Contenido

Introducción

Este documento describe los pasos para capturar un flujo de tráfico que esté totalmente fuera del Cisco Unified Computing System (UCS) y para dirigirlo a una máquina virtual (VM) que funciona con una herramienta del sniffer dentro del UCS.

La fuente y el destino del tráfico que es capturado está fuera del UCS. La captura se puede iniciar en un Switch físico que se asocie directamente al UCS o podría ser algunos saltos lejos.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene un conocimiento sobre el funcionamiento de estos temas:

- Cisco Unified Computing System (UCS)
- Versión 4.1 o posterior de VMware ESX
- Analizador del puerto encapsulado del switch remoto (ERSPAN)

Componentes Utilizados

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

- Cisco Catalyst 6503 12.2(18)ZYA3c que se ejecutan
- Funcionamiento de la serie de Cisco UCS B 2.2(3e)
- Estructura 1331820 de VMware ESXi 5.5

Antecedentes

El UCS no tiene la característica del SPAN remoto (RSPAN) para recibir el tráfico del SPAN de un switch conectado y para dirigirlo a un puerto local. Tan la única forma de lograr esto en un entorno UCS está usando la característica encapsulada RSPAN (ERSPAN) en un Switch físico y el envío del tráfico capturado al VM usando el IP.

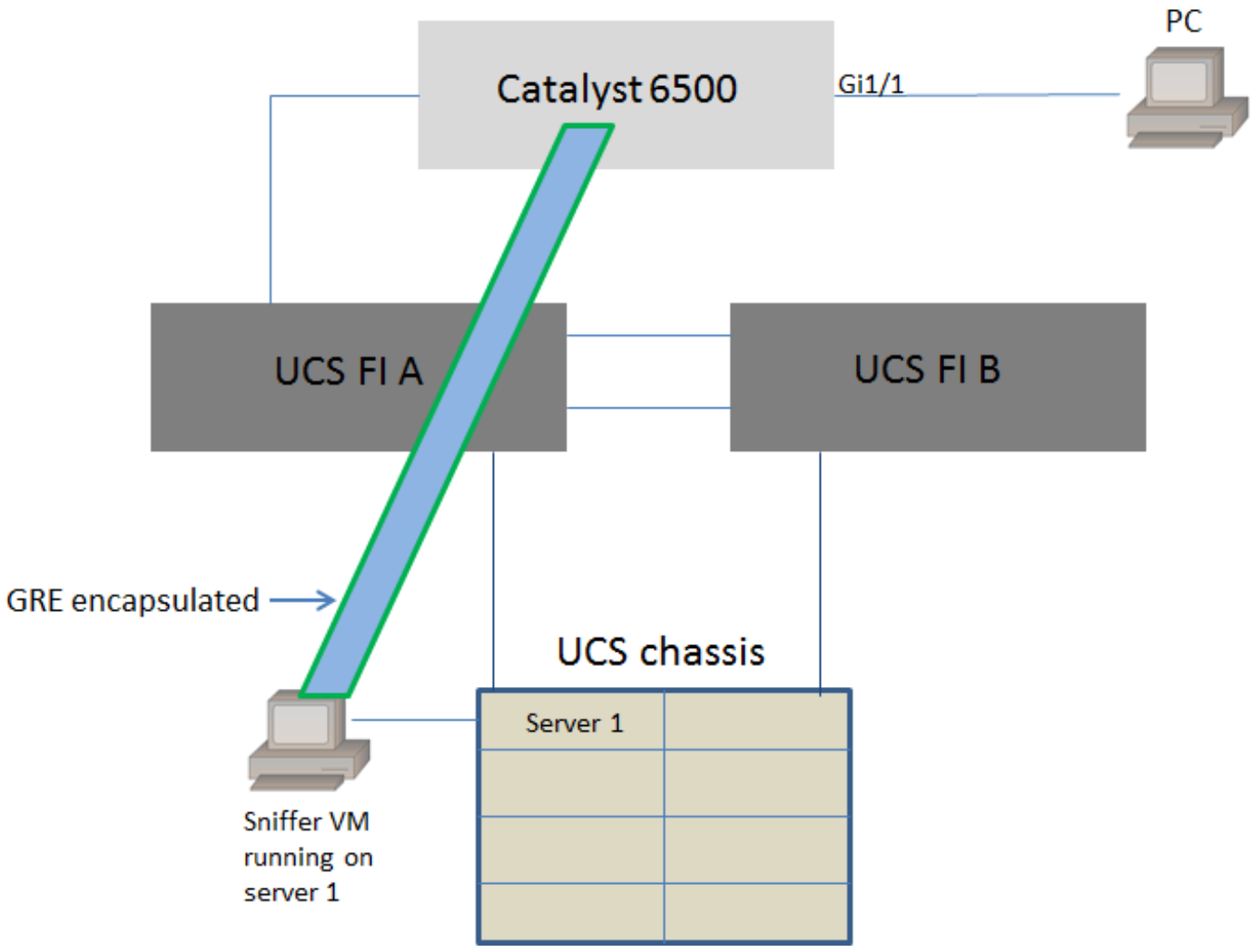
En ciertas implementaciones, el VM que funciona con la herramienta del sniffer no puede tener una dirección IP. Este documento explica la configuración requerida cuando el sniffer VM tiene una dirección IP así como el escenario sin una dirección IP. La limitación del onl aquí es que el sniffer VM necesita poder leer la encapsulación GRE/ERSPAN del tráfico que se envía ella.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Diagrama de la red

Esta topología se ha considerado en este documento:



El PC asociado a GigabitEthernet1/1 del Catalyst 6500 se está monitoreando. El tráfico en

GigabitEthernet1/1 se captura y se envía al sniffer VM que se ejecute dentro de Cisco UCS en el server1.

ERSPAN la característica en el 6500 Switch captura el tráfico, lo encapsula usando el GRE y lo envía a la dirección IP del sniffer el VM.

Configuraciones

Sniffer VM con una dirección IP

> Nota: Los pasos descritos en esta sección se pueden también utilizar en el escenario adonde el sniffer se ejecuta en un servidor del descubierto-metal en una cuchilla UCS en vez de ejecutarse en un VM.

Se requieren estos pasos cuando el sniffer VM puede tener una dirección IP:

- Configure el sniffer VM dentro del entorno UCS con una dirección IP que sea accesible de los 6500
- Funcione con la herramienta del sniffer dentro del VM
- Configure ERSPAN una sesión de la fuente sobre los 6500 y envíe el tráfico capturado directamente a la dirección IP VM

Los pasos para la configuración en el 6500 Switch:

En este ejemplo, la dirección IP del sniffer VM es 192.0.2.2

Sniffer VM sin una dirección IP

Se requieren estos pasos cuando el sniffer VM no puede tener una dirección IP:

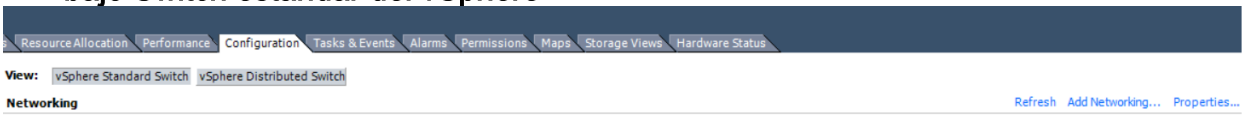
- Configure el sniffer VM dentro del entorno UCS
- Funcione con la herramienta del sniffer dentro del VM
- Cree un segundo VM que pueda tener una dirección IP en el mismo host y configurarla con una dirección IP que sea accesible de los 6500
- Configure al grupo de puertos en el vSwitch de VMware para estar en el modo promiscuo
- Configure ERSPAN una sesión de la fuente sobre los 6500 y envíe el tráfico capturado a la dirección IP del segundo VM

Estos pasos muestran la configuración requerida en VMware ESX:

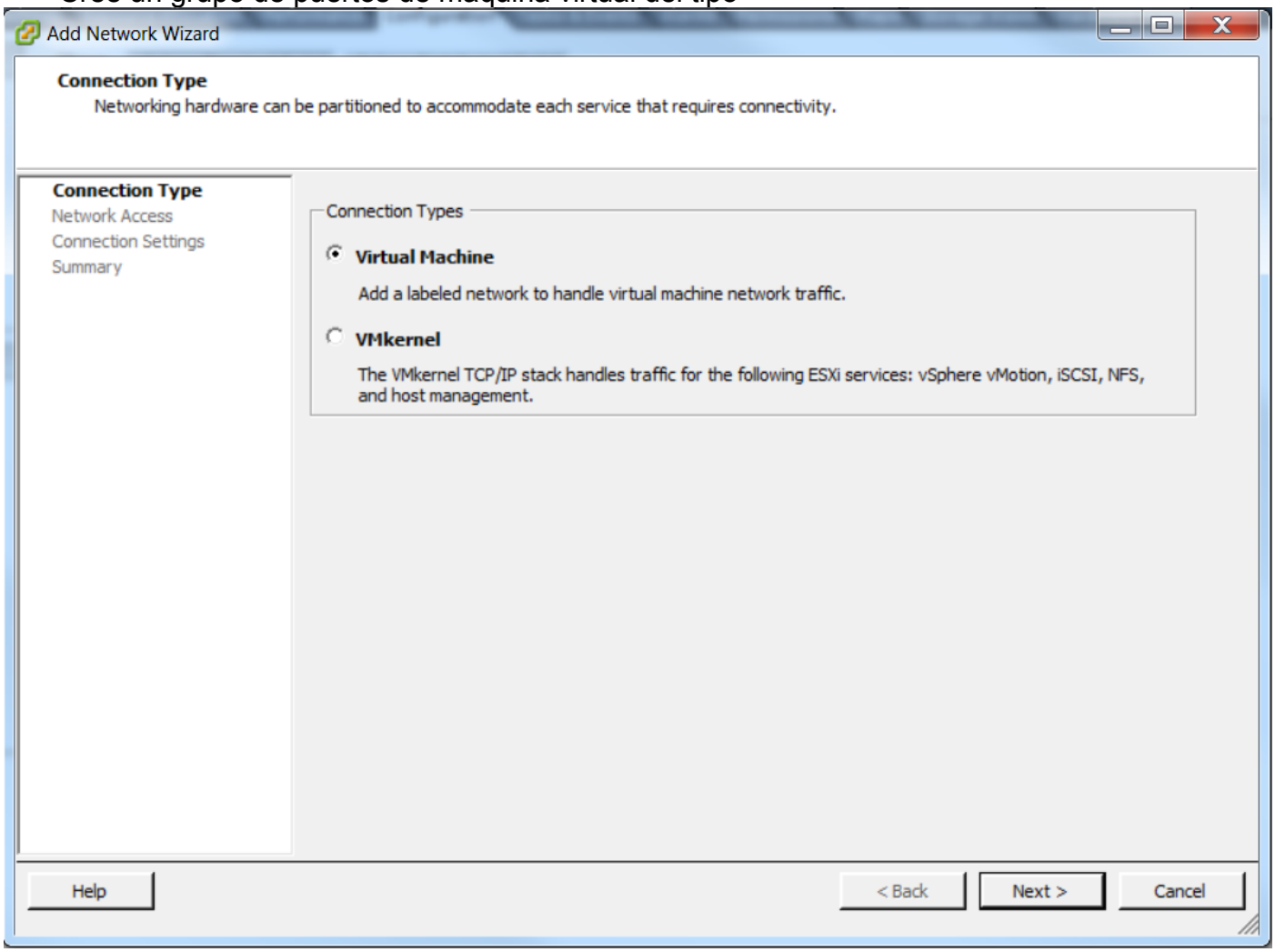
Vaya al paso 2 directamente si usted tiene ya un grupo de puertos configurado.

1. Cree un grupo de puertos de la máquina virtual y asígnele las dos máquinas virtuales

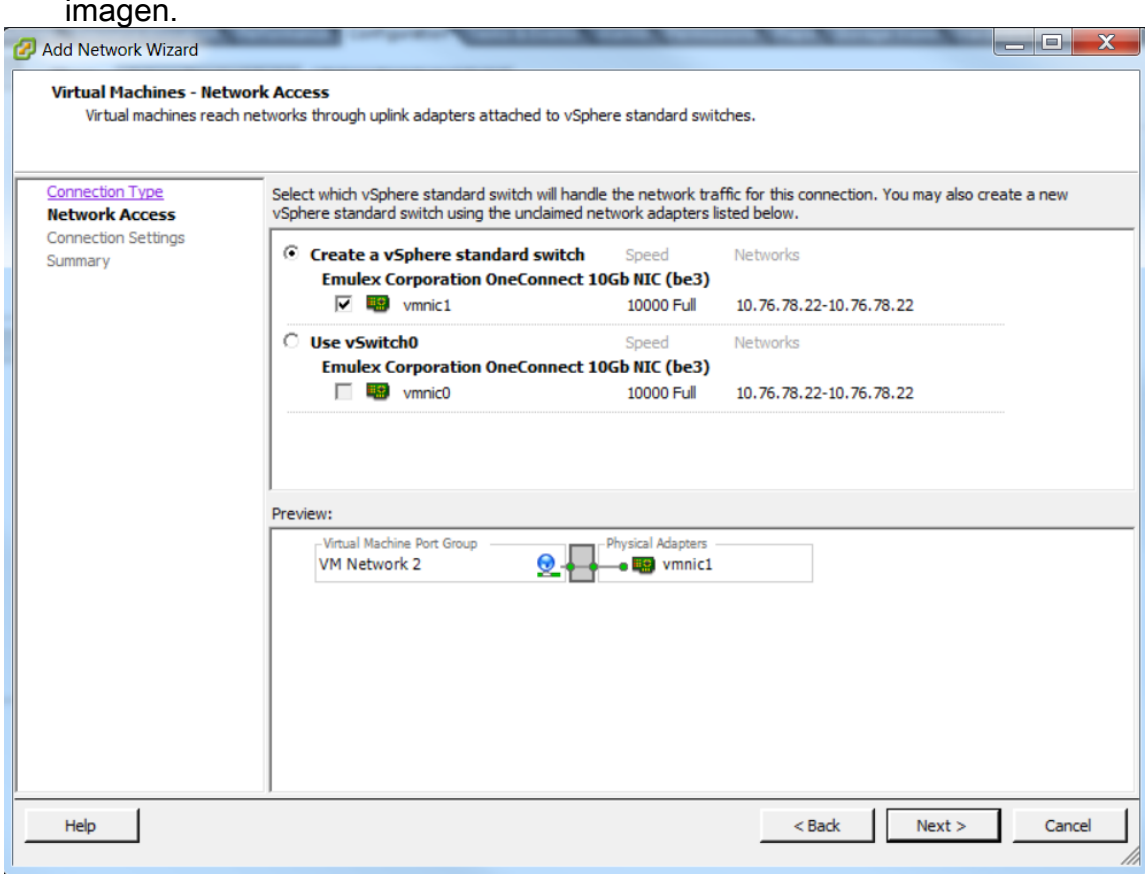
- Navegue a la **ficha de interconexión de redes** y el tecleo **agrega el establecimiento de una red bajo Switch estándar del vSphere**



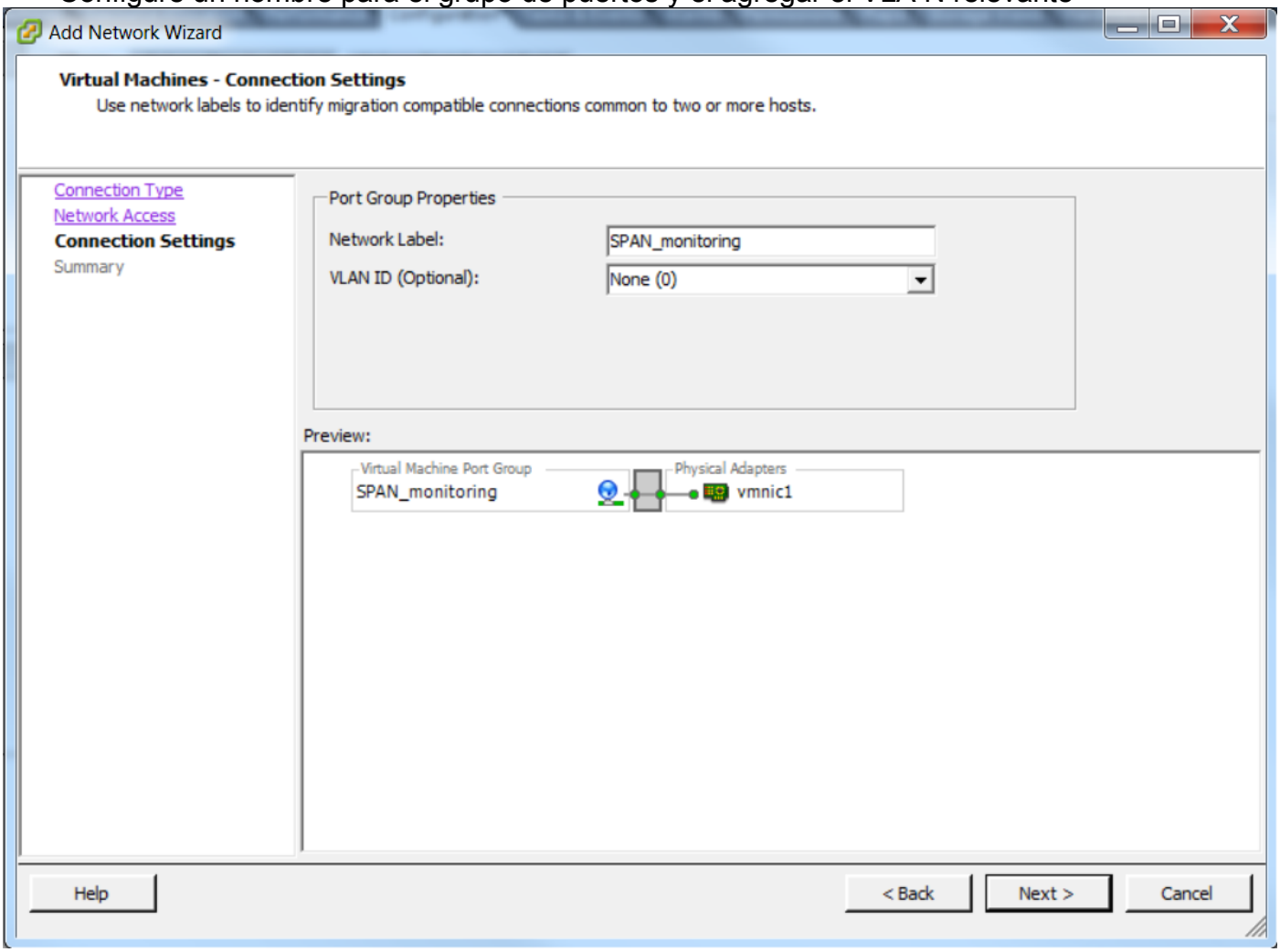
- Cree un grupo de puertos de máquina virtual del tipo



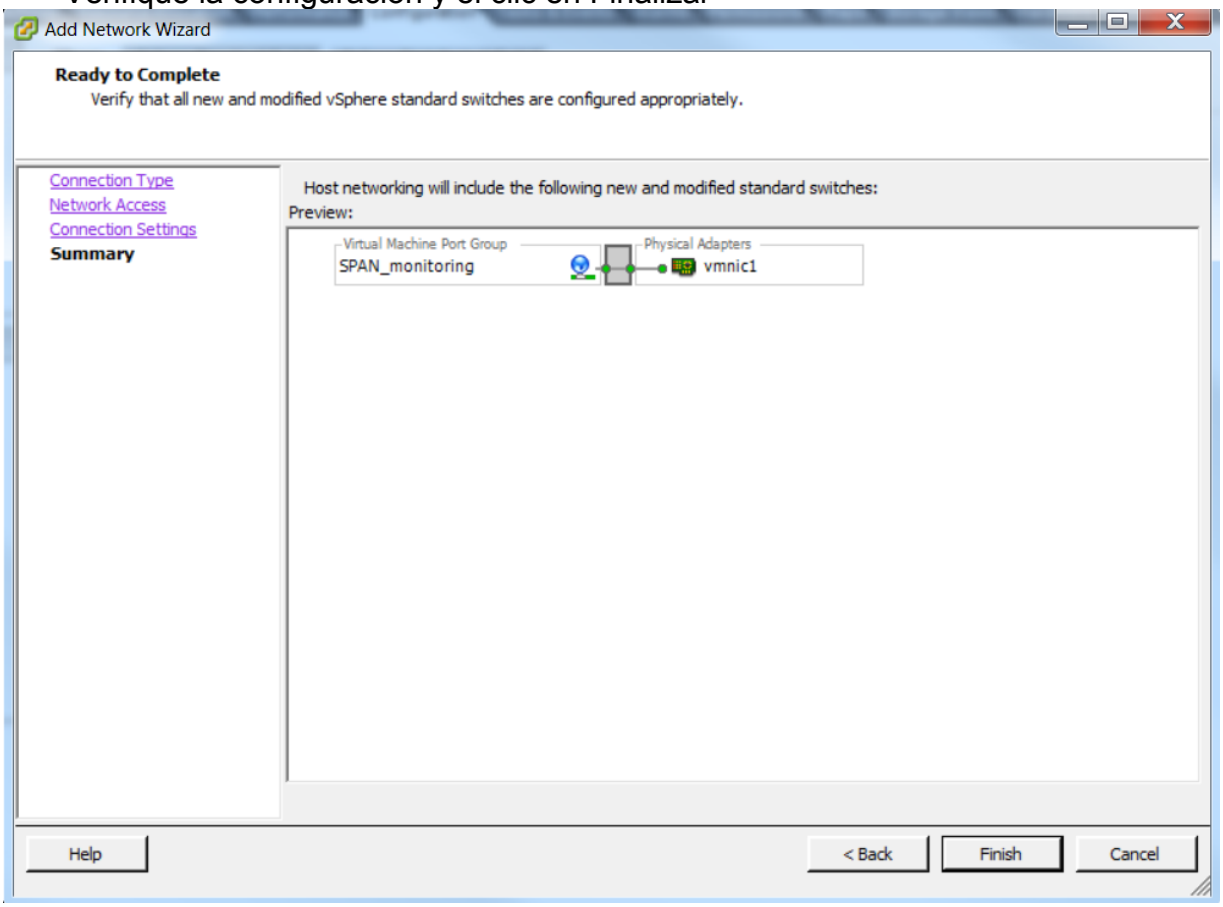
- Asigne una interfaz física (vmnic) al grupo de puertos tal y como se muestra en de esta imagen.



- Configure un nombre para el grupo de puertos y el agregar el VLA N relevante



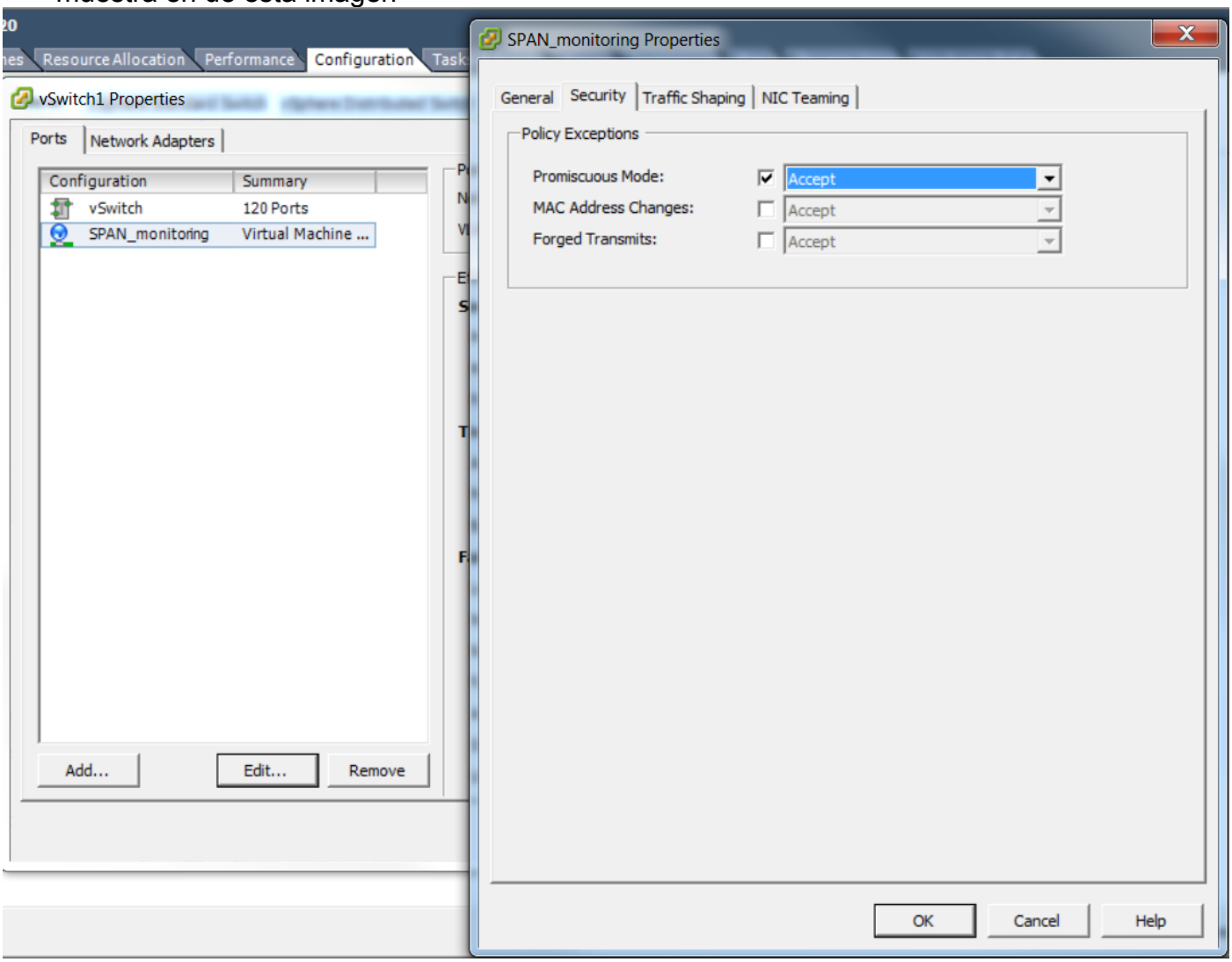
- Verifique la configuración y el clic en Finalizar



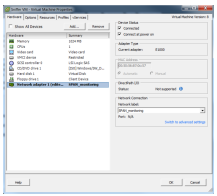
2. Configure al grupo de puertos para estar en el modo promiscuo.

- El grupo de puertos debe ahora aparecer conforme a la **ficha de interconexión de redes**
- **Propiedades del** tecleo

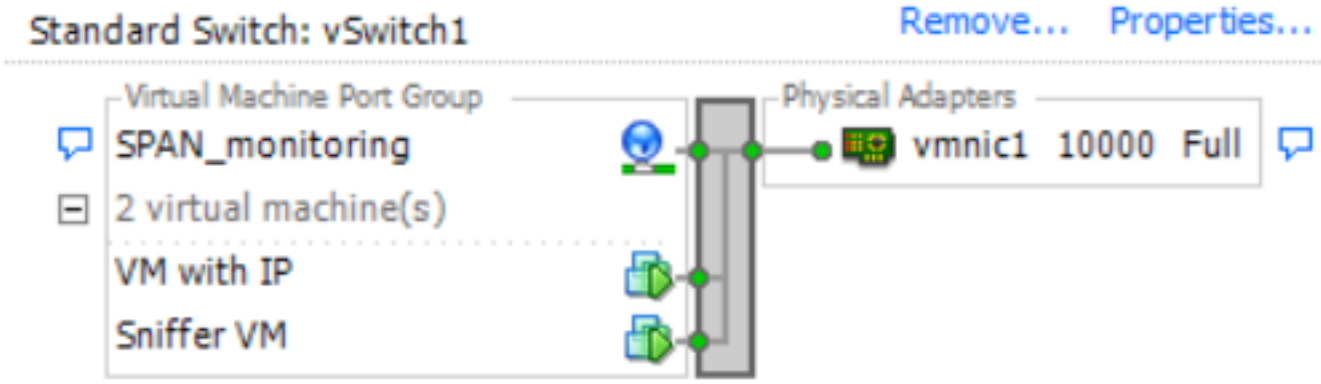
- Seleccione al grupo de puertos y el tecleo **edita**
- Vaya a la **ficha de seguridad** y cambie al modo promiscuo que fija para validar tal y como se muestra en de esta imagen



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



4. Las dos máquinas virtuales deben ahora aparecer en el grupo de puertos conforme a la **ficha de interconexión de redes**.



En este ejemplo, el VM con el IP es el segundo VM que tiene una dirección IP y el sniffer VM es el VM con la herramienta del sniffer sin una dirección IP.

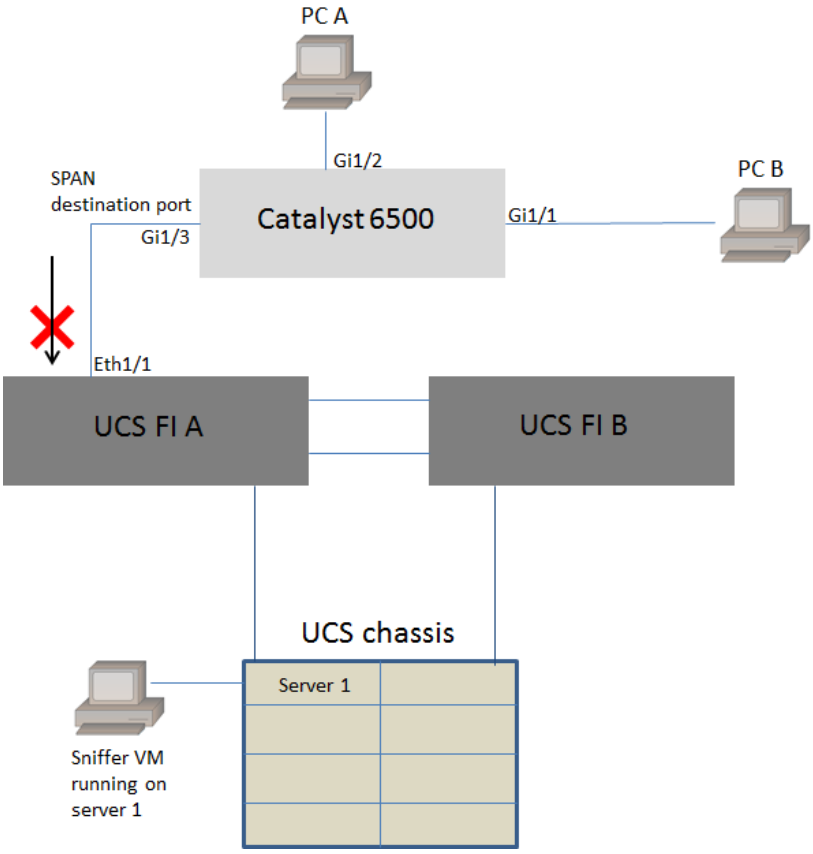
5. Esto muestra los pasos para la configuración en el 6500 Switch:

En este ejemplo, la dirección IP del segundo VM (VM con el IP) es 192.0.2.3.

Con esta configuración, los 6500 encapsula los paquetes capturados y los envía al VM con la dirección IP. El modo promiscuo en el vSwitch de VMware permite al sniffer VM para considerar estos paquetes también.

Escenario de falla

Esta sección describe un escenario de la falla común al usar la característica del SPAN local en un Switch físico en vez ERSPAN de la característica. Esta topología se considera aquí:



El tráfico del PC A al PC B se monitorea usando la característica del SPAN local. El destino del tráfico del SPAN se dirige al puerto conectado con la interconexión de la tela UCS (FI).

La máquina virtual con la herramienta del sniffer se ejecuta dentro del UCS en el server1.

Ésta es la configuración en el 6500 Switch:

Todo el flujo de tráfico en los puertos Gig1/1 y Gig1/2 será replicado encendido para virar Gig1/3 hacia el lado de babor. Los MAC Address de origen y destino de estos paquetes serán desconocidos al UCS FI.

En el modo del host extremo de los Ethernetes UCS, el FI cae estos paquetes de la unidifusión desconocida.

En el modo del Ethernet Switching UCS, el FI aprende el MAC Address de origen en el puerto conectado con los 6500 (Eth1/1) y después inunda los paquetes rio abajo a los servidores. Esta Secuencia de eventos sucede:

1. Para la facilidad de la comprensión, considere el tráfico que va solamente entre el PC A (con el MAC address aaaa.aaaa.aaaa) y el PC B (con el MAC address bbbb.bbbb.bbbb) en las interfaces Gig1/1 y Gig1/2
2. El primer paquete es de PC A al PC B y esto se ve en el UCS FI Eth1/1
3. El FI aprende el MAC address aaaa.aaaa.aaaa en Eth1/1
4. El FI no conoce a la dirección MAC de destino bbbb.bbbb.bbbb e inunda el paquete a todos los puertos en el mismo VLA N
5. El sniffer VM, en el mismo VLA N, también ve este paquete
6. El próximo paquete es de PC B al PC A
7. Cuando esto golpea Eth1/1, el MAC address bbbb.bbbb.bbbb se aprende en Eth1/1
8. El destino del paquete está para el MAC address aaaa.aaaa.aaaa

9. El FI cae este paquete mientras que el MAC address aaaa.aaaa.aaaa se aprende en Eth1/1 y el paquete fue recibido en Eth1/1 sí mismo
10. Los paquetes subsiguientes, destinados para el MAC address aaaa.aaaa.aaaa o el MAC address bbbb.bbbb.bbbb se caen por la misma razón

Información relacionada

- Configurar al modo promiscuo en un switch virtual o un portgroup
- SPAN, RSPAN, y ERSPAN en el Catalyst 6500
- Del Decapsulation tráfico ERSPAN con las herramientas de origen abierto
- Soporte Técnico y Documentación - Cisco Systems