Configurar a máquina virtual no servidor blade UCS como destino de SPAN

Contents

Introduction

Este documento descreve as etapas para capturar um fluxo de tráfego que está completamente fora do Cisco Unified Computing System (UCS) e direcioná-lo para uma máquina virtual (VM) executando uma ferramenta de farejador dentro do UCS. A origem e o destino do tráfego capturado estão fora do UCS. A captura pode ser iniciada em um switch físico diretamente conectado ao UCS ou pode estar a alguns saltos de distância.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- UCS
- VMware ESX versão 4.1 ou posterior
- Analisador de Porta de Switch Remoto Encapsulado (ERSPAN - Encapsulated Remote Switch Port Analyzer)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Catalyst 6503 executando 12.2(18)ZYA3c
- Cisco UCS B Series executando 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.

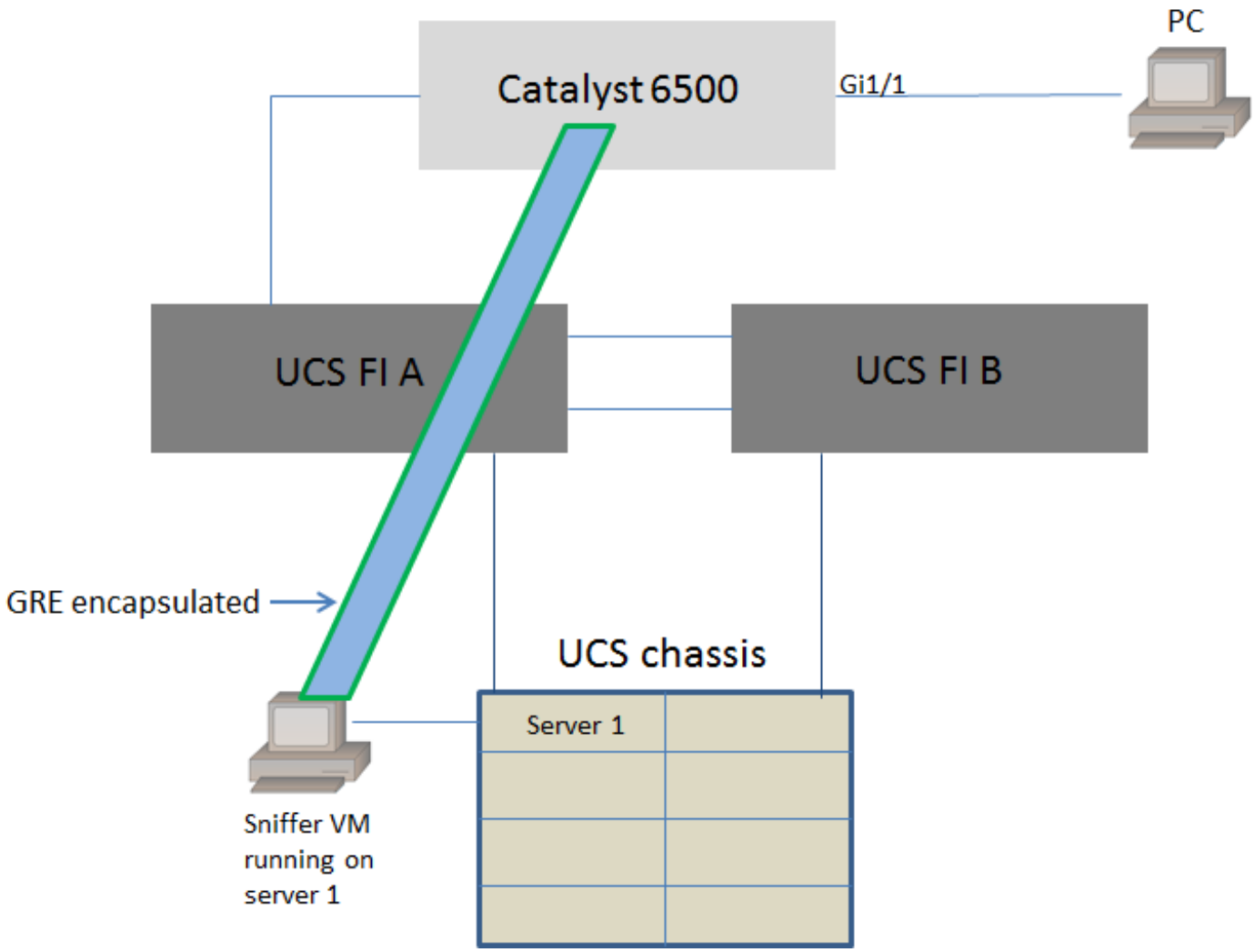
Informações de Apoio

O UCS não tem o recurso RSPAN (Remote SPAN, SPAN remoto) para receber tráfego de SPAN de um switch conectado e direcioná-lo para uma porta local. Assim, a única maneira de fazer isso em um ambiente UCS é usando o recurso RSPAN (ERSPAN) encapsulado em um switch físico e enviando o tráfego capturado para a VM usando IP. Em determinadas implementações, a VM que está executando a ferramenta sniffer não pode ter um endereço IP. Este documento explica a configuração necessária quando a VM do sniffer tem um endereço IP, bem como o cenário sem um endereço IP. A única limitação aqui é que a VM do sniffer precisa ser capaz de ler o encapsulamento GRE/ERSPAN do tráfego enviado para ela.

Configurar

Diagrama de Rede

Esta topologia foi considerada neste documento:



O PC conectado a GigabitEthernet1/1 do Catalyst 6500 está sendo monitorado. O tráfego em GigabitEthernet1/1 é capturado e enviado para o sniffer VM executado dentro do Cisco UCS no servidor 1. O recurso ERSPAN no switch 6500 captura o tráfego, encapsula-o usando GRE e o envia ao endereço IP do sniffer VM.

Sniffer VM com endereço IP

> **Note**: As etapas descritas nesta seção também podem ser usadas no cenário em que o sniffer é executado em um servidor bare-metal em um blade UCS em vez de ser executado em uma VM.

Estas etapas são necessárias quando a VM do sniffer pode ter um endereço IP:

- Configure a VM do sniffer dentro do ambiente UCS com um endereço IP acessível do 6500
- Execute a ferramenta de farejador dentro da VM
- Configure uma sessão de origem de ERSPAN no 6500 e envie o tráfego capturado diretamente para o endereço IP da VM

As etapas de configuração no switch 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
```

Neste exemplo, o endereço IP da VM do sniffer é 192.0.2.2

Sniffer VM sem endereço IP

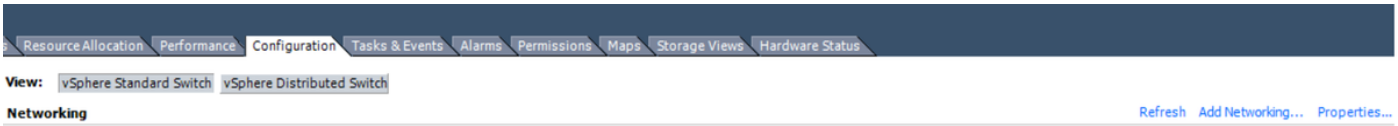
Estas etapas são necessárias quando a VM do sniffer não pode ter um endereço IP:

- Configurar a VM do sniffer no ambiente UCS
- Execute a ferramenta de farejador dentro da VM
- Crie uma segunda VM que possa ter um endereço IP no mesmo host e configure-a com um endereço IP alcançável do 6500
- Configure o grupo de portas no VMWare vSwitch para estar no modo promíscuo
- Configure uma sessão de origem de ERSPAN no 6500 e envie o tráfego capturado para o endereço IP da segunda VM

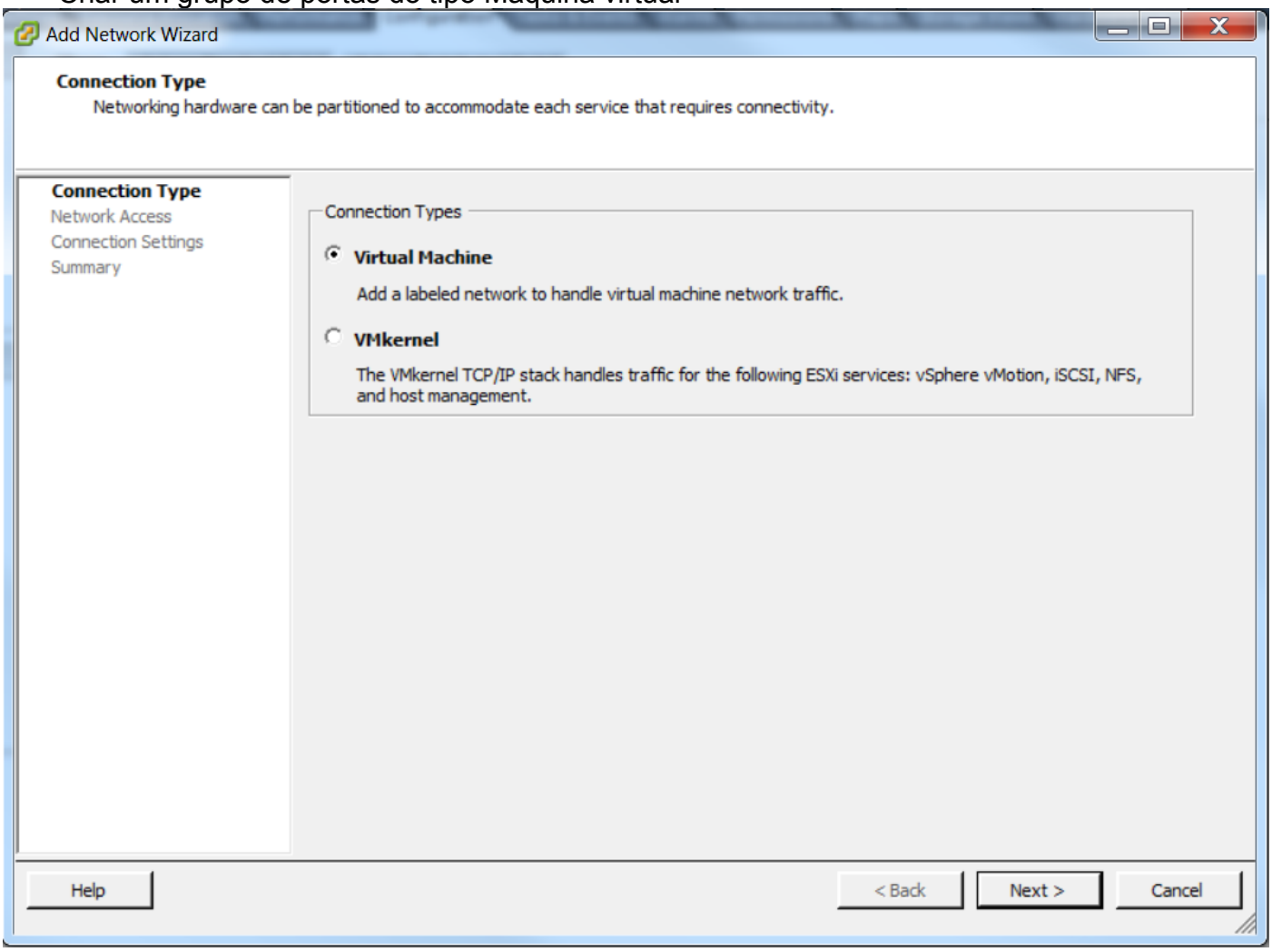
Estas etapas mostram a configuração necessária no VMWare ESX: Vá diretamente para a Etapa 2 se já tiver um grupo de portas configurado.

1. Crie um grupo de portas de máquina virtual e atribua as duas máquinas virtuais a ele

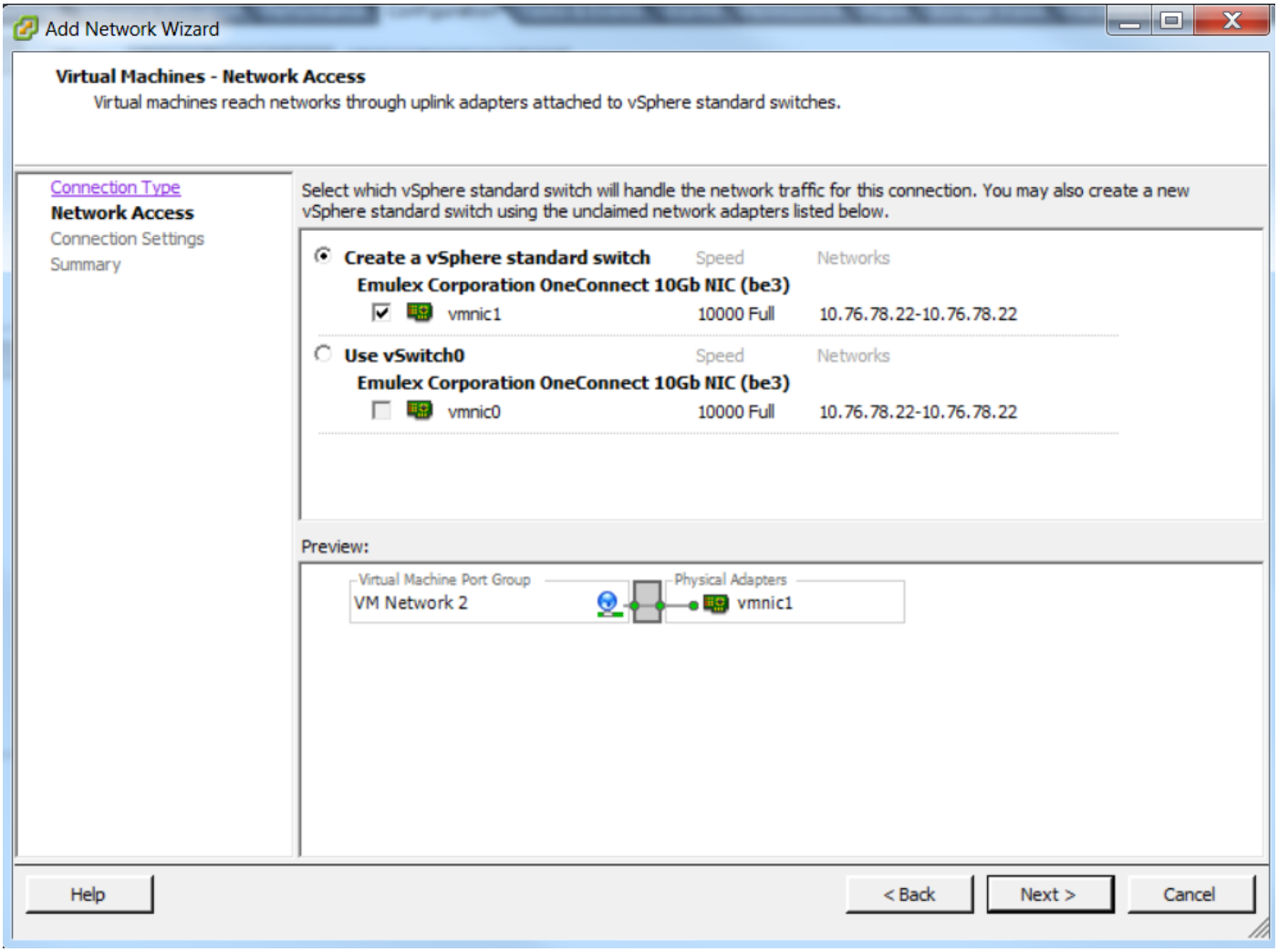
- Navegue até a guia **Rede** e clique em **Adicionar rede em Switch padrão vSphere**



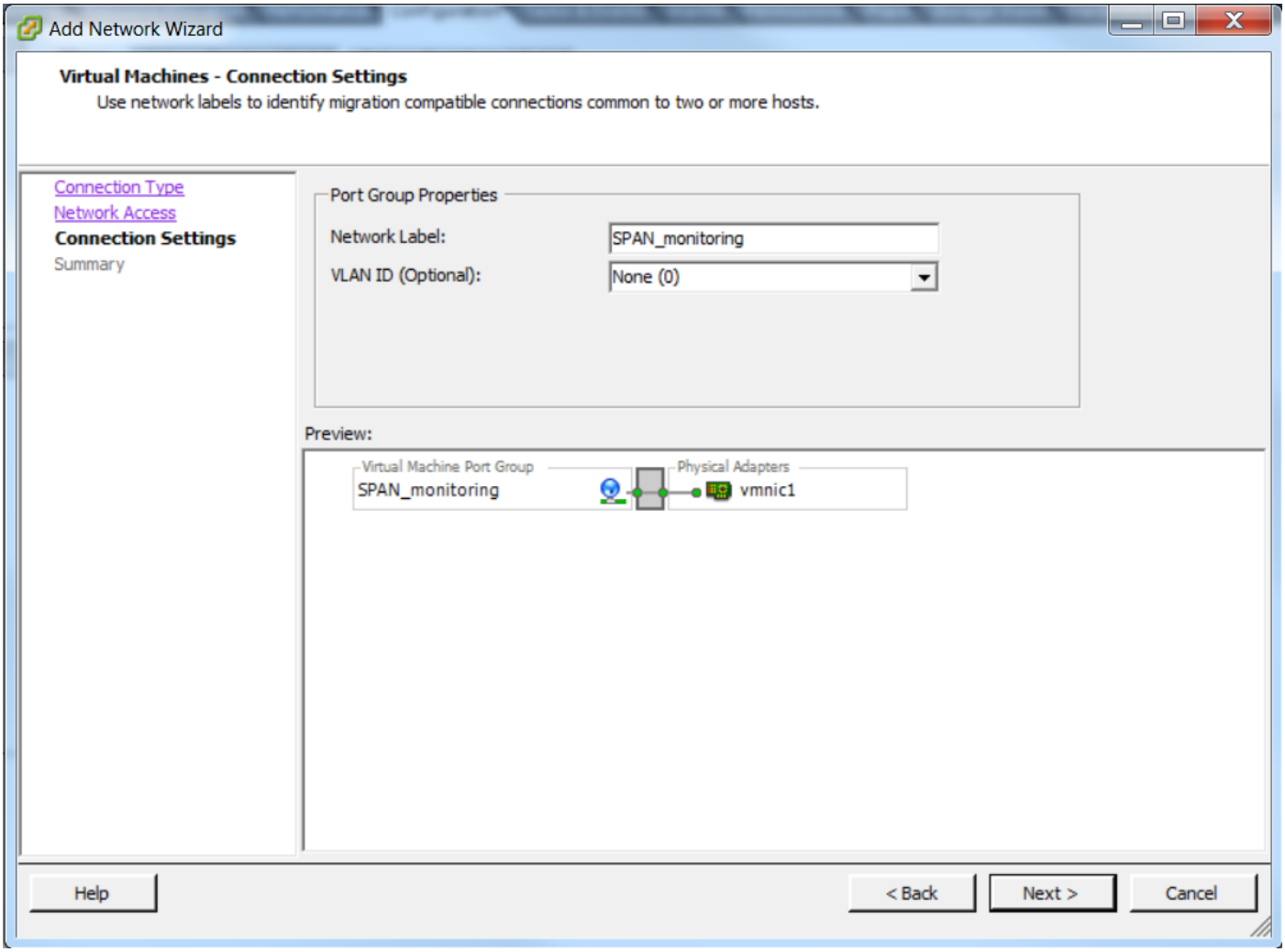
- Criar um grupo de portas do tipo Máquina virtual



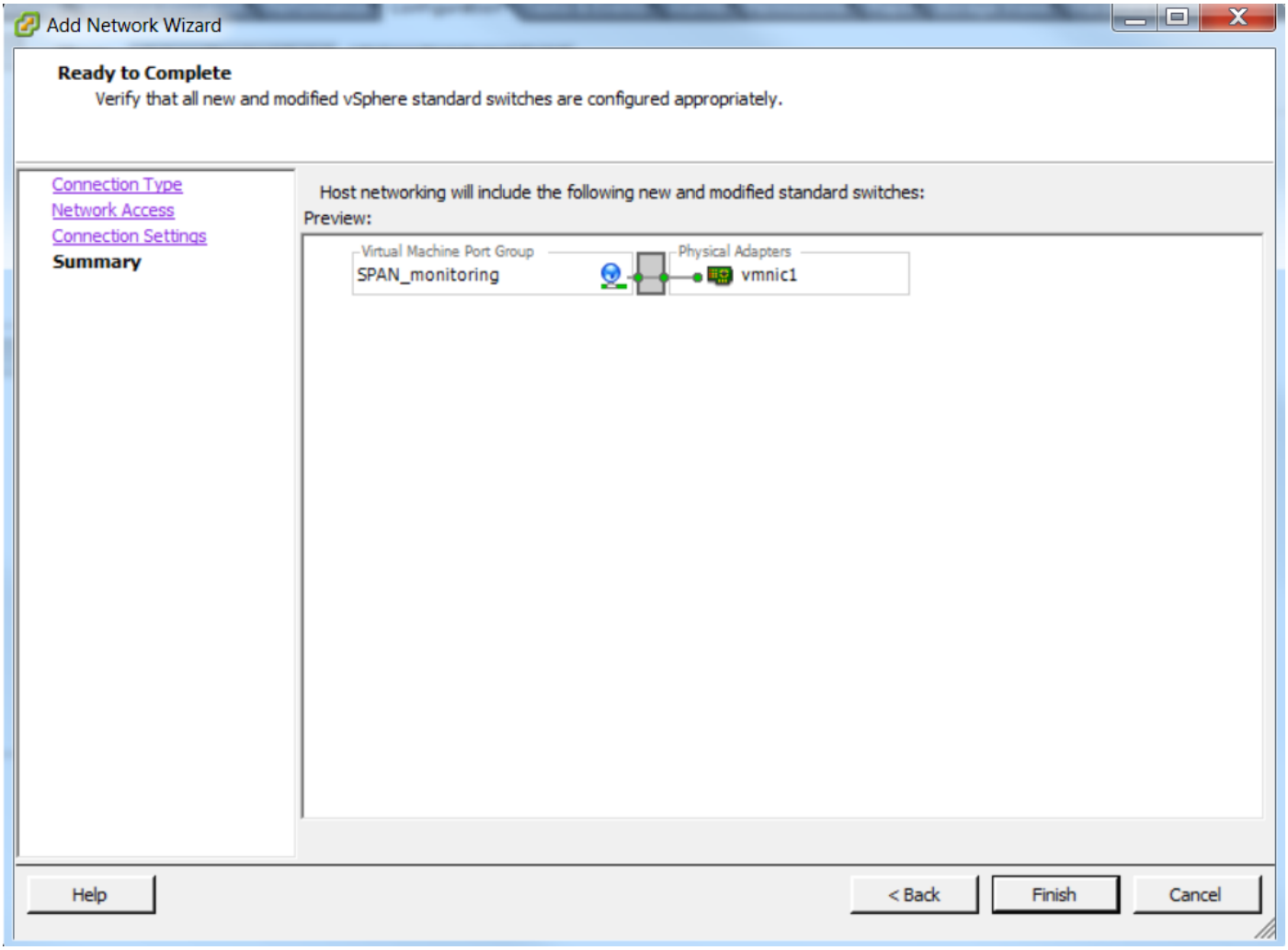
- Atribua uma interface física (vmnic) ao grupo de portas como mostrado nesta imagem.



- Configure um nome para o grupo de portas e adicione a VLAN relevante conforme mostrado na imagem.



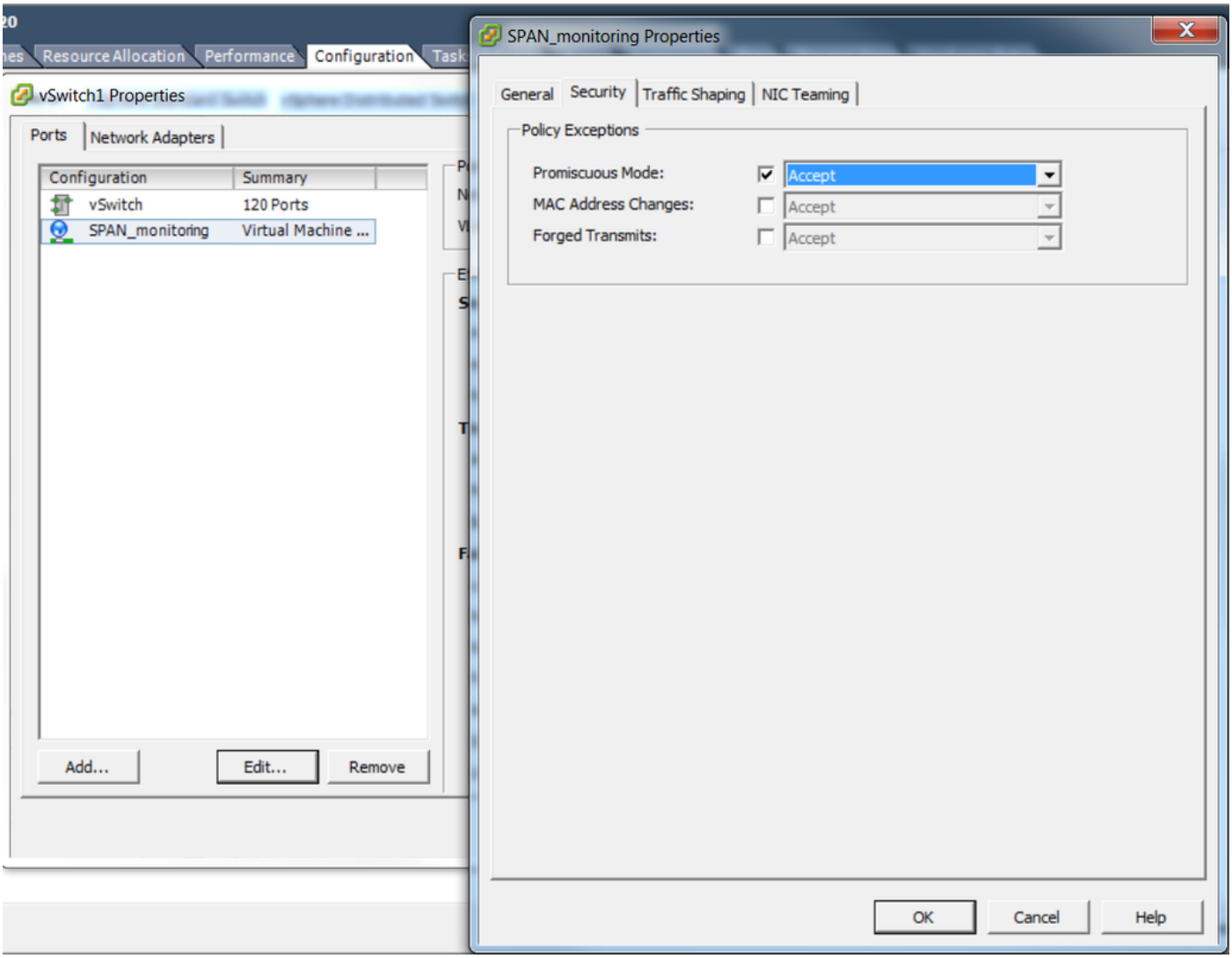
- Verifique a configuração e clique em **Concluir** como mostrado na imagem.



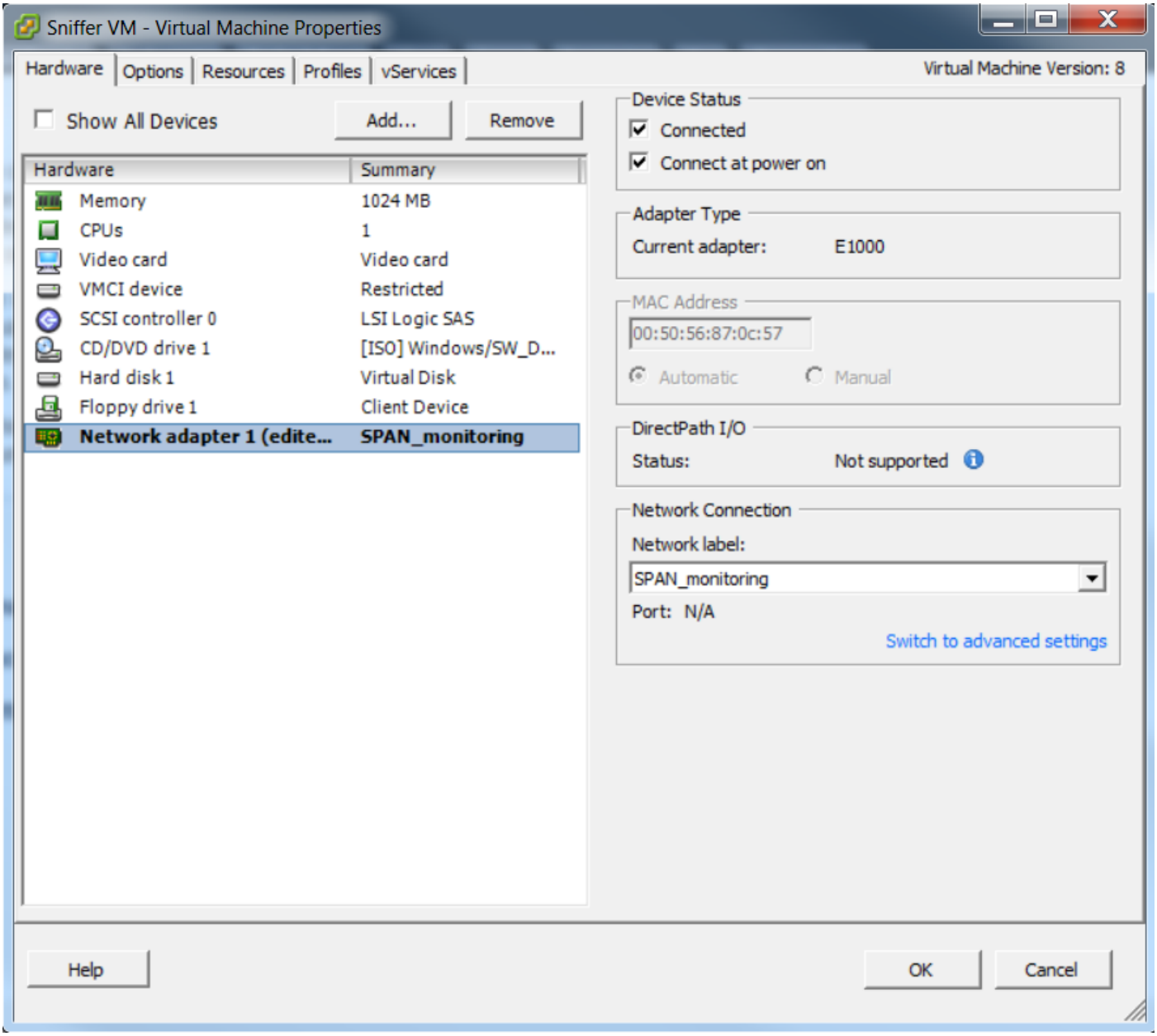
2. Configure o grupo de portas para estar no modo promíscuo como mostrado na imagem.

- O grupo de portas deve aparecer na guia **Networking (Rede)** agora
- Clique em Propriedades

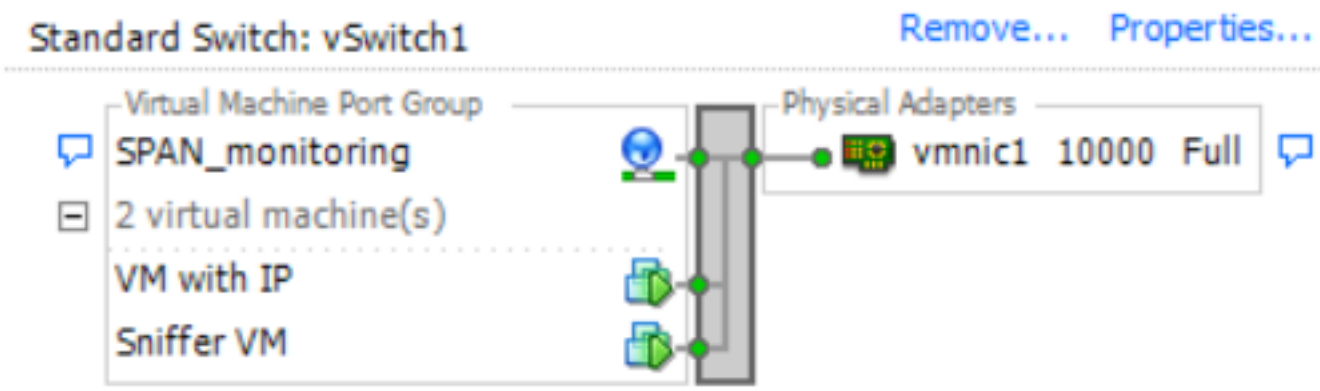
- Selecione o grupo de portas e clique em **Editar**
- Vá até a guia **Segurança** e altere a configuração do modo Promiscuous para Accept (Aceitar), conforme mostrado nesta imagem



3. Atribua as duas máquinas virtuais ao grupo de portas na seção de configurações da máquina virtual.



4. As duas máquinas virtuais devem aparecer no grupo de portas na guia **Networking** agora.



Neste exemplo, VM com IP é a segunda VM que tem um endereço IP e Sniffer VM é a VM com a ferramenta sniffer sem um endereço IP.

5. Mostra as etapas de configuração no switch 6500:

```
CAT6K-01(config)#monitor session 1 type erspan-source
```

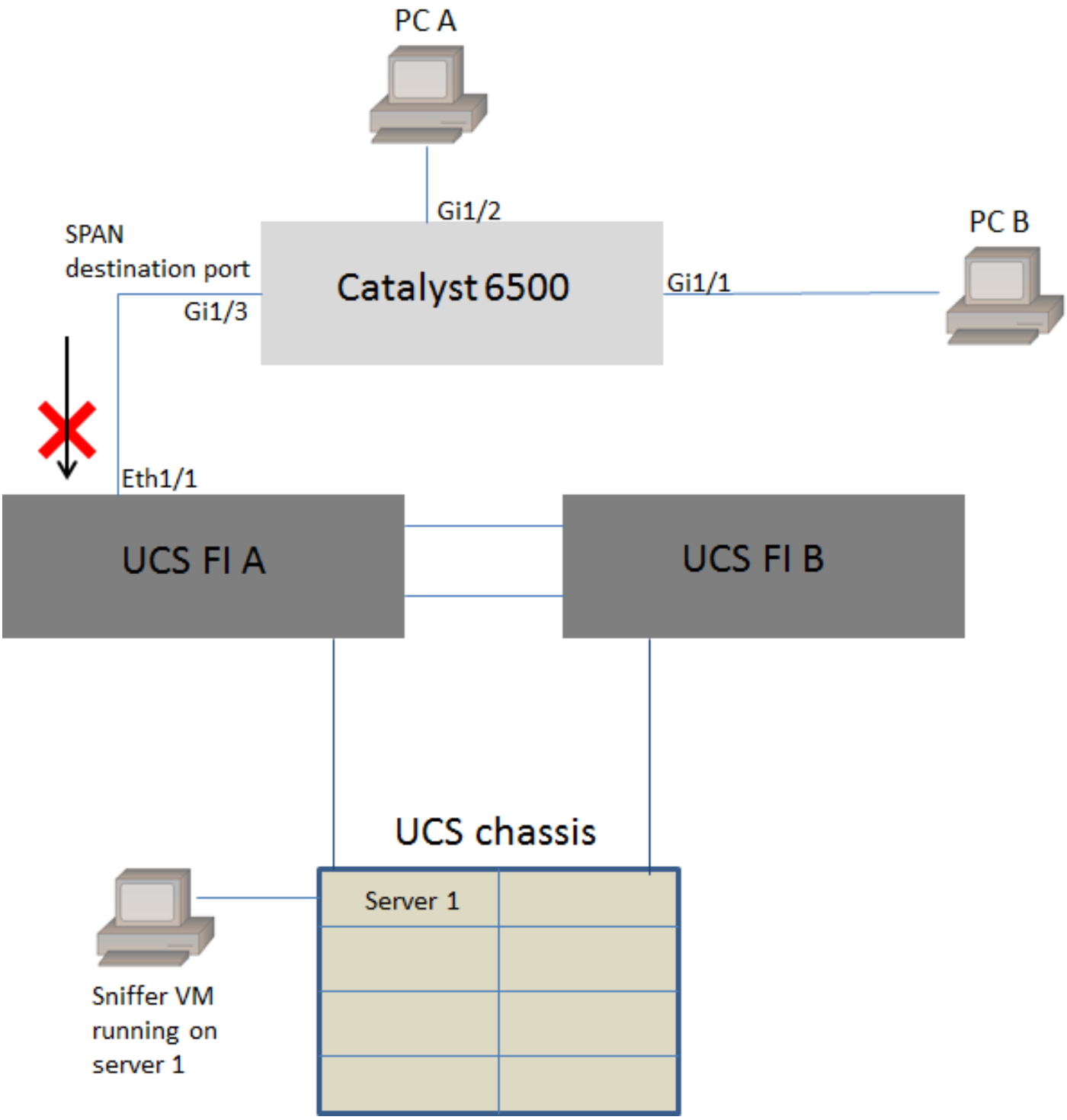
```
CAT6K-01(config-mon-erspan-src)#source interface gi1/1
CAT6K-01(config-mon-erspan-src)#destination
CAT6K-01(config-mon-erspan-src-dst)#ip address 192.0.2.3
CAT6K-01(config-mon-erspan-src-dst)#origin ip address 192.0.2.1
CAT6K-01(config-mon-erspan-src-dst)#erspan-id 1
CAT6K-01(config-mon-erspan-src-dst)#exit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

Neste exemplo, o endereço IP da segunda VM (VM com IP) é 192.0.2.3.

Com essa configuração, o 6500 encapsula os pacotes capturados e os envia para a VM com o endereço IP. O modo promíscuo no VMWare vSwitch permite que o sniffer VM veja esses pacotes também.

Cenário de falha

Esta seção descreve um cenário de falha comum ao usar o recurso SPAN local em um switch físico em vez do recurso ERSPAN. Esta topologia é considerada aqui:



O tráfego do PC A para o PC B é monitorado usando o recurso de SPAN local. O destino do tráfego de SPAN é direcionado à porta conectada ao UCS Fabric Interconnect (FI).

A máquina virtual com a ferramenta sniffer é executada dentro do UCS no servidor 1.

Esta é a configuração no switch 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
```

Todo o tráfego que flui nas portas Gig1/1 e Gig1/2 será replicado na porta Gig1/3. Os endereços mac origem e destino desses pacotes serão desconhecidos para o UCS FI.

No modo de host final Ethernet UCS, o FI descarta esses pacotes unicast desconhecidos.

No modo de comutação Ethernet UCS, o FI aprende o endereço MAC de origem na porta conectada ao 6500 (Eth1/1) e depois inunda os pacotes abaixo dos servidores. Esta sequência de eventos acontece:

1. Para facilitar a compreensão, considere o tráfego que ocorre somente entre o PC A (com mac-address aaaa.aaaa.aaaa) e o PC B (com mac-address bbbbb.bbbb.bbbb) nas interfaces Gig1/1 e Gig1/2
2. O primeiro pacote é do PC A ao PC B e isso é visto no UCS FI Eth1/1
3. O FI aprende mac-address aaaa.aaaa.aaaa em Eth1/1
4. O FI não sabe o endereço mac de destino bbbb.bbbb.bbbb e inunda o pacote para todas as portas na mesma VLAN
5. A VM sniffer, na mesma VLAN, também vê este pacote
6. O próximo pacote é do PC B ao PC A
7. Quando isso atinge Eth1/1, mac-address bbbbb.bbbb.bbbb é aprendido em Eth1/1
8. O destino do pacote é mac-address aaaa.aaaa.aaaa
9. O FI descarta esse pacote como mac-address aaaa.aaaa.aaaa é aprendido em Eth1/1 e o pacote foi recebido no próprio Eth1/1
10. Pacotes subsequentes destinados a mac-address aaaa.aaaa.aaaa ou mac-address bbbbb.bbbb.bbbb são descartados pelo mesmo motivo

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Configuração do modo promíscuo em um switch virtual ou grupo de portas
- SPAN, RSPAN e ERSPAN no Catalyst 6500
- Desencapsulamento do tráfego ERSPAN com ferramentas de código aberto
- Suporte Técnico e Documentação - Cisco Systems