

# 配置在UCS前端服务器的虚拟机作为SPAN目的地

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[背景信息](#)

[Configure](#)

[Network Diagram](#)

[嗅探器VM用IP地址](#)

[没有IP地址的嗅探器VM](#)

[故障情景](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

## Introduction

本文描述步骤捕获完全是思科统一计算系统的通信流(UCS)的外部和处理它到运行一个嗅探器工具在UCS里面的虚拟机。是的数据流的来源和目的地获取的是UCS的外部。捕获在直接地附有UCS的一台物理交换机可以被启动或它可能是一些次跳跃。

## Prerequisites

### Requirements

Cisco 建议您了解以下主题：

- UCS
- VMware ESX版本4.1或以上
- 被封装的远程交换机端口分析程序(ERSPAN)

### Components Used

本文档中的信息基于以下软件和硬件版本：

- 运行12.2(18)ZYA3c的Cisco Catalyst 6503
- 运行2.2(3e)的Cisco UCS B系列
- VMWare ESXi 5.5修造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.

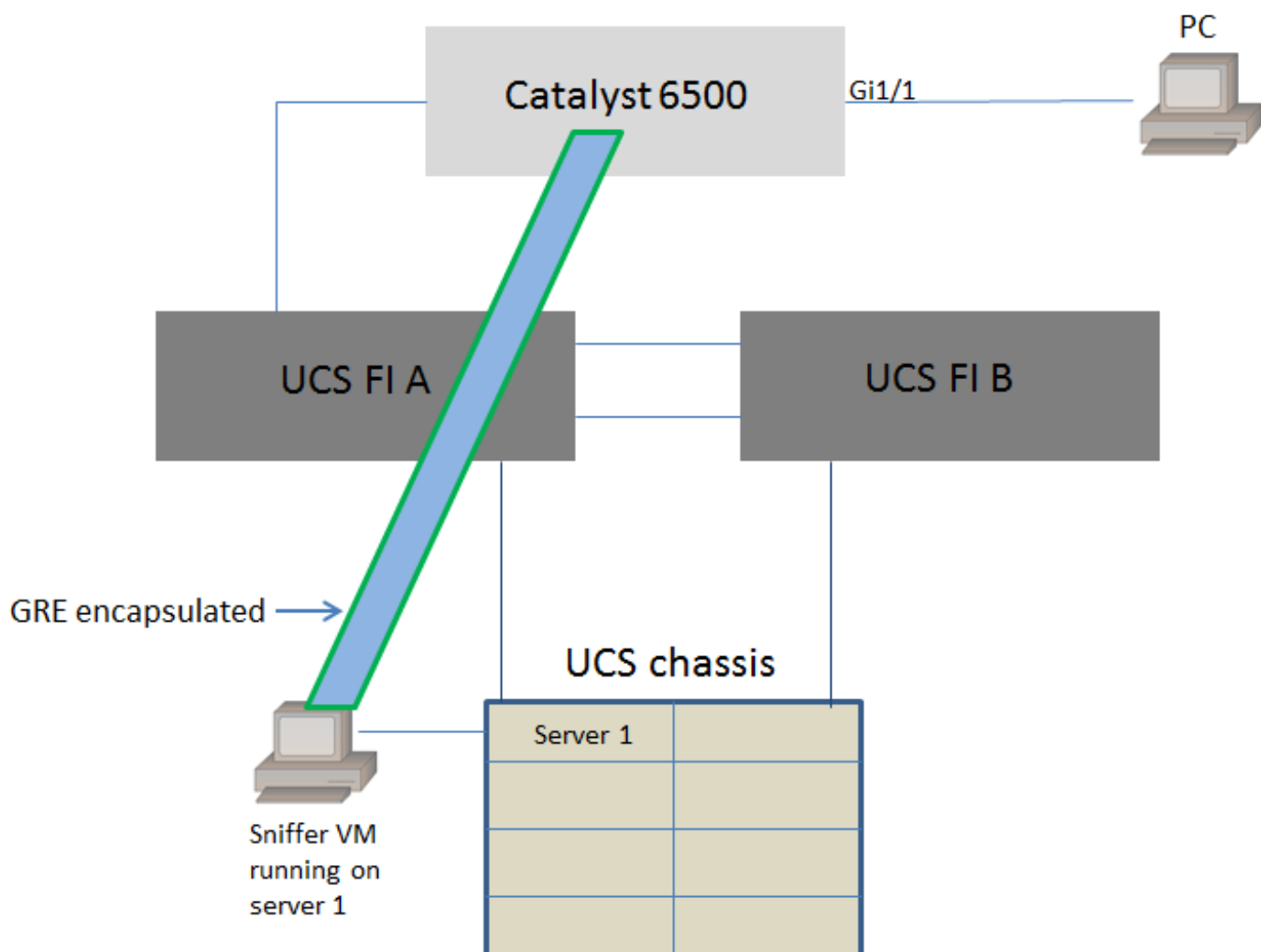
## 背景信息

UCS没有远程SPAN (RSPAN)功能收到SPAN数据流从一台连接的交换机和处理它对一个本地端口。因此完成此的唯一方法在UCS环境里是通过使用在一台物理交换机和发送捕获的流量的被封装的RSPAN (ERSPAN)功能到VM使用IP。在某些实施，运行嗅探器工具的VM不能有IP地址。当嗅探器VM有一个IP地址以及方案，不用IP地址时，本文解释需要的配置。这里唯一的限制是嗅探器VM需要能读从被发送到它的数据流的GRE/ERSPAN封装。

## Configure

### Network Diagram

此拓扑在本文考虑：



PC附有Catalyst 6500的GigabitEthernet1/1被监控。在GigabitEthernet1/1的数据流是获取和发送到运行在服务器1. ERSPAN功能的Cisco UCS里面在6500交换机捕获数据流，封装它使用GRE的嗅探器VM并且发送它到嗅探器VM的IP地址。

### 嗅探器VM用IP地址

**Note:**在此部分描述的步骤可以也用于嗅探器在UCS前端的一个仅有金属服务器运行的方案而不是运行在VM。

这些步骤，当嗅探器VM能有IP地址时，需要：

- 用从6500是可达的IP地址配置嗅探器VM在UCS环境里面
- 运行嗅探器工具在VM里面
- 配置在6500的一次ERSPAN来源会话并且发送捕获的流量直接地到VM的IP地址

在6500交换机的配置步骤：

```
CAT6K-01(config)#monitor session 1 type erspan-source
CAT6K-01(config-mon-erspan-src)#source interface gil/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
```

在本例中，嗅探器VM的IP地址是192.0.2.2

## 没有IP地址的嗅探器VM

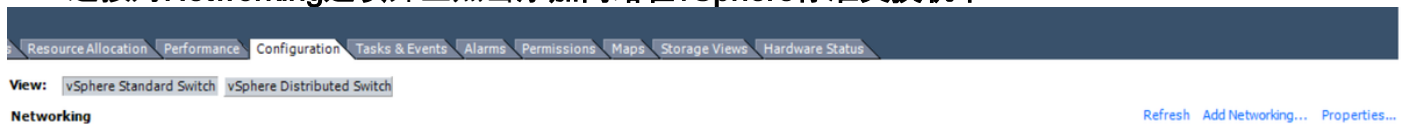
这些步骤，当嗅探器VM不能有IP地址时，需要：

- 配置嗅探器VM在UCS环境里面
- 运行嗅探器工具在VM里面
- 创建能有在同一台主机的一个IP地址和用IP地址配置它从6500是可达的秒钟VM
- 配置在VMWare vSwitch的端口组在混杂模式下
- 配置在6500的一次ERSPAN来源会话并且发送捕获的流量到第二个VM的IP地址

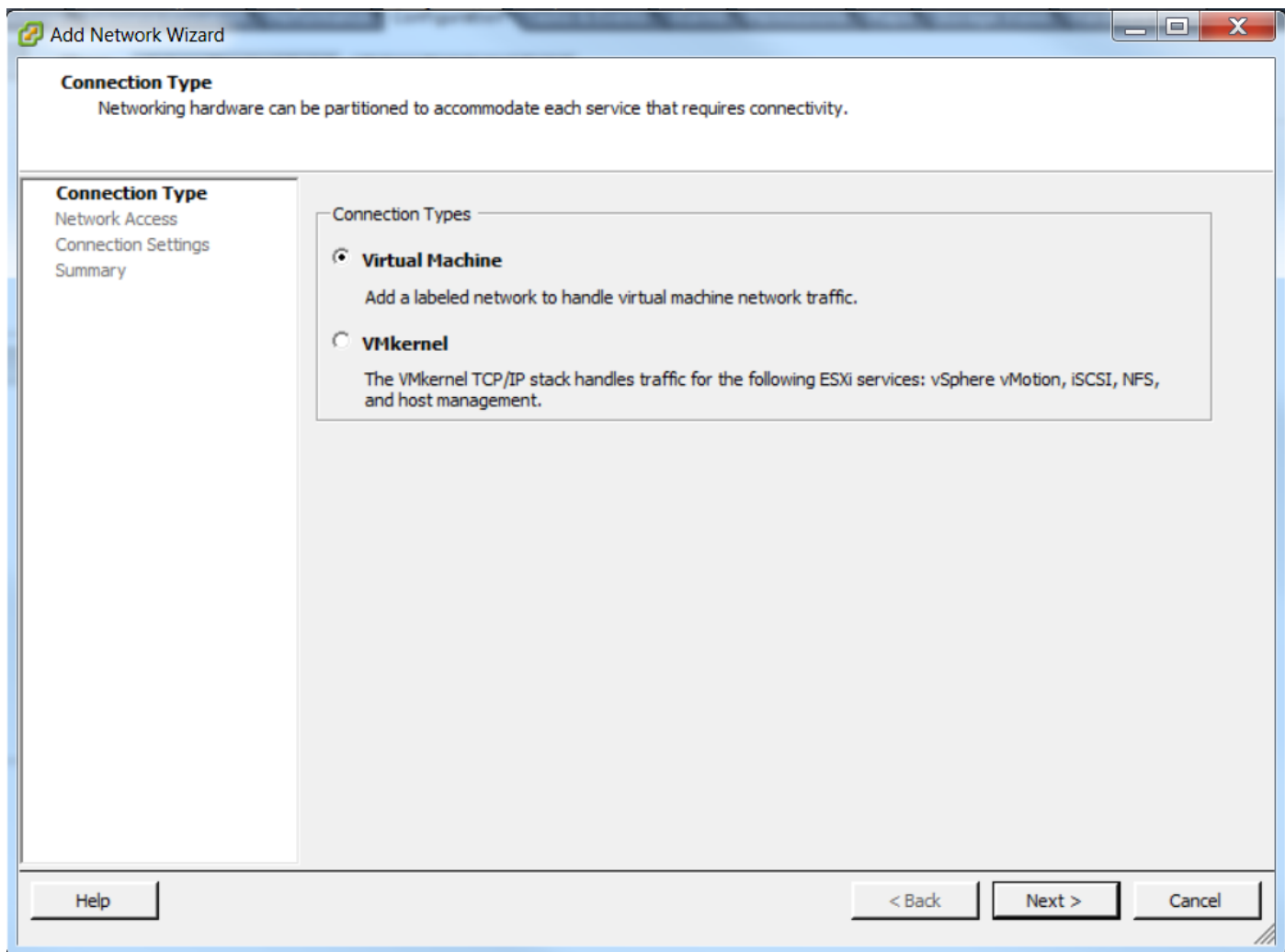
这些步骤显示在VMWare需要的配置ESX：如果已经安排一个端口组配置，请直接地进入步骤2。

1. 创建一个虚拟机端口组并且分配两台虚拟机到它

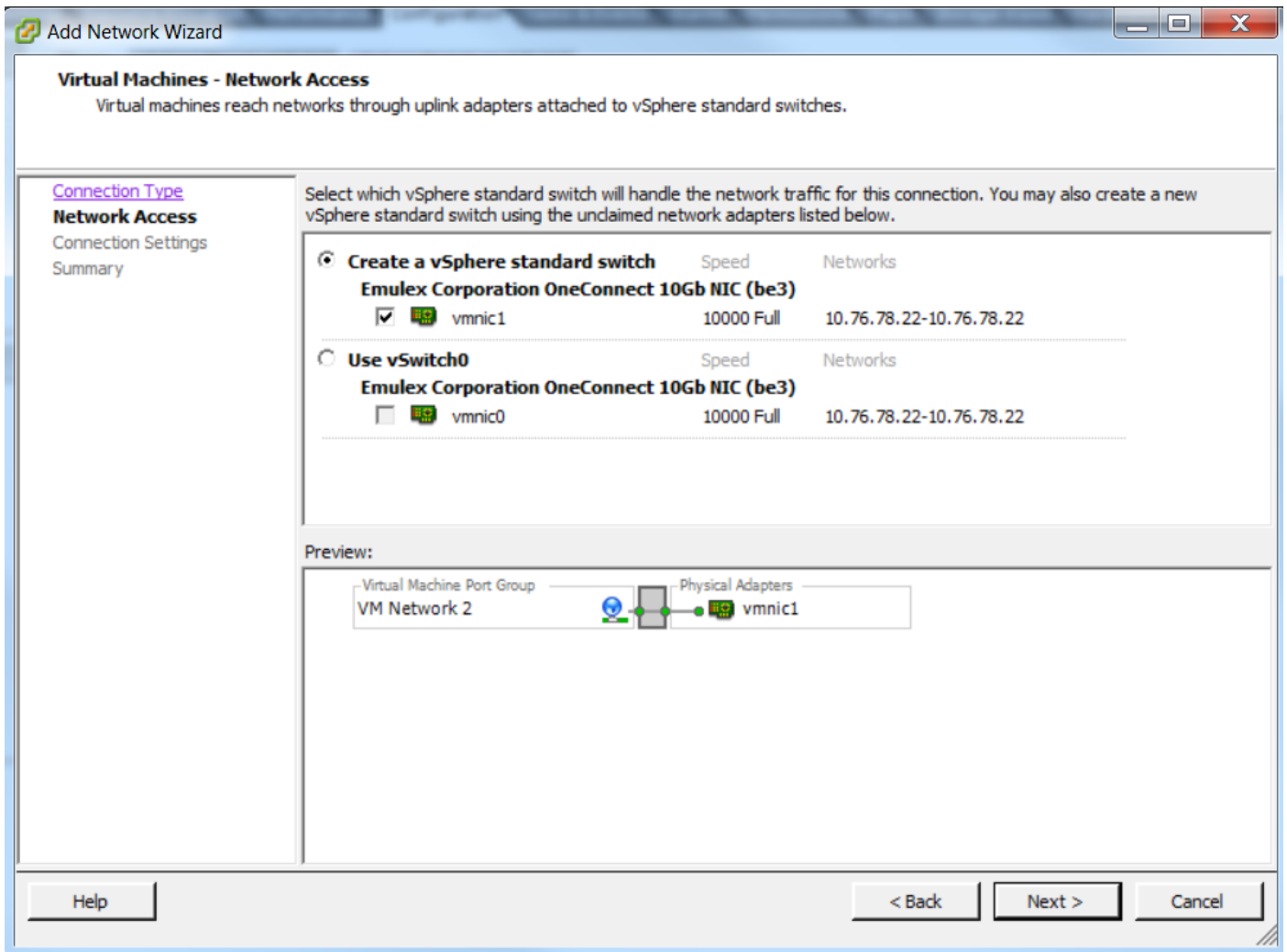
- 连接对**Networking**选项并且点击**添加网络在vSphere标准交换机下**



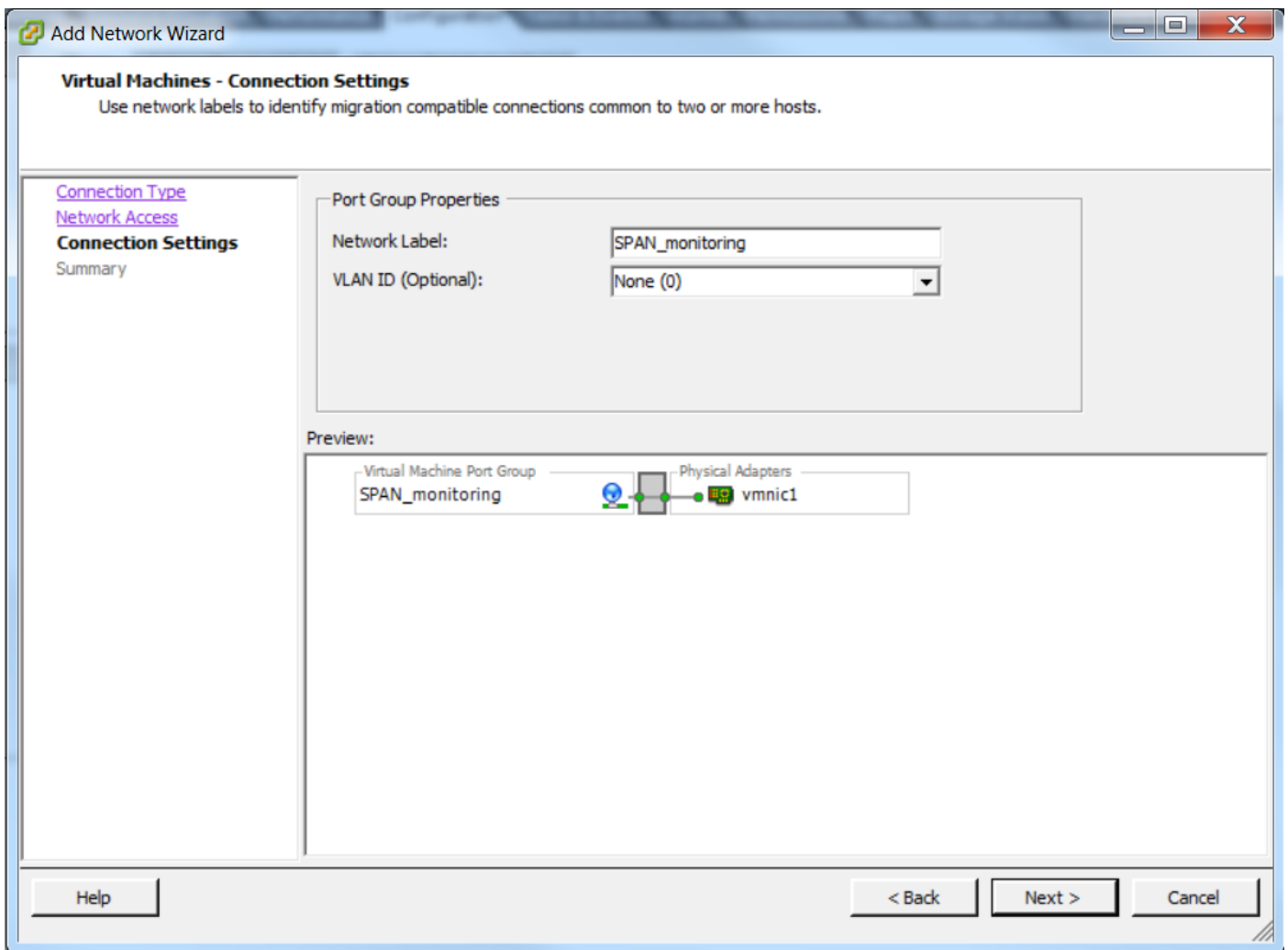
- 创建一个端口组类型虚拟机



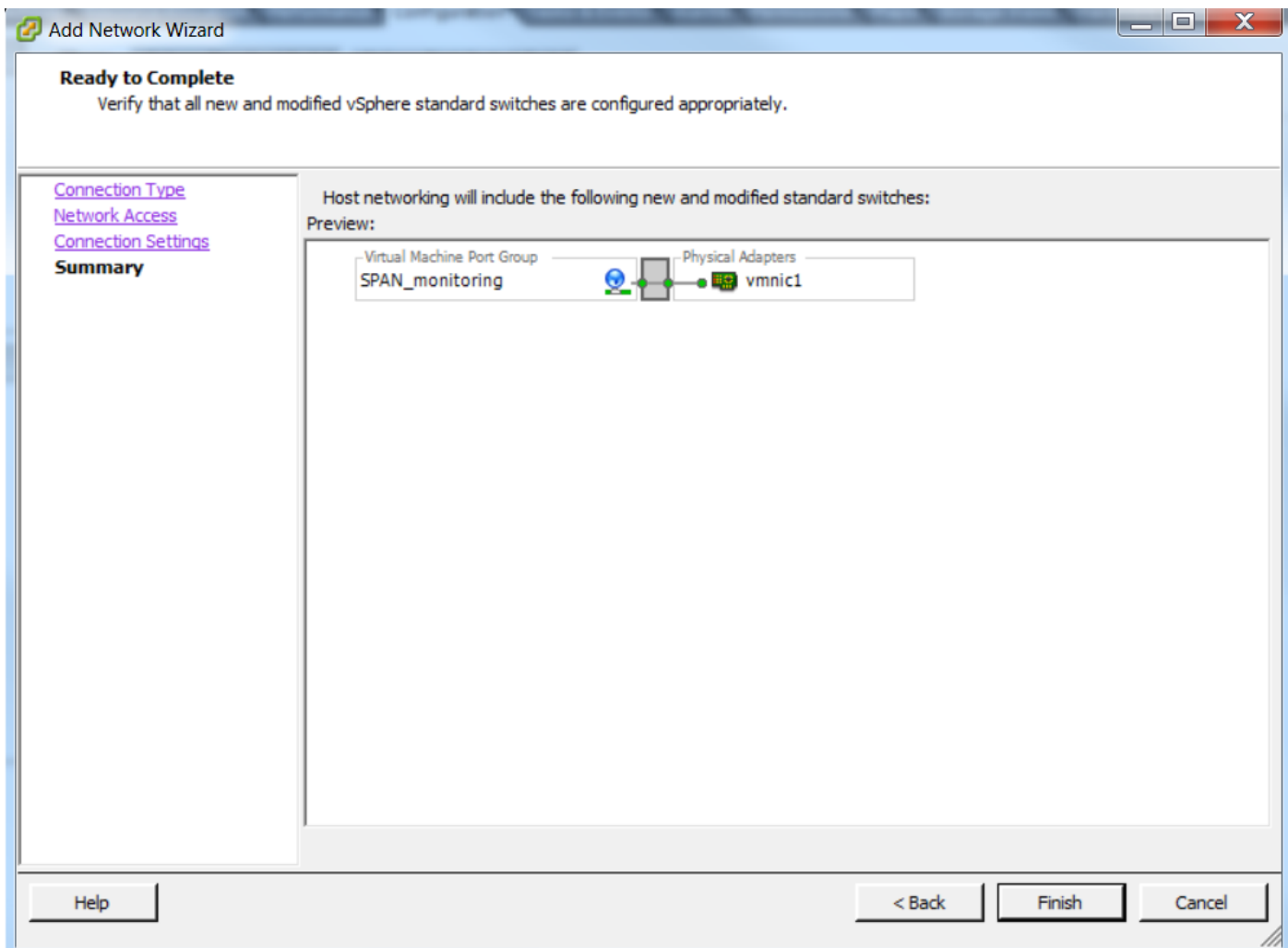
- 分配一个物理接口(vmnic)如此镜像所显示，到端口组。



- 如镜像所显示，配置一个名字对于端口组和添加相关VLAN。



- 如镜像所显示，验证配置并且点击完成。

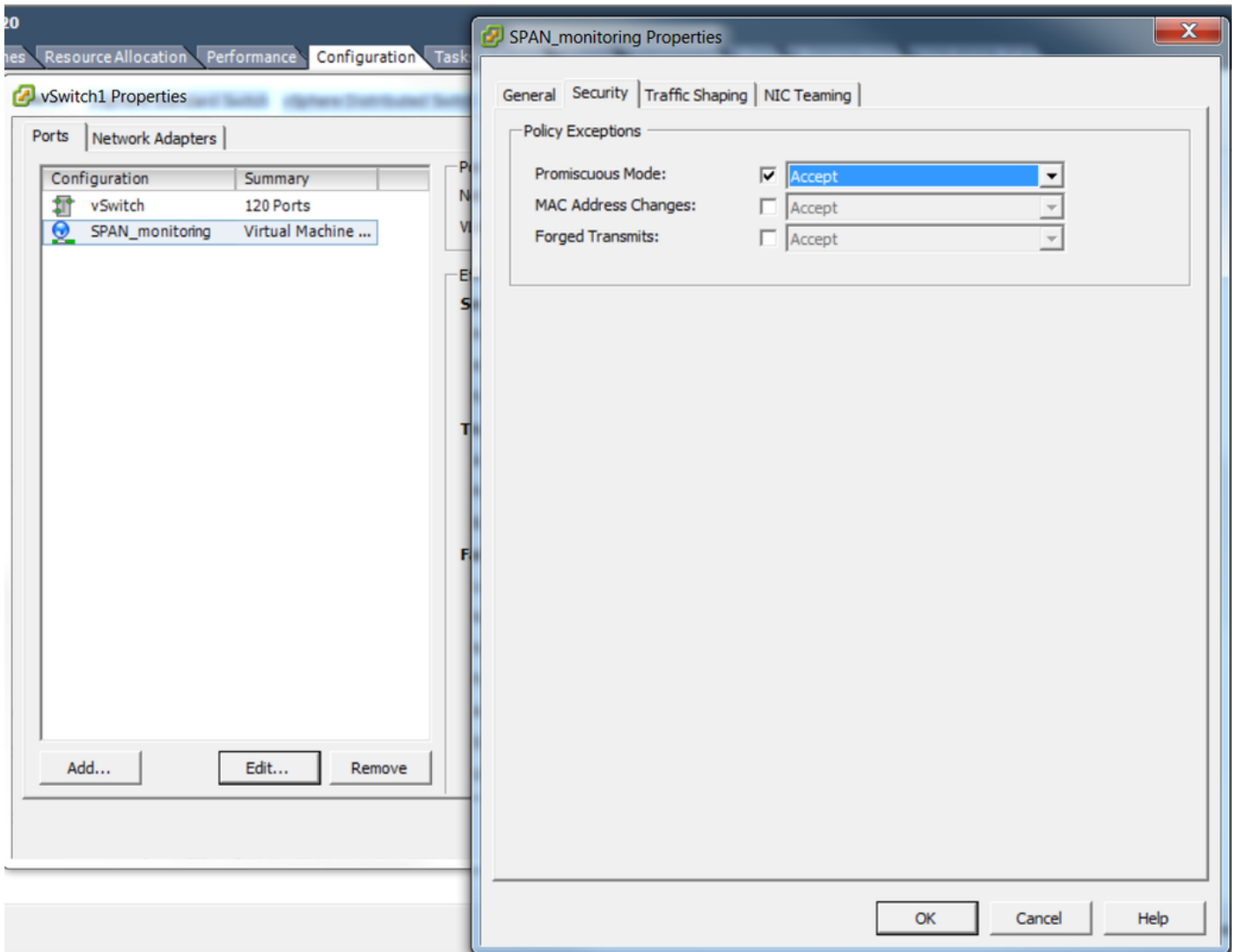


2. 如镜像所显示，配置端口组在混杂模式下。

- 端口组必须当前出现在**Networking**选项下
- 点击**属性**

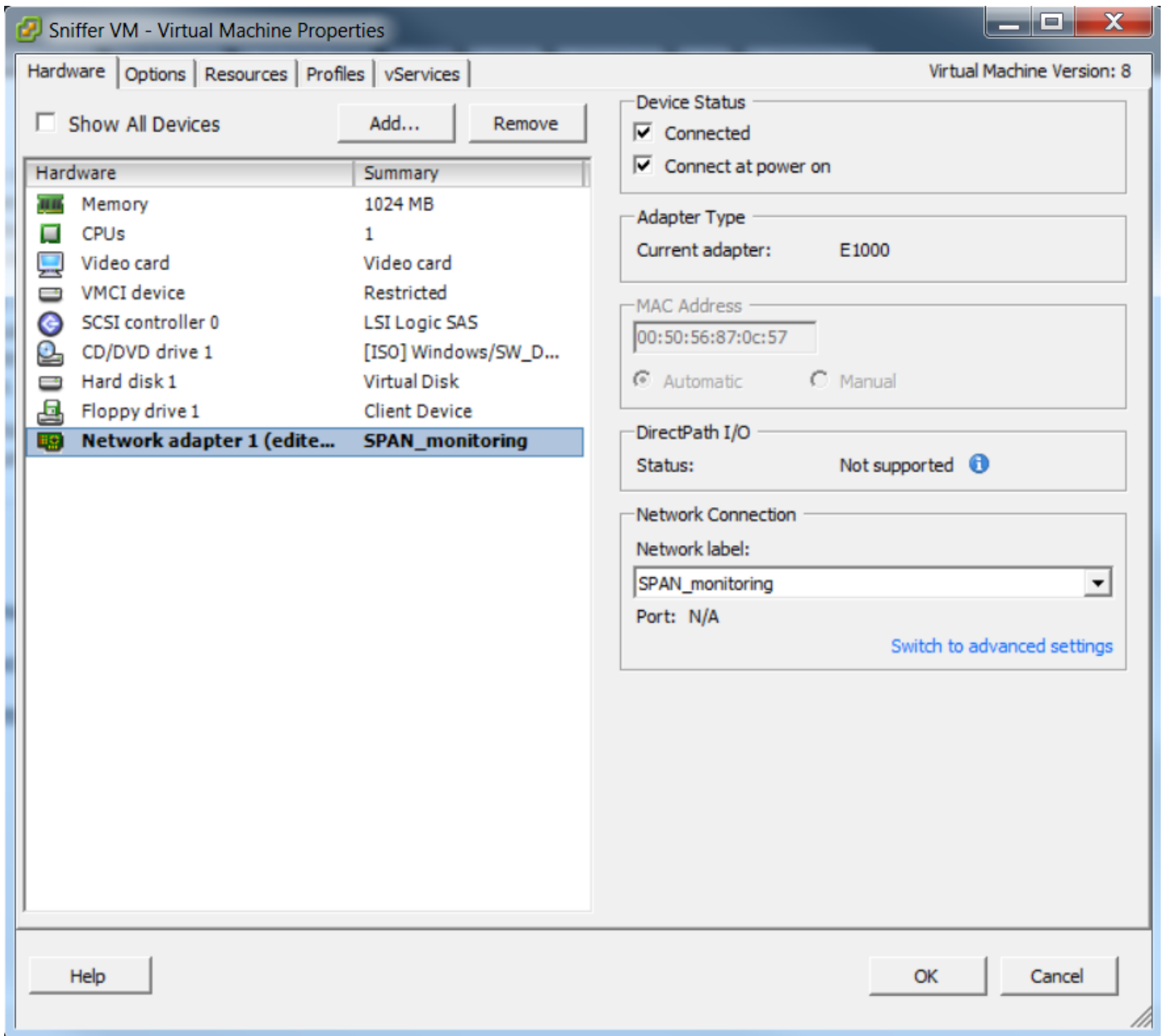


- 选择端口组并且点击**编辑**
- 如此镜像所显示，去**安全**选项并且更改混杂模式设置接受

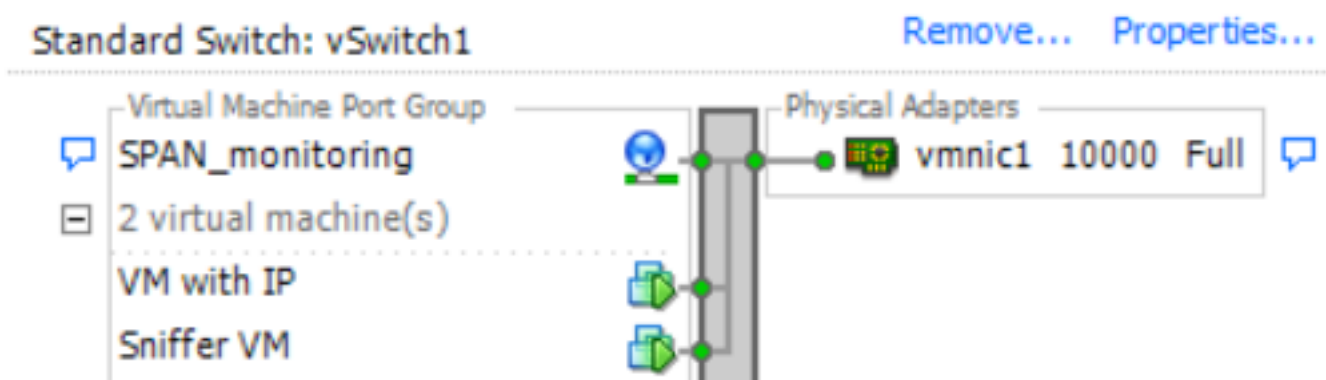


3. 分配两台虚拟机到从虚拟机设置部分的端口组。





4. 两台虚拟机必须当前出现于端口组在Networking选项下。



在本例中，与没有IP地址，有一个IP地址，并且嗅探器VM是VM用嗅探器工具的IP的VM是第二个VM。

5. 这显示在6500交换机的配置步骤：

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

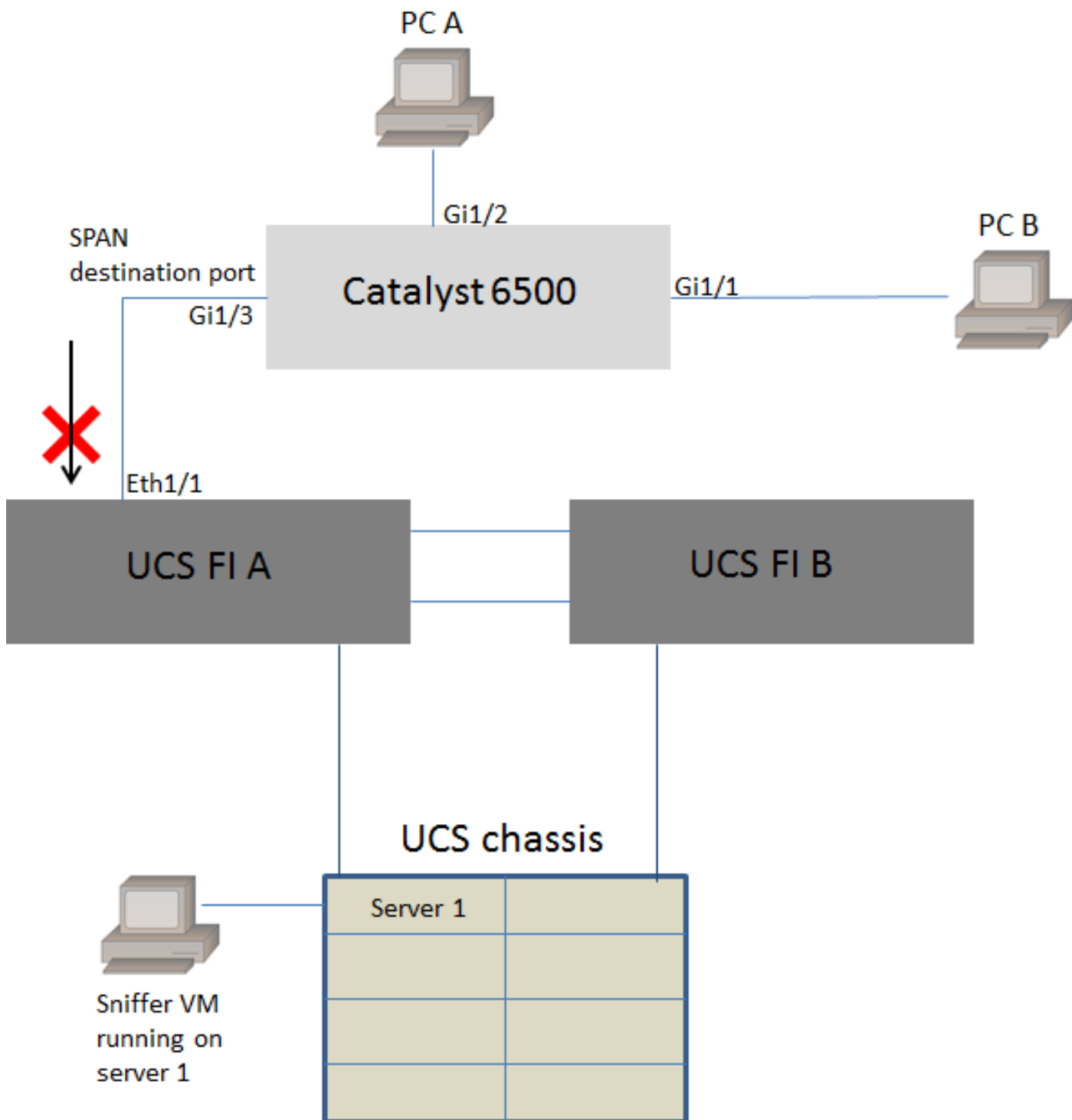
```
CAT6K-01(config-mon-erspan-src)#source interface gi1/1
CAT6K-01(config-mon-erspan-src)#destination
CAT6K-01(config-mon-erspan-src-dst)#ip address 192.0.2.3
CAT6K-01(config-mon-erspan-src-dst)#origin ip address 192.0.2.1
CAT6K-01(config-mon-erspan-src-dst)#erspan-id 1
CAT6K-01(config-mon-erspan-src-dst)#exit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

在本例中，第二个VM (与IP的VM的) IP地址是192.0.2.3。

使用此配置，6500封装获取信息包并且发送它到VM用IP地址。在VMWare vSwitch enable (event)的混杂模式看到这些信息包的嗅探器VM。

## 故障情景

当曾经在一台物理交换机的本地SPAN功能而不是ERSPAN功能时，此部分描述一个常见故障方案。此拓扑考虑得这里：



使用本地SPAN功能，从PC A的数据流对PC B被监控。SPAN数据流的目的地处理对端口被连接到UCS结构互连(FI)。

虚拟机用嗅探器工具运行在server1的UCS里面。

这是在6500交换机的配置：

```
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
```

在端口Gig1/1和Gig1/2的所有数据流将被复制对端口Gig1/3。这些信息包源及目的地MAC地址将是未知对UCS FI。

在UCS以太网终端主机模式下，FI丢弃这些未知单播信息包。

在UCS以太网交换模式，FI了解在端口的源MAC地址被连接到6500 (Eth1/1)然后充斥信息包下行到服务器。此事件顺序发生：

1. 对于方便了解，请考虑仅去在接口Gig1/1和Gig1/2的PC A (与MAC地址aaaa.aaaa.aaaa)和PC B之间的数据流(与MAC地址bbbb.bbbb.bbbb)
2. 第一个信息包是从PC A到PC B，并且这在UCS FI Eth1/1被看到
3. FI了解在Eth1/1的MAC地址aaaa.aaaa.aaaa
4. FI不认识目的地MAC地址bbbb.bbbb.bbbb并且充斥信息包对在同样VLAN的所有端口
5. 嗅探器VM，在同样VLAN，也看到此信息包
6. 下一个信息包是从PC B到PC A
7. 当这击中Eth1/1时，MAC地址bbbb.bbbb.bbbb在Eth1/1了解
8. 信息包的目的地是为MAC地址aaaa.aaaa.aaaa
9. FI丢弃此信息包，当MAC地址aaaa.aaaa.aaaa在Eth1/1了解，并且信息包在Eth1/1收到了
10. 后续信息包，注定为MAC地址aaaa.aaaa.aaaa或MAC地址bbbb.bbbb.bbbb由于同样的原因被丢弃

## Verify

当前没有可用于此配置的验证过程。

## Troubleshoot

目前没有针对此配置的故障排除信息。

## Related Information

- [配置在虚拟交换机或portgroup的混杂模式](#)
- [SPAN、RSPAN和ERSPAN在Catalyst 6500](#)
- [皮膜剥脱术ERSPAN数据流用开放源工具](#)
- [Technical Support & Documentation - Cisco Systems](#)