Konfigurieren eines virtuellen Systems auf einem UCS Blade-Server als SPAN-Ziel

Inhalt

Einführung

Dieses Dokument beschreibt die Schritte zur Erfassung eines Datenverkehrsflusses, der sich vollständig außerhalb des Cisco Unified Computing System (UCS) befindet, und zur Weiterleitung an ein virtuelles System (VM), auf dem ein Sniffer-Tool im UCS ausgeführt wird. Quelle und Ziel des erfassten Datenverkehrs befinden sich außerhalb des UCS. Die Erfassung kann auf einem physischen Switch initiiert werden, der direkt mit dem UCS verbunden ist, oder sie kann einige Hops entfernt sein.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- UCS
- VMware ESX ab Version 4.1
- Encapsulated Remote Switch Port Analyzer (ERSPAN)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Catalyst 6503 mit 12.2(18)ZYA3c
- Cisco UCS B-Serie mit 2.2(3e)

- VMware ESXi 5.5 Build 1331820

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

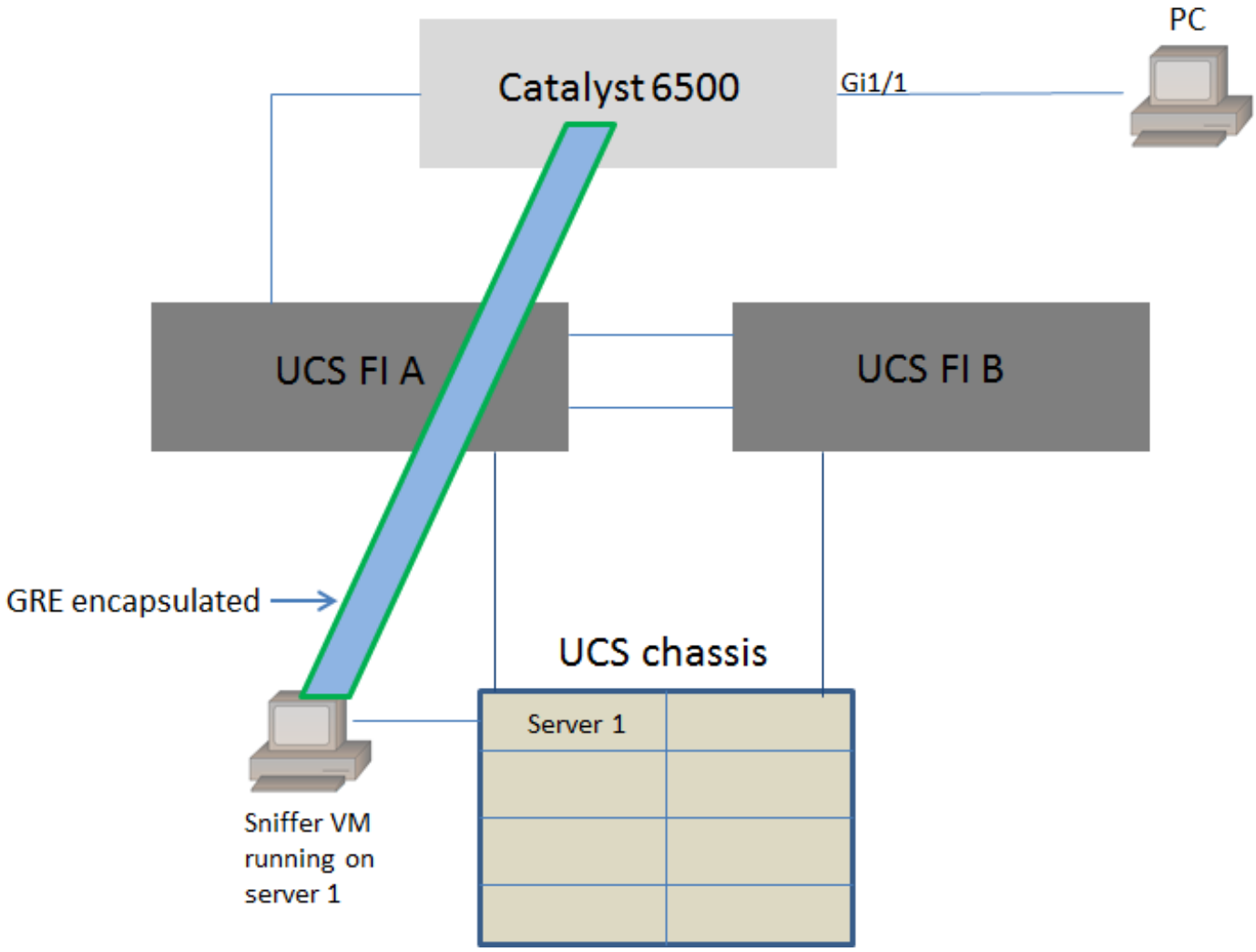
Hintergrundinformationen

Das UCS verfügt nicht über die Remote SPAN (RSPAN)-Funktion, um SPAN-Datenverkehr von einem angeschlossenen Switch zu empfangen und an einen lokalen Port weiterzuleiten. Die einzige Möglichkeit, dies in einer UCS-Umgebung zu erreichen, ist die Verwendung der ERSPAN-Funktion (Encapsulated RSPAN) auf einem physischen Switch und das Senden des erfassten Datenverkehrs an das virtuelle System über IP. In bestimmten Implementierungen kann die VM, die das Sniffer-Tool ausführt, keine IP-Adresse haben. In diesem Dokument wird die erforderliche Konfiguration erläutert, wenn die Sniffer VM über eine IP-Adresse verfügt, sowie das Szenario ohne IP-Adresse. Die einzige Einschränkung ist, dass die Sniffer VM die GRE/ERSPAN-Kapselung aus dem an sie gesendeten Datenverkehr lesen kann.

Konfigurieren

Netzwerkdiagramm

Diese Topologie wurde in diesem Dokument berücksichtigt:



PC, der an GigabitEthernet1/1 des Catalyst 6500 angeschlossen ist, wird überwacht. Der Datenverkehr auf GigabitEthernet1/1 wird erfasst und an die Sniffer VM gesendet, die im Cisco UCS auf Server 1 ausgeführt wird. Die ERSPAN-Funktion des 6500-Switches erfasst den Datenverkehr, kapselt ihn mithilfe der GRE und sendet ihn an die IP-Adresse des Sniffer VM.

Sniffer VM mit IP-Adresse

> **Hinweis**: Die in diesem Abschnitt beschriebenen Schritte können auch in Szenarien verwendet werden, in denen der Sniffer auf einem Bare-Metal-Server auf einem UCS-Blade ausgeführt wird, anstatt auf einem virtuellen System ausgeführt zu werden.

Diese Schritte sind erforderlich, wenn die Sniffer VM über eine IP-Adresse verfügen kann:

- Konfigurieren Sie das Sniffer VM in der UCS-Umgebung mit einer IP-Adresse, die vom 6500 aus erreichbar ist.
- Führen Sie das Sniffer-Tool in der VM aus.
- Konfigurieren einer ERSPAN-Quellsitzung auf dem 6500 und Senden des erfassten Datenverkehrs direkt an die IP-Adresse des virtuellen Systems

Die Konfigurationsschritte für den 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
```

In diesem Beispiel lautet die IP-Adresse des Sniffer VM 192.0.2.2.

Sniffer VM ohne IP-Adresse

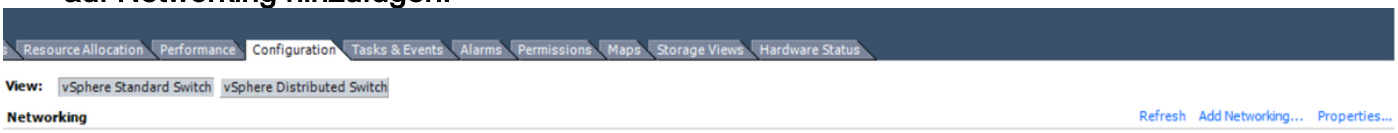
Diese Schritte sind erforderlich, wenn die Sniffer VM keine IP-Adresse haben kann:

- Konfigurieren der Sniffer VM in der UCS-Umgebung
- Führen Sie das Sniffer-Tool in der VM aus.
- Erstellen Sie eine zweite VM, die eine IP-Adresse im gleichen Host haben kann, und konfigurieren Sie sie mit einer IP-Adresse, die vom 6500 aus erreichbar ist.
- Konfigurieren Sie die Portgruppe auf dem VMWare vSwitch so, dass sie sich im Promiscuous-Modus befindet.
- Konfigurieren einer ERSPAN-Quellsitzung auf dem 6500 und Senden des erfassten Datenverkehrs an die IP-Adresse des zweiten virtuellen Systems

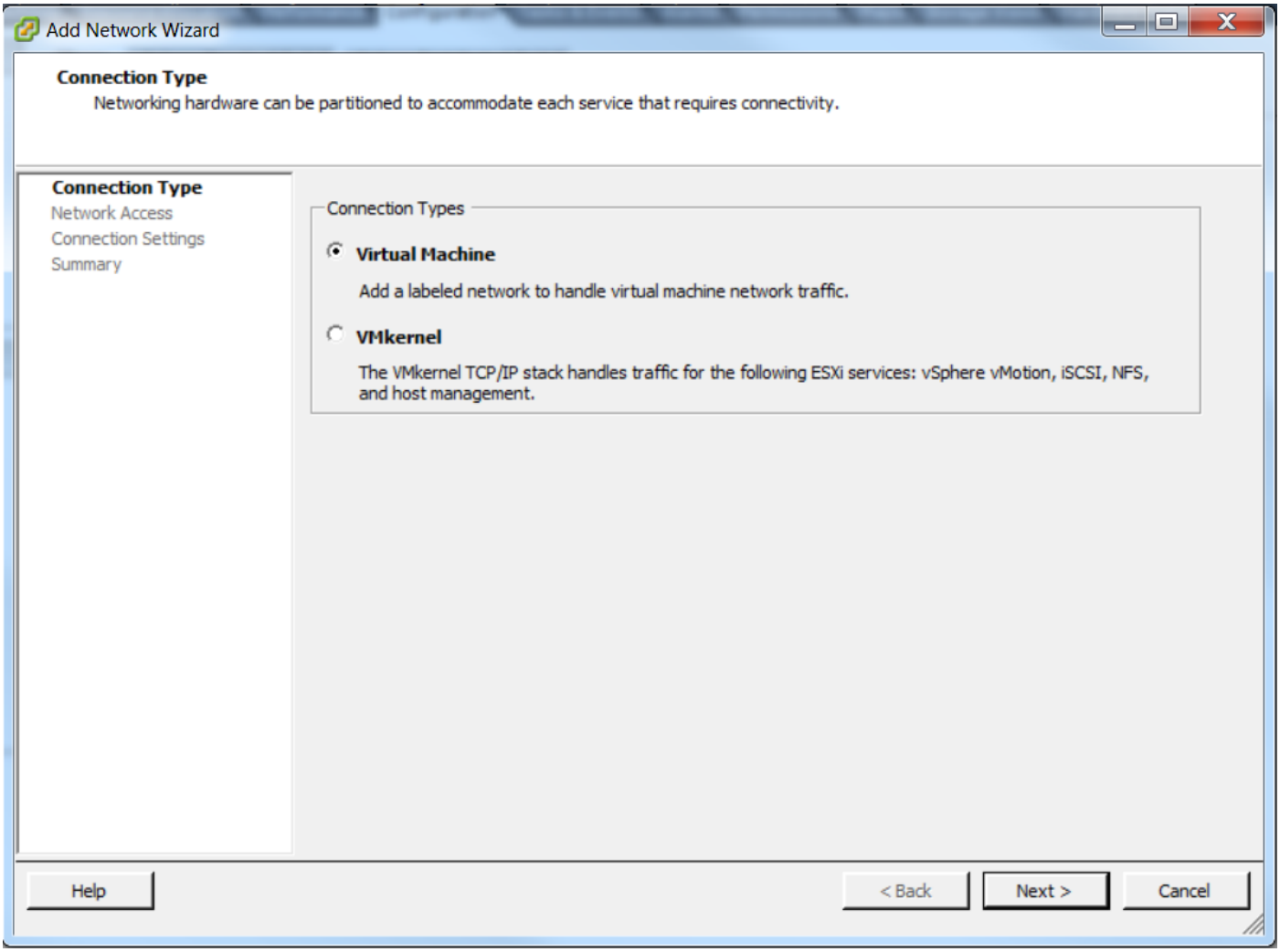
Diese Schritte zeigen die erforderliche Konfiguration für den VMWare ESX: Gehen Sie direkt zu Schritt 2, wenn Sie bereits eine Portgruppe konfiguriert haben.

1. Erstellen Sie eine Port-Gruppe für virtuelle Systeme, und weisen Sie dieser die beiden virtuellen Systeme zu.

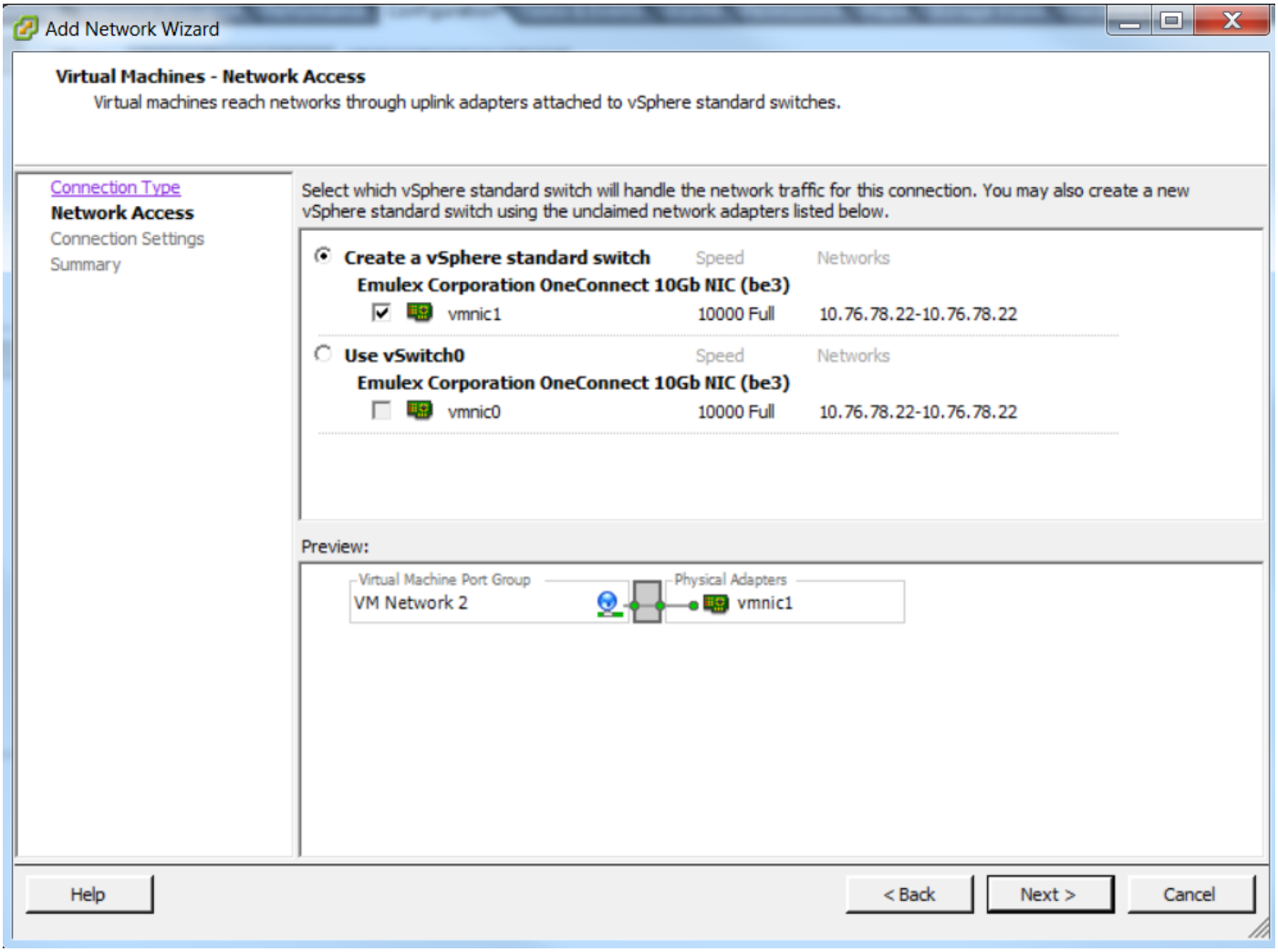
- Navigieren Sie zur Registerkarte **Networking** und klicken Sie **unter vSphere Standard Switch auf Networking hinzufügen.**



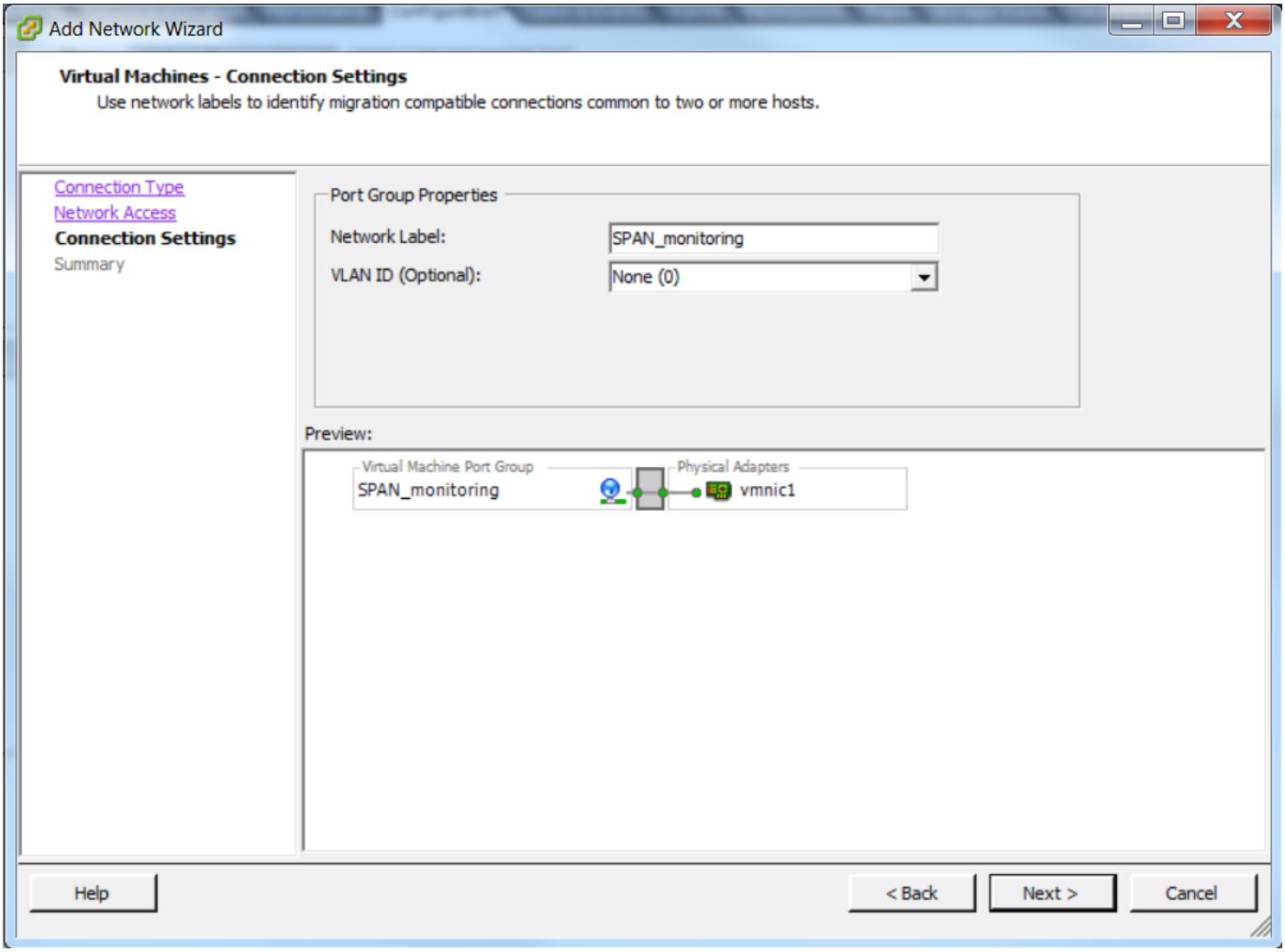
- Erstellen einer Portgruppe vom Typ "Virtuelles System"



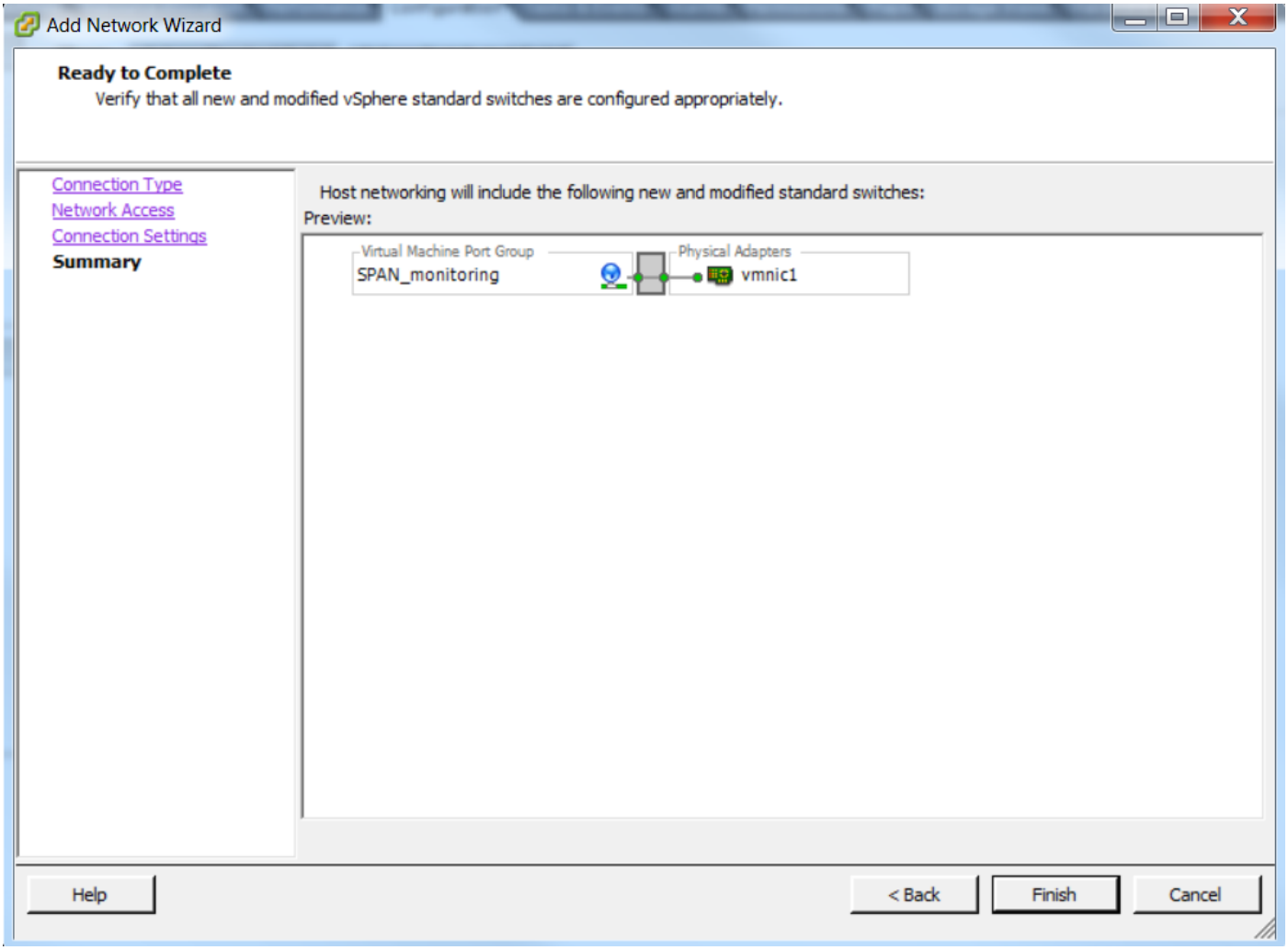
- Weisen Sie der Portgruppe wie in diesem Bild gezeigt eine physische Schnittstelle (vmnic) zu.



- Konfigurieren Sie einen Namen für die Port-Gruppe, und fügen Sie das relevante VLAN wie im Bild gezeigt hinzu.



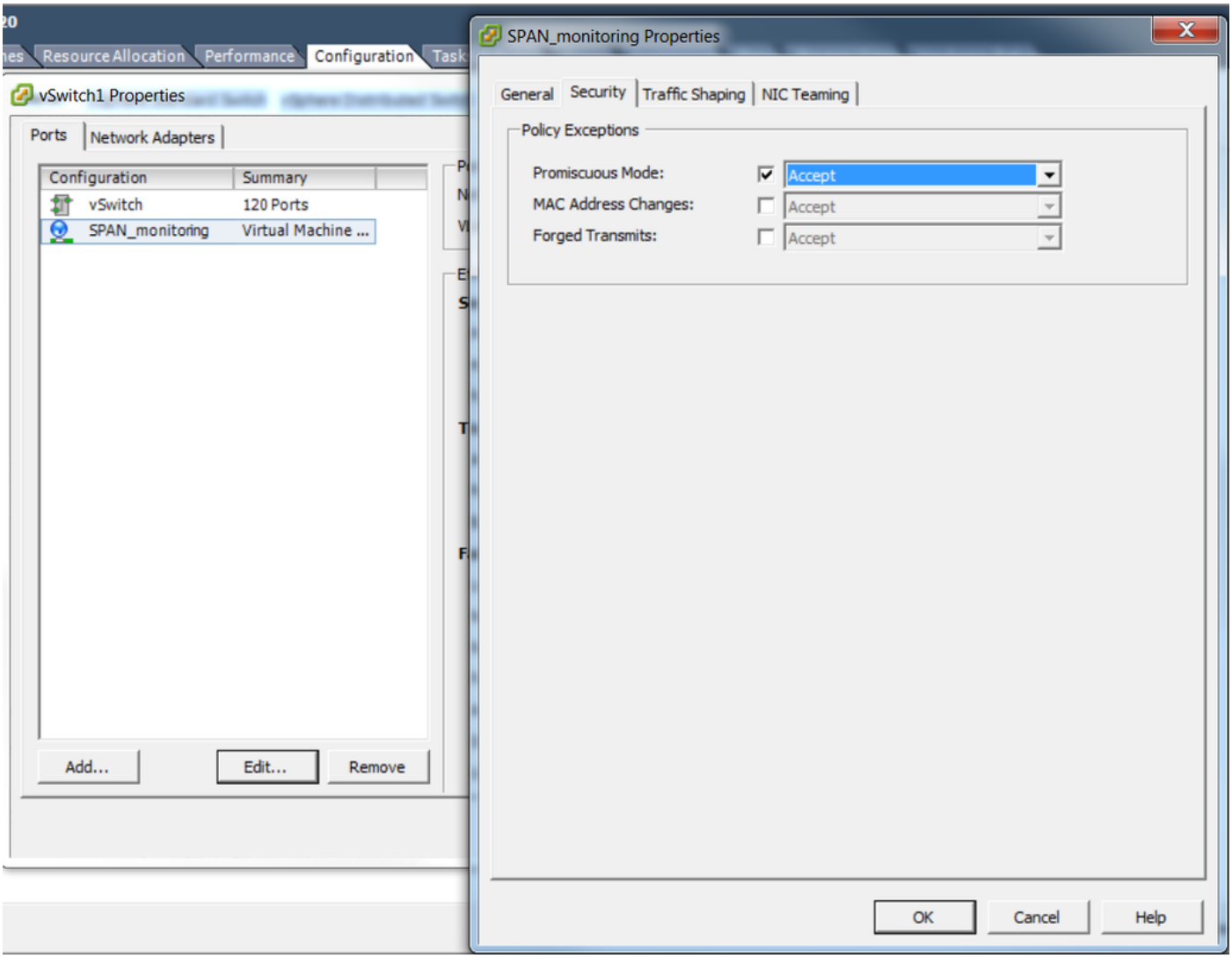
- Überprüfen Sie die Konfiguration, und klicken Sie auf **Fertig stellen** wie im Bild gezeigt.



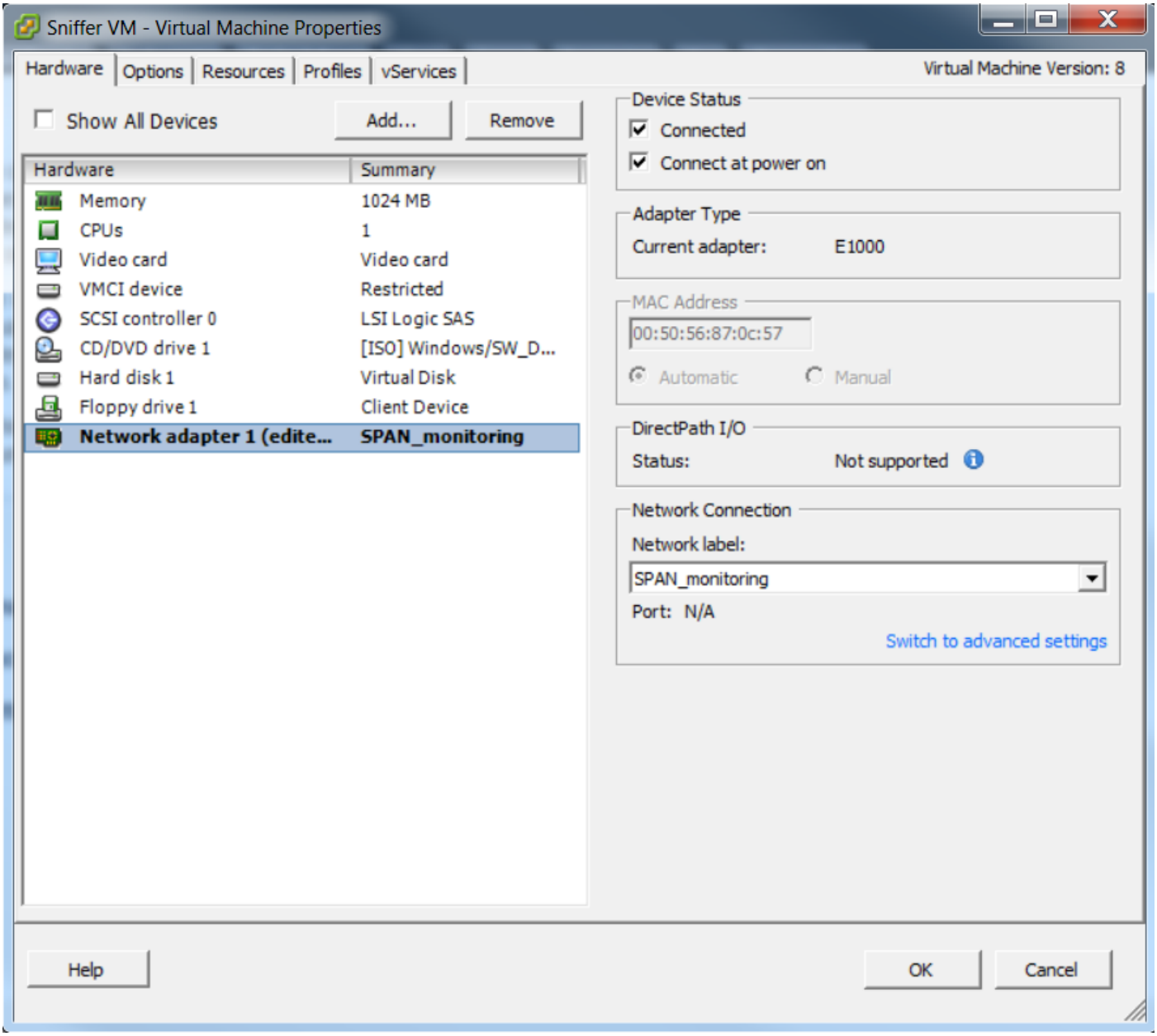
2. Konfigurieren Sie die Portgruppe so, dass sie sich im Promiscuous-Modus befindet, wie im Bild gezeigt.

- Die Portgruppe muss jetzt unter der Registerkarte **Netzwerk** angezeigt werden.
- Klicken Sie auf **Eigenschaften**

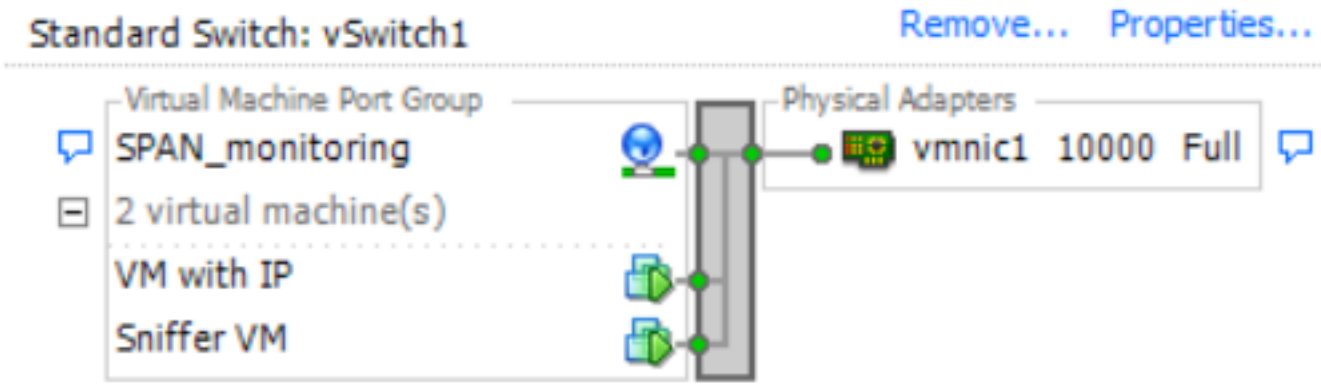
- Wählen Sie die Port-Gruppe aus, und klicken Sie auf **Bearbeiten.**
- Wechseln Sie zur Registerkarte **Sicherheit**, und ändern Sie die Einstellung Promiscuous mode (Promiscuous-Modus) wie in diesem Bild gezeigt auf Accept (Akzeptieren).



3. Weisen Sie die beiden virtuellen Systeme der Portgruppe aus dem Abschnitt "Einstellungen für virtuelle Systeme" zu.



4. Die beiden virtuellen Systeme müssen jetzt unter der Registerkarte **Netzwerk** in der Portgruppe angezeigt werden.



In diesem Beispiel ist VM mit IP die zweite VM mit einer IP-Adresse und Sniffer VM die VM mit dem Sniffer-Tool ohne IP-Adresse.

5. Hier sehen Sie die Konfigurationsschritte für den Switch der Serie 6500:

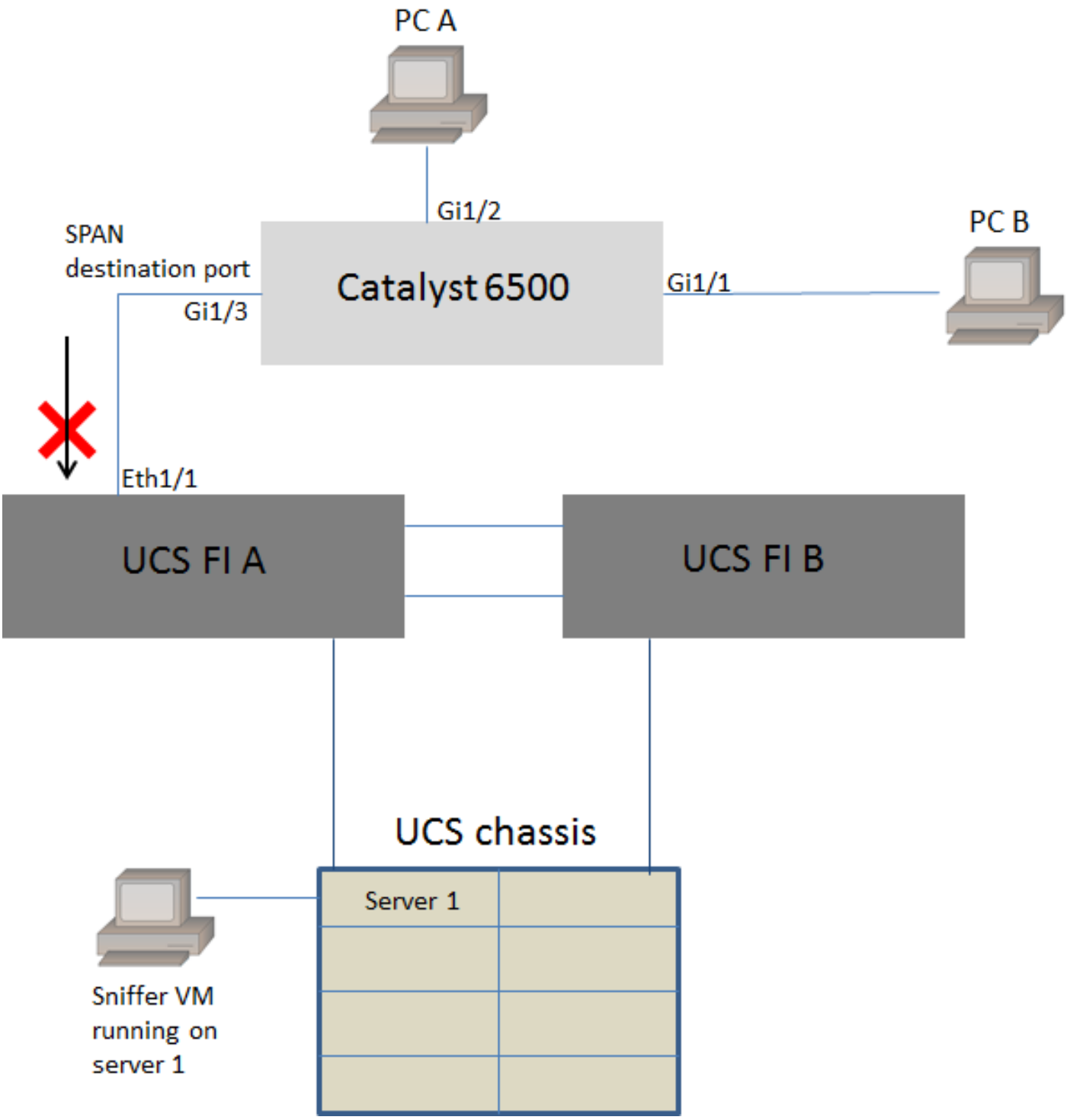
```
CAT6K-01(config)#monitor session 1 type erspan-source
CAT6K-01(config-mon-erspan-src)#source interface gi1/1
CAT6K-01(config-mon-erspan-src)#destination
CAT6K-01(config-mon-erspan-src-dst)#ip address 192.0.2.3
CAT6K-01(config-mon-erspan-src-dst)#origin ip address 192.0.2.1
CAT6K-01(config-mon-erspan-src-dst)#erspan-id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

In diesem Beispiel ist die IP-Adresse des zweiten virtuellen Systems (VM mit IP) 192.0.2.3.

Bei dieser Konfiguration kapselt der 6500 die erfassten Pakete und sendet sie mit der IP-Adresse an das virtuelle System. Der Promiscuous-Modus auf dem VMWare vSwitch ermöglicht dem Sniffer VM, diese Pakete ebenfalls anzuzeigen.

Fehlerszenario

In diesem Abschnitt wird ein häufiges Fehlerszenario beschrieben, wenn die lokale SPAN-Funktion auf einem physischen Switch anstelle der ERSPAN-Funktion verwendet wird. Diese Topologie wird hier berücksichtigt:



Der Datenverkehr von PC A zu PC B wird mithilfe der lokalen SPAN-Funktion überwacht. Das Ziel des SPAN-Datenverkehrs wird an den Port weitergeleitet, der mit dem UCS Fabric Interconnect (FI) verbunden ist.

Das virtuelle System mit dem Sniffer-Tool wird im UCS auf Server 1 ausgeführt.

Dies ist die Konfiguration auf dem 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
```

Der gesamte Datenverkehr, der auf den Ports Gig1/1 und Gig1/2 fließt, wird auf Port Gig1/3 repliziert. Die Quell- und Ziel-MAC-Adressen dieser Pakete sind dem UCS FI nicht bekannt.

Im End-Host-Modus für das UCS-Ethernet verwirft das FI diese unbekannten Unicast-Pakete.

Im UCS Ethernet-Switching-Modus erfasst das FI die Quell-MAC-Adresse des mit dem 6500 verbundenen Ports (Eth1/1) und überflutet anschließend die Pakete im Downstream zu den Servern. Diese Abfolge von Ereignissen geschieht:

1. Um das Verständnis zu erleichtern, sollten Sie den Datenverkehr zwischen PC A (mit der MAC-Adresse aaa.aaa.aaaa) und PC B (mit der MAC-Adresse bbb.bbb.bbb) an den Schnittstellen Gig1/1 und Gig1/2 berücksichtigen.
2. Das erste Paket stammt von PC A zu PC B. Dieses wird auf UCS FI Eth1/1 angezeigt.
3. Die FI lernt die MAC-Adresse aaa.aaa.aaaa auf Eth1/1.
4. Der FI kennt die MAC-Zieladresse bbb.bbbb.bbb.bbb nicht und überflutet das Paket an alle Ports im selben VLAN.
5. Das Sniffer VM im gleichen VLAN sieht dieses Paket ebenfalls.
6. Das nächste Paket ist von PC B zu PC A
7. Wenn dies Eth1/1 erreicht, wird die MAC-Adresse bbbb.bbb.bbb auf Eth1/1 gelernt.
8. Das Ziel des Pakets ist für die MAC-Adresse aaa.aaaa.aaa.
9. Das FI verwirft dieses Paket, da die MAC-Adresse aaa.aaa.aaa.aaa auf Eth1/1 und das Paket auf Eth1/1 selbst empfangen wurde.
10. Nachfolgende Pakete, die entweder für die MAC-Adresse aaa.aaaa.aaa oder die MAC-Adresse bbb.bbb.bbb.bbb bestimmt sind, werden aus demselben Grund verworfen

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Konfigurieren des Promiscuous-Modus auf einem virtuellen Switch oder einer Portgruppe
- SPAN, RSPAN und ERSPAN auf Catalyst 6500
- Entkapselung des ERSPAN-Datenverkehrs mit Open Source-Tools
- Technischer Support und Dokumentation - Cisco Systems