Configurar máquina virtual en servidor blade UCS como destino SPAN

Contenido

Introducción

Este documento describe los pasos para capturar un flujo de tráfico que se encuentra completamente fuera de Cisco Unified Computing System (UCS) y dirigirlo a una máquina virtual (VM) que ejecuta una herramienta de rastreo dentro de UCS. El origen y el destino del tráfico capturado se encuentran fuera de UCS. La captura se puede iniciar en un switch físico que está conectado directamente a UCS o podría estar a pocos pasos de distancia.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- UCS
- VMware ESX versión 4.1 o posterior
- Analizador de puerto de switch remoto encapsulado (ERSPAN)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Catalyst 6503 con 12.2(18)ZYA3c
- Cisco UCS serie B con 2.2(3e)

- VMWare ESXi 5.5 compilación 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.

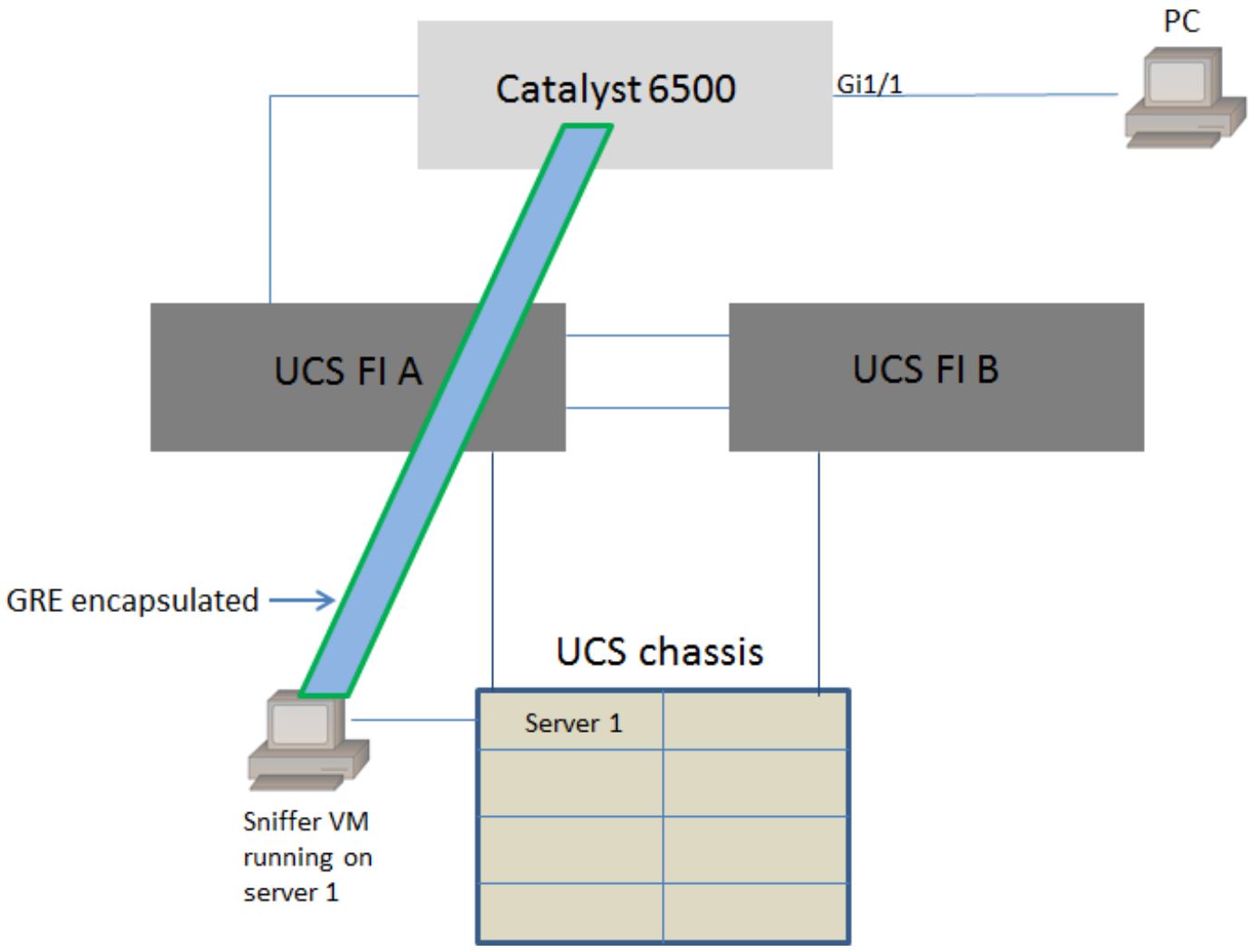
Antecedentes

UCS no tiene la función SPAN remoto (RSPAN) para recibir tráfico SPAN de un switch conectado y dirigirlo a un puerto local. Por lo tanto, la única forma de lograrlo en un entorno UCS es mediante la función RSPAN encapsulado (ERSPAN) en un switch físico y enviando el tráfico capturado a la máquina virtual mediante IP. En ciertas implementaciones, la máquina virtual que ejecuta la herramienta de sabueso no puede tener una dirección IP. Este documento explica la configuración requerida cuando la VM del sabueso tiene una dirección IP así como el escenario sin una dirección IP. La única limitación aquí es que la VM del sabueso necesita poder leer la encapsulación GRE/ERSPAN del tráfico que se le envía.

Configurar

Diagrama de la red

Esta topología se ha considerado en este documento:



Se está supervisando el PC conectado a GigabitEthernet1/1 del Catalyst 6500. El tráfico en GigabitEthernet1/1 se captura y se envía a la máquina virtual del rastreador que se ejecuta dentro de Cisco UCS en el servidor 1. La función ERSPAN en el switch 6500 captura el tráfico, lo encapsula usando GRE y lo envía a la dirección IP de la máquina virtual del sniffer.

VM de sniffer con dirección IP

> **Nota:** Los pasos descritos en esta sección también se pueden utilizar en el escenario en el que el sniffer se ejecuta en un servidor sin software específico en un blade UCS en lugar de ejecutarse en una VM.

Estos pasos son necesarios cuando la VM del sniffer puede tener una dirección IP:

- Configure la máquina virtual del rastreador dentro del entorno UCS con una dirección IP accesible desde el 6500
- Ejecute la herramienta sniffer dentro de la VM
- Configure una sesión de origen ERSPAN en el 6500 y envíe el tráfico capturado directamente a la dirección IP de la máquina virtual

Los pasos de configuración en el 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
```

En este ejemplo, la dirección IP de la máquina virtual del sabueso es 192.0.2.2

VM de sniffer sin dirección IP

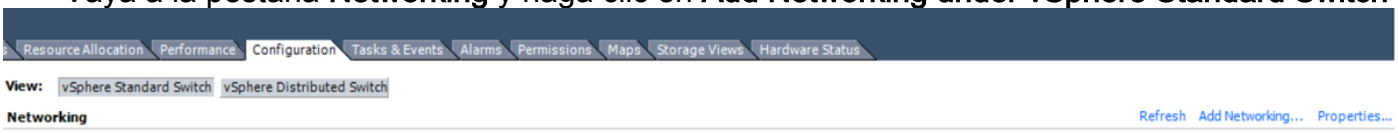
Estos pasos son necesarios cuando la VM del sniffer no puede tener una dirección IP:

- Configure la máquina virtual del rastreador dentro del entorno UCS
- Ejecute la herramienta sniffer dentro de la VM
- Cree una segunda VM que pueda tener una dirección IP en el mismo host y configúrela con una dirección IP accesible desde el 6500
- Configure el grupo de puertos en el vSwitch VMWare para que se encuentre en el modo promiscuo
- Configure una sesión de origen ERSPAN en el 6500 y envíe el tráfico capturado a la dirección IP de la segunda VM

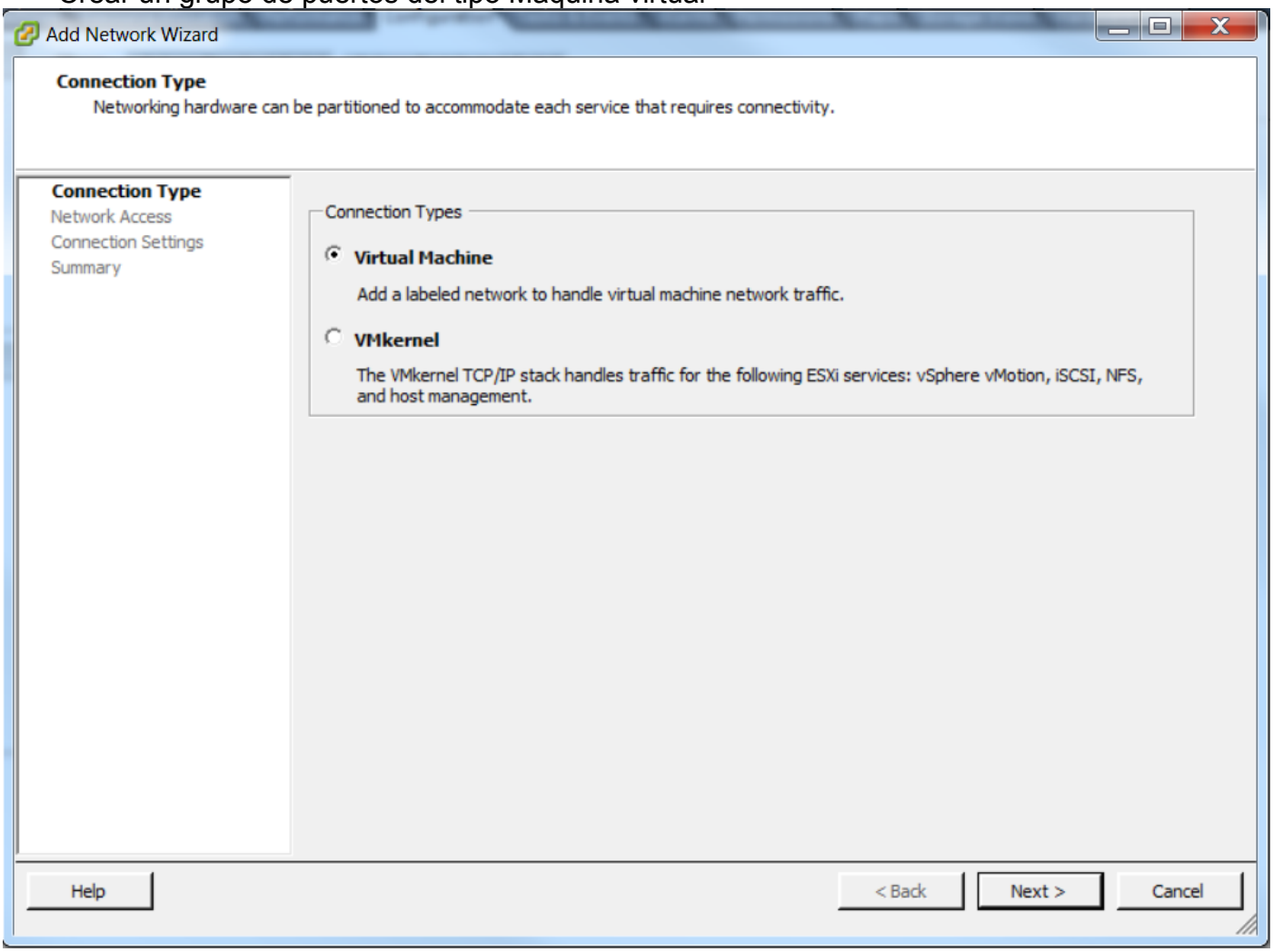
Estos pasos muestran la configuración requerida en VMWare ESX: Vaya directamente al paso 2 si ya tiene configurado un grupo de puertos.

1. Crear un grupo de puertos de máquina virtual y asignarle las dos máquinas virtuales

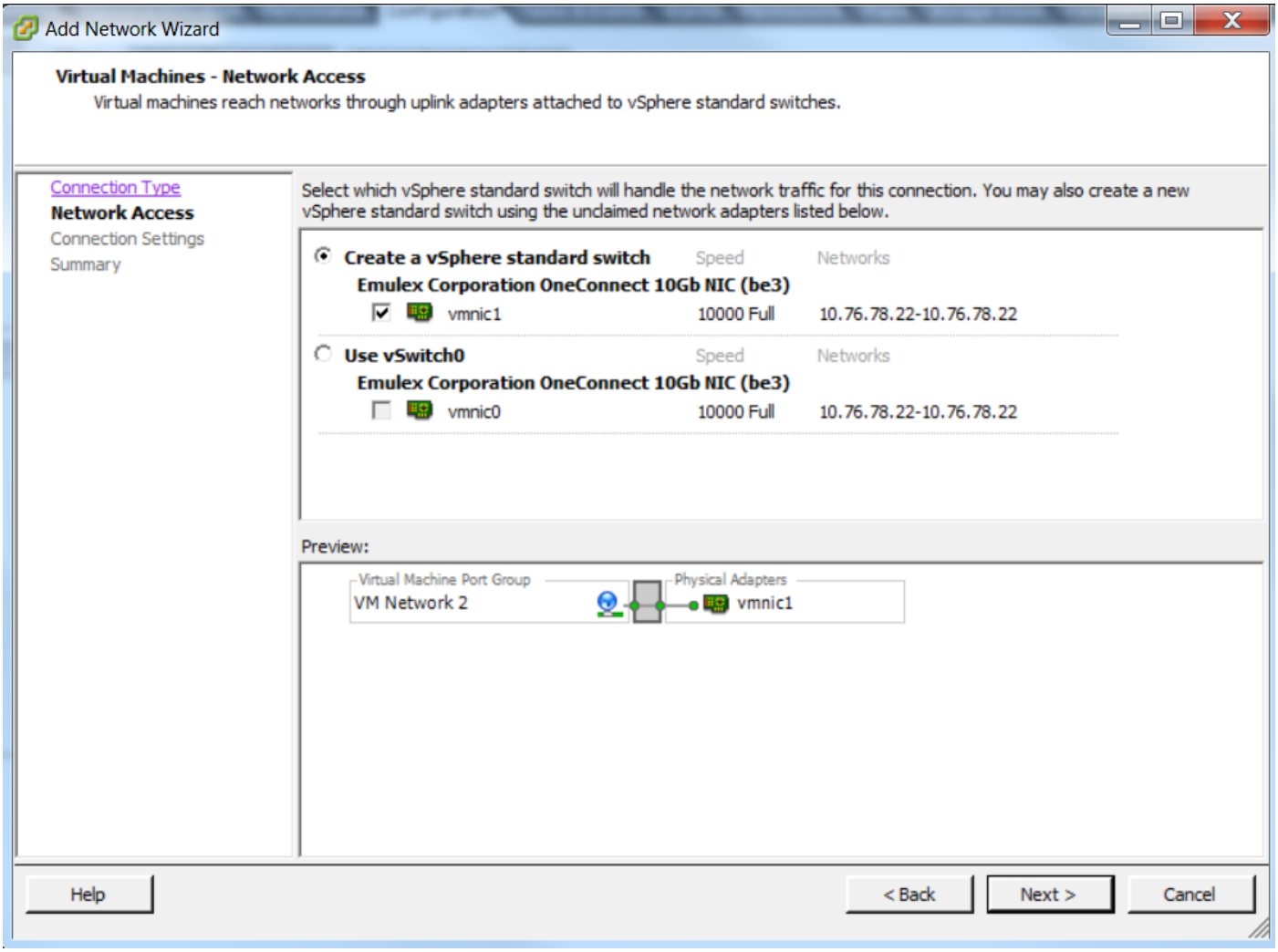
- Vaya a la pestaña **Networking** y haga clic en **Add Networking under vSphere Standard Switch**



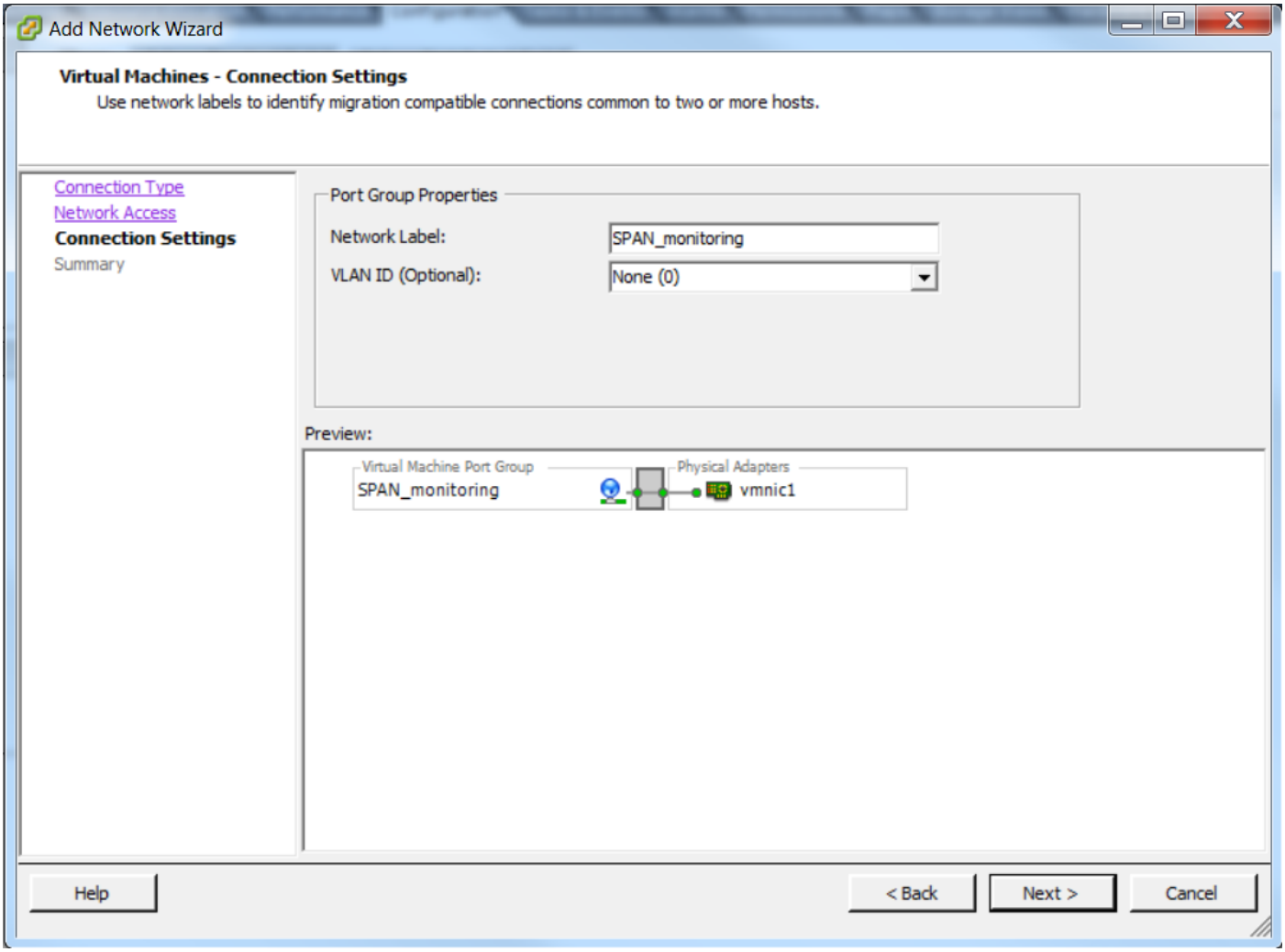
- Crear un grupo de puertos del tipo Máquina virtual



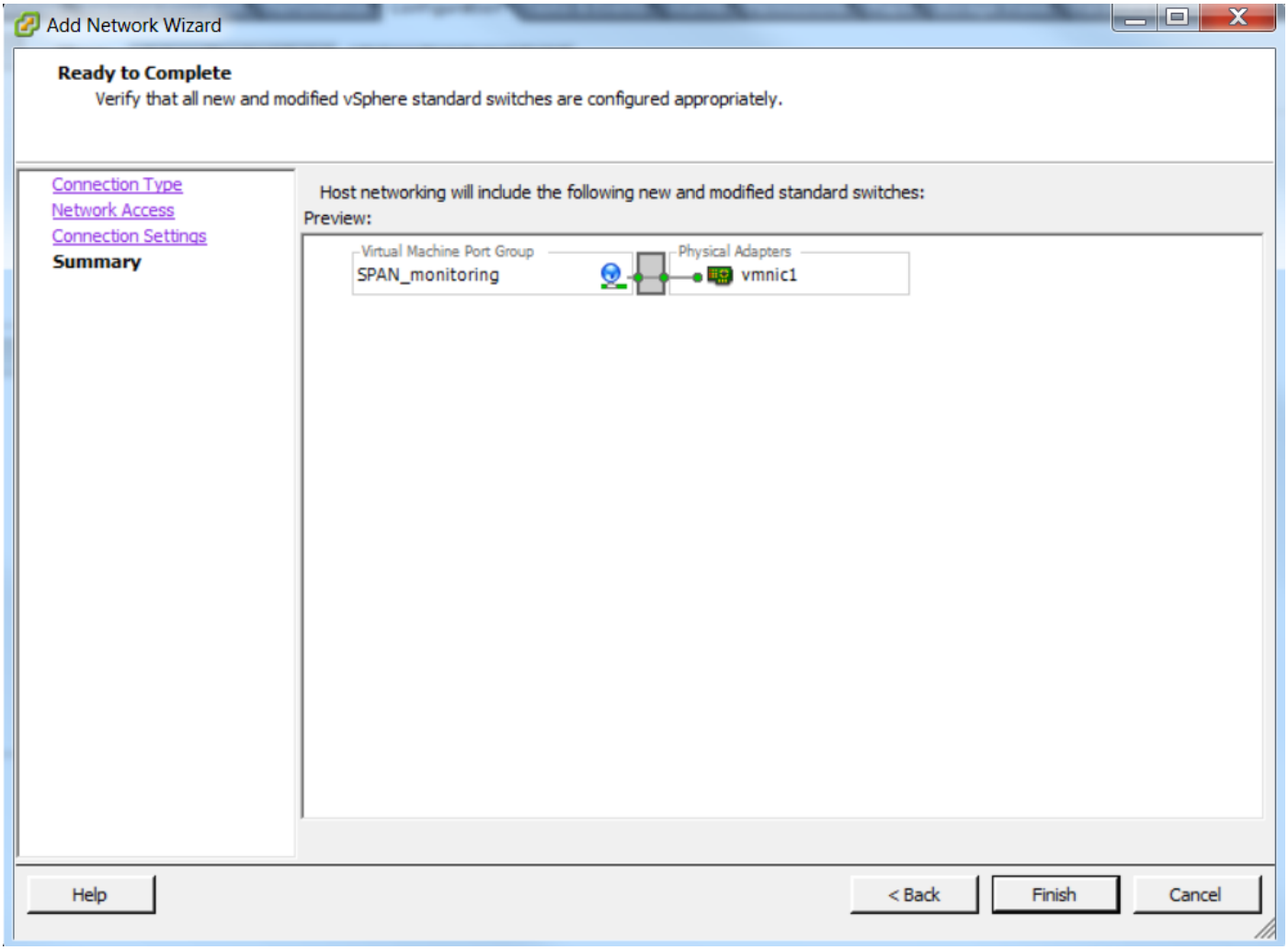
- Asigne una interfaz física (vmnic) al grupo de puertos como se muestra en esta imagen.



- Configure un nombre para el grupo de puertos y agregue la VLAN relevante como se muestra en la imagen.



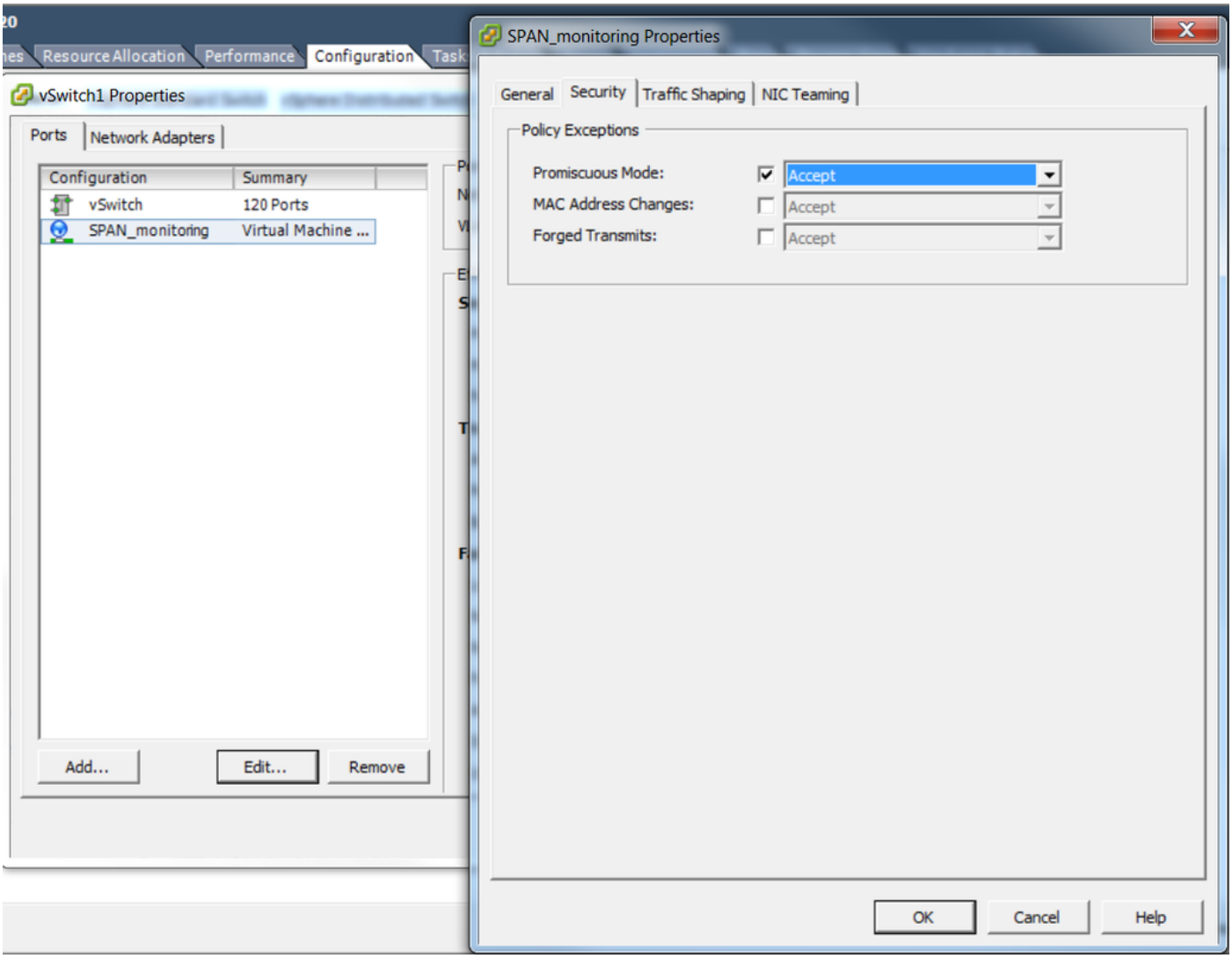
- Verifique la configuración y haga clic en **Finalizar** como se muestra en la imagen.



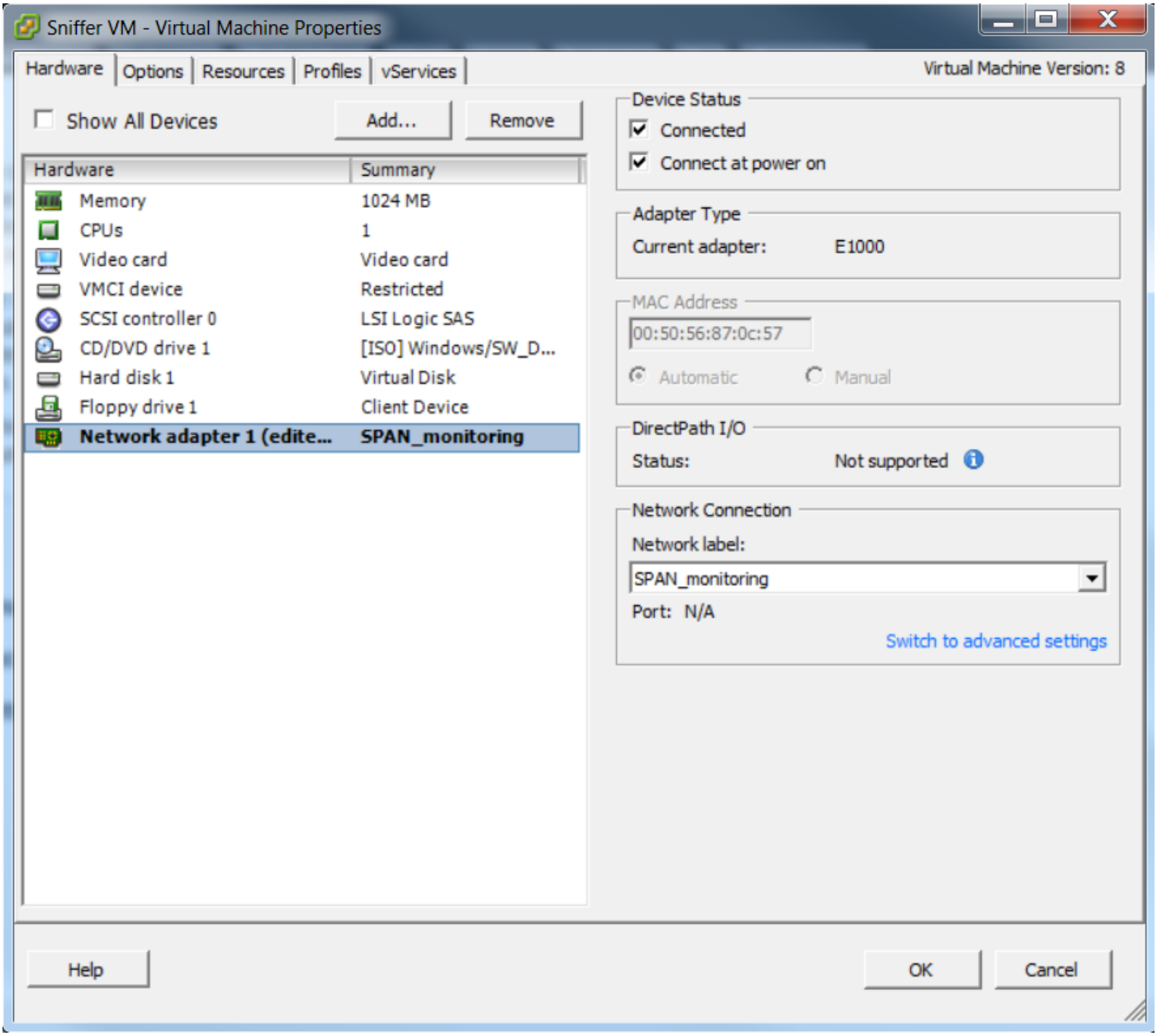
2. Configure el grupo de puertos para que esté en el modo promiscuo como se muestra en la imagen.

- El grupo de puertos debe aparecer en la pestaña **Networking** ahora
- Haga clic en Properties (Propiedades)

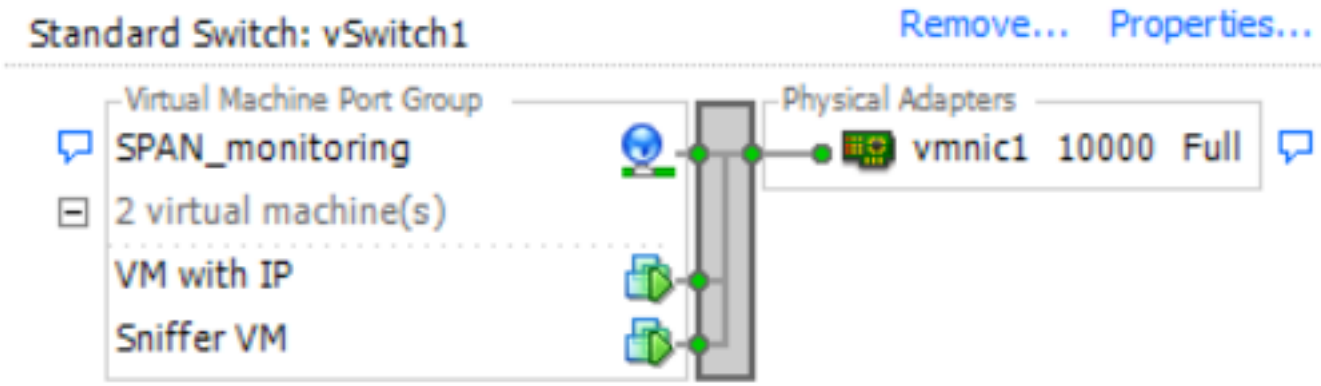
- Seleccione el grupo de puertos y haga clic en **Editar**
- Vaya a la ficha **Seguridad** y cambie la configuración del modo Promiscuous a Accept como se muestra en esta imagen



3. Asigne las dos máquinas virtuales al grupo de puertos desde la sección Configuración de la máquina virtual.



4. Las dos máquinas virtuales deben aparecer en el grupo de puertos bajo la pestaña **Networking** ahora.



En este ejemplo, VM con IP es la segunda VM que tiene una dirección IP y Sniffer VM es la VM con la herramienta sniffer sin una dirección IP.

5. Esto muestra los pasos de configuración en el switch 6500:

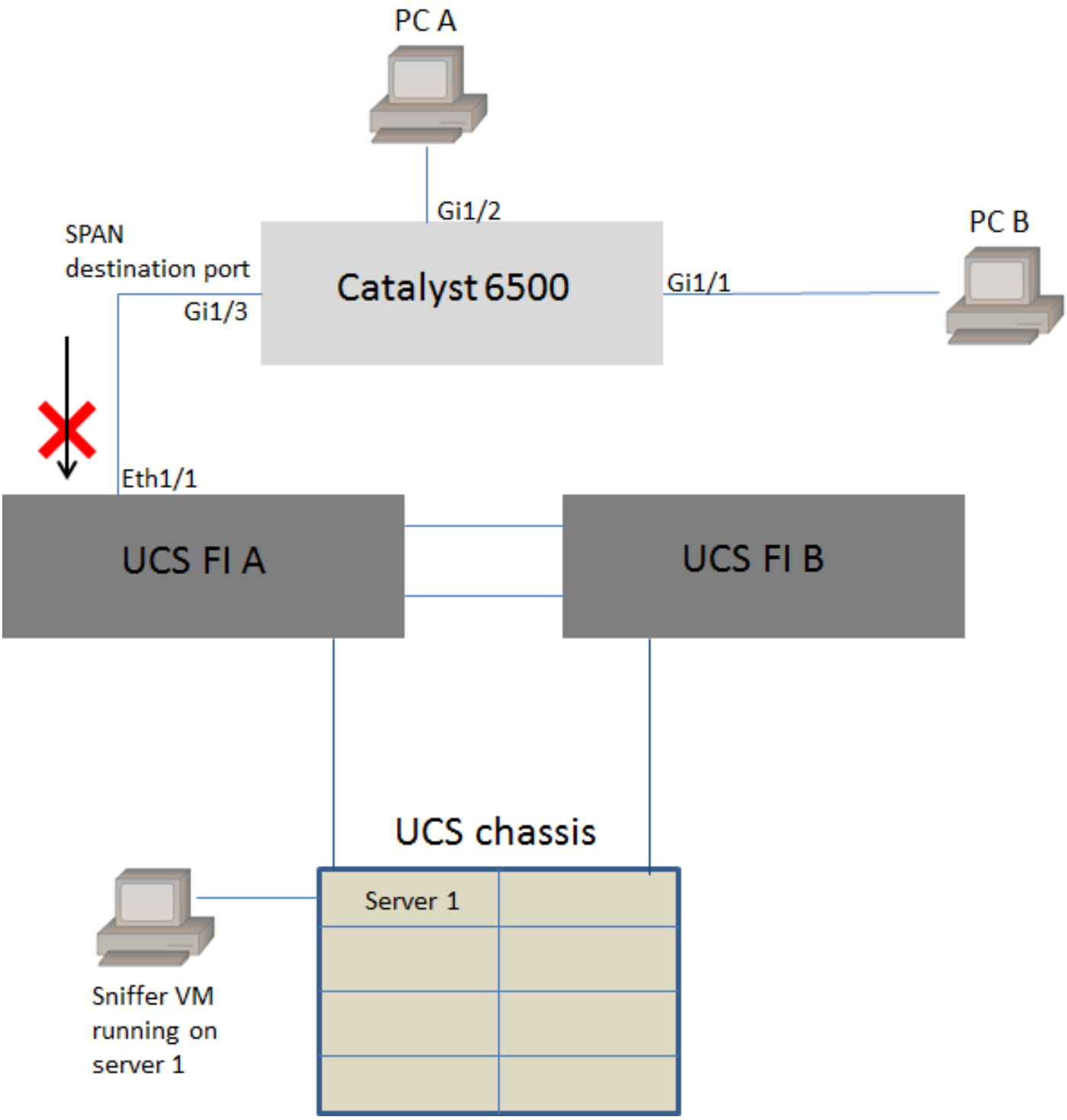
```
CAT6K-01(config)#monitor session 1 type erspan-source
CAT6K-01(config-mon-erspan-src)#source interface gi1/1
CAT6K-01(config-mon-erspan-src)#destination
CAT6K-01(config-mon-erspan-src-dst)#ip address 192.0.2.3
CAT6K-01(config-mon-erspan-src-dst)#origin ip address 192.0.2.1
CAT6K-01(config-mon-erspan-src-dst)#erspan-id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

En este ejemplo, la dirección IP de la segunda VM (VM con IP) es 192.0.2.3.

Con esta configuración, el 6500 encapsula los paquetes capturados y los envía a la VM con la dirección IP. El modo promiscuo en el vSwitch VMWare permite que la VM del rastreador también vea estos paquetes.

Escenario de falla

Esta sección describe un escenario de falla común cuando se utiliza la función SPAN local en un switch físico en lugar de la función ERSPAN. Esta topología se considera aquí:



El tráfico de la PC A a la PC B se monitorea mediante la función SPAN local. El destino del tráfico SPAN se dirige al puerto conectado a Fabric Interconnect (FI) de UCS.

La máquina virtual con la herramienta sniffer se ejecuta dentro de UCS en el servidor 1.

Esta es la configuración en el 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 el tráfico que fluye en los puertos Gig1/1 y Gig1/2 se replicará en el puerto Gig1/3. Las direcciones MAC de origen y destino de estos paquetes serán desconocidas para la FI UCS.

En el modo de host final de Ethernet de UCS, la FI descarta estos paquetes de unidifusión

desconocidos.

En el modo de conmutación Ethernet de UCS, la FI aprende la dirección MAC de origen en el puerto conectado al 6500 (Eth1/1) y luego inunda los paquetes de flujo descendente a los servidores. Esta secuencia de eventos ocurre:

1. Para facilitar la comprensión, considere el tráfico que circula solamente entre PC A (con mac-address aaaaa.aaaa.aaaa) y PC B (con mac-address bbbb.bbbb.bbb) en las interfaces Gig1/1 y Gig1/2
2. El primer paquete es de PC A a PC B y esto se ve en UCS FI Eth1/1
3. La FI aprende mac-address aaaaa.aaaa.aaaa en Eth1/1
4. La FI no conoce el destino mac-address bbbb.bbbb.bbbb e inunda el paquete a todos los puertos en la misma VLAN
5. La VM del rastreador, en la misma VLAN, también ve este paquete
6. El siguiente paquete es de PC B a PC A
7. Cuando esto llega a Eth1/1, se aprende mac-address bbbb.bbb.bbbb en Eth1/1
8. El destino del paquete es para mac-address aaaaa.aaaa.aaaa
9. La FI descarta este paquete como mac-address aaaaa.aaaa.aaaa se aprende en Eth1/1 y el paquete se recibió en Eth1/1
10. Los paquetes subsiguientes, ya sea destinados a mac-address aaaaa.aaaa.aaaa o mac-address bbbb.bbbb.bbbb, se descartan por la misma razón

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Configuración del modo promiscuo en un switch o grupo de puertos virtual
- SPAN, RSPAN y ERSPAN en Catalyst 6500
- Desencapsulación del tráfico ERSPAN con herramientas de código abierto
- Soporte Técnico y Documentación - Cisco Systems