Configurar uma máquina virtual em um server da lâmina UCS como o destino do PERÍODO

Índice

Introdução

Este documento descreve as etapas para capturar um fluxo de tráfego que seja completamente fora do Cisco Unified Computing System (UCS) e para dirigi-lo a uma máquina virtual (VM) que executa uma ferramenta do sniffer dentro do UCS.

A fonte e o destino do tráfego que está sendo capturado são fora do UCS. A captação pode ser iniciada em um interruptor físico que seja anexado diretamente ao UCS ou poderia ser alguns saltos afastado.

Pré-requisitos

Requisitos

Cisco recomenda que você tem um conhecimento em funcionamento destes assuntos:

- Cisco Unified Computing System (UCS)
- Versão 4.1 ou mais recente de VMware ESX
- Analisador de porta encapsulado do switch remoto (ERSPAN)

Componentes Utilizados

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

- Cisco catalyst 6503 12.2(18)ZYA3c sendo executado
- Corredor da série de Cisco UCS B 2.2(3e)
- Construção 1331820 de VMware ESXi 5.5

Informações de Apoio

O UCS não tem a característica do Remote SPAN (RSPAN) para receber o tráfego do PERÍODO de um switch conectado e para dirigi-lo a uma porta local. Assim a única maneira de realizar isto em um ambiente UCS é usando a característica encapsulada RSPAN (ERSPAN) em um interruptor físico e enviando o tráfego capturado ao VM usando o IP.

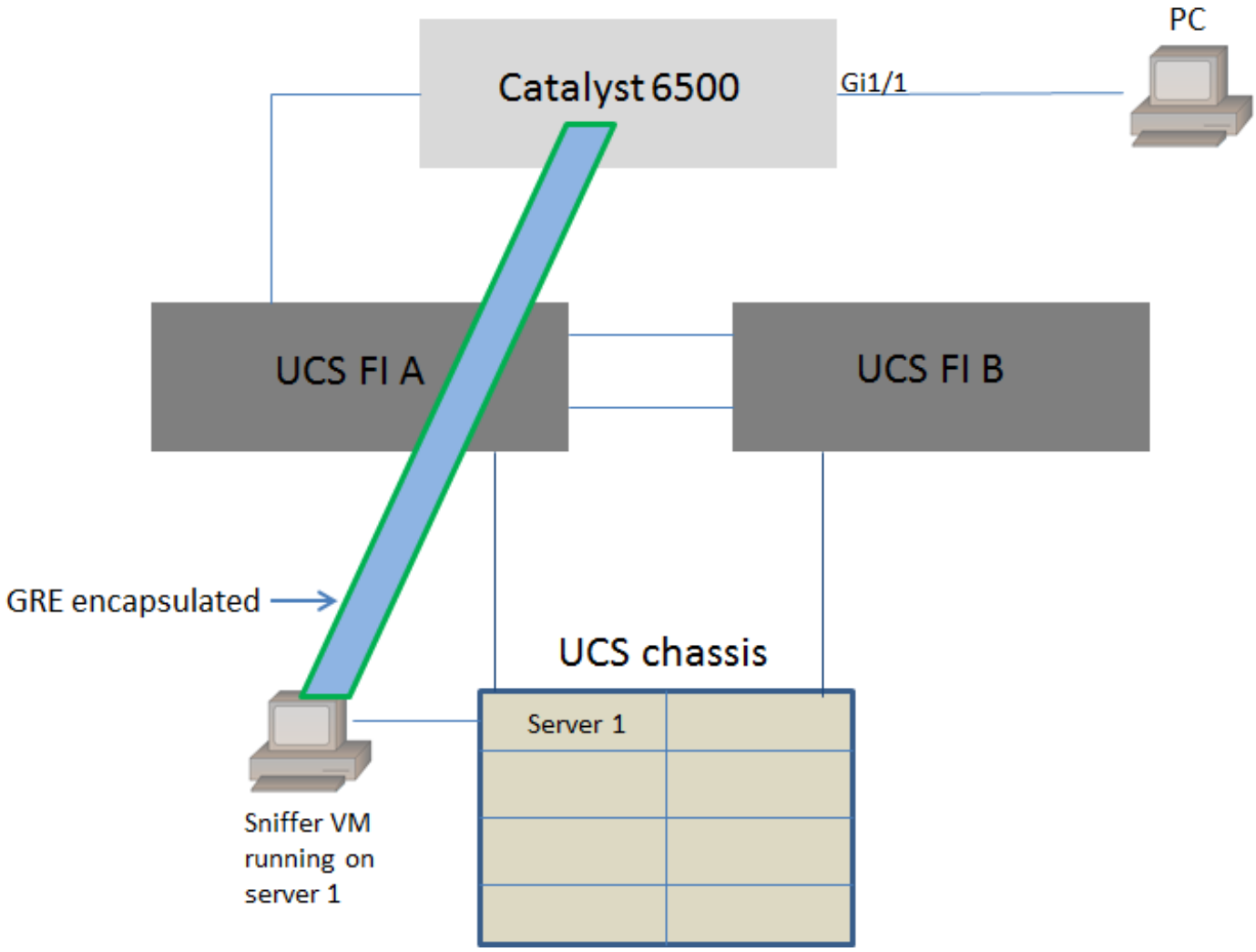
Em determinadas aplicações, o VM que executa a ferramenta do sniffer não pode ter um endereço IP de Um ou Mais Servidores Cisco ICM NT. Este documento explica a configuração exigida quando o sniffer VM tem um endereço IP de Um ou Mais Servidores Cisco ICM NT assim como a encenação sem um endereço IP de Um ou Mais Servidores Cisco ICM NT. A limitação do onl aqui é que o sniffer VM precisa de poder ler o encapsulamento GRE/ERSPAN do tráfego que lhe é enviado.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede

Esta topologia foi considerada neste documento:



O PC anexado a GigabitEthernet1/1 do Catalyst 6500 está sendo monitorado. O tráfego em GigabitEthernet1/1 é capturado e enviado ao sniffer VM que é executado dentro de Cisco UCS no servidor1.

A característica ERSPAN no 6500 Switch captura o tráfego, encapsular-lo que usa o GRE e envia-o ao endereço IP de Um ou Mais Servidores Cisco ICM NT do sniffer o VM.

Configurações

Sniffer VM com um endereço IP de Um ou Mais Servidores Cisco ICM NT

> Nota: As etapas descritas nesta seção podem igualmente ser usadas na encenação aonde o sniffer é executado em um server do desencapado-metal em uma lâmina UCS em vez de ser executado em um VM.

Estas etapas são exigidas quando o sniffer VM pode ter um endereço IP de Um ou Mais Servidores Cisco ICM NT:

- Configurar o sniffer VM dentro do ambiente UCS com um endereço IP de Um ou Mais Servidores Cisco ICM NT que seja alcançável dos 6500
- Execute a ferramenta do sniffer dentro do VM

- Configurar uma sessão da fonte ERSPAN nos 6500 e envie o tráfego capturado diretamente ao endereço IP de Um ou Mais Servidores Cisco ICM NT do VM

As etapas de configuração no 6500 Switch:

```
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 de Um ou Mais Servidores Cisco ICM NT do sniffer VM é 192.0.2.2

Sniffer VM sem um endereço IP de Um ou Mais Servidores Cisco ICM NT

Estas etapas são exigidas quando o sniffer VM não pode ter um endereço IP de Um ou Mais Servidores Cisco ICM NT:

- Configurar o sniffer VM dentro do ambiente UCS
- Execute a ferramenta do sniffer dentro do VM
- Crie um segundo VM que possa ter um endereço IP de Um ou Mais Servidores Cisco ICM NT no mesmo host e o configurar com um endereço IP de Um ou Mais Servidores Cisco ICM NT que seja alcançável dos 6500
- Configurar o grupo de porta no vSwitch de VMware para reagir do modo misturado
- Configurar uma sessão da fonte ERSPAN nos 6500 e envie o tráfego capturado ao endereço IP de Um ou Mais Servidores Cisco ICM NT do segundo VM

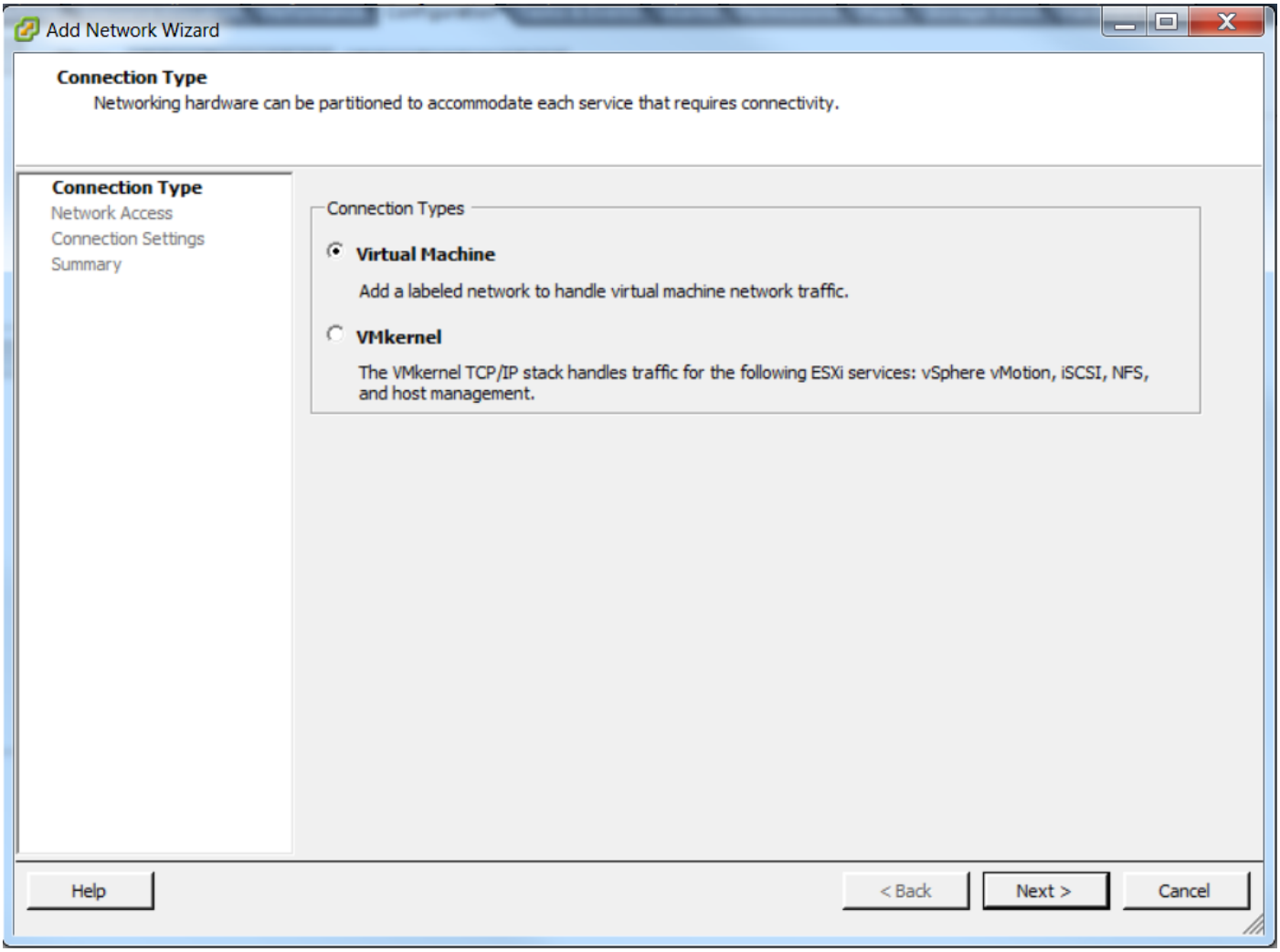
Estas etapas mostram a configuração exigida em VMware ESX:

Passe a etapa 2 diretamente se você já tem um grupo de porta configurado.

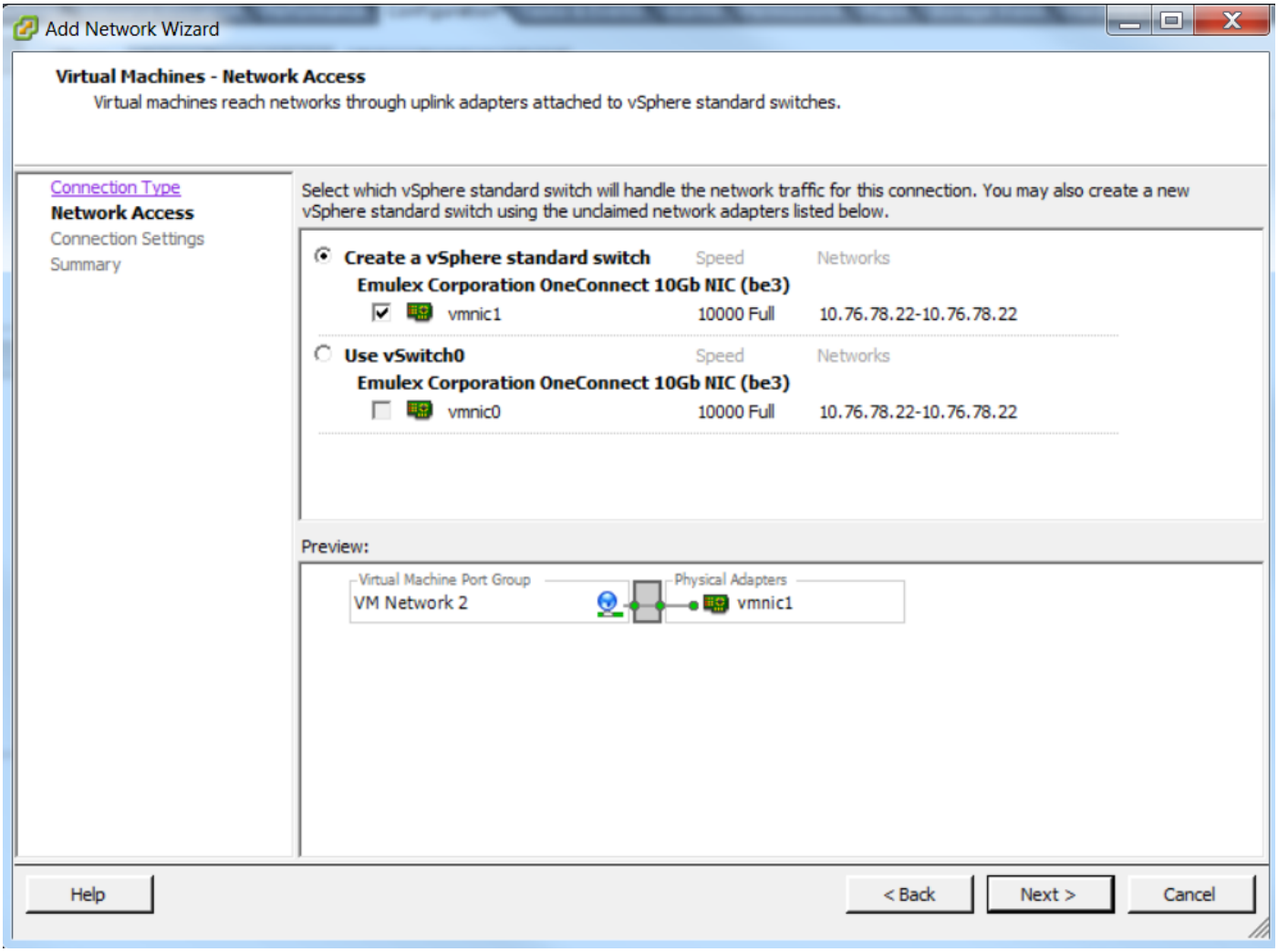
1. Crie um grupo de porta da máquina virtual e atribua-lhe as duas máquinas virtuais

- Navegue à **ABA de rede de comunicação** e o clique **adiciona trabalhos em rede sob o interruptor do padrão do vSphere**

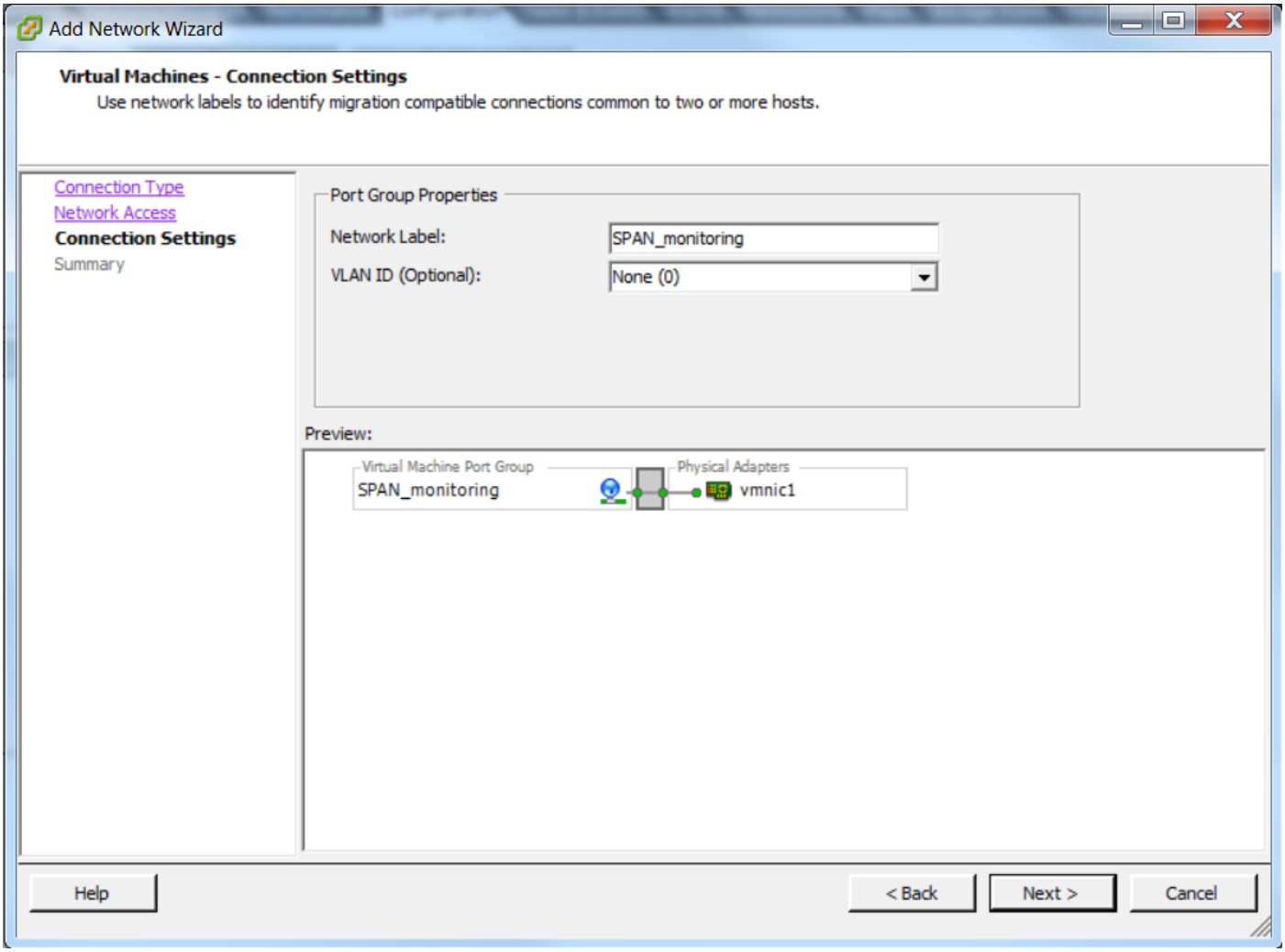
- Crie um grupo de porta de tipo máquina virtual



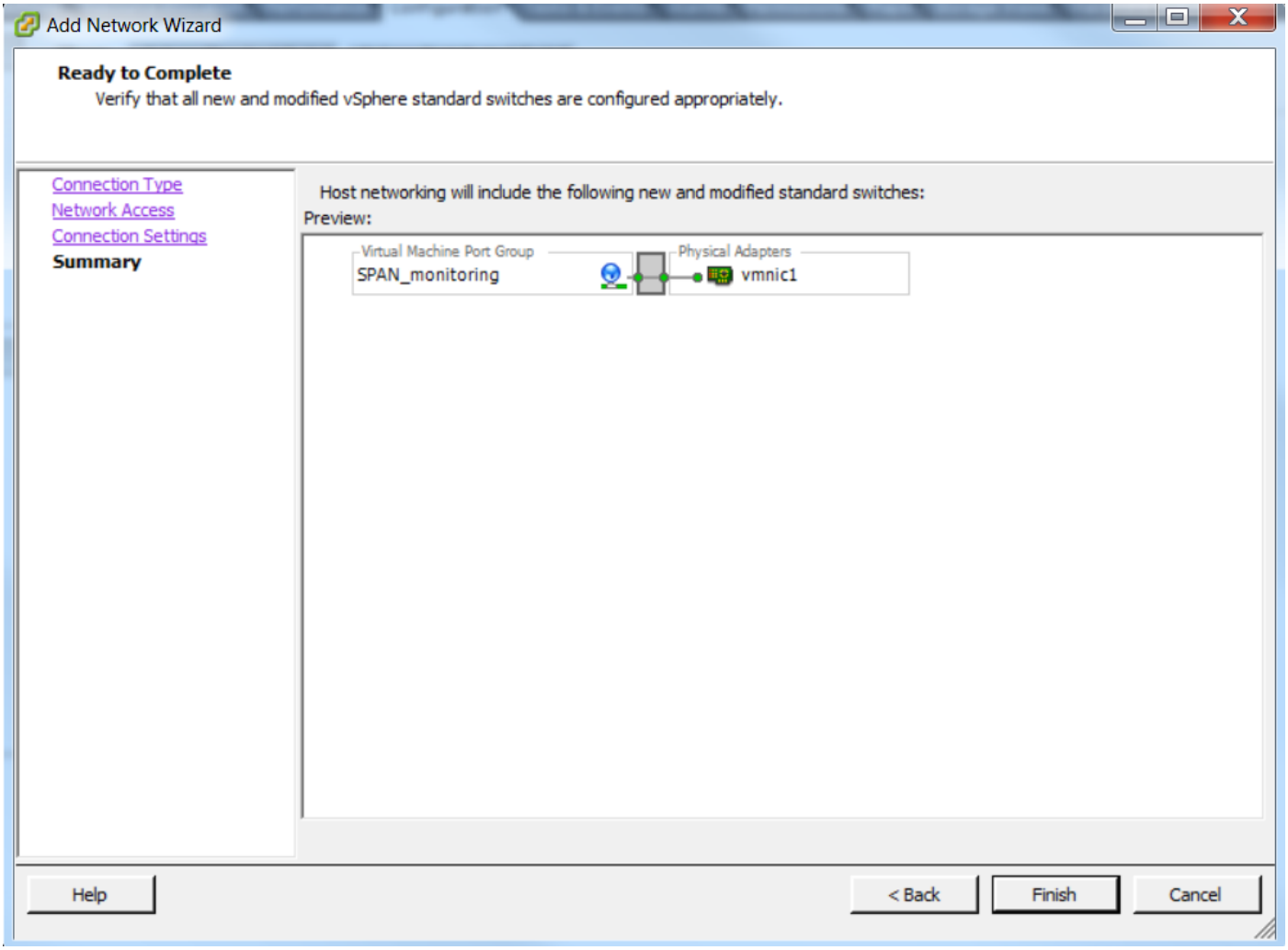
- Atribua uma interface física (vmnic) ao grupo de porta segundo as indicações desta imagem.



- Configurar um nome para o grupo de porta e adicionar o VLAN relevante



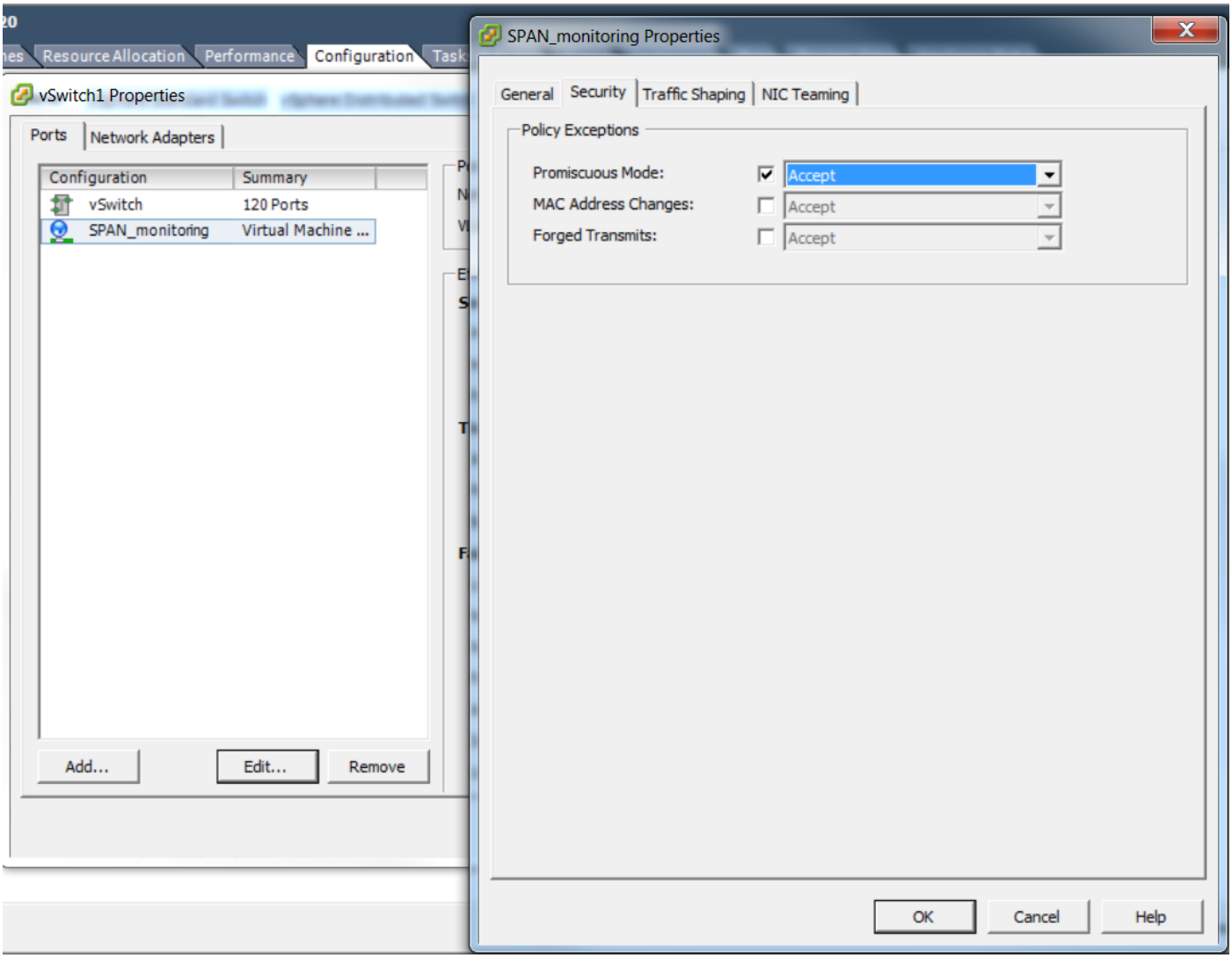
- Verifique a configuração e clique o **revestimento**



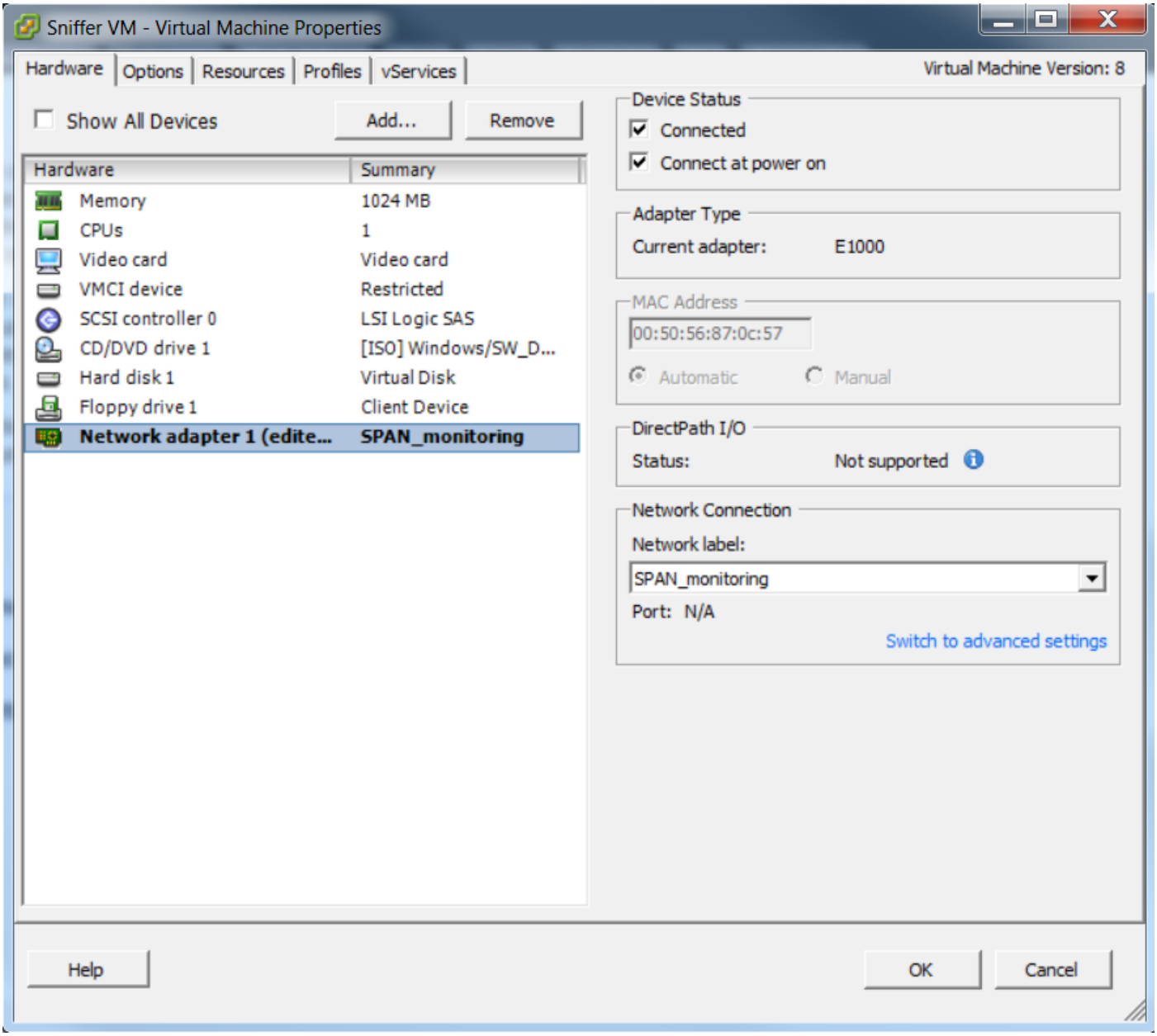
2. Configurar o grupo de porta para reagir do modo misturado.

- O grupo de porta deve aparecer sob a **ABA de rede de comunicação** agora
- **Propriedades do** clique

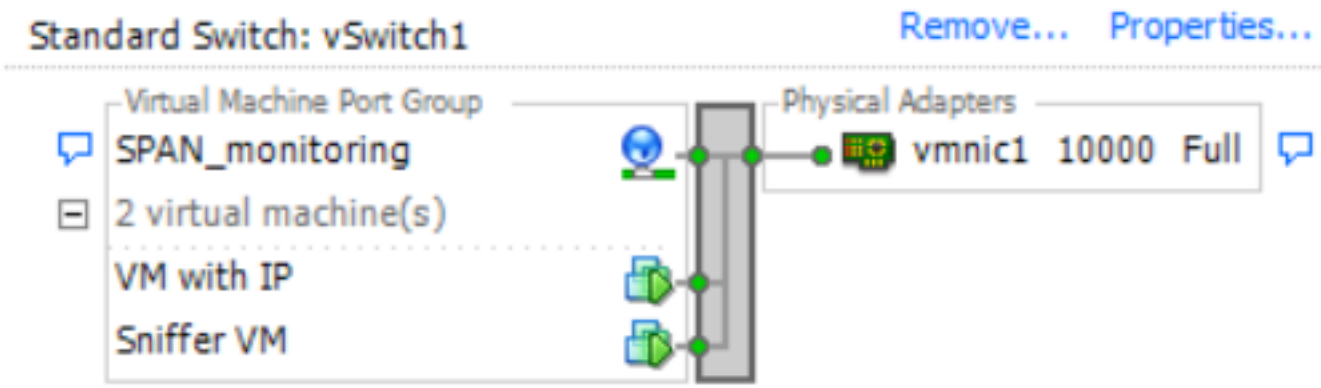
- Selecione o grupo de porta e o clique **edita**
- Vá à **ABA de segurança** e mude o modo misturado que ajusta-se para aceitar segundo as indicações desta imagem



3. Atribua as duas máquinas virtuais ao grupo de porta da seção dos ajustes da máquina virtual.



4. As duas máquinas virtuais devem aparecer no grupo de porta sob a **ABA de rede de comunicação** agora.



Neste exemplo, o VM com IP é o segundo VM que tem um endereço IP de Um ou Mais Servidores Cisco ICM NT e o sniffer VM é o VM com a ferramenta do sniffer sem um endereço IP de Um ou Mais Servidores Cisco ICM NT.

5. Isto mostra as etapas de configuração no 6500 Switch:

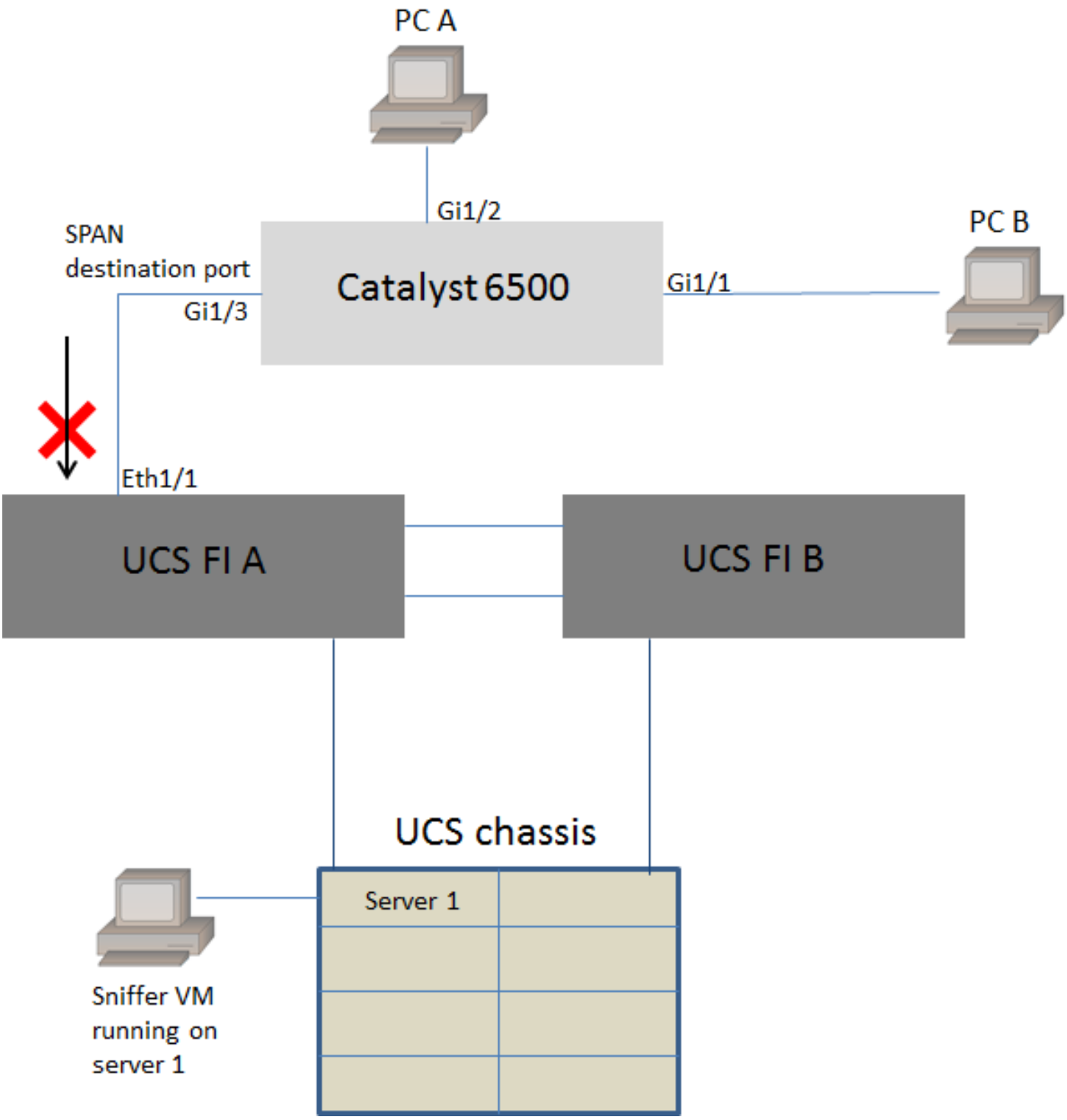
```
CAT6K-01(config)#monitor session 1 type erspan-source
CAT6K-01(config-mon-erspan-src)#source interface gi1/1
CAT6K-01(config-mon-erspan-src)#destination
CAT6K-01(config-mon-erspan-src-dst)#ip address 192.0.2.3
CAT6K-01(config-mon-erspan-src-dst)#origin ip address 192.0.2.1
CAT6K-01(config-mon-erspan-src-dst)#erspan-id 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 de Um ou Mais Servidores Cisco ICM NT do segundo VM (VM com IP) é 192.0.2.3.

Com esta configuração, os 6500 encapsulam os pacotes capturados e enviam-nos ao VM com o endereço IP de Um ou Mais Servidores Cisco ICM NT. O modo misturado no vSwitch de VMware permite o sniffer VM de considerar também estes pacotes.

Cenário de falha

Esta seção descreve uma encenação da falha comum ao usar a característica do SPAN local em um interruptor físico em vez da característica ERSPAN. Esta topologia é considerada aqui:



O tráfego do PC A ao PC B é monitorado usando a característica do SPAN local. O destino do tráfego do PERÍODO é dirigido à porta conectada à interconexão da tela UCS (FI).

A máquina virtual com a ferramenta do sniffer é executado dentro do UCS no servidor1.

Esta é a configuração no 6500 Switch:

```
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 fluxo de tráfego nas portas Gig1/1 e Gig1/2 replicated sobre para mover Gig1/3. Os endereços MAC de origem e de destino destes pacotes serão desconhecidos ao UCS FI.

No modo do host final dos Ethernet UCS, o FI deixa cair estes pacotes do unicast desconhecido.

No modo do switching de Ethernet UCS, o FI aprende o endereço MAC de origem na porta conectada aos 6500 (Eth1/1) e inunda então os pacotes rio abaixo aos server. Esta sequência de evento acontece:

1. Para a facilidade da compreensão, considere o tráfego que vai somente entre o PC A (com endereço MAC aaaa.aaaa.aaaa) e o PC B (com endereço MAC bbbb.bbbb.bbbb) nas relações Gig1/1 e Gig1/2
2. O primeiro pacote é do PC A ao PC B e este é visto no UCS FI Eth1/1
3. O FI aprende o endereço MAC aaaa.aaaa.aaaa em Eth1/1
4. O FI não conhece o endereço MAC de destino bbbb.bbbb.bbbb e inunda o pacote a todas as portas no mesmo VLAN
5. O sniffer VM, no mesmo VLAN, igualmente vê este pacote
6. O próximo pacote é do PC B ao PC A
7. Quando isto bate Eth1/1, o endereço MAC bbbb.bbbb.bbbb está aprendido em Eth1/1
8. O destino do pacote é para o endereço MAC aaaa.aaaa.aaaa
9. O FI deixa cair este pacote enquanto o endereço MAC aaaa.aaaa.aaaa é aprendido em Eth1/1 e o pacote esteve recebido em Eth1/1 próprio
10. Os pacotes subsequente, destinados para o endereço MAC aaaa.aaaa.aaaa ou o endereço MAC bbbb.bbbb.bbbb são deixados cair pela mesma razão

Informação relacionada

- Configurando o modo misturado em um virtual switch ou em um portgroup
- PERÍODO, RSPAN, e ERSPAN no Catalyst 6500
- Tráfego do Decapsulation ERSPAN com ferramentas de código aberto
- Suporte Técnico e Documentação - Cisco Systems