

Virtuele machine op UCS bladeserver configureren als SPAN-bestemming

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Snijd VM met IP-adres](#)

[Snijd VM zonder IP-adres](#)

[Foutenscenario](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

In dit document worden de stappen beschreven om een verkeersstroom op te nemen die volledig buiten Cisco Unified Computing System (UCS) is en deze naar een virtuele machine (VM) te sturen met een scherpgereedschap binnen UCS. De bron en bestemming van het verkeer dat wordt opgenomen is buiten het UCS. De opname kan worden gestart op een fysieke schakelaar die direct op UCS is aangesloten of kan een paar sprongen verderop zijn.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- UCS
- VMware ESX versie 4.1 of hoger
- Inkapselde Remote-switchpoortanalyzer (ERSPAN)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Catalyst 6503 Series 12.2(18)ZYA3c
- Cisco UCS B-serie met 2.2(3e)
- VMWare ESXi 5.5-gebouw 1331820

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.

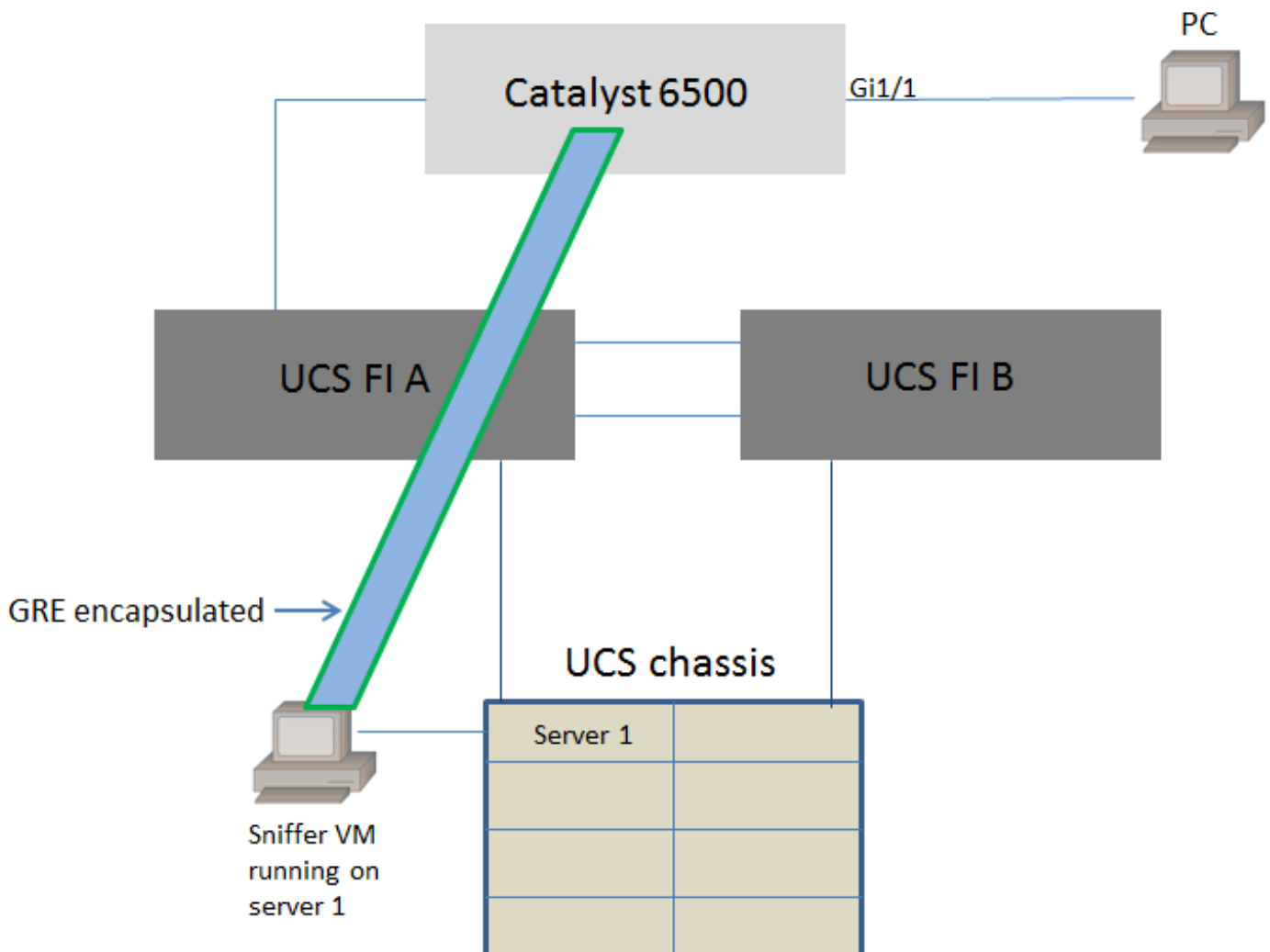
Achtergrondinformatie

UCS heeft niet de optie Remote SPAN (RSPAN) om SPAN-verkeer van een aangesloten switch te ontvangen en deze naar een lokale poort te leiden. De enige manier om dit in een UCS-omgeving te bereiken, is door gebruik te maken van de ingekapselde RSPAN-functie (ERSPAN) op een fysieke switch en door het opgenomen verkeer naar de VM te sturen met behulp van IP. Bij bepaalde implementaties kan de VM die het sniffer-gereedschap uitvoert geen IP-adres hebben. Dit document verklaart de configuratie die vereist is wanneer de sniffer VM een IP-adres heeft en het scenario zonder IP-adres. De enige beperking hier is dat de sniffer VM de GRE/ERSPAN-insluiting moet kunnen lezen uit het verkeer dat naar deze insluiting wordt gestuurd.

Configureren

Netwerkdigram

Deze topologie wordt in dit document in overweging genomen:



PC die aan Gigabit Ethernet1/1 van Catalyst 6500 is aangesloten wordt gecontroleerd. Het verkeer op Gigabit Ethernet1/1 wordt opgenomen en naar de sniffer VM verzonden die in Cisco UCS op server 1 draait. De ERSPAN-functie op de 6500-schakelaar neemt het verkeer op, kapselt het in met GRE en stuurt het naar het IP-adres van de sluipschutter.

Snijd VM met IP-adres

Opmerking: De in dit deel beschreven stappen kunnen ook worden gebruikt in het scenario waarin de sniffer in een server met kale metalen op een UCS-blad draait in plaats van op een VM.

Deze stappen zijn vereist wanneer de sniffer VM een IP-adres kan hebben:

- Configureer de sniffer VM binnen de UCS-omgeving met een IP-adres dat bereikbaar is vanaf de 6500
- Draai het snuifgereedschap binnen de VM
- Configureer een ERSPAN-bronsessie op de 6500 en verstuur het opgenomen verkeer rechtstreeks naar het IP-adres van de VM

De configuratiestappen in de 6500-schakelaar:

```
CAT6K-01(config)#monitor session 1 type erspan-source
CAT6K-01(config-mon-erspan-src)#source interface gil/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
```

In dit voorbeeld is het IP-adres van de snuiver VM 192.0.2.2

Snijd VM zonder IP-adres

Deze stappen zijn vereist wanneer de klant VM geen IP-adres kan hebben:

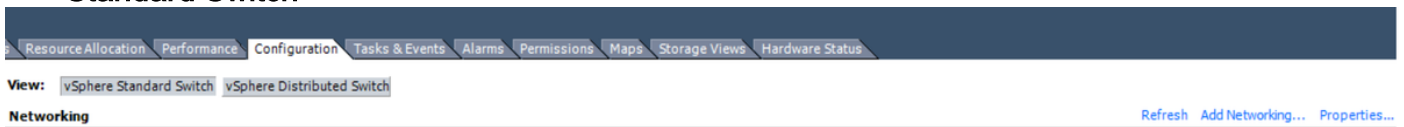
- VM configureren in de UCS-omgeving
- Draai het snuifgereedschap binnen de VM
- Maak een tweede VM die een IP-adres in dezelfde host kan hebben en stel deze aan met een IP-adres dat bereikbaar is vanaf de 6500
- Configuratie van de poortgroep van de VMWare vSwitch in de veelbelovende modus
- Configureer een ERSPAN-bronsessie op de 6500 en verstuur het opgenomen verkeer naar het IP-adres van de tweede VM

Deze stappen tonen de configuratie die vereist is voor de VMWare ESX: Ga rechtstreeks naar Stap 2 als u al een poortgroep hebt ingesteld.

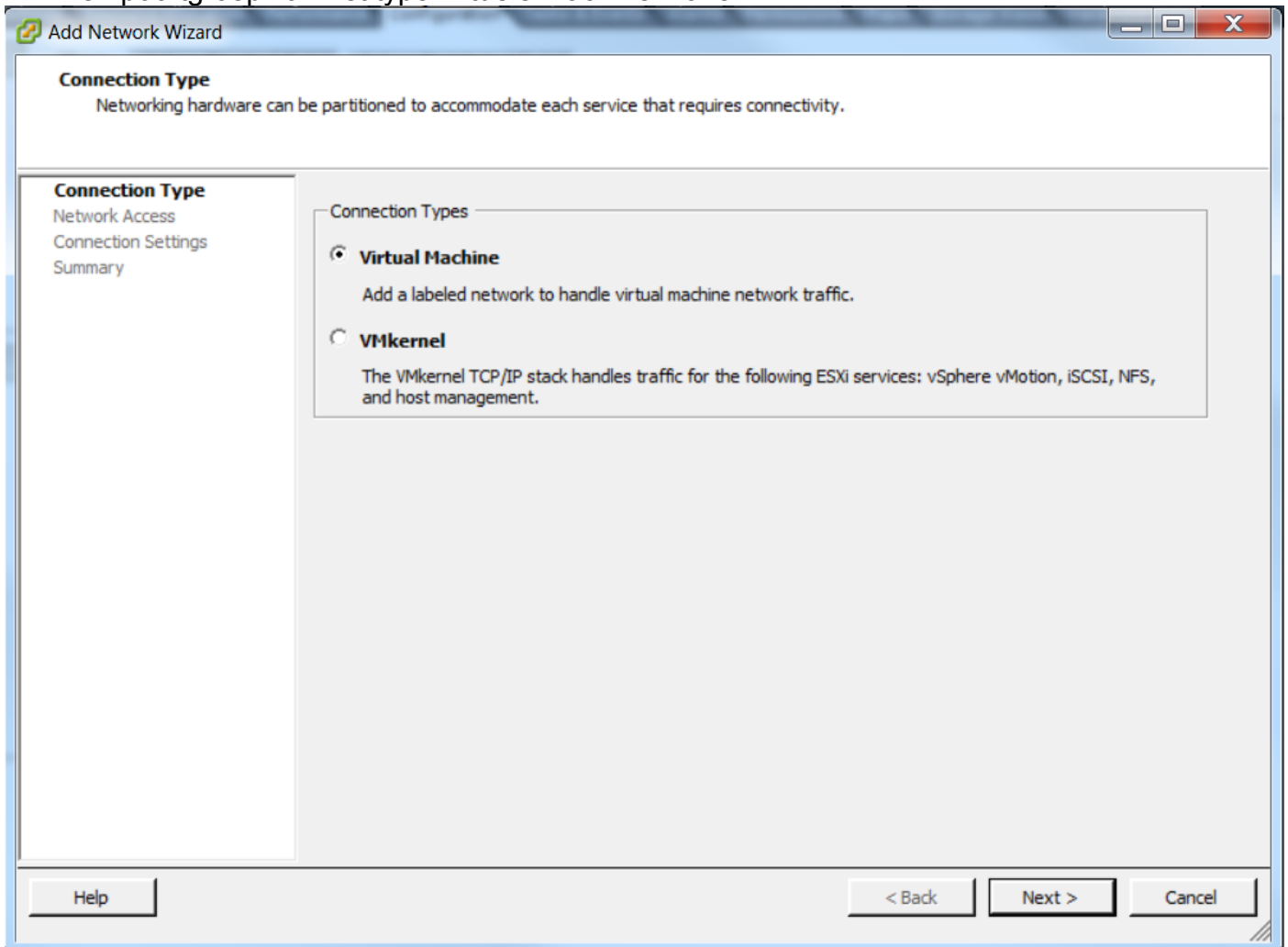
1. Maak een poortgroep van de virtuele machine en verdeel de twee virtuele machines er aan

- Navigeer naar het tabblad **Netwerk** en klik op **Netwerken toevoegen onder het kopje vSphere**

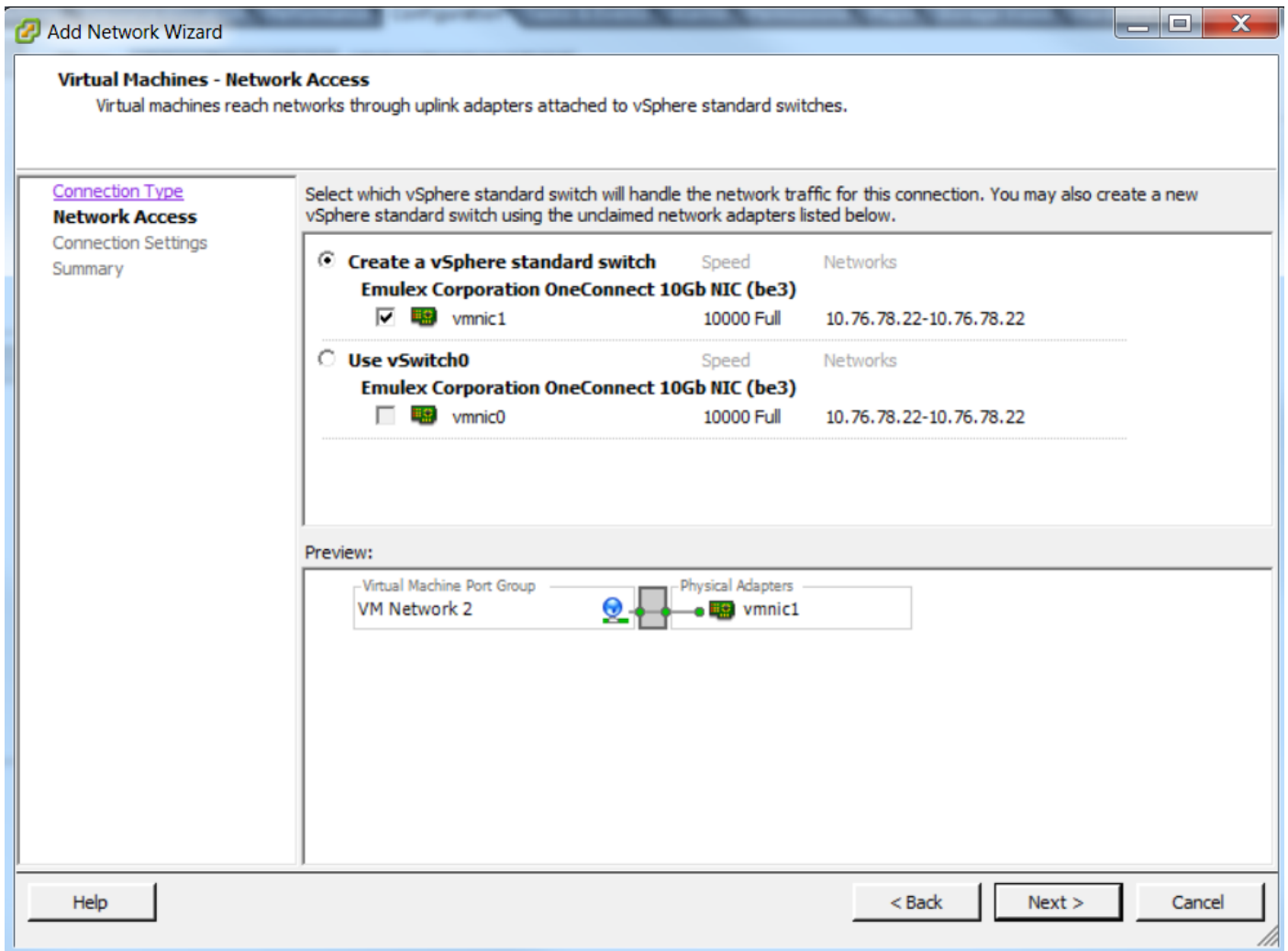
Standard Switch



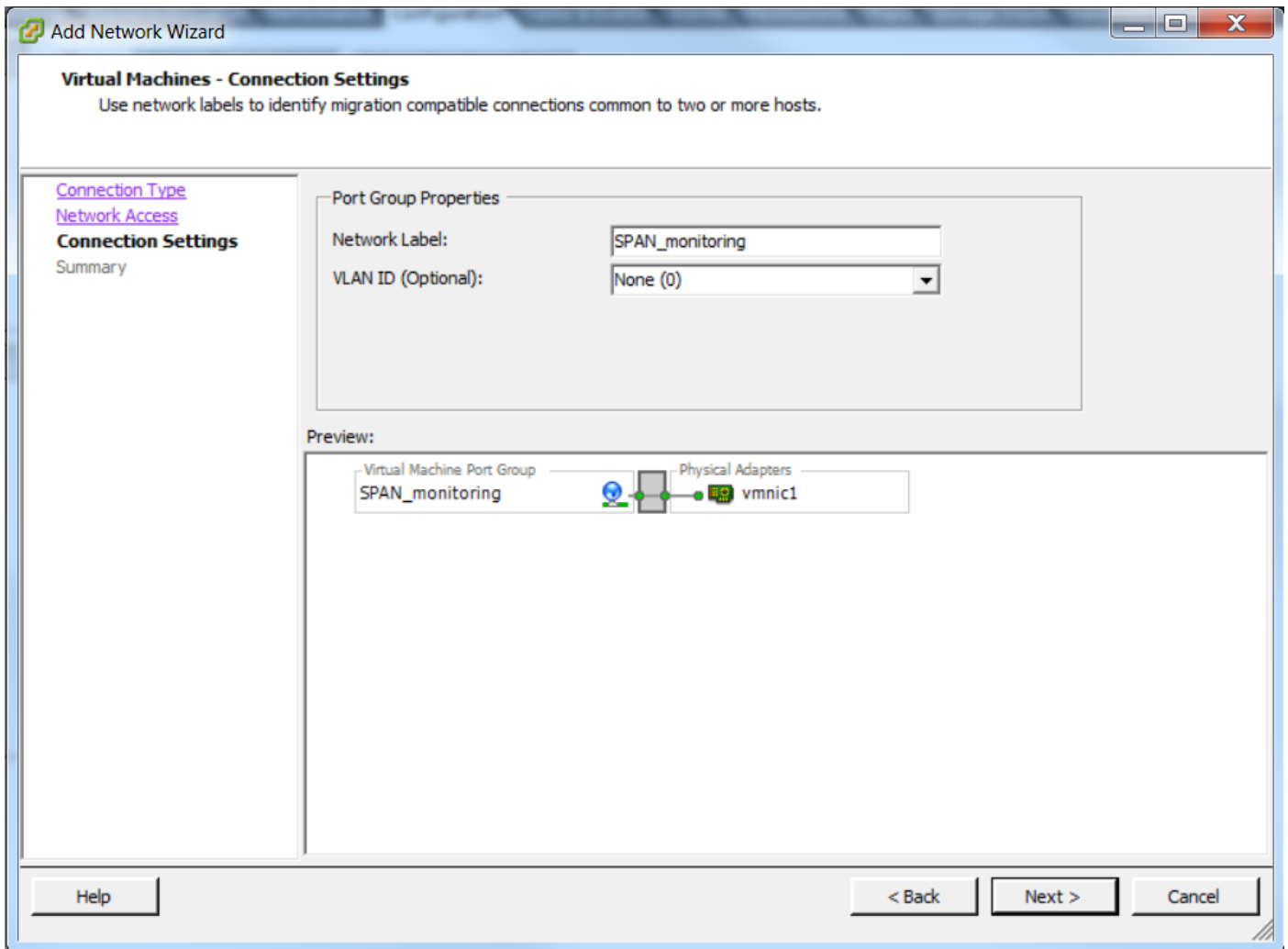
- Een poortgroep van het type virtuele machine maken



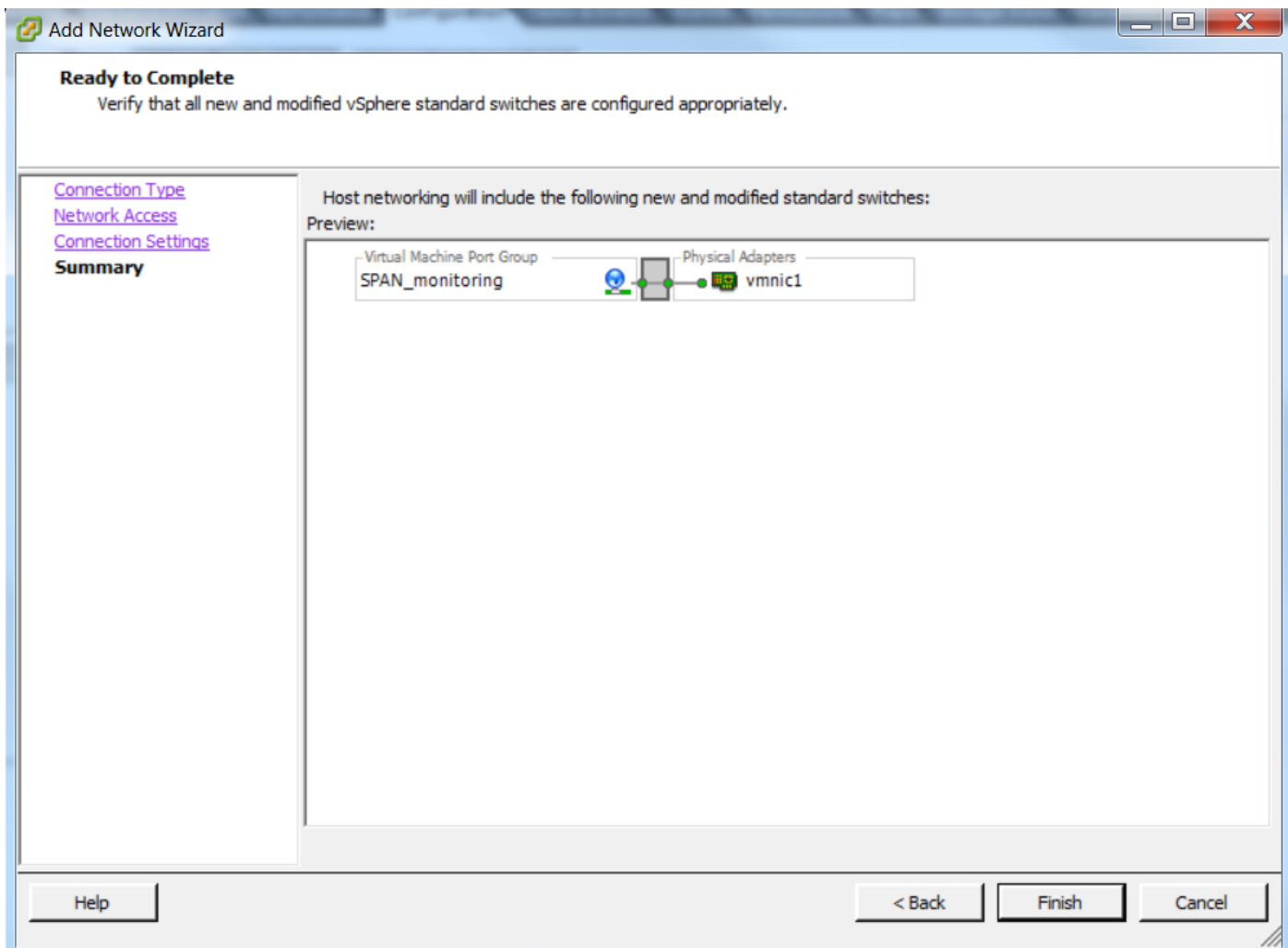
- Pas een fysieke interface (vmnic) aan de poortgroep toe zoals in deze afbeelding.



- Configureer een naam voor de poortgroep en voeg het desbetreffende VLAN toe zoals in de afbeelding.



- Controleer de configuratie en klik op **Voltoeien** zoals in de afbeelding wordt weergegeven.

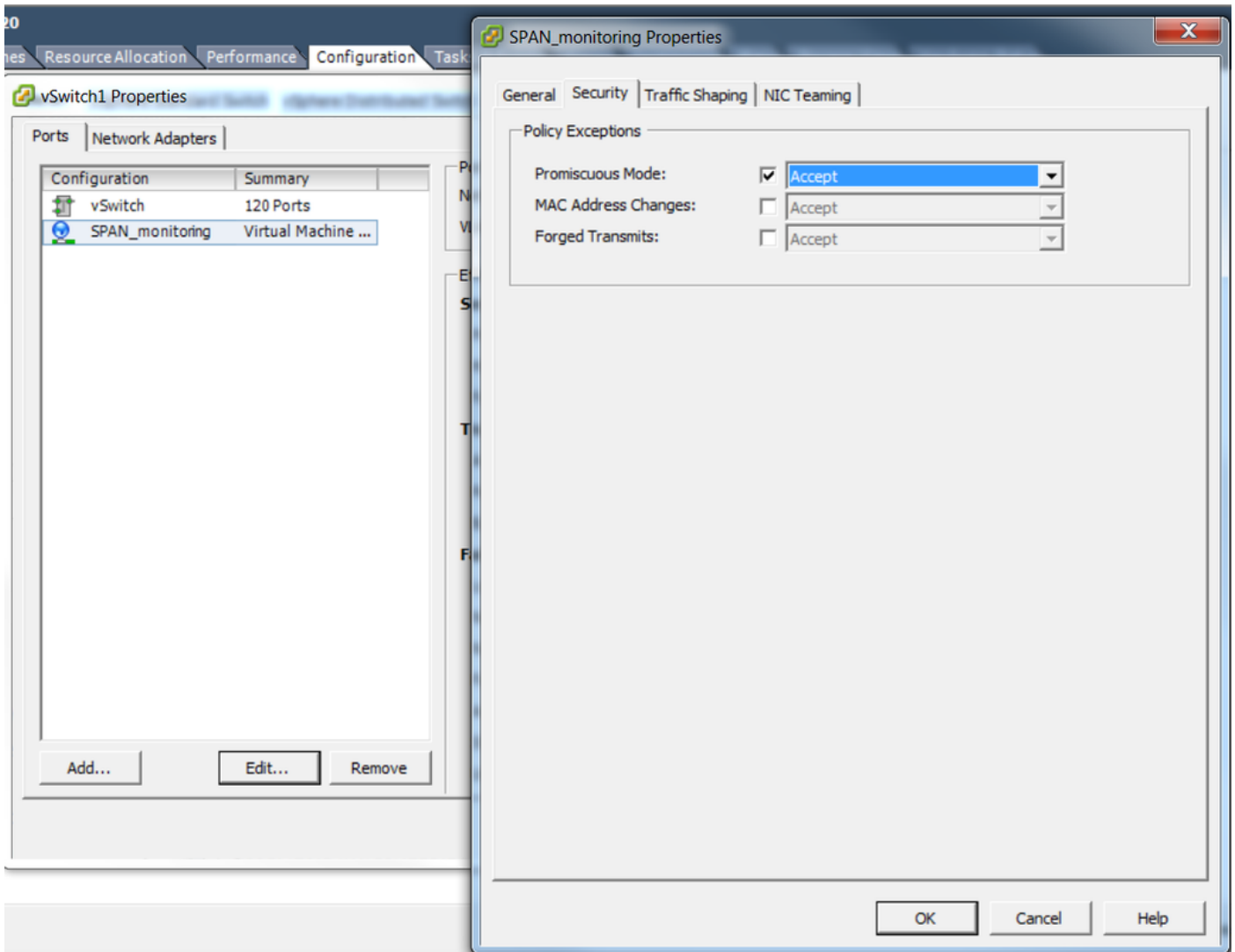


2. Configureer de poortgroep in de veelbelovende modus zoals in de afbeelding.

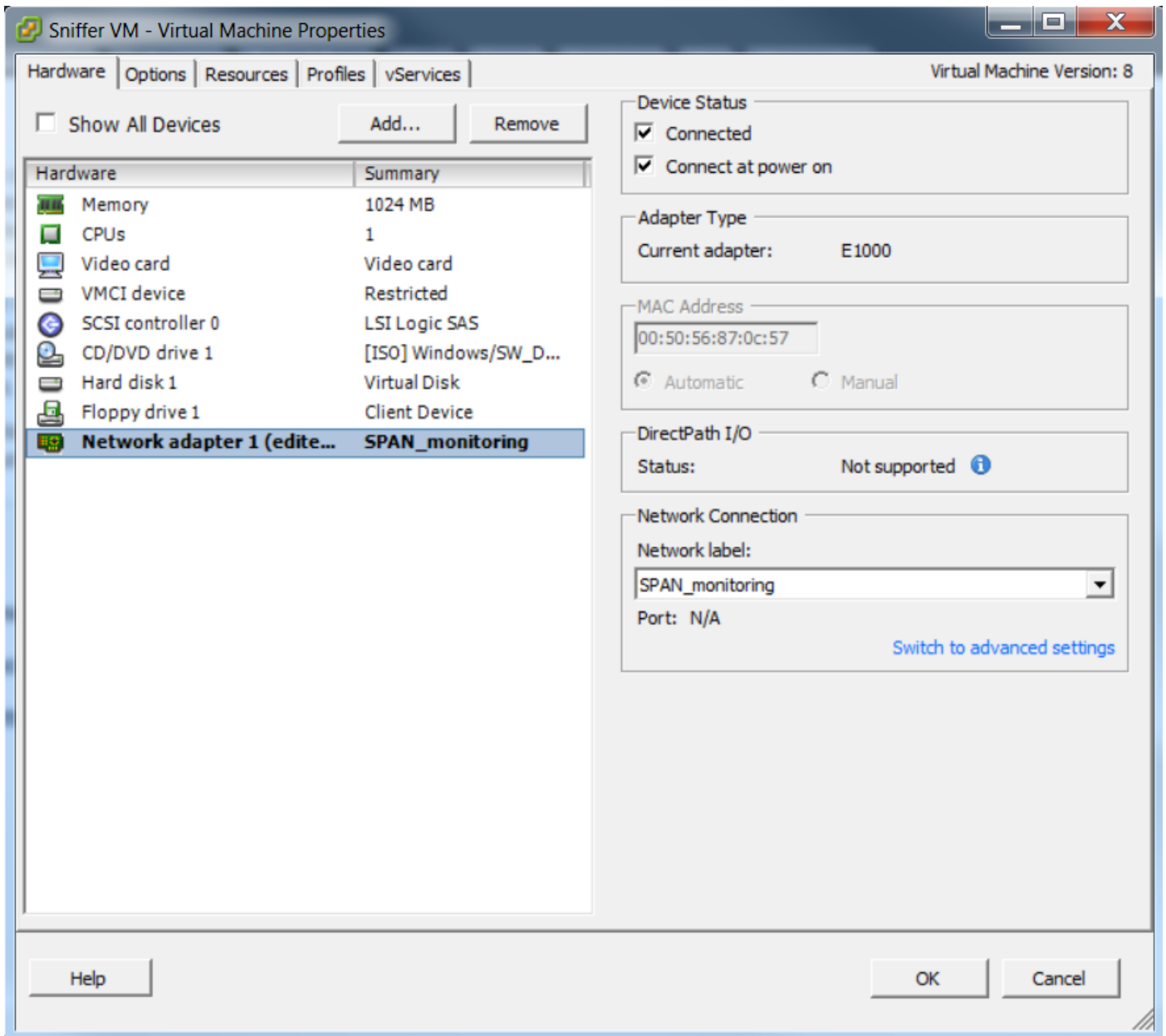
- De poortgroep moet nu onder het tabblad **Netwerk** verschijnen
- Klik op **Eigenschappen**



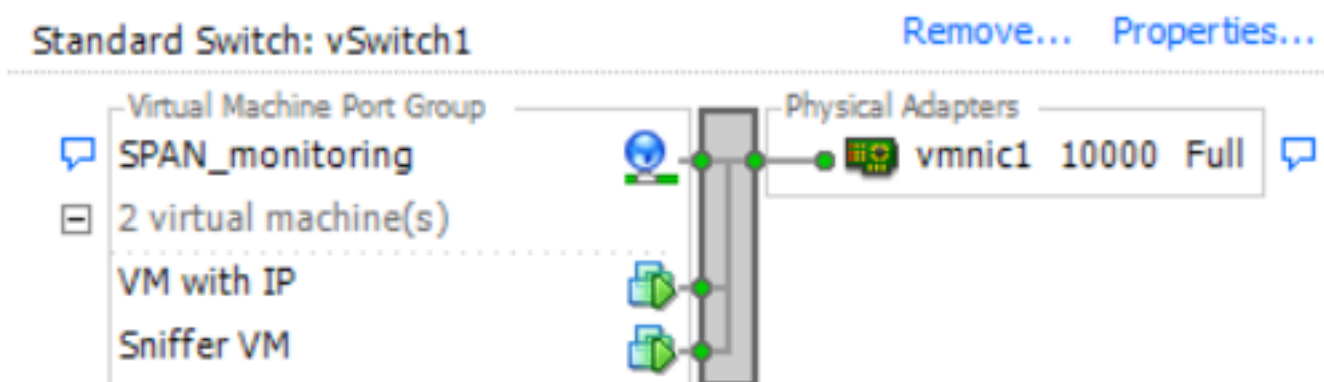
- Selecteer de poortgroep en klik op **Bewerken**
- Ga naar het tabblad **Beveiliging** en wijzig de instelling Promiscuous Mode in om te accepteren zoals in deze afbeelding wordt weergegeven



3. Pas de twee virtuele machines aan de poortgroep toe in het gedeelte virtuele machine-instellingen.



4. De twee virtuele machines moeten nu worden weergegeven in de poortgroep onder het tabblad **Netwerk**.



In dit voorbeeld is VM met IP de tweede VM met een IP-adres en Sniffer VM de VM met het snuifgereedschap zonder IP-adres.

5. Dit toont de configuratiestappen op de 6500-schakelaar:

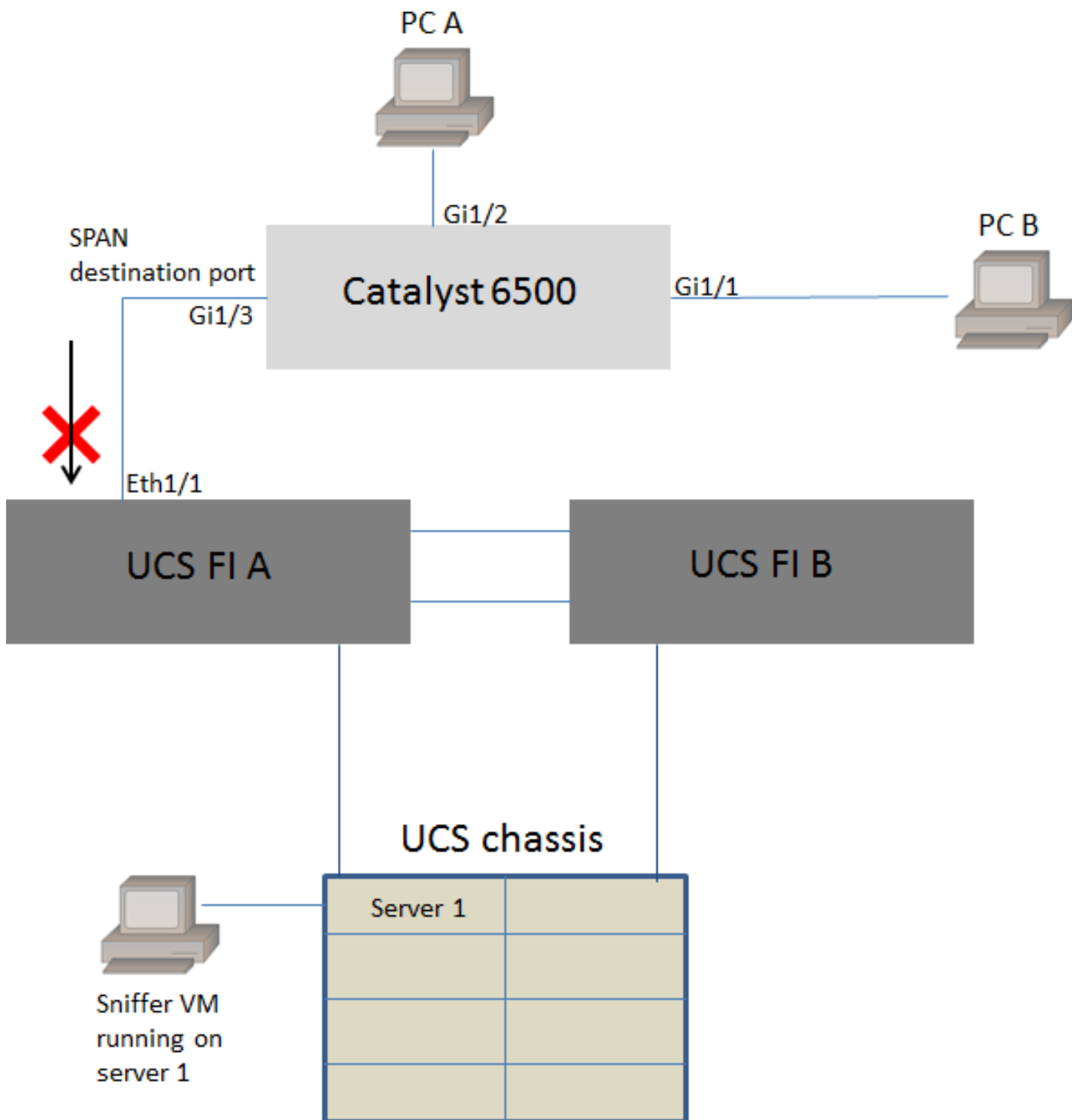
```
CAT6K-01(config)#monitor session 1 type erspan-source
CAT6K-01(config-mon-erspan-src)#source interface gi1/1
CAT6K-01(config-mon-erspan-src)#destination
CAT6K-01(config-mon-erspan-src-dst)#ip address 192.0.2.3
CAT6K-01(config-mon-erspan-src-dst)#origin ip address 192.0.2.1
CAT6K-01(config-mon-erspan-src-dst)#erspan-id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

In dit voorbeeld is het IP-adres van de tweede VM (VM met IP) 192.0.2.3.

Met deze configuratie worden de opgenomen pakketten in de 6500 ingekapseld en met het IP-adres naar de VM verzonden. Promiscuous Mode op de VMWare vSwitch stelt VM in staat om deze pakketten ook te zien.

Foutenscenario

In dit gedeelte wordt een algemeen mislukkingsscenario beschreven bij gebruik van de functie Local SPAN op een fysieke schakelaar in plaats van de functie ERSPAN. Deze topologie wordt hier bekeken:



Het verkeer van PC A naar PC B wordt gecontroleerd met behulp van de lokale SPAN optie. De bestemming van het SPAN-verkeer wordt gericht naar de poort die wordt aangesloten op UCS Fabric Interconnect (FI).

De virtuele machine met het snuffelgereedschap voert in op UCS op server 1.

Dit is de configuratie op de 6500-schakelaar:

```
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
```

Al het verkeer dat op poorten Gig1/1 en Gig1/2 stroomt, wordt ook uitgevoerd naar poort Gig1/3. De bron- en doeladressen van deze pakketten zijn onbekend aan UCS FI.

In de UCS Ethernet eindhost-modus laat de FI deze onbekende unicast-pakketten vallen.

In de UCS Ethernet switchmodus leert de FI het bron-MAC-adres op de poort die op de 6500 (Eth1/1) is aangesloten en stroomafwaarts de pakketten naar de servers stroomafwaarts. Deze opeenvolging van gebeurtenissen gebeurt:

1. Neem voor meer informatie over het verkeer dat alleen tussen PC A (met mac-adres aaa.aaa.aaa) en PC B (met mac-adres bbb.bbb.bb) gaat op interfaces Gig1/1 en Gig1/2
2. Het eerste pakket bestaat van PC A tot PC B en dit wordt gezien op UCS FI Eth1/1
3. De FI leert mac-Address Aa.aaa.aaa op Eth1/1
4. De FI weet niet wat het doeladres mac-adres bb.bbb.bb is en overstromingen het pakket naar alle poorten in hetzelfde VLAN
5. Knipper VM, in hetzelfde VLAN, ziet ook dit pakket
6. Het volgende pakket is van PC B naar PC A
7. Wanneer dit Eth1/1 raakt, wordt het mac-adres bbb.bbb.bb geleerd op Eth1/1
8. De bestemming van het pakket is voor mac-adres aaa.aaa.aaa
9. De FI laat dit pakket vallen omdat mac-adres aaa.aaa.aaa wordt geleerd op ETT1/1 en het pakket is ontvangen op Eth1/1 zelf
10. Volgende pakketten, die bestemd zijn voor mac-adres aaa.aaa.aaa of mac-adres bbb.bbb.bb, worden om dezelfde reden verwijderd

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- [De veelbelovende modus op een virtuele switch of poortgroep configureren](#)
- [SPAN, RSPAN en ERSPAN op Catalyst 6500](#)
- [Decapsatie ERSPAN-verkeer met open brontools](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)