UCSブレードサーバ上の仮想マシンをSPAN宛先として設定する

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[設定](#)
[ネットワーク図](#)
[IPアドレスを持つスニファVM](#)
[IPアドレスのないスニファVM](#)
[障害シナリオ](#)
[確認](#)
[トラブルシュート](#)
[関連情報](#)

概要

このドキュメントでは、Cisco Unified Computing System(UCS)の外部にあるトラフィックフローをキャプチャし、UCS内でスニファツールを実行する仮想マシン(VM)に転送する手順について説明します。キャプチャされるトラフィックの送信元と宛先はUCSの外部です。キャプチャは、UCSに直接接続されている物理スイッチで開始することも、数ホップ離れた場所で開始することもできます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- UCS
- VMware ESXバージョン4.1以降
- Encapsulated Remote Switch Port Analyzer(ERSPAN)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 12.2(18)ZYA3cを実行するCisco Catalyst 6503
- 2.2(3e)を実行するCisco UCS Bシリーズ
- VMWare ESXi 5.5ビルド1331820

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

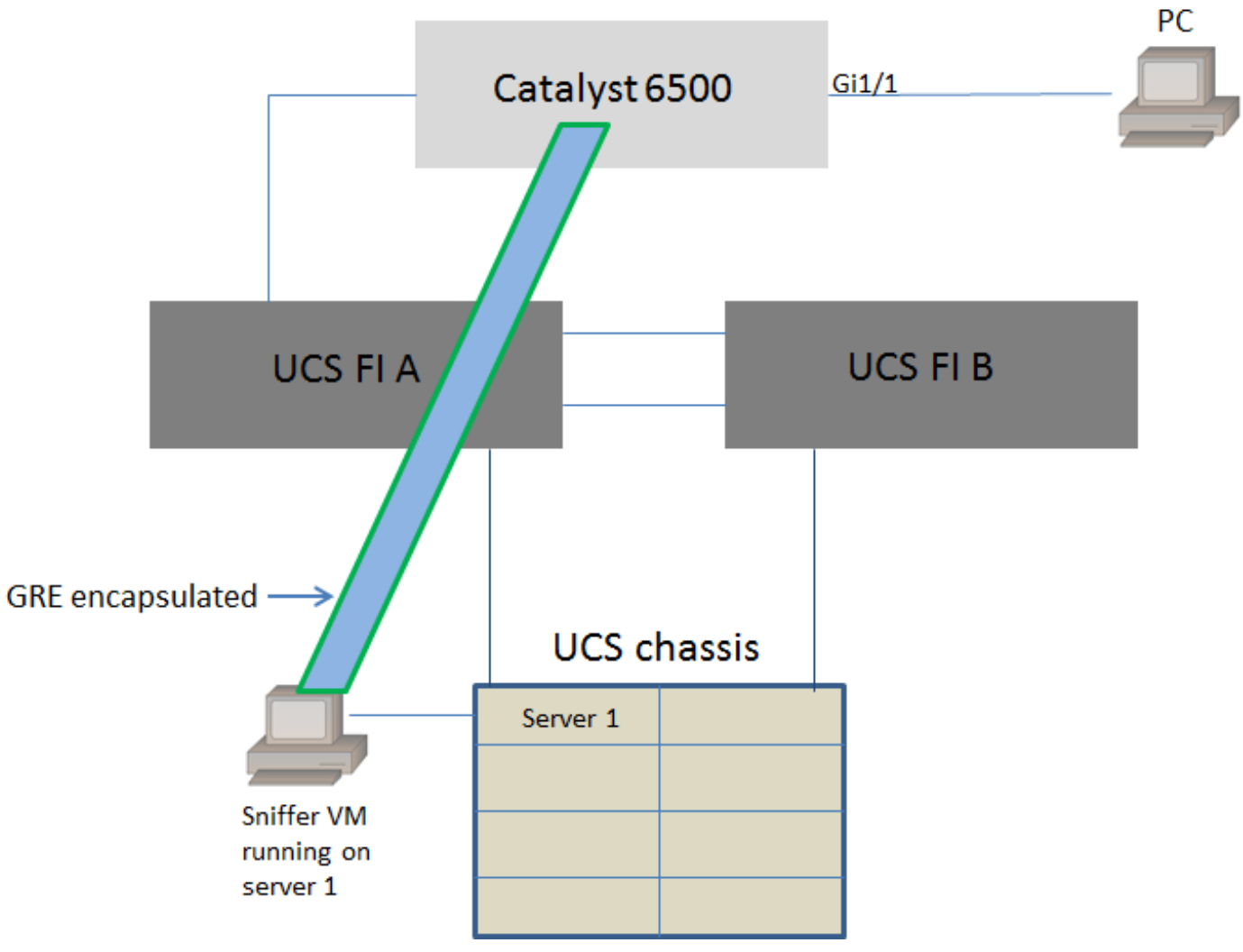
背景説明

UCSには、接続されたスイッチからSPANトラフィックを受信し、ローカルポートに送信するリモートSPAN(RSPAN)機能はありません。UCS環境でこれを実現する唯一の方法は、物理スイッチでEncapsulated RSPAN(ERSPAN)機能を使用し、IPを使用してキャプチャされたトラフィックをVMに送信することです。特定の実装では、スニファツールを実行しているVMにIPアドレスを割り当てることはできません。このドキュメントでは、スニファVMにIPアドレスがある場合に必要な設定と、IPアドレスのないシナリオについて説明します。ここでの唯一の制限は、スニファVMが送信されたトラフィックからGRE/ERSPANカプセル化を読み取れる必要があることです。

設定

ネットワーク図

このドキュメントでは、次のトポロジを考慮しています。



Catalyst 6500のGigabitEthernet1/1に接続されているPCがモニタされています。

GigabitEthernet1/1のトラフィックがキャプチャされ、サーバ1のCisco UCS内で稼働するスニファVMに送信されます。6500スイッチのERSPAN機能は、トラフィックをキャプチャし、GREを使用してカプセル化し、スニファVMののIPアドレスにに送信します。

IPアドレスを持つスニファVM

> **注**：このセクションで説明する手順は、VM上で実行するのではなく、UCSブレード上のベアメタルサーバでスニファが実行されるシナリオでも使用できます。

スニファVMにIPアドレスを設定できる場合、次の手順が必要です。

- UCS環境内のスニファVMに、6500から到達可能なIPアドレスを設定します
- VM内でスニファツールを実行します
- 6500でERSPAN送信元セッションを設定し、キャプチャされたトラフィックをVMのIPアドレスに直接送信します

6500スイッチの設定手順：

```
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
```

この例では、スニファVMのIPアドレスは192.0.2.2です

IPアドレスのないスニファVM

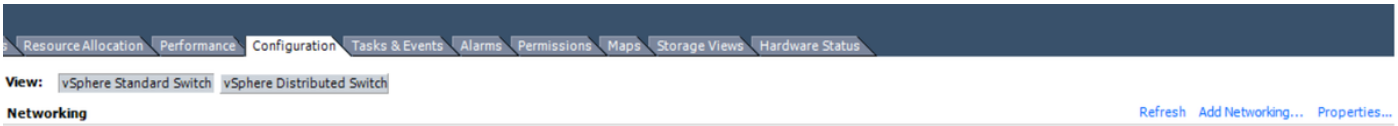
スニファVMにIPアドレスを設定できない場合、次の手順が必要です。

- UCS環境内のスニファVMの設定
- VM内でスニファツールを実行します
- 同じホストにIPアドレスを持つことができる2番目のVMを作成し、6500から到達可能なIPアドレスを使用して設定します
- VMWare vSwitchのポートグループを混合モードに設定します
- 6500でERSPAN送信元セッションを設定し、キャプチャされたトラフィックを2番目のVMのIPアドレスに送信します

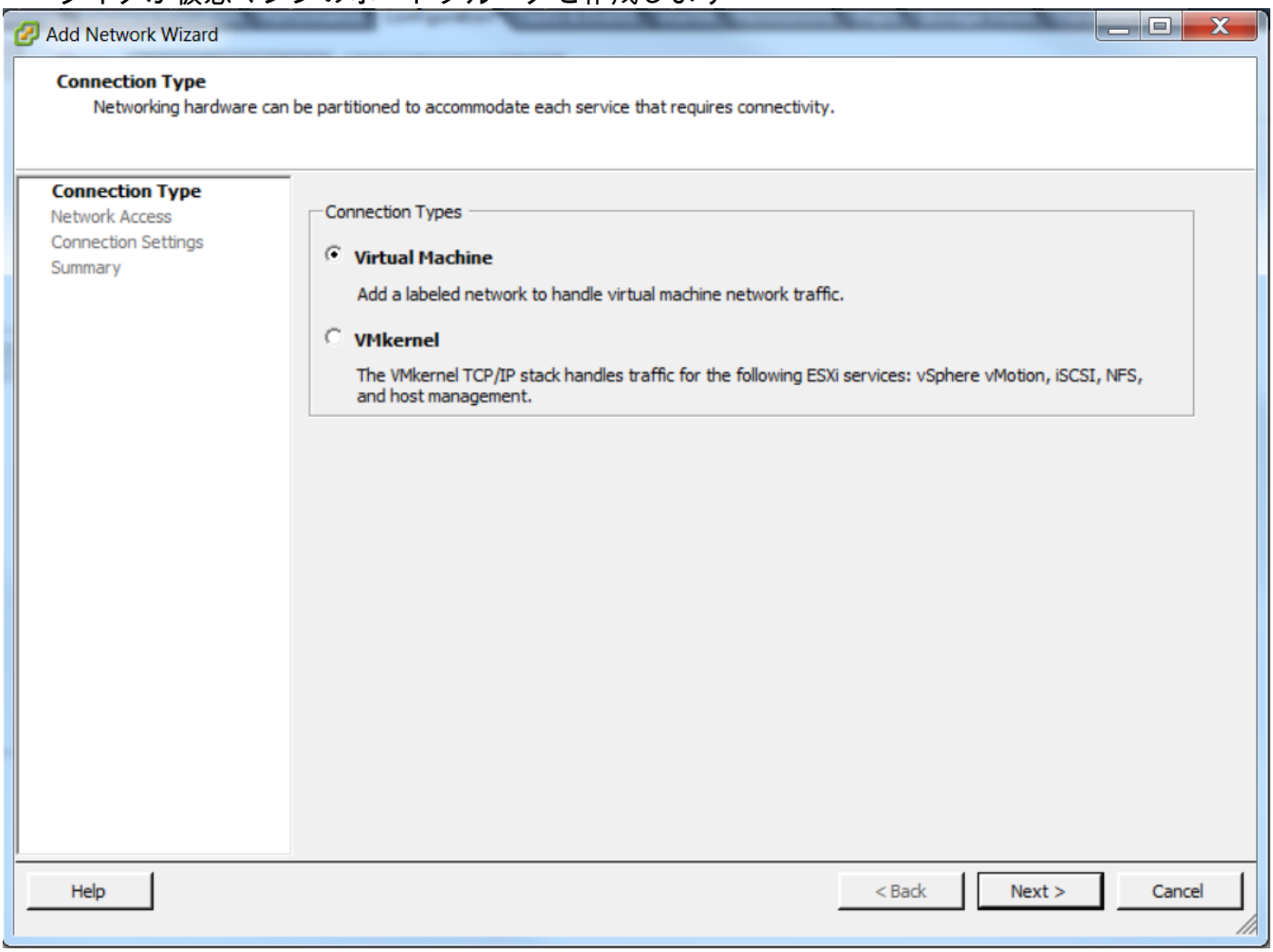
次の手順は、VMWare ESXで必要な設定を示しています。ポートグループがすでに設定されている場合は、ステップ2に直接進みます。

1.仮想マシンポートグループを作成し、2つの仮想マシンをそれに割り当てます

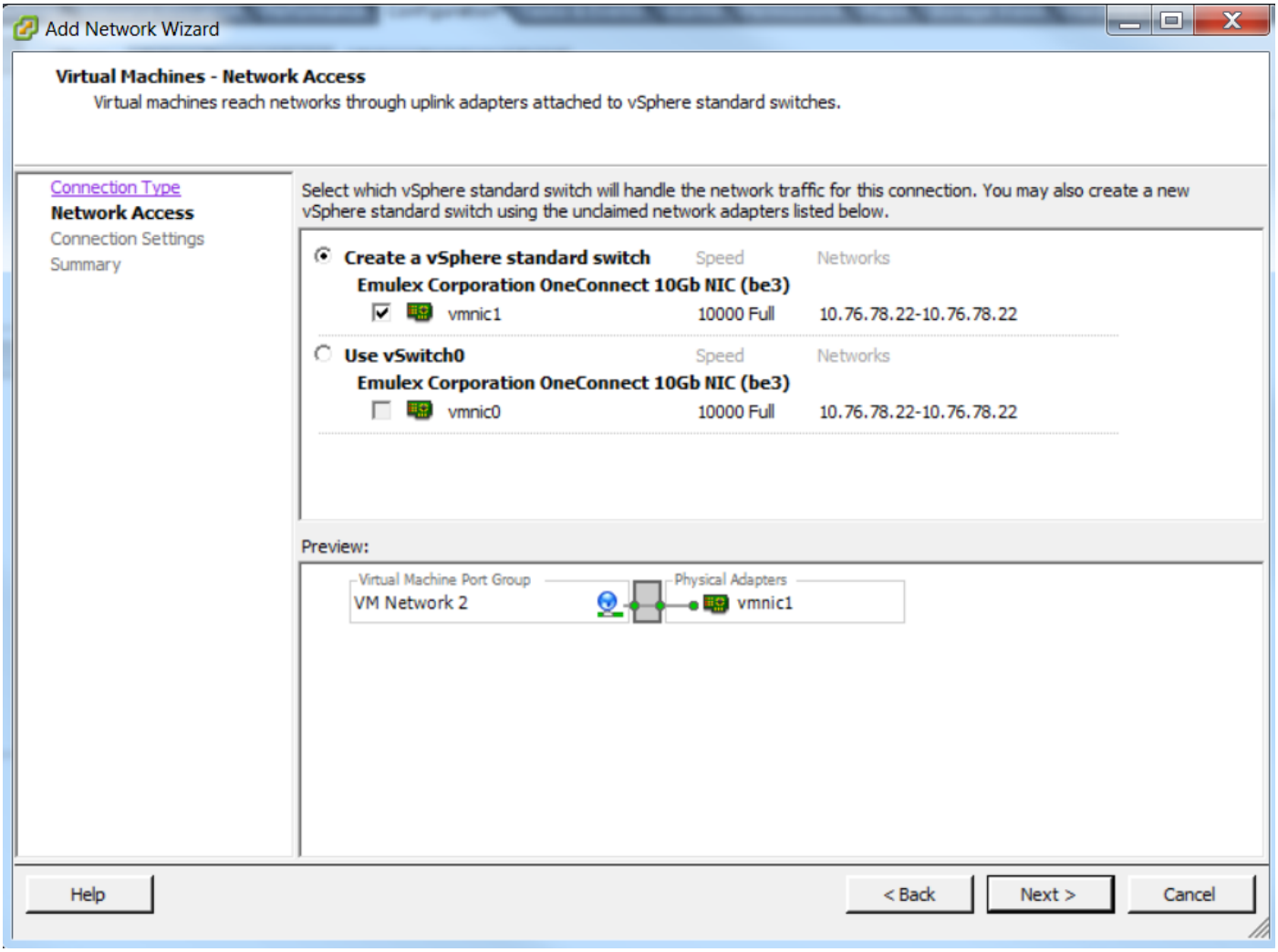
- [Networking]タブに移動し、**[vSphere Standard Switch]**の下の**[Add Networking]をクリックします**



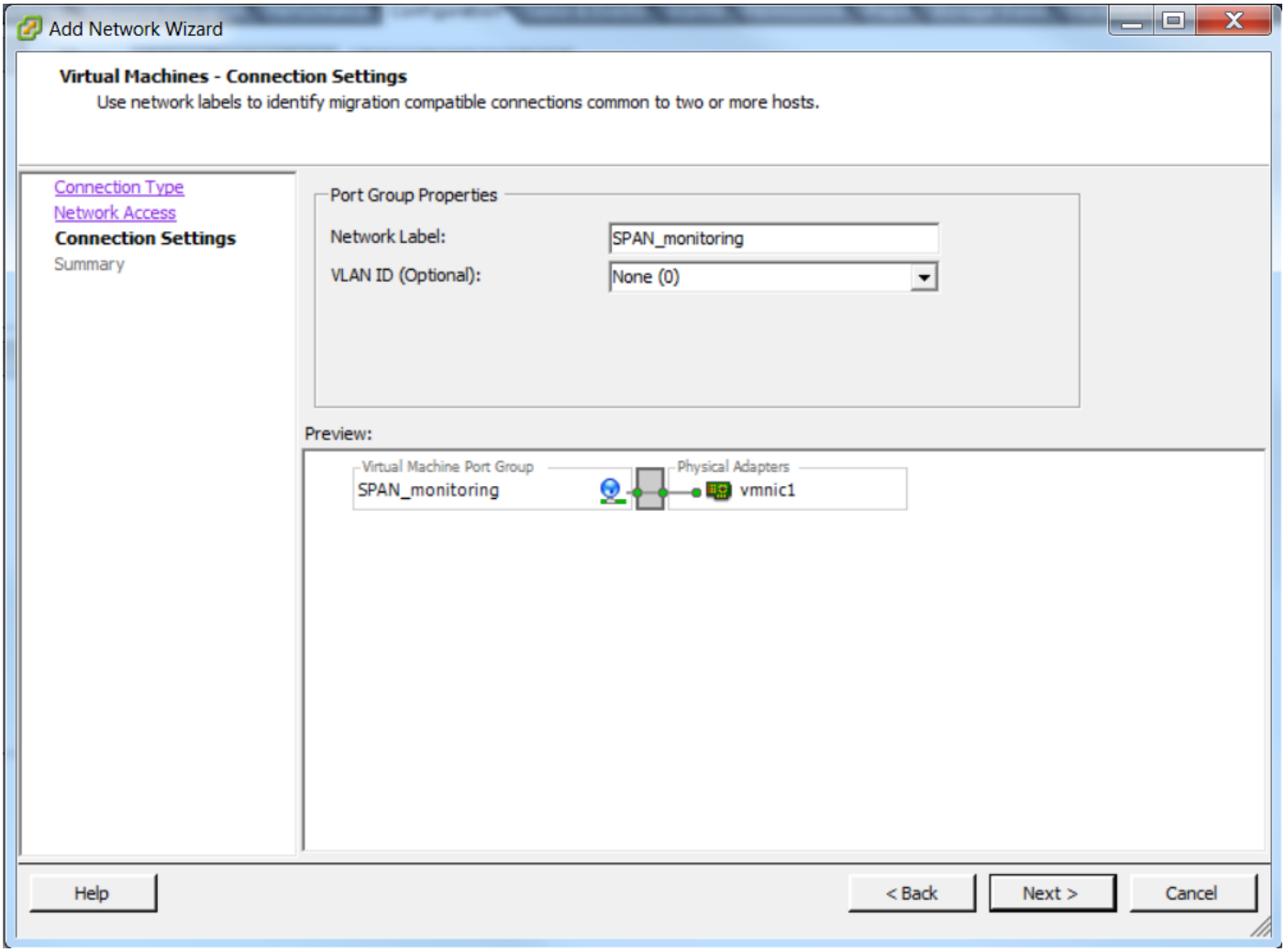
- タイプが仮想マシンのポートグループを作成します



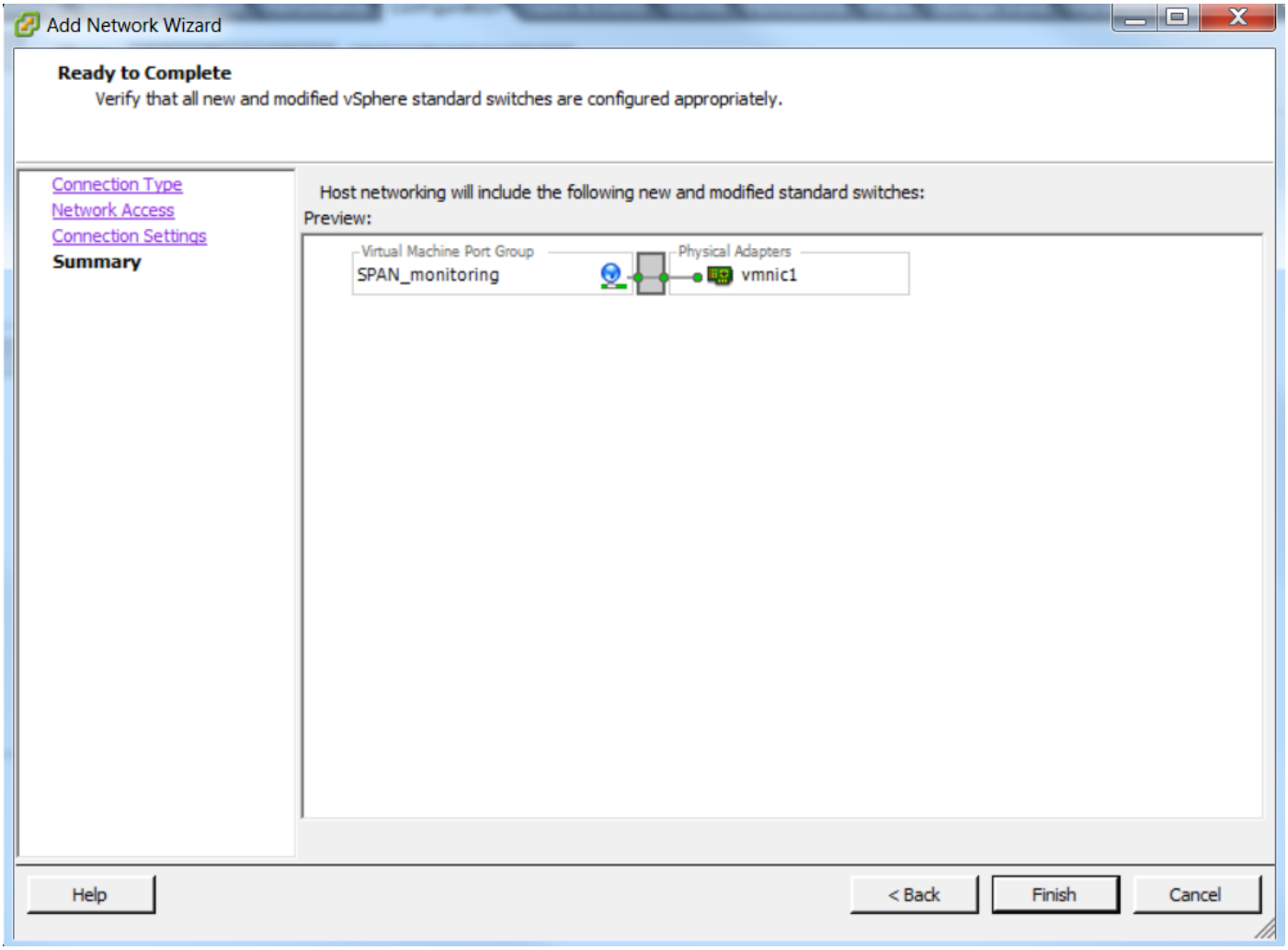
- 次の図に示すように、物理インターフェイス(vmnic)をポートグループに割り当てます。



- 図に示すように、ポートグループの名前を設定し、関連するVLANを追加します。



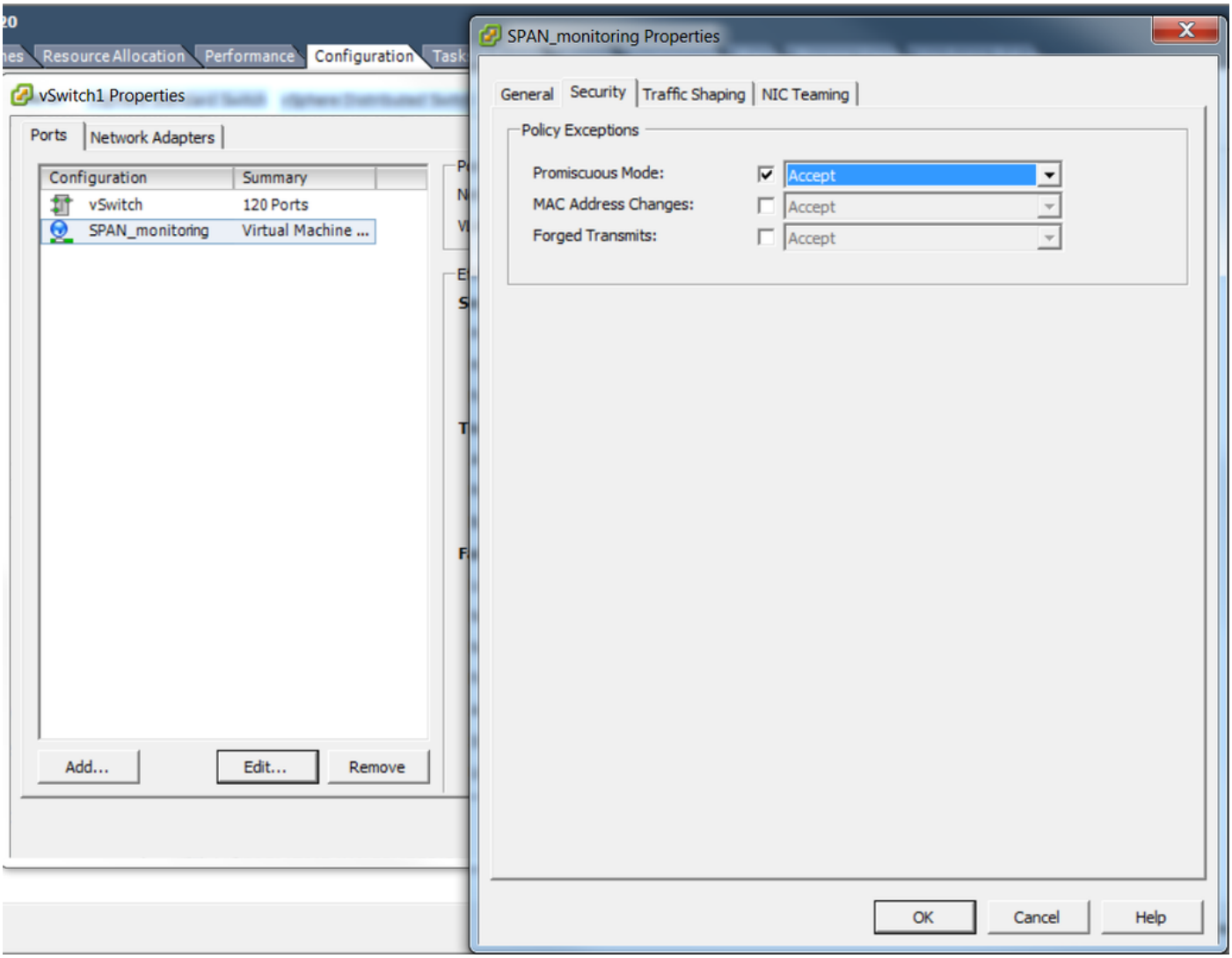
- 設定を確認し、図に示すように[Finish]をクリックします。



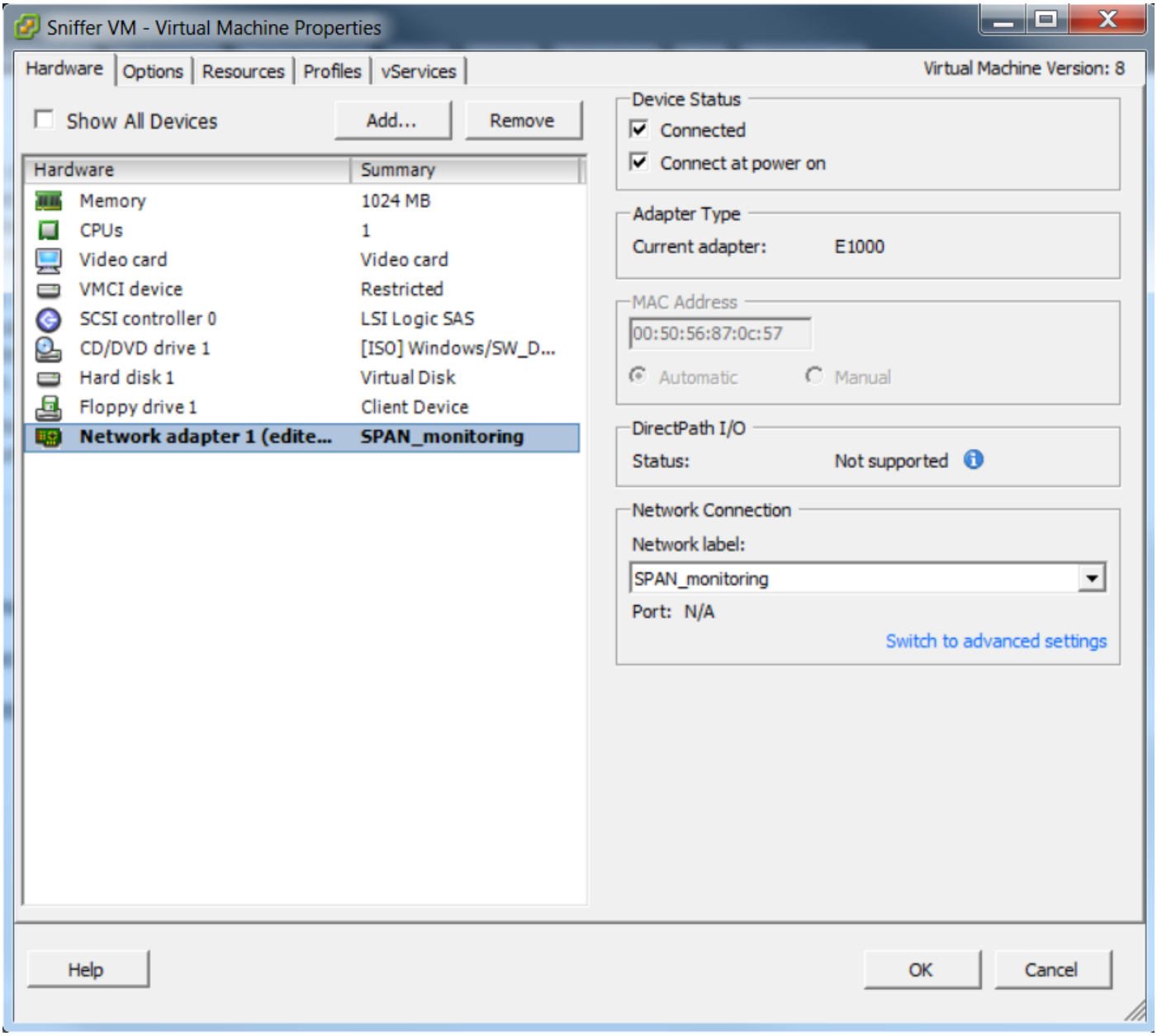
2.図に示すように、ポートグループを無差別モードに設定します。

- ポートグループは、[Networking]タブの下に表示される必要があります
- [プロパティ]をクリックします

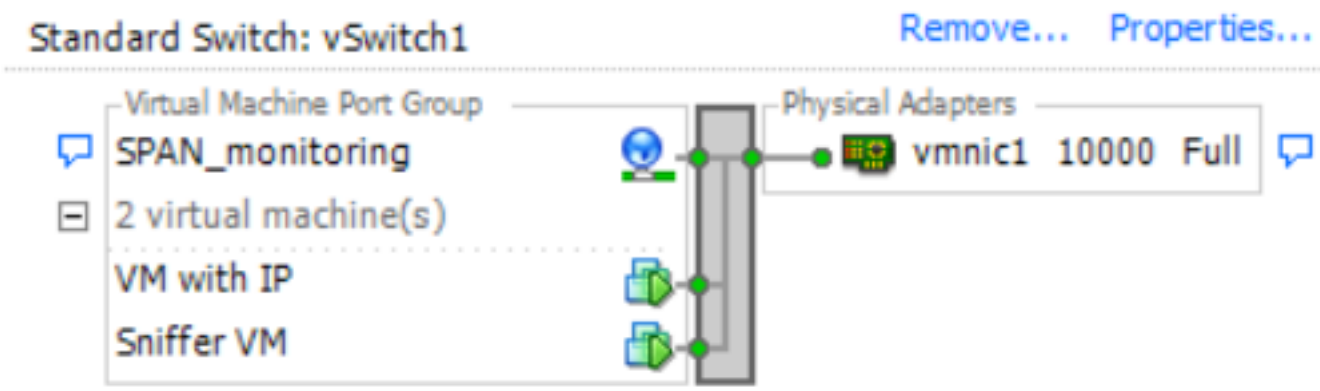
- ポートグループを選択し、[Edit]をクリックします
- 次の図に示すように、[Security]タブに移動し、[Promiscuous mode]の設定を[Accept]に変更します



3. 2台の仮想マシンを、仮想マシン設定セクションからポートグループに割り当てます。



4. 2台の仮想マシンがポートグループのNetworkingタブに表示されます。



この例では、IPアドレスを持つ2番目のVMがIPを持つVMであり、Sniffer VMはIPアドレスを持たないスニファツールを持つVMです。

5.6500スイッチの設定手順を次に示します。

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

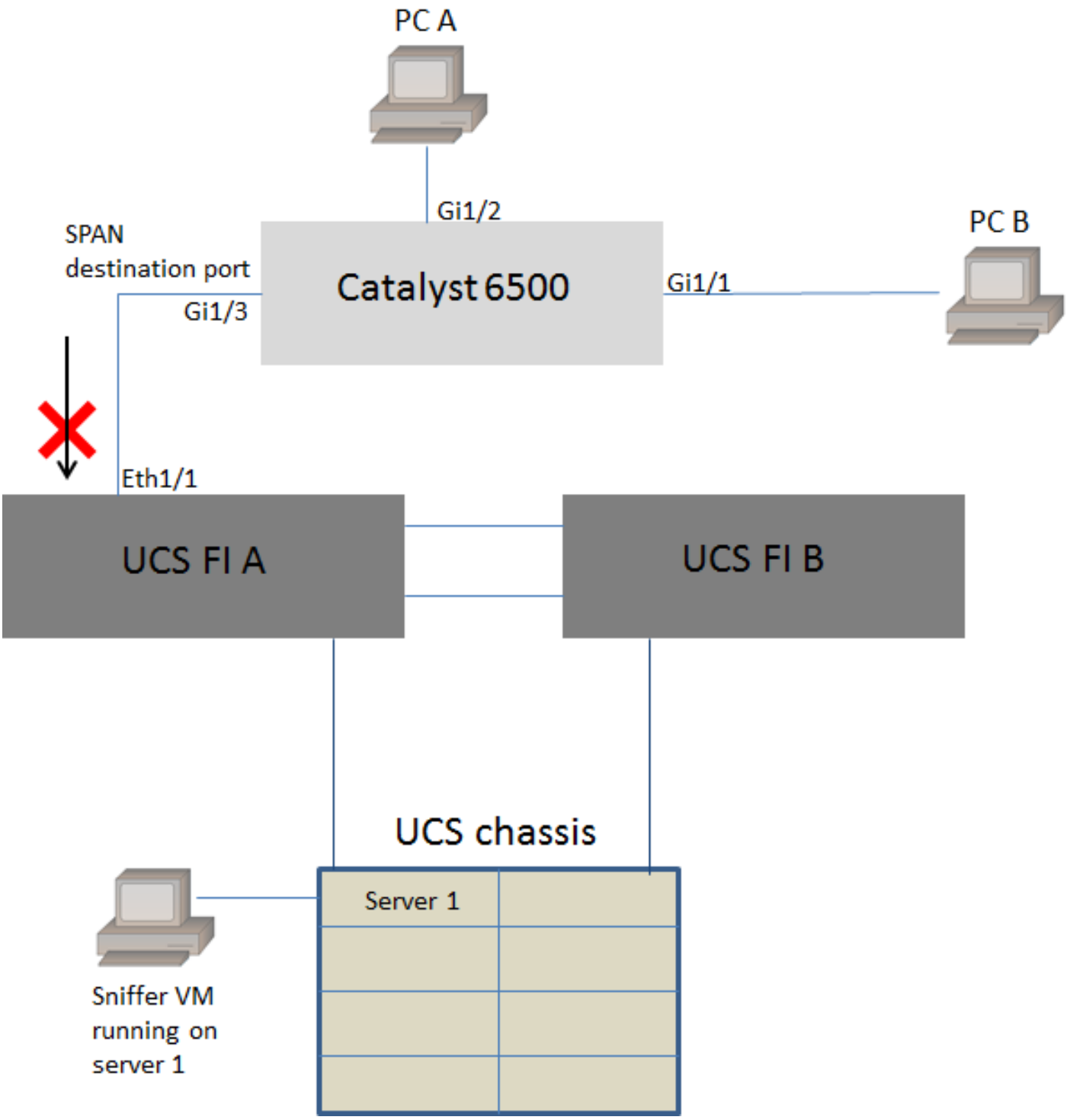
```
CAT6K-01(config-mon-erspan-src)#source interface gi1/1
CAT6K-01(config-mon-erspan-src)#destination
CAT6K-01(config-mon-erspan-src-dst)#ip address 192.0.2.3
CAT6K-01(config-mon-erspan-src-dst)#origin ip address 192.0.2.1
CAT6K-01(config-mon-erspan-src-dst)#erspan-id 1
CAT6K-01(config-mon-erspan-src-dst)#exit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

この例では、2番目のVM（IPを持つVM）のIPアドレスは192.0.2.3です。

この設定では、6500はキャプチャされたパケットをカプセル化し、IPアドレスを持つVMに送信します。VMWare vSwitchの混合モードでは、スニファVMがこれらのパケットも表示できます。

障害シナリオ

この項では、ERSPAN機能の代わりに物理スイッチでローカルSPAN機能を使用する場合の一般的な障害シナリオについて説明します。次のトポロジが考慮されます。



PC AからPC Bへのトラフィックは、ローカルSPAN機能を使用してモニタされます。SPANトラフィックの宛先は、UCSファブリックインターコネクト(FI)に接続されたポートに向けられます。

スニファツールを備えた仮想マシンは、サーバ1のUCS内で動作します。

6500スイッチの設定を次に示します。

```
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
```

ポートGig1/1およびGig1/2を流れるすべてのトラフィックは、ポートGig1/3に複製されます。これらのパケットの送信元と宛先のMACアドレスは、UCS FIでは認識されません。

UCSイーサネットエンドホストモードでは、FIがこれらの不明なユニキャストパケットをドロップします。

UCSイーサネットスイッチングモードでは、FIは6500(Eth1/1)に接続されたポートの送信元MACアドレスを学習し、ダウンストリームのパケットをサーバにフラッディングします。次の一連のイベントが発生します。

1. 理解しやすいように、PC A(mac-address aaaa.aaaa.aaaa)とPC B(mac-address bbbb.bbbb.bbbb)の間（Gig1/1とGig1/2のインターフェイス）でのみ行われるトラフィックを検討します
2. 最初のパケットはPC AからPC Bに送信され、これはUCS FI Eth1/1に表示されます
3. FIはEth1/1でmac-address aaaa.aaaa.aaaaを学習します
4. FIは宛先mac-address bbbb.bbbb.bbbbを認識せず、同じVLAN内のすべてのポートにパケットをフラッディングします
5. 同じVLAN内のスニファVMにも、このパケットが表示されます
6. 次のパケットはPC BからPC Aです
7. これがEth1/1にヒットすると、mac-address bbbb.bbbb.bbbbがEth1/1で学習されます
8. パケットの宛先はmac-address aaaa.aaaa.aaaaです
9. FIは、Eth1/1でmac-address aaaa.aaaa.aaaaが学習され、パケットがEth1/1自体で受信されたとして、このパケットをドロップします
10. mac-address aaaa.aaaa.aaaaまたはmac-address bbbb.bbbb.bbbb宛ての後続のパケットも、同じ理由で廃棄されます

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- 仮想スイッチまたはポートグループでの無差別モードの設定
- Catalyst 6500でのSPAN、RSPAN、およびERSPAN
- オープンソースツールによるERSPANトラフィックのカプセル化解除
- テクニカル サポートとドキュメント – Cisco Systems