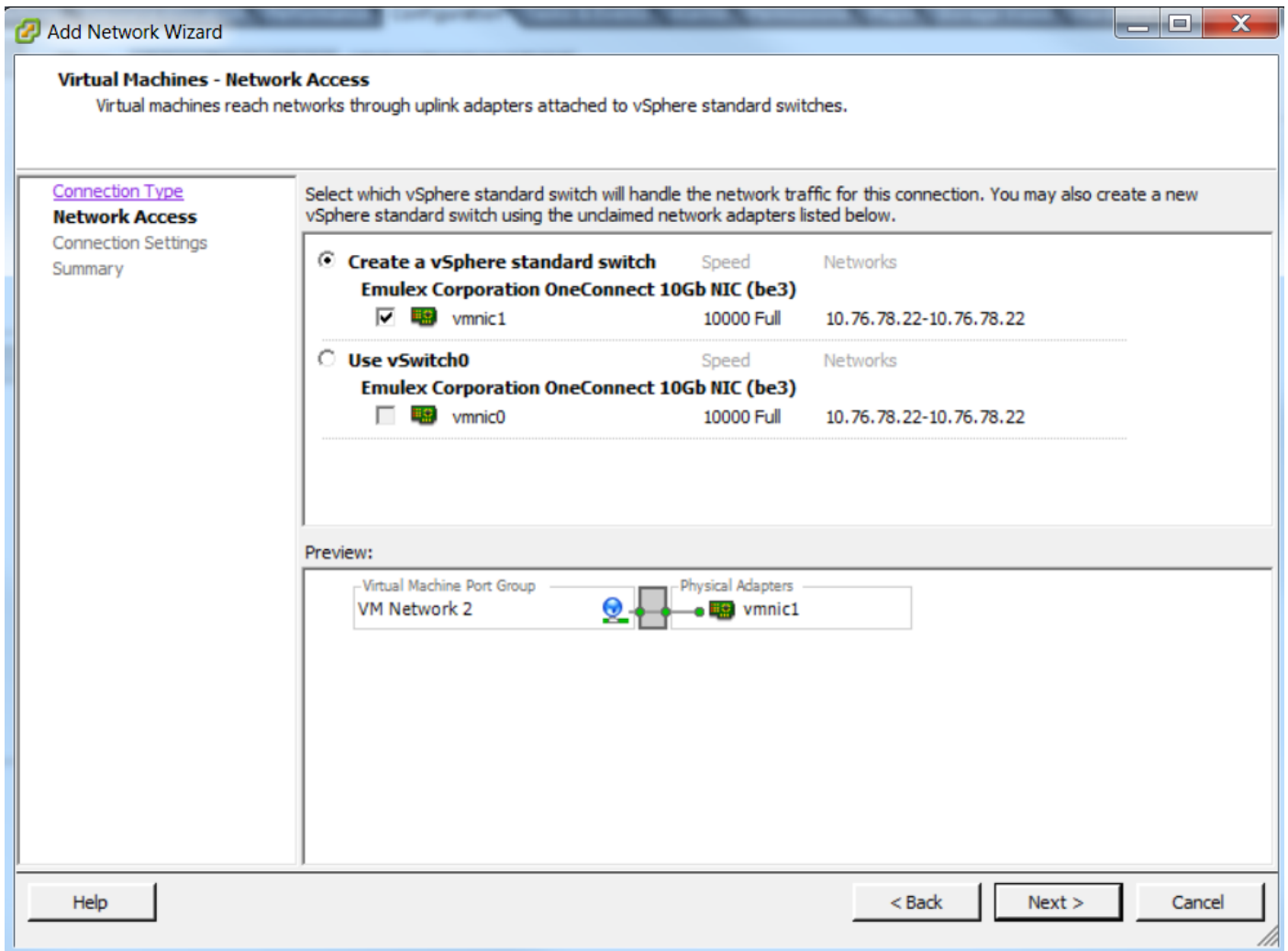
- Accédez à l'onglet **Networking** et cliquez sur **Add Networking** sous **vSphere Standard Switch**



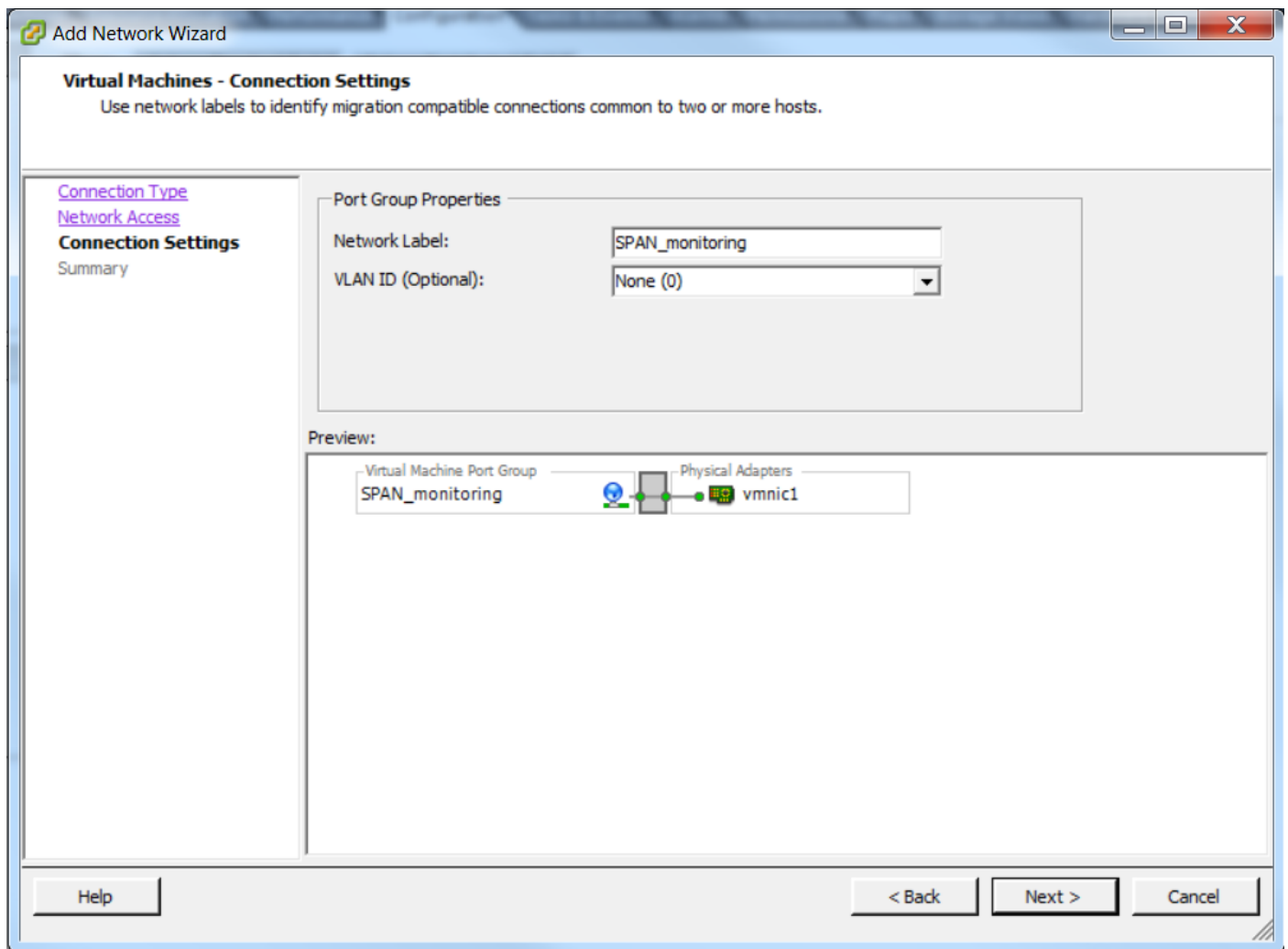
- Créer un groupe de ports de type Machine virtuelle



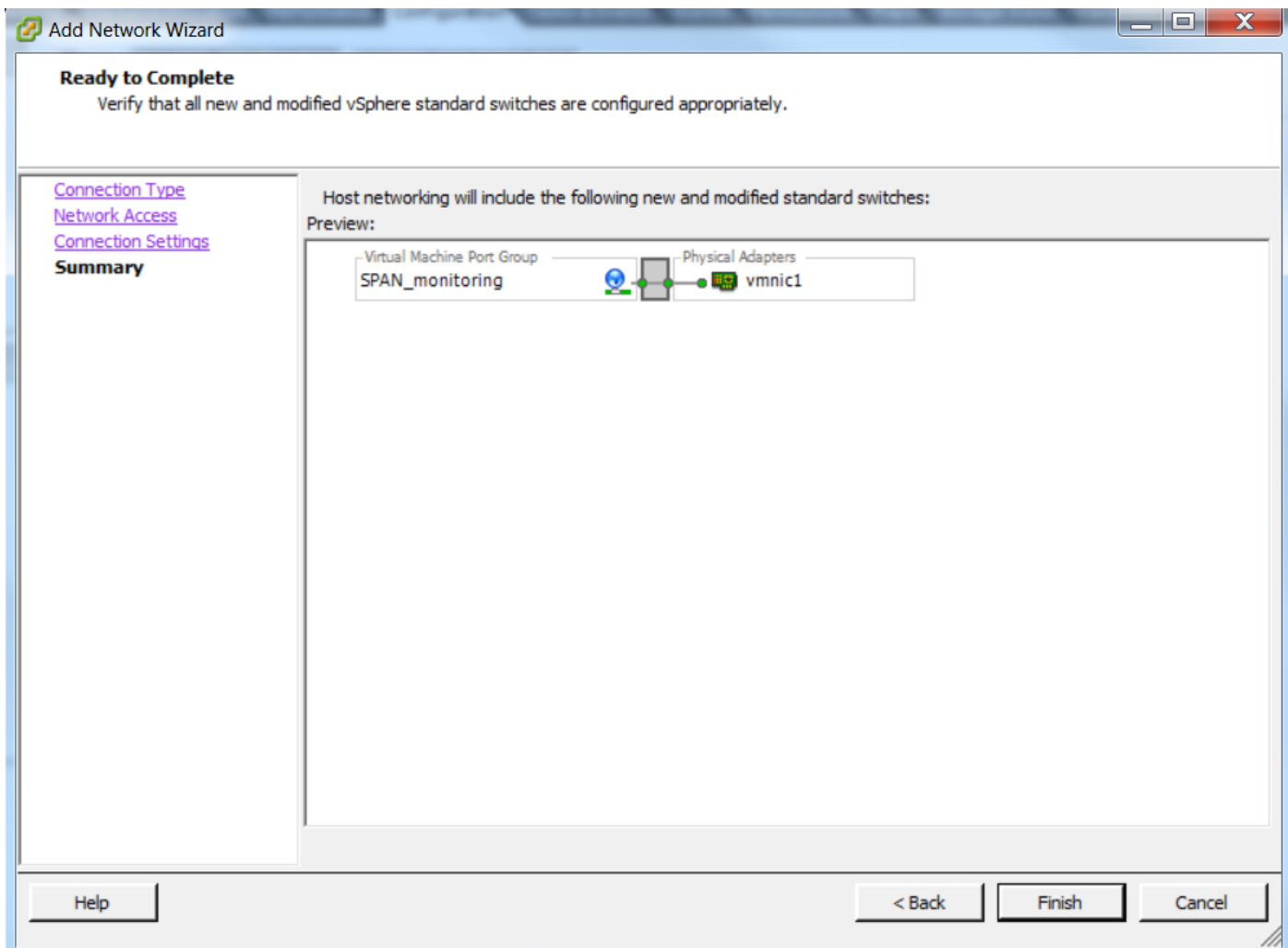
- Attribuez une interface physique (vmnic) au groupe de ports comme illustré dans cette image.



- Configurez un nom pour le groupe de ports et ajoutez le VLAN approprié comme indiqué dans l'image.



- Vérifiez la configuration et cliquez sur **Terminer** comme indiqué dans l'image.

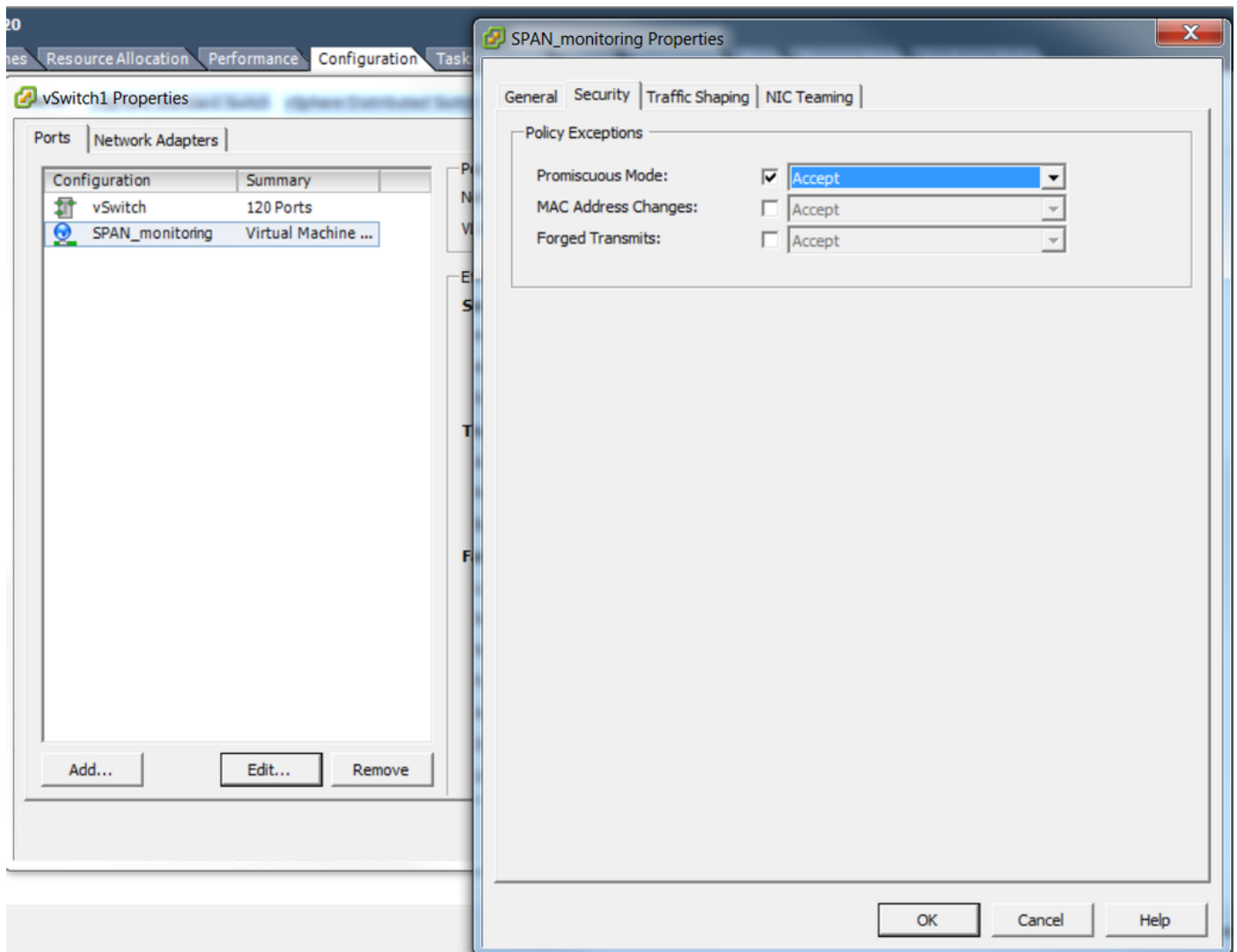


2. Configurez le groupe de ports pour qu'il soit en mode proche, comme l'illustre l'image.

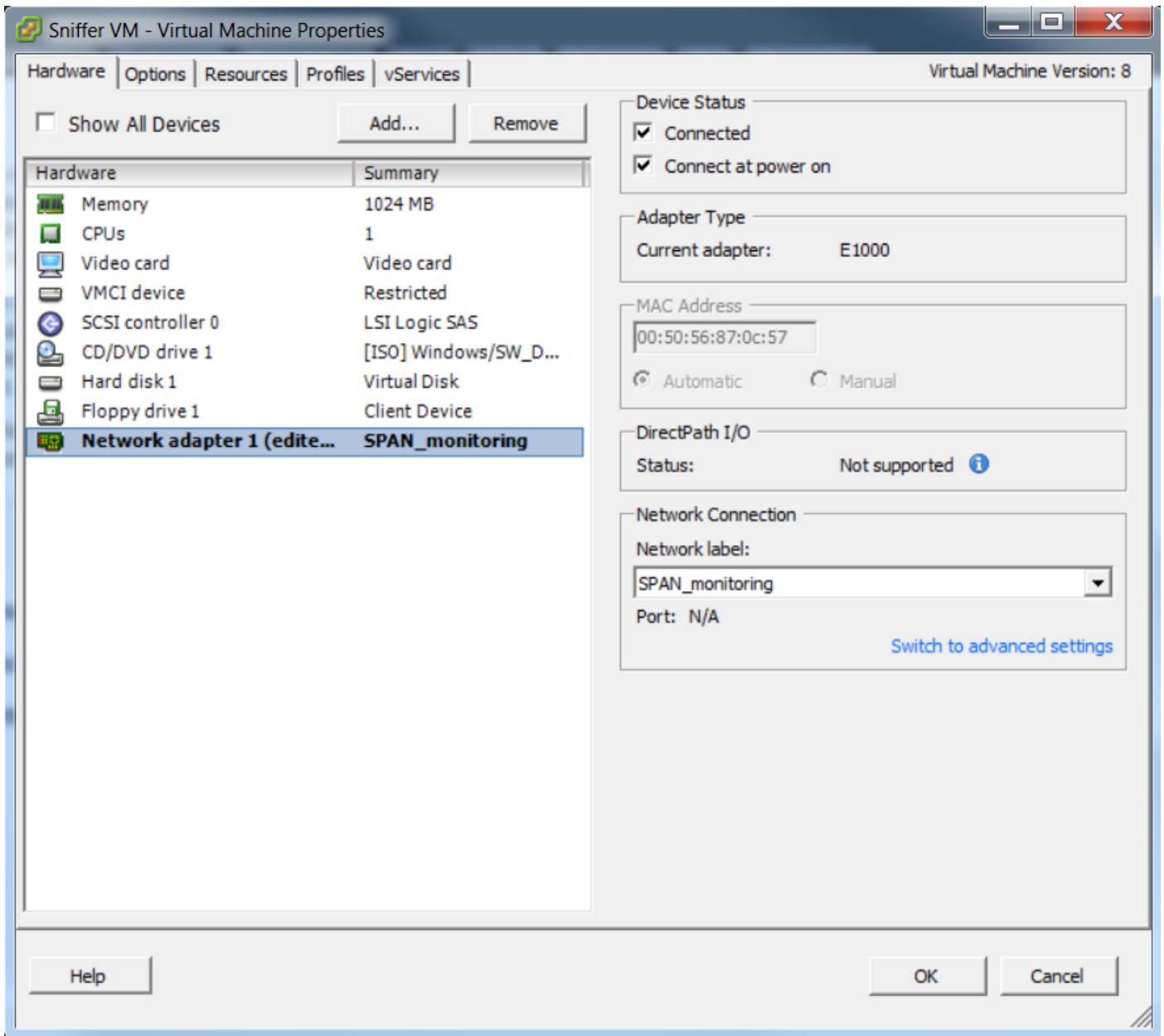
- Le groupe de ports doit apparaître sous l'onglet **Mise en réseau** maintenant
- Cliquez sur **Propriétés**



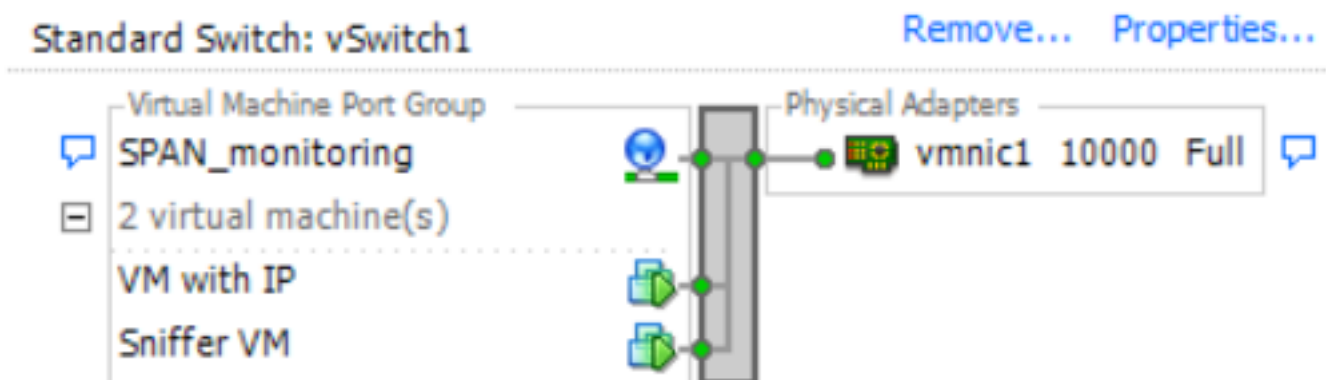
- Sélectionnez le groupe de ports et cliquez sur **Modifier**
- Accédez à l'onglet **Sécurité** et modifiez le paramètre du mode Promiscuité en Accept comme illustré dans cette image



3. Attribuez les deux machines virtuelles au groupe de ports à partir de la section des paramètres de la machine virtuelle.



4. Les deux machines virtuelles doivent apparaître dans le groupe de ports sous l'onglet **Mise en réseau** maintenant.



Dans cet exemple, VM avec IP est la deuxième VM qui a une adresse IP et Sniffer VM est la VM avec l'outil de renifleur sans adresse IP.

5. Voici les étapes de configuration du commutateur 6500 :

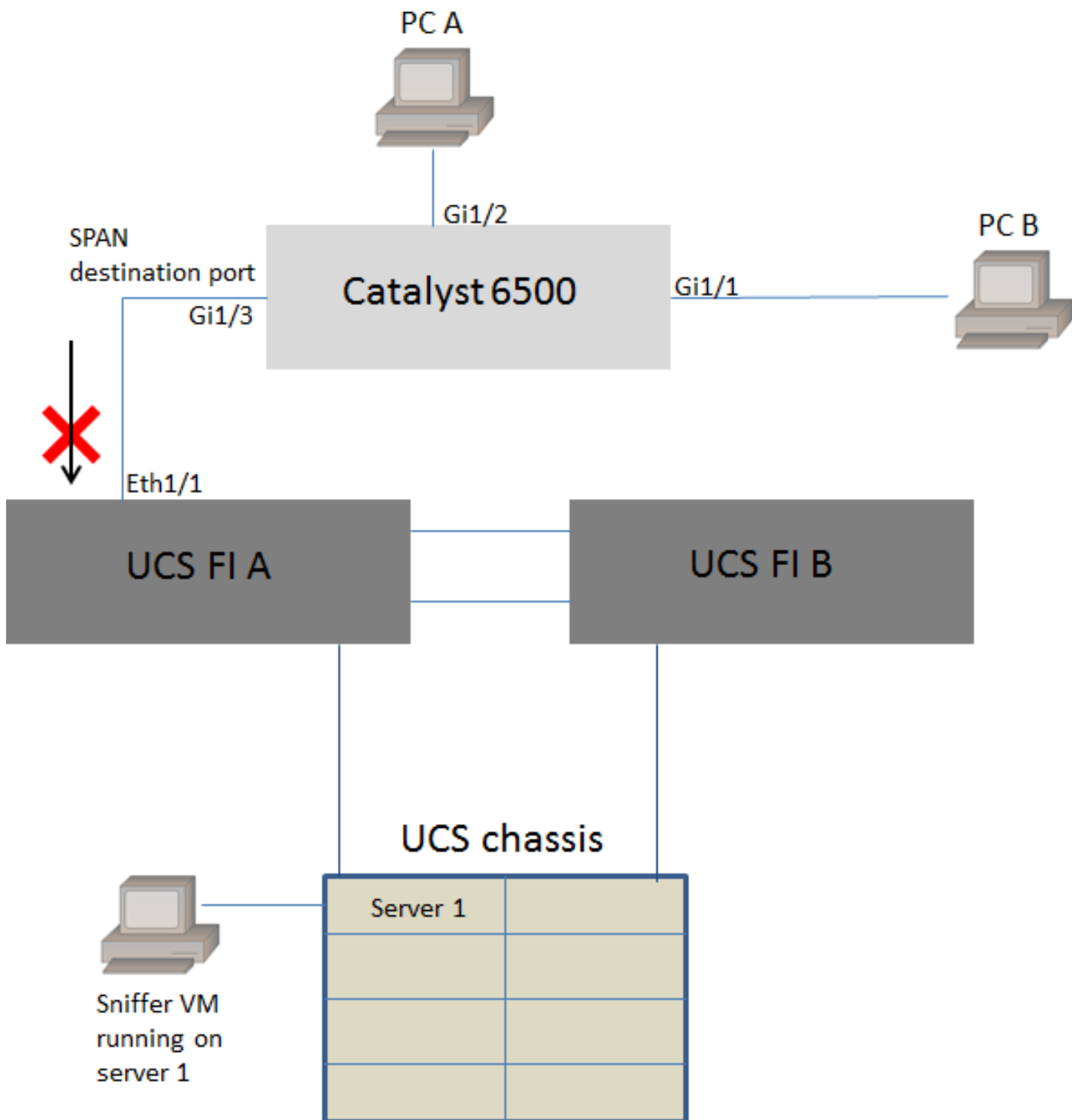
```
CAT6K-01(config)#monitor session 1 type erspan-source
CAT6K-01(config-mon-erspan-src)#source interface gi1/1
CAT6K-01(config-mon-erspan-src)#destination
CAT6K-01(config-mon-erspan-src-dst)#ip address 192.0.2.3
CAT6K-01(config-mon-erspan-src-dst)#origin ip address 192.0.2.1
CAT6K-01(config-mon-erspan-src-dst)#erspan-id 1
CAT6K-01(config-mon-erspan-src-dst)#exit
CAT6K-01(config-mon-erspan-src)#no shut
CAT6K-01(config-mon-erspan-src)#end
```

Dans cet exemple, l'adresse IP de la deuxième machine virtuelle (VM avec IP) est 192.0.2.3.

Avec cette configuration, le commutateur 6500 encapsule les paquets capturés et les envoie à la machine virtuelle avec l'adresse IP. Le mode de promiscuité sur le vSwitch VMWare permet à la machine virtuelle du renifleur de voir également ces paquets.

Scénario d'échec

Cette section décrit un scénario d'échec courant lors de l'utilisation de la fonctionnalité SPAN locale sur un commutateur physique au lieu de la fonctionnalité ERSPAN. Cette topologie est considérée ici :



Le trafic entre PC A et PC B est surveillé à l'aide de la fonctionnalité SPAN locale. La destination du trafic SPAN est dirigée vers le port connecté à l'interconnexion de fabric UCS (FI).

La machine virtuelle avec l'outil de renifleur s'exécute à l'intérieur d'UCS sur le serveur 1.

Voici la configuration du commutateur 6500 :

```
CAT6K-01(config)#monitor session 1 source interface gigabitEthernet 1/1, gigabitEthernet 1/2
CAT6K-01(config)#monitor session 1 destination interface gigabitEthernet 1/3
```

Tout le trafic circulant sur les ports Gig1/1 et Gig1/2 sera répliqué sur le port Gig1/3. Les adresses MAC source et de destination de ces paquets seront inconnues de l'FI UCS.

En mode hôte d'extrémité Ethernet UCS, l'IF abandonne ces paquets de monodiffusion inconnus.

En mode de commutation Ethernet UCS, l'interface FI apprend l'adresse MAC source sur le port connecté au 6500 (Eth1/1), puis diffuse les paquets en aval vers les serveurs. Cette séquence d'événements se produit :

1. Pour faciliter la compréhension, considérez le trafic circulant uniquement entre PC A (avec mac-address aaaa.aaaa.aaaa) et PC B (avec mac-address bbbb.bbb.bbb) sur les interfaces Gig1/1 et Gig1/2
2. Le premier paquet va du PC A au PC B, comme le montre l'UCS FI Eth1/1
3. L'IF apprend mac-address aaaa.aaaa.aaaa sur Eth1/1
4. L'IF ne connaît pas l'adresse MAC de destination bbbb.bbb.bbb et diffuse le paquet à tous les ports du même VLAN
5. La machine virtuelle du renifleur, dans le même VLAN, voit également ce paquet
6. Le paquet suivant va du PC B au PC A
7. Lorsque cela atteint Eth1/1, l'adresse mac bbbb.bbb.bbb est apprise sur Eth1/1
8. La destination du paquet est pour mac-address aaaa.aaaa.aaaa
9. L'IF abandonne ce paquet car mac-address aaaa.aaaa.aaaa est appris sur Eth1/1 et le paquet a été reçu sur Eth1/1 lui-même
10. Les paquets suivants, destinés à mac-address aaaa.aaaa.aaaa ou mac-address bbbb.bbb.bbbb, sont supprimés pour la même raison

Vérification

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

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Configuration du mode promiscuité sur un commutateur virtuel ou un groupe de ports](#)
- [SPAN, RSPAN et ERSPAN sur Catalyst 6500](#)
- [Décapsulation du trafic ERSPAN avec les outils Open Source](#)
- [Support et documentation techniques - Cisco Systems](#)