目录

简介

本文描述步骤捕获是完全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。

捕获的流量的源和目的是UCS的外部。捕获在直接地附加对UCS的一物理交换机可以启动或它可能是离开一些的跳。

先决条件

要求

思科建议您有这些主题运行知识：

- 思科统一计算系统(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)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科Catalyst 6503运行的12.2(18)ZYA3c
- 思科UCS B系列运行2.2(3e)
- VMWare ESXi 5.5构建1331820

背景信息

UCS没有远程SPAN (RSPAN)功能收到从连接的交换机的SPAN流量和处理它对本地端口。因此完成此的唯一方法在UCS环境是通过使用在一物理交换机和发送捕获的流量的被封装的RSPAN

(ERSPAN)使用IP，功能对VM。

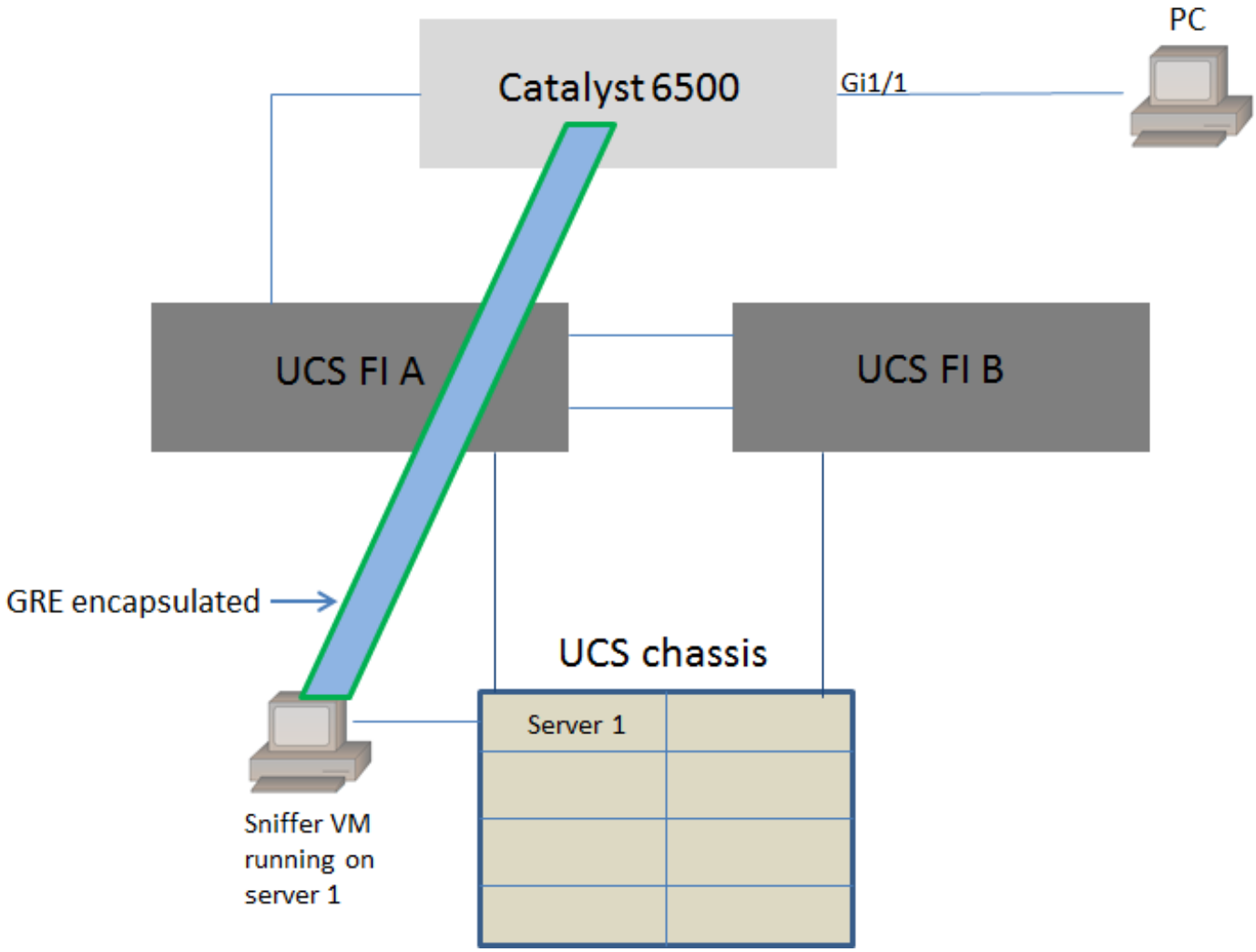
在某些实施，运行嗅探器工具的VM不能有IP地址。当嗅探器VM有一个IP地址以及方案，不用IP地址时，本文解释要求的配置。此处onl限制是嗅探器VM需要能读从发送对它的流量的GRE/ERSPAN封装。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

网络图

此拓扑在本文考虑：



PC附加对Catalyst 6500的GigabitEthernet1/1监控。运行在server1的思科UCS里面在GigabitEthernet1/1的流量捕获并且发送对嗅探器VM。

在6500交换机的ERSPAN功能捕获流量，封装它使用GRE并且发送它对嗅探器VM的IP地址。

配置

嗅探器VM用IP地址

> **注意**：在此部分描述的步骤可以也用于嗅探器在UCS刀片的一个仅有金属服务器运行而不是在VM的运行的方案。

当嗅探器VM能有IP地址时，这些步骤要求：

- 配置嗅探器VM在UCS环境里面用从6500是可及的IP地址
- 运行嗅探器工具在VM里面
- 配置6500的一ERSPAN来源会话并且发送捕获的流量直接地对VM的IP地址

在6500交换机的配置步骤：

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

当嗅探器VM不能有IP地址时，这些步骤要求：

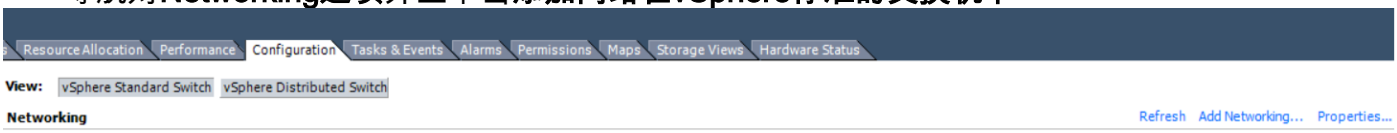
- 配置嗅探器VM在UCS环境里面
- 运行嗅探器工具在VM里面
- 创建能有在同一台主机的一个IP地址和用IP地址配置它从6500是可及的秒钟VM
- 配置VMWare vSwitch的端口组在混杂模式
- 配置6500的一ERSPAN来源会话并且发送捕获的流量对第二个VM的IP地址

这些步骤显示在VMWare要求的配置ESX ：

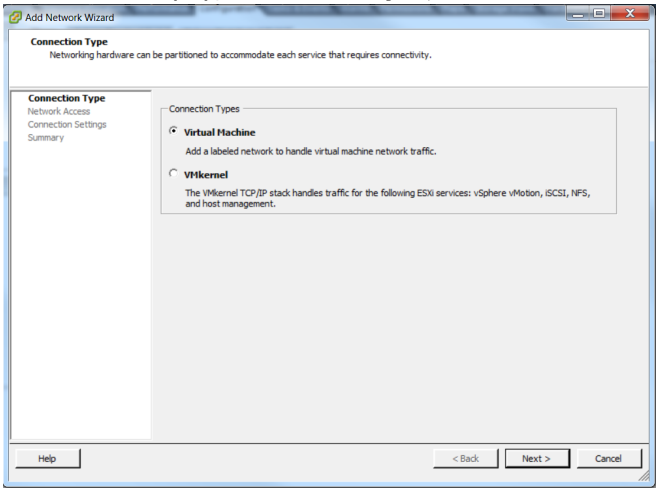
如果已经让一个端口组配置，请直接地进入步骤2。

1. 创建虚拟机端口组并且分配两台虚拟机到它

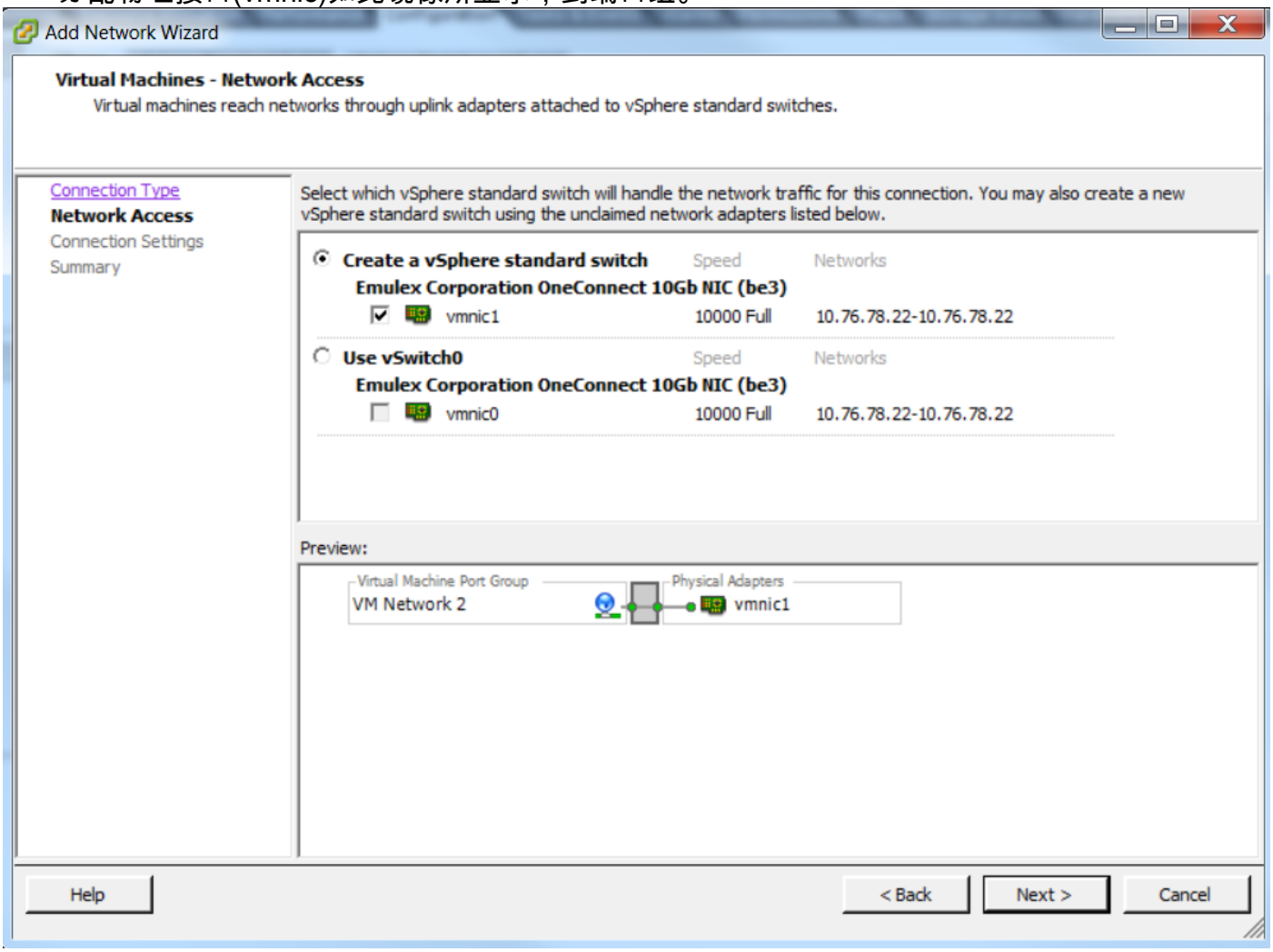
- 导航对**Networking选项**并且单击**添加网络在vSphere标准的交换机下**



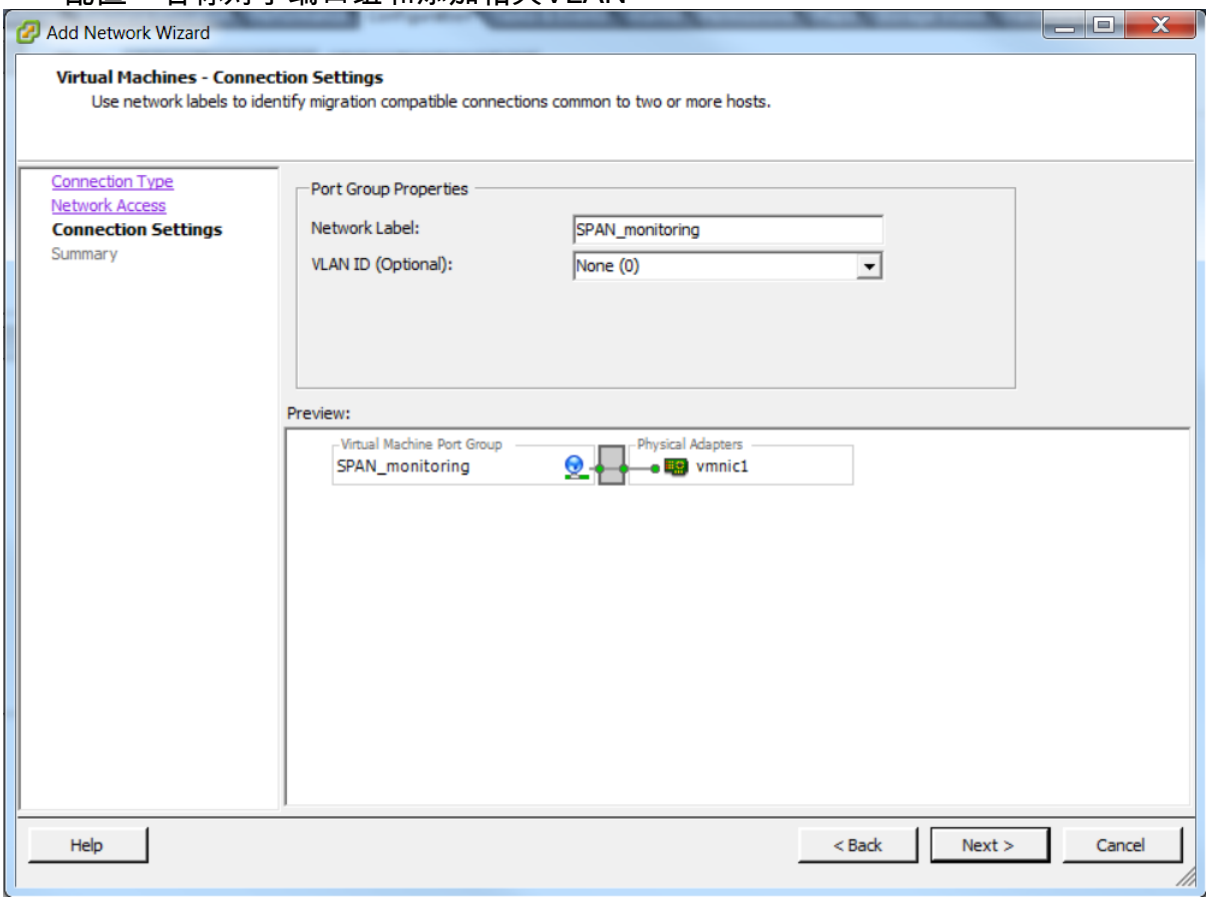
- 创建一个端口组类型虚拟机



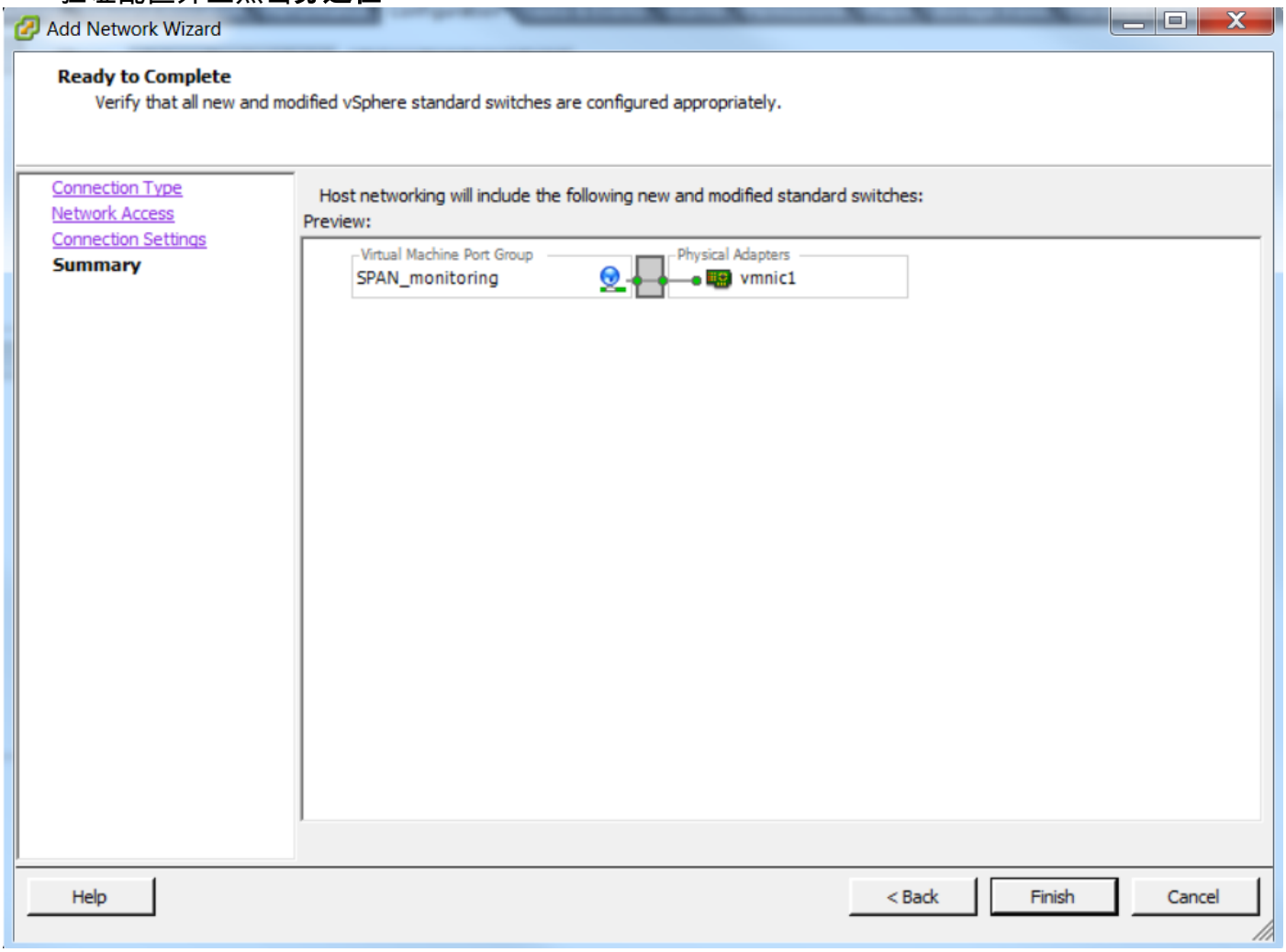
- 分配物理接口(vmnic)如此镜像所显示，到端口组。



- 配置一名称对于端口组和添加相关VLAN



- 验证配置并且点击**芬通社**

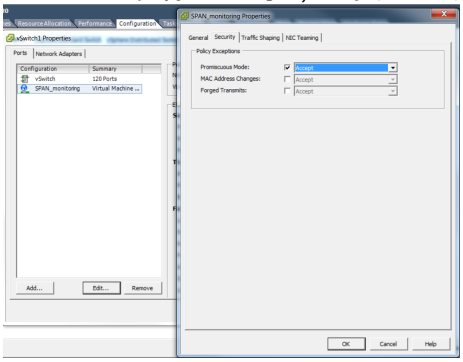


2. 配置端口组在混杂模式。

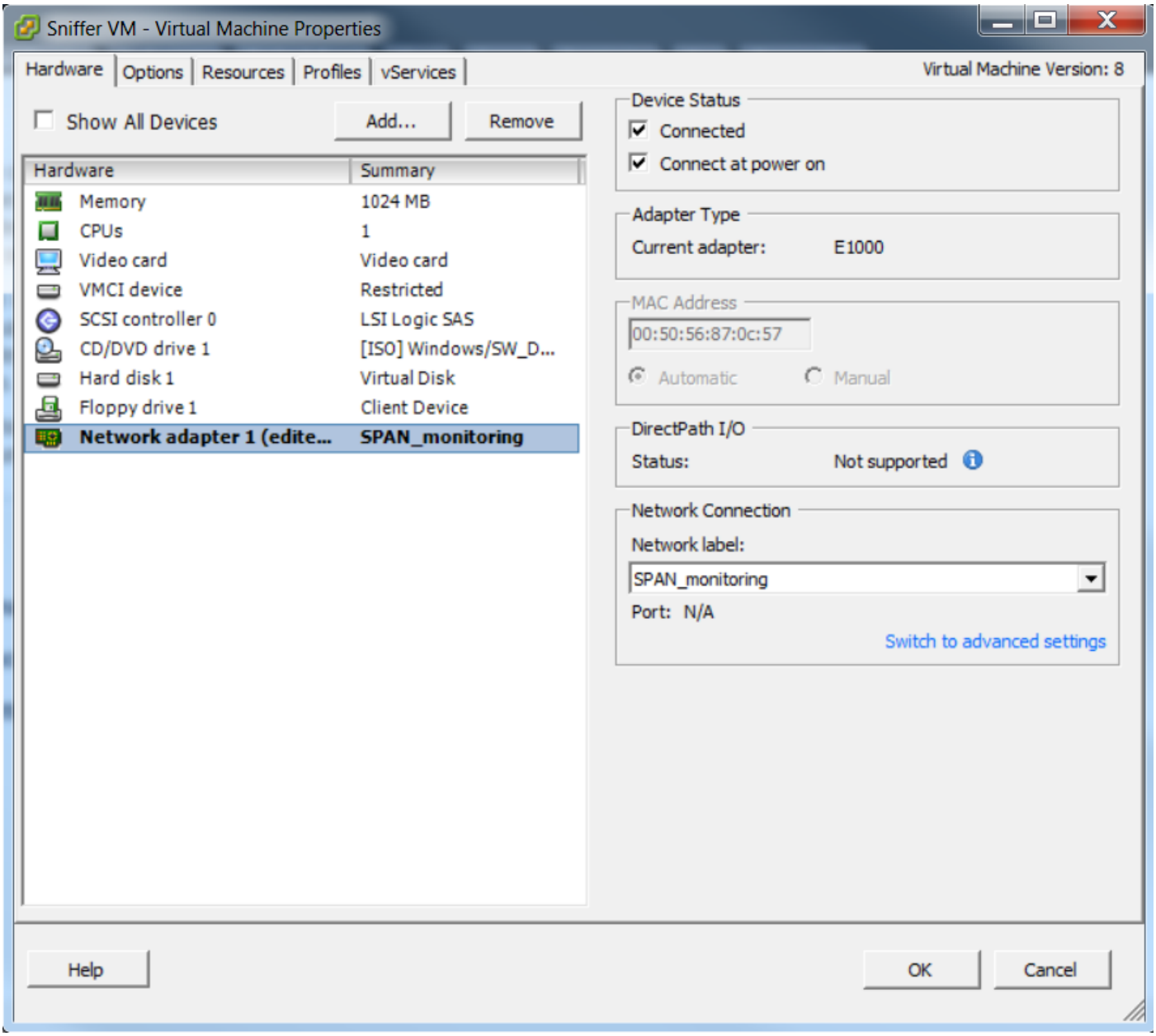
- 端口组必须当前出现在**Networking选项下**
- 点击**属性**

- 选择端口组并且单击**编辑**

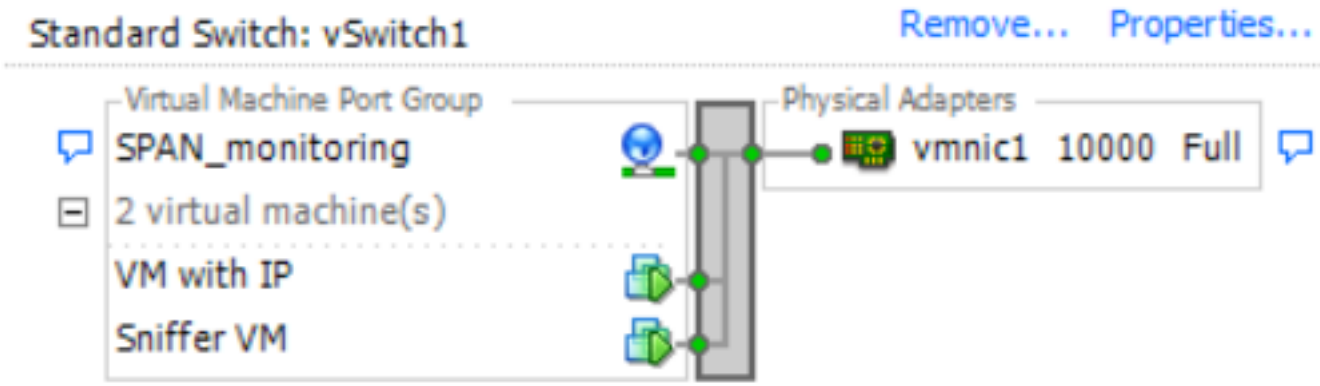
- 如此镜像所显示，去**安全选项卡**并且更改设置的混杂模式接受



3. 分配两台虚拟机到从虚拟机设置部分的端口组。



4. 两台虚拟机必须在端口组中当前出现在**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。

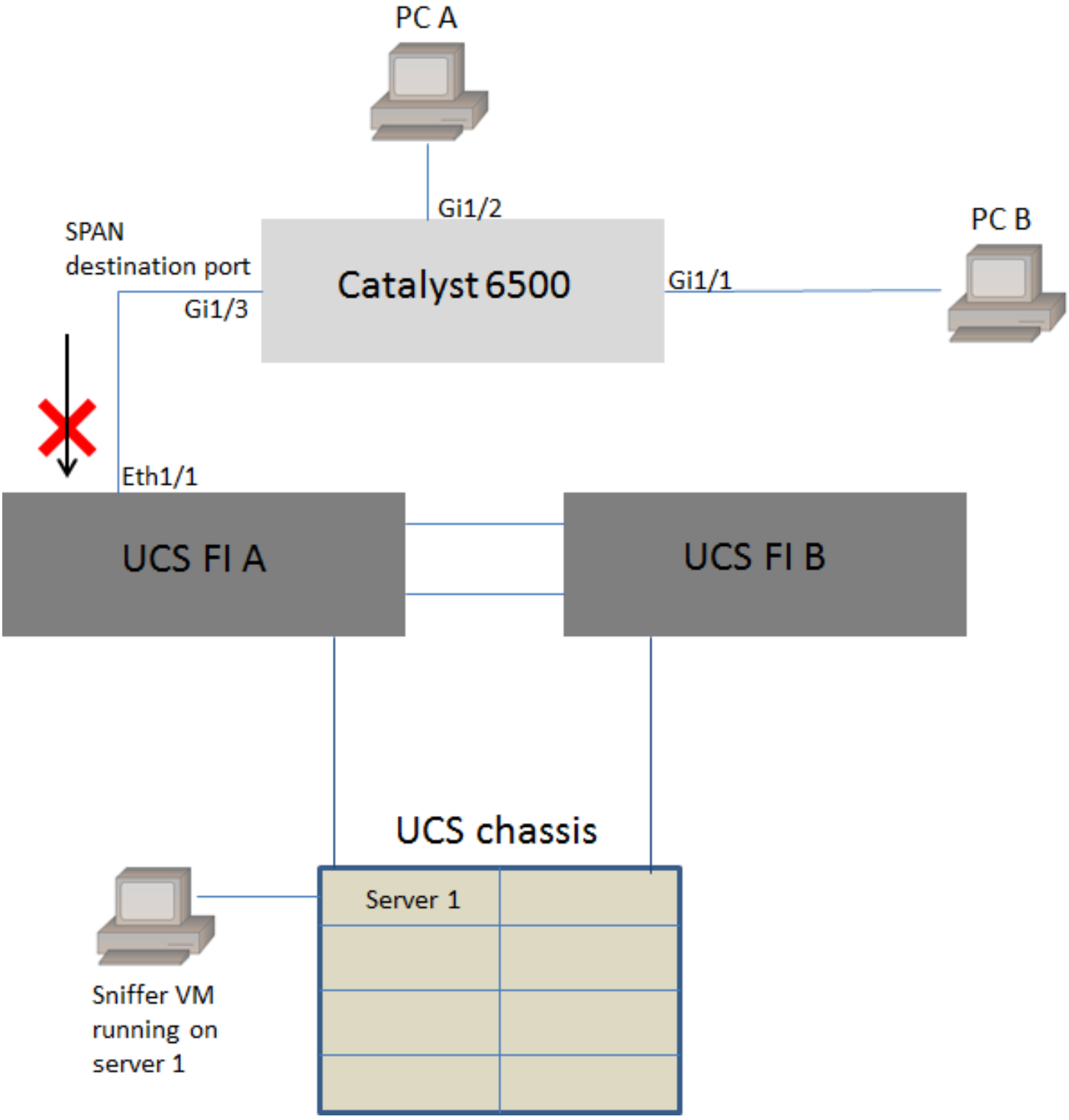
5. 这显示在6500交换机的配置步骤：

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封装获取数据包并且发送它对VM用IP地址。在VMWare vSwitch的混杂模式使嗅探器VM发现这些数据包。

故障情景

当曾经在一物理交换机的本地SPAN功能而不是ERSPAN功能时，此部分描述常见故障方案。此拓扑考虑得此处：



使用本地SPAN功能，从PC A的流量对PC B监控。SPAN流量的目的地处理到端口连接对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：

在端口Gig1/1和Gig1/2的所有数据流将复制到端口Gig1/3。这些数据包源及目的地MAC地址将是未知对UCS FI。

在UCS以太网终端主机模式， FI丢弃这些未知单播数据包。

在UCS以太网交换模式， FI了解在连接的端口的源MAC地址到6500 (Eth1/1)然后充斥数据包下行对服务器。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之间的流量(与MAC地址bbbb.bbbb.bbbb)
2. 第一数据包是从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不认识目标MAC地址bbbb.bbbb.bbbb并且充斥数据包到同样VLAN的所有端口
5. 嗅探器VM，在同样VLAN，也看到此数据包
6. 下一个信息包是从PC B到PC A
7. 当这点击Eth1/1时， MAC地址bbbb.bbbb.bbbb在Eth1/1了解
8. 数据包的目的地是为MAC地址aaaa.aaaa.aaaa
9. FI丢弃此数据包，当MAC地址aaaa.aaaa.aaaa在Eth1/1了解，并且数据包在Eth1/1接收
10. 后续信息包，注定为MAC地址aaaa.aaaa.aaaa或MAC地址bbbb.bbbb.bbbb由于同样的原因丢弃

相关信息

- 配置在虚拟交换机或portgroup的混杂模式
- SPAN、RSPAN和ERSPAN在Catalyst 6500
- 解封装ERSPAN流量用开放源工具
- 技术支持和文档 - Cisco Systems