用VMware DVS或Cisco连结1000v配置专用VLAN和UCS

目录

简介

本文描述思科统一计算系统(以后UCS)的专用VLAN (PVLAN)技术支持在2.2(2c)版本和。

> **Caution**:有在开始从UCS固件版本3.1(3a)的工作情况上的一个变化正如**与UCS版本3.1(3)和以上部分的工作情况更改所描述**。

先决条件

要求

Cisco 建议您了解以下主题：

- UCS
- Cisco连结1000V (N1K)或VMware分配了虚拟交换机(DVS)
- VMware

- 第2层(L2)交换

使用的组件

本文档不限于特定的软件和硬件版本。

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。

背景信息

专用VLAN是为L2从其他端口的隔离配置的VLAN在同样专用VLAN内。属于PVLAN的端口与共同的一套技术支持VLAN产生关联，用于为了创建PVLAN结构。

有三种类型的 PVLAN 端口：

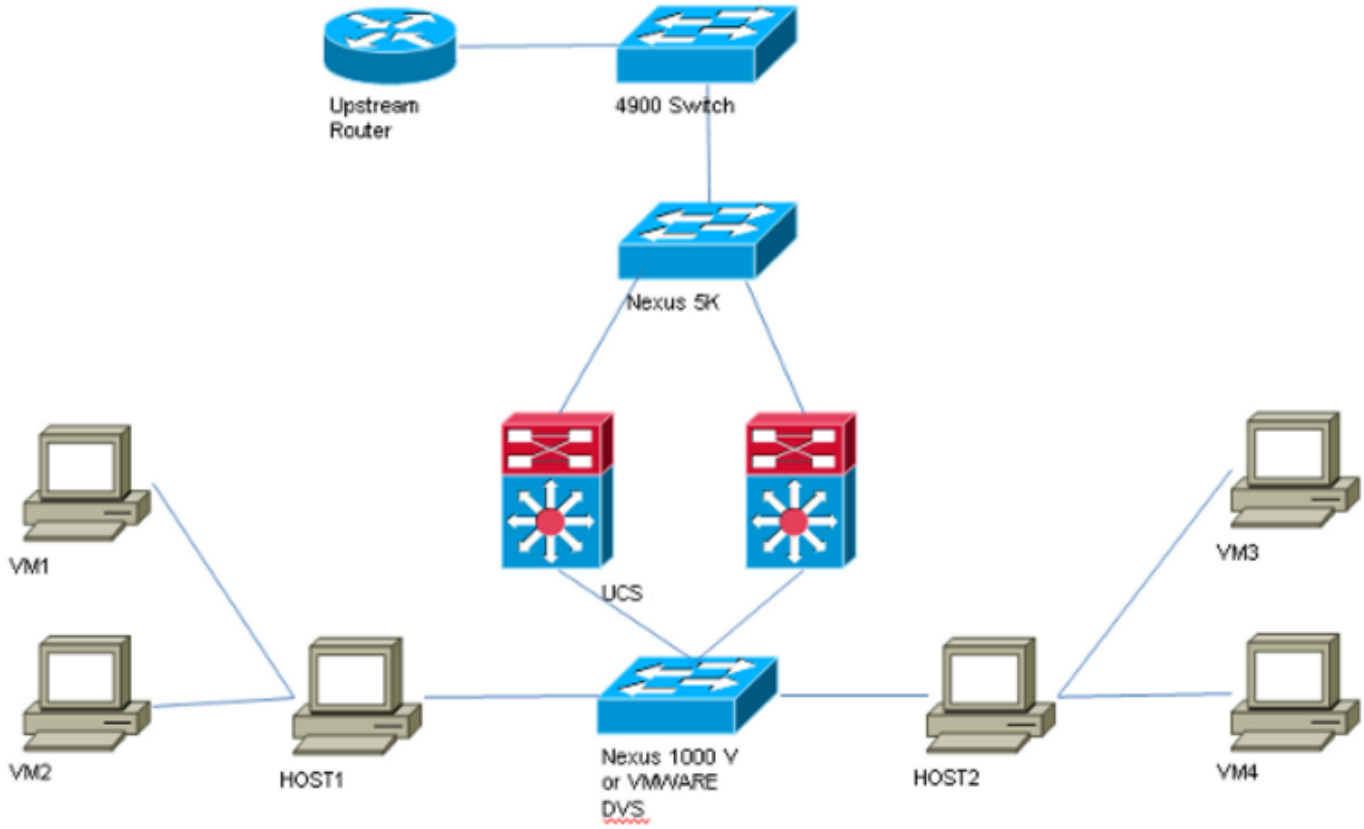
- 一个混乱端口与其他PVLAN端口沟通并且是用于的端口为了与设备沟通在PVLAN外面。
- 除混乱端口外，一个隔离的端口有包括广播)的完全L2分离(从在同样PVLAN内的其他端口。
- 社区端口能与在同样PVLAN以及混乱端口的其他端口沟通。公共端口查出在从端口的L2在其他社区或查出的PVLAN端口。广播只被传播对在社区和混乱端口的其他端口。

参考RFC 5517，Cisco系统的专用VLAN：可升级的安全在多客户端环境里为了了解PVLAN的理论、操作和概念。

配置

网络图

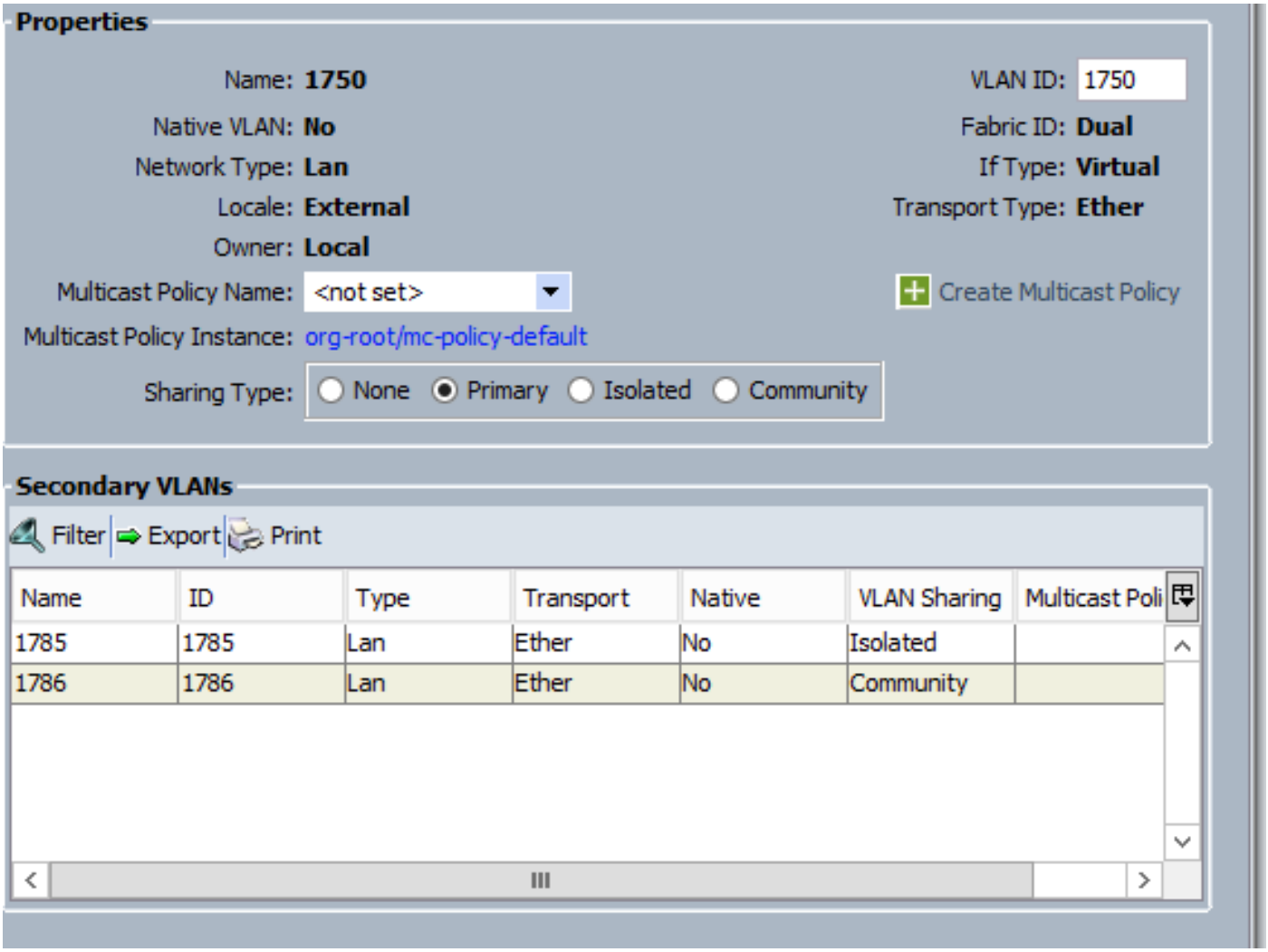
使用连结1000v或VMware DVS



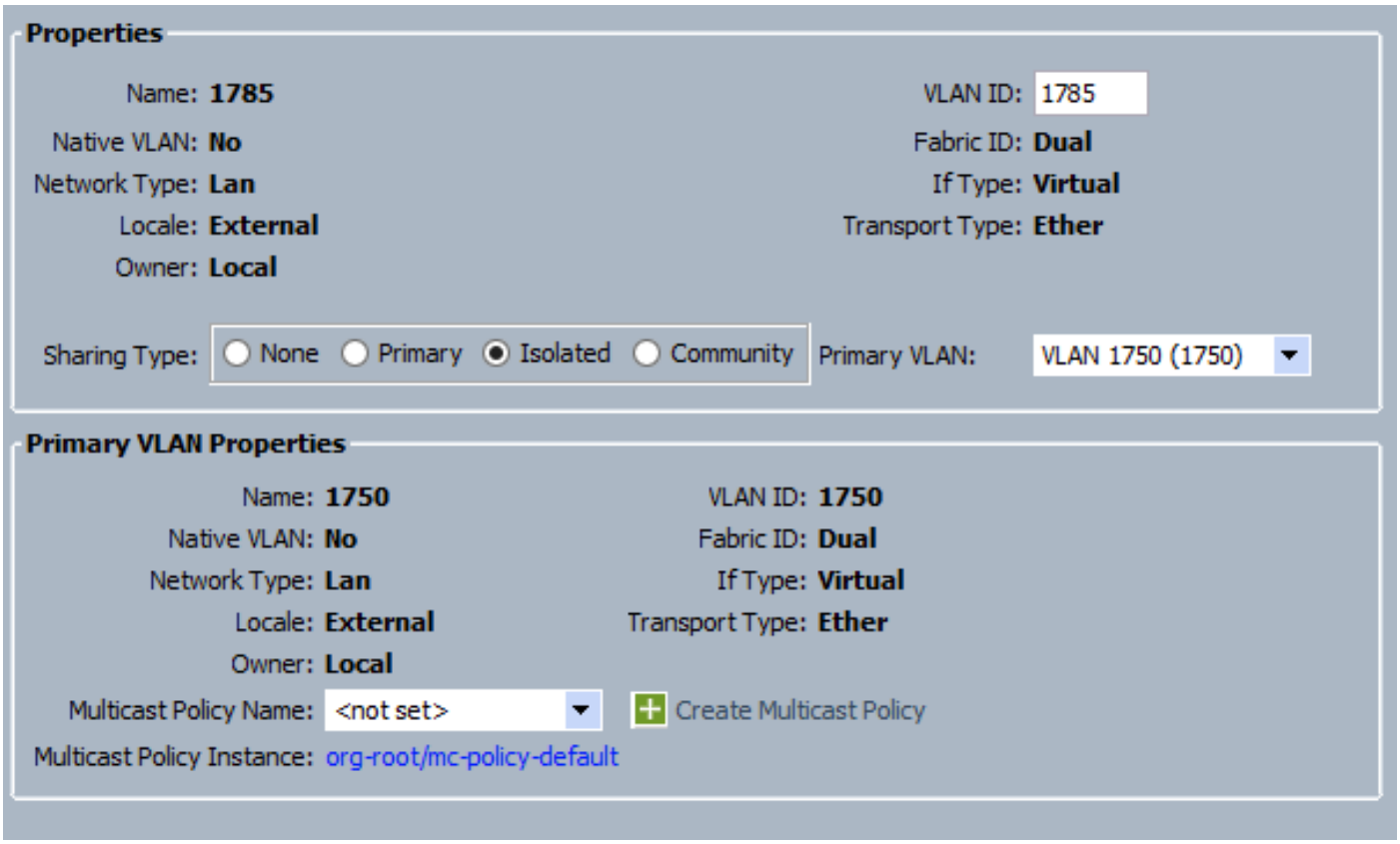
Note:此示例使用VLAN 1750作为主要的， 1785如查出和1786作为团体VLAN。

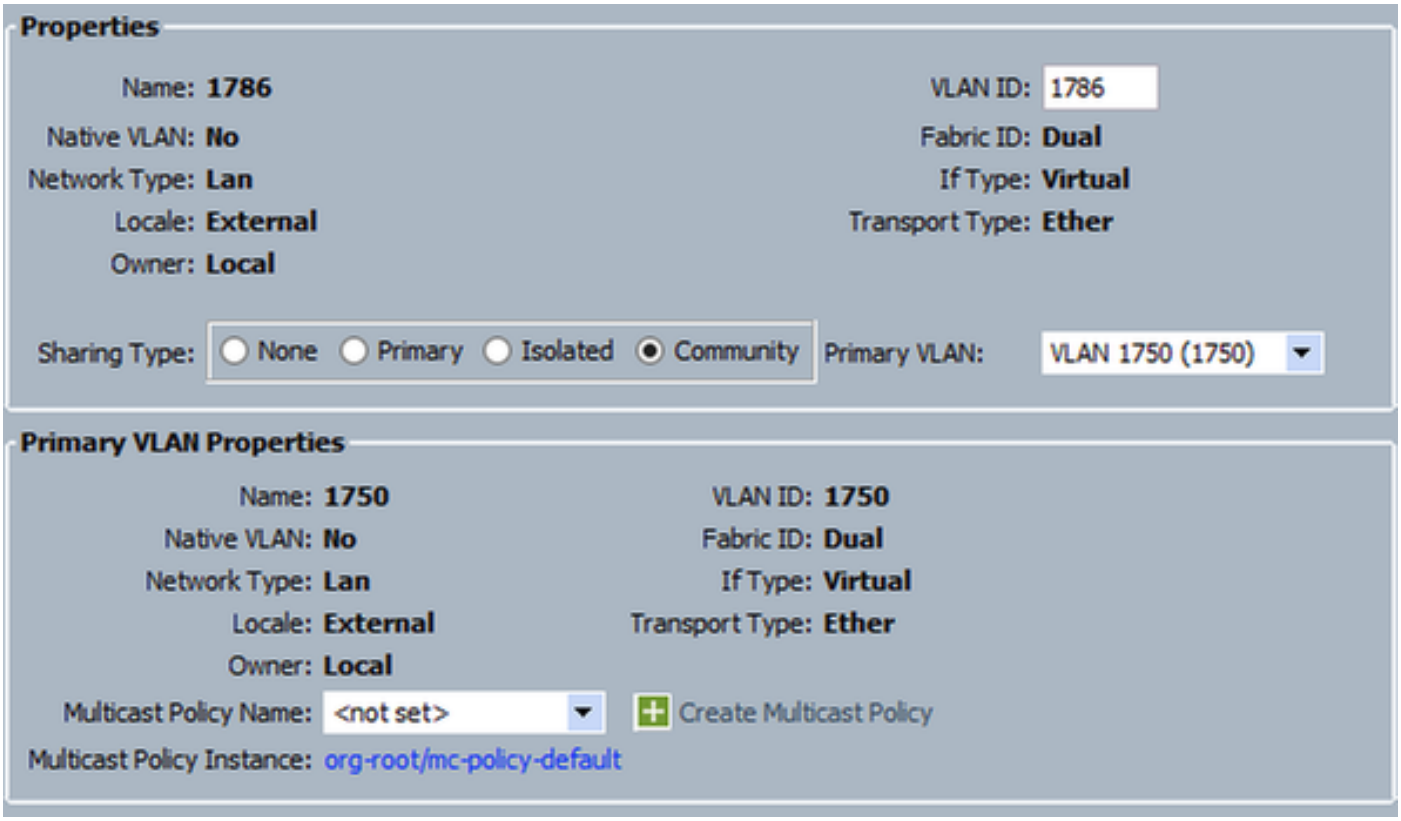
与VMware DVS的UCS

1. 如镜像所显示，为了创建主VLAN，请点击**主要的**单选按钮作为共享的类型，并且输入**VLAN ID** 1750。

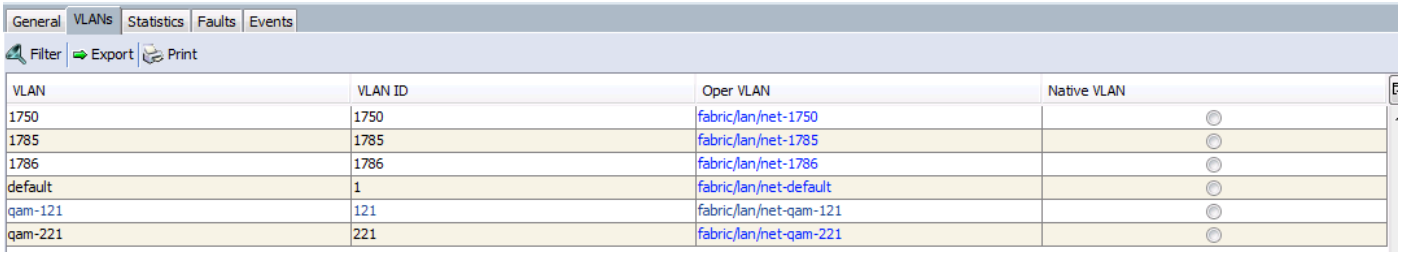


2. 创建相应地**查出**和**团体VLAN**如镜像所显示。这些都不必须是本地VLAN。





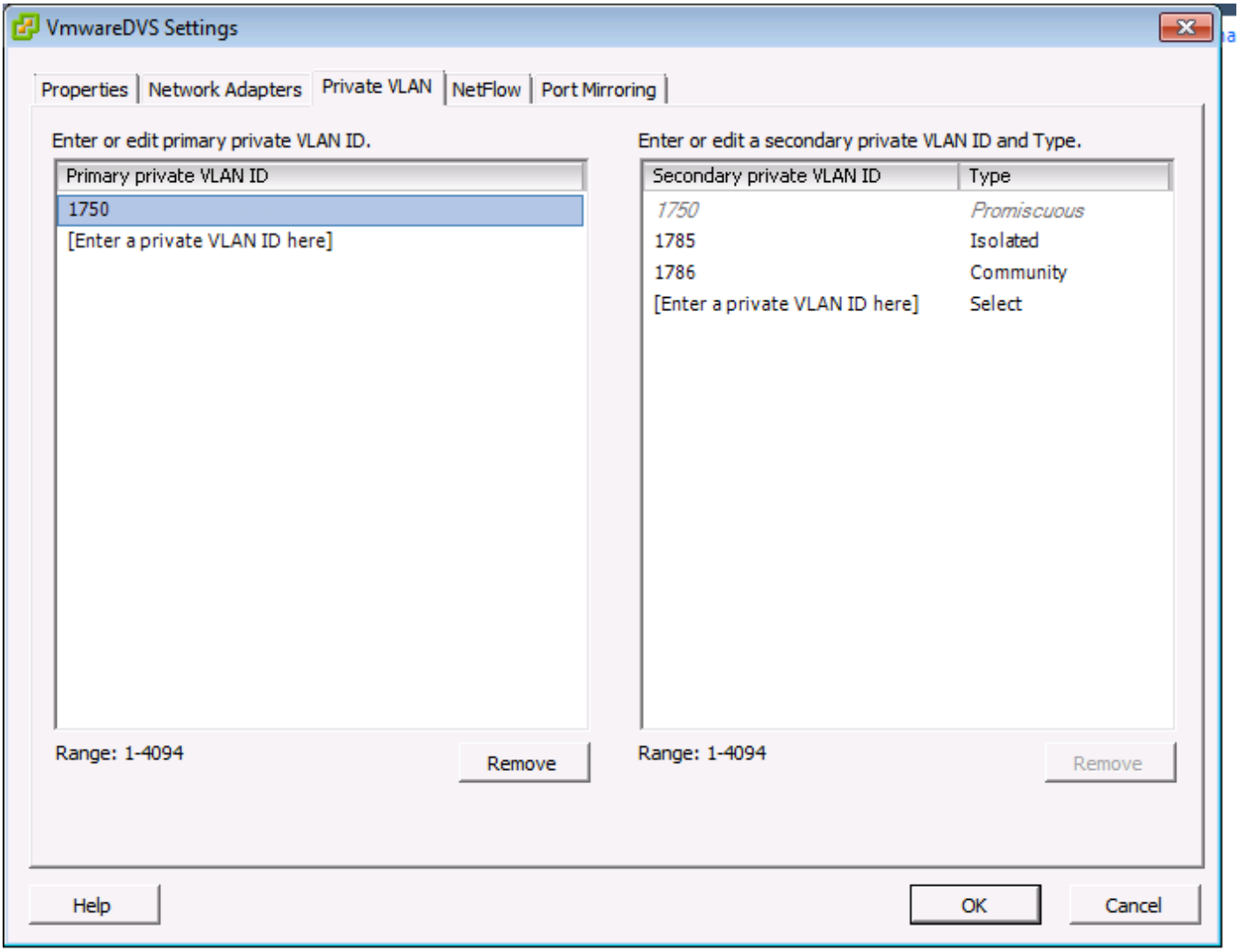
3. 虚拟网络网络界面卡(vNIC)在服务档案如在镜像中看到运载常规VLAN以及PVLAN。

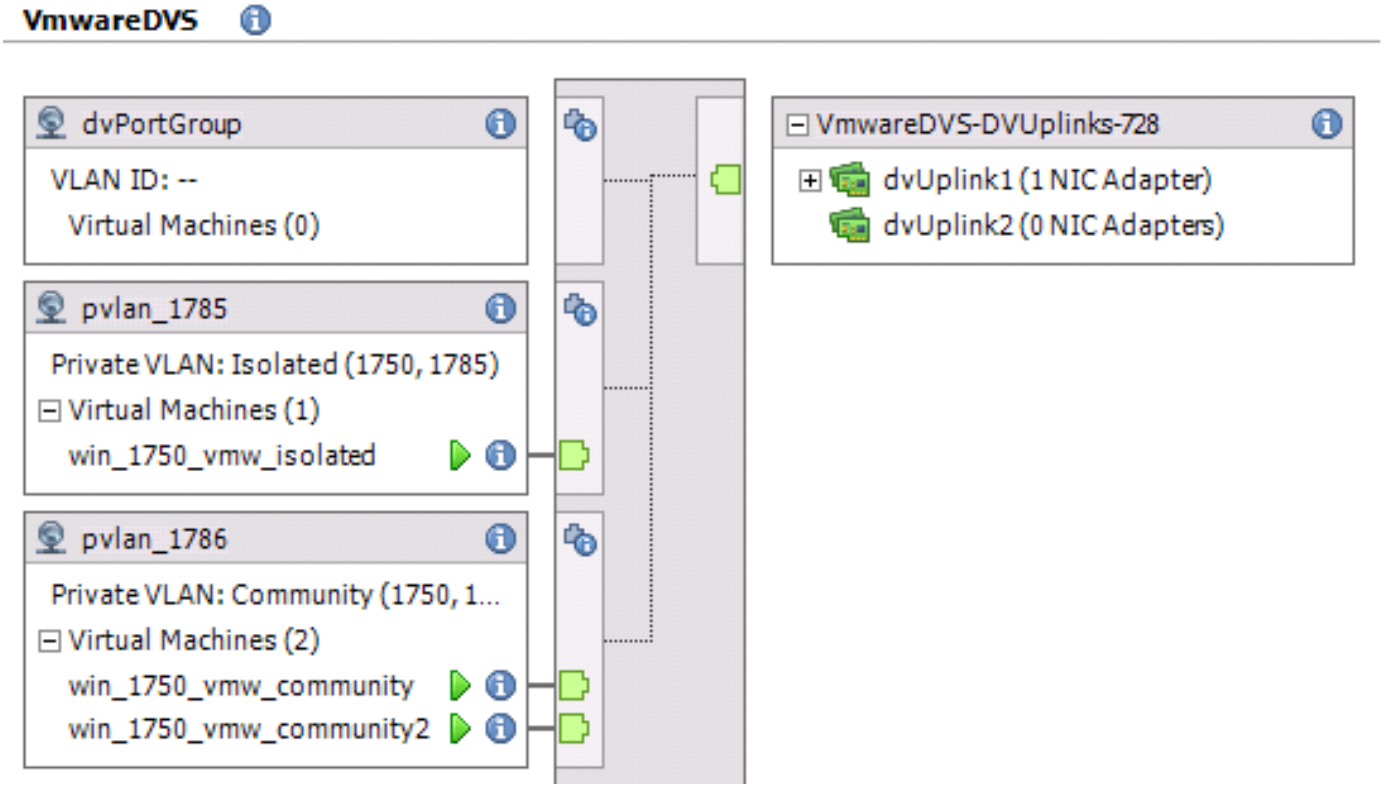


4. 在UCS的上行链路Port-Channel运载常规VLAN以及PVLAN ：

```
interface port-channel1
description U: Uplink
switchport mode trunk
pinning border
switchport trunk allowed vlan 1,121,221,321,1750,1785-1786
speed 10000

F240-01-09-UCS4-A(nxos)#


F240-01-09-UCS4-A(nxos)# show vlan private-vlan
Primary Secondary Type Ports
------- --------- --------------- ----------------------------------------

1750     1785          isolated
1750     1786          community
```

VMware DVS


VmwareDVS Settings
Properties
Network Adapters
Private VLAN
NetFlow
Port Mirroring
Enter or edit primary private VLAN ID.
Primary private VLAN ID
1750
[Enter a private VLAN ID here]
Range: 1-4094
Remove
Enter or edit a secondary private VLAN ID and Type.
Secondary private VLAN ID
Type
1750
Promiscuous
1785
Isolated
1786
Community
[Enter a private VLAN ID here]
Select
Range: 1-4094
Remove
Help
OK
Cancel


VmwareDVS
dvPortGroup
VLAN ID: --
Virtual Machines (0)
pvlan_1785
Private VLAN: Isolated (1750, 1785)
Virtual Machines (1)
win_1750_vmw_isolated
pvlan_1786
Private VLAN: Community (1750, 1...
Virtual Machines (2)
win_1750_vmw_community
win_1750_vmw_community2
VmwareDVS-DVUplinks-728
dvUplink1 (1 NIC Adapter)
dvUplink2 (0 NIC Adapters)

上行N5k交换机

```
feature private-vlan


vlan 1750 private-vlan primary private-vlan association 1785-1786


vlan 1785 private-vlan isolated

vlan 1786 private-vlan community




interface Vlan1750

ip address 10.10.175.252/24 private-vlan mapping 1785-1786

no shutdown


interface port-channel114

Description To UCS
switchport mode trunk
switchport trunk allowed vlan 1,121,154,169,221,269,321,369,1750,1785-1786
spanning-tree port type edge
spanning-tree bpduguard enable
spanning-tree bpdufilter enable
vpc 114 <=== if there is a 5k pair in vPC configuration only then add this line to both N5k
```

与UCS版本3.1(3)和以上的工作情况更改

在UCS版本3.1(3)之前，您可能安排在团体VLAN的VM与在主VLAN的VM联络在主VLAN VM驻留在UCS里面的VMware DVS。此工作情况是不正确的，虽然主要的VM一定总是向北或外部UCS。此工作情况通过缺陷ID CSCvh87378描述 。

从向前UCS版本2.2(2)，由于在代码的一个缺陷，团体VLAN能与在FI后是存在的主VLAN沟通。但是查出不能与主要的沟通在FI后。两个(查出和社区) VMs能与主要的沟通FI的外部。

从3.1(3)向前，此缺陷允许社区与主要的沟通在FI后，被纠正了，并且因而社区VMs不能与在UCS内驻留的主VLAN的VM沟通。

为了解决此情况，主要的VM会任一需要被移动(向北)在UCS外面。如果那不是选项，则主要的VM将需要搬入是正常VLAN而不是专用VLAN的另一个VLAN。

例如，在固件3.1(3)之前，在团体VLAN 1786的VM可能沟通到在UCS内驻留，然而，此通信在固件3.1(3)将中断及以后，如镜像所显示的主VLAN 1750的VM。

```
F240-01-09-UCS4-A(nxos)# show mac address-table | inc 76d7
* 1786      0050.568e.76d7    dynamic   440         F    F  Veth3148
F240-01-09-UCS4-A(nxos)#
```

```
   VLAN     MAC Address      Type      age     Secure NTFY   Ports/SWID.SSID.LID
---------+----------------+--------+---------+------+----+------------------
* 1750     0050.568e.476f    dynamic   0          F    F  Veth3240
F240-01-09-UCS4-B(nxos)#
```

上行4900交换机

> **Note**:在本例中， 4900是L3接口对外部网络。如果您的L3的拓扑是不同的，则请相应地亲切地做变动

在4900交换机上，请采取这些步骤，并且设置混乱端口。在混乱端口的PVLAN末端。

1. 如果必须打开PVLAN功能。
2. 创建并且关联VLAN如执行在连结5K。
3. 创建在4900交换机的输出端口的混乱端口。从这时起，自VLAN 1785 & 1786的信息包在VLAN 1750在这种情况下被看到。

```
Switch(config-if)#switchport mode trunk
switchport private-vlan mapping 1785-1786
switchport mode private-vlan promiscuous
```

在上游路由器上，仅请创建VLAN的1750一个子接口。在这个阶层，需求取决于您使用的网络配置：

```
interface GigabitEthernet0/1.1

encapsulation dot1Q 1750

IP address10.10.175.254/24
```

验证

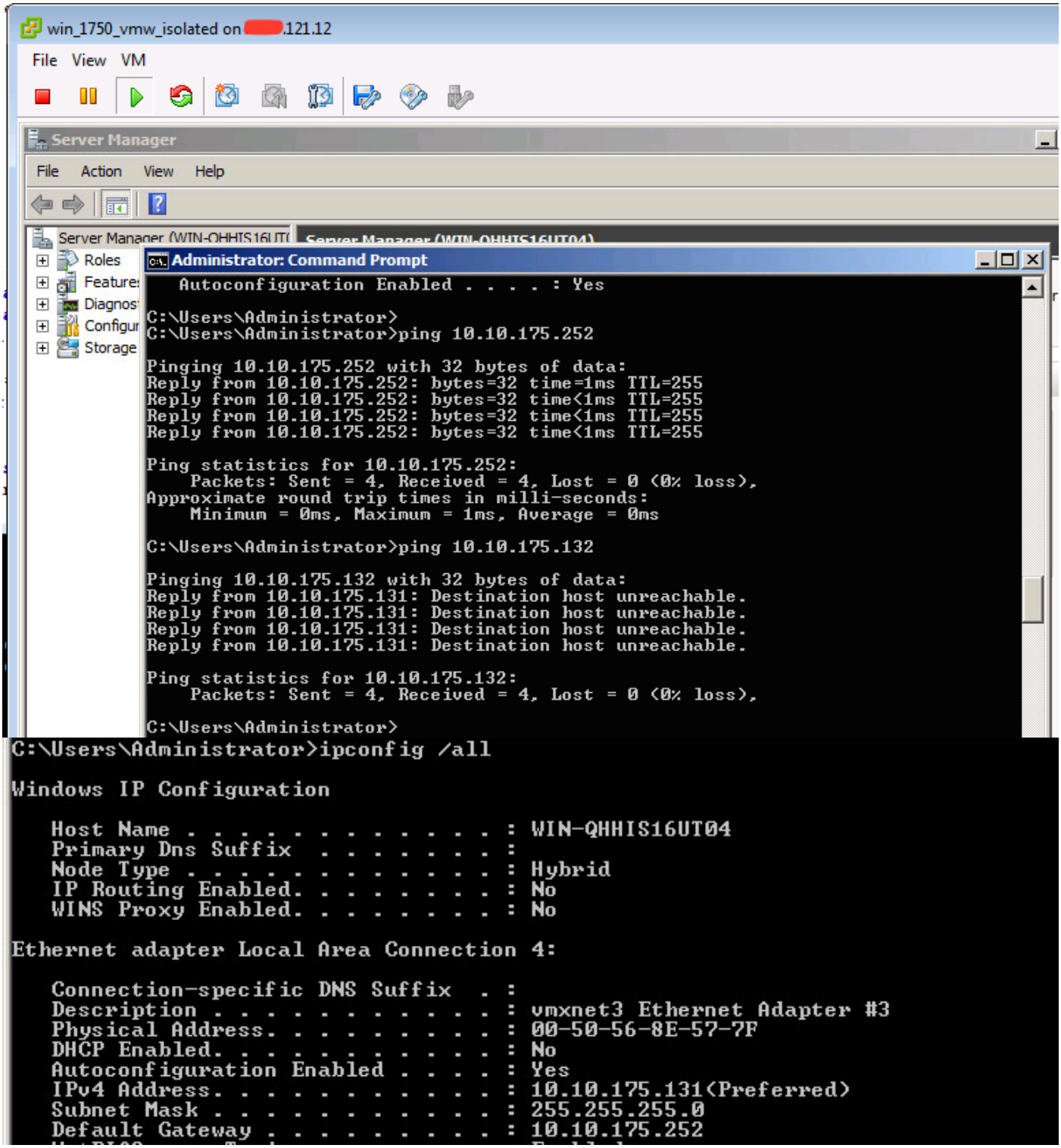
当前没有可用于此配置的验证过程。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

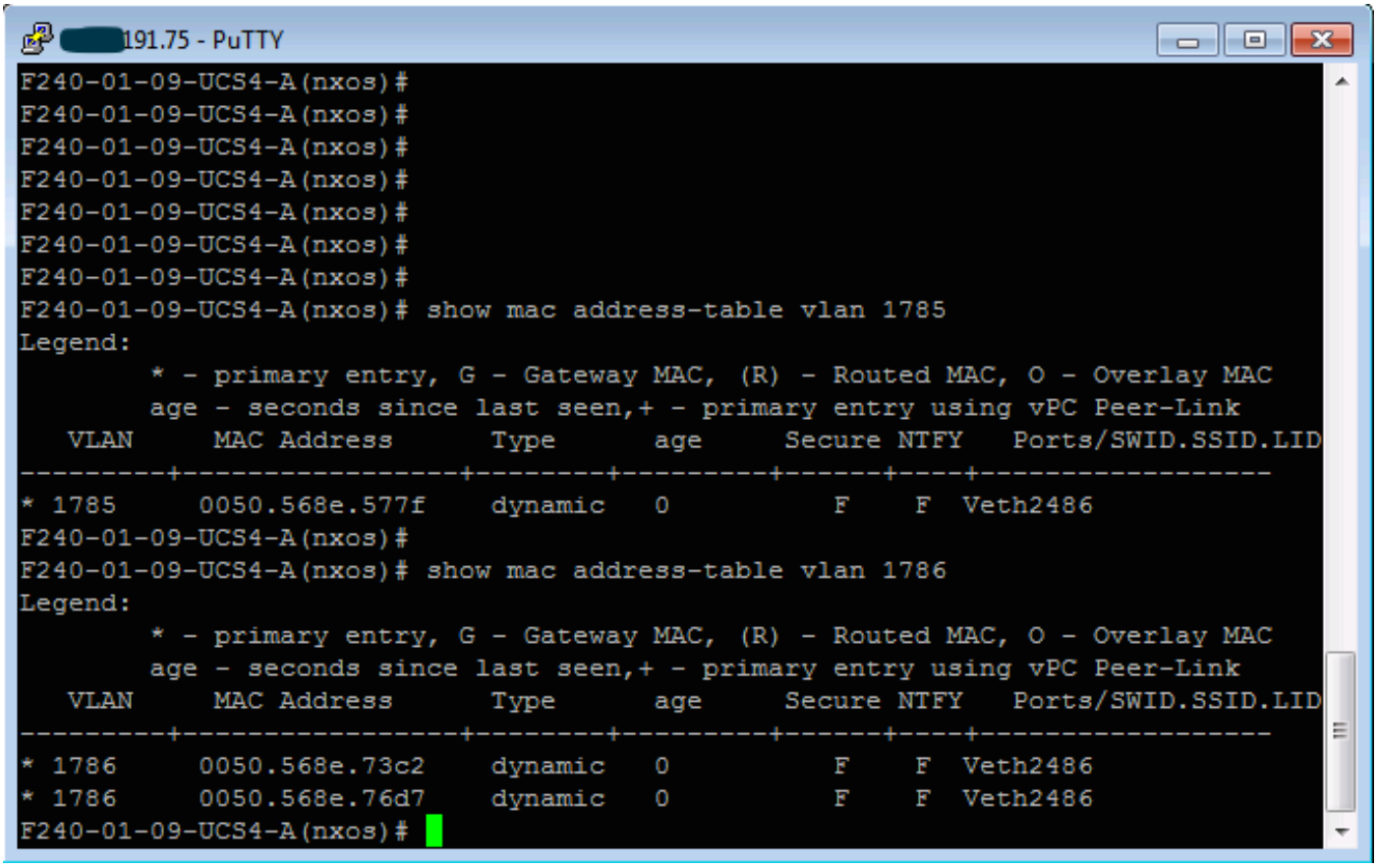
此程序描述如何为与使用的VMware DVS测试配置PVLAN。

1. 运行ping到在端口组配置的其他系统以及路由器或者其它设备在混乱端口。如镜像所显示，而那些对在隔离VLAN的其它设备必须失效对设备的Ping通过混乱端口必须工作。



检查MAC地址表为了发现您的MAC哪里获知。在所有交换机上， MAC必须在除了在交换机的隔离VLAN有混乱端口的。在混乱交换机上， MAC必须在主VLAN。

2. 如镜像所显示的UCS。



3. 检查在上行n5k同样MAC，类似的输出及早输出一定是存在n5k和如镜像所显示。

```
f241-01-08-5596-a# show mac address-table | inc 577f
* 1785      0050.568e.577f    dynamic   170         F     F  Po114
f241-01-08-5596-a#
f241-01-08-5596-a# show mac address-table | inc 73c2
* 1786      0050.568e.73c2    dynamic   10          F     F  Po114
f241-01-08-5596-a# show mac address-table | inc 76d7
* 1786      0050.568e.76d7    dynamic   30          F     F  Po114
f241-01-08-5596-a#
```

与连结1000v的配置与在上行N5k的混乱端口

UCS配置

包括服务档案vNIC配置)的UCS配置(根据与VMware DVS的示例坚持同样。

N1k配置

```
feature private-vlan

vlan 1750 private-vlan primary private-vlan association 1785-1786

vlan 1785 private-vlan isolated

vlan 1786 private-vlan community
```

```
same uplink port-profile is being used for regular vlans & pvlans. In this example vlan 121 &
221 are regular vlans but you can change them accordingly

port-profile type ethernet pvlan-uplink-no-prom
switchport mode trunk
mtu 9000
switchport trunk allowed vlan 121,221,1750,1785-1786
channel-group auto mode on mac-pinning

system vlan 121 no shutdown state enabled vmware port-group

port-profile type vethernet pvlan_1785
switchport mode private-vlan host
switchport private-vlan host-association 1750 1785
switchport access vlan 1785
no shutdown
state enabled
vmware port-group

port-profile type vethernet pvlan_1786 switchport mode private-vlan host switchport access vlan
1786 switchport private-vlan host-association 1750 1786 no shutdown state enabled vmware port-
group
```

此程序描述如何测试配置。

1. 运行ping到在端口组配置的其他系统以及路由器或者其它设备在混乱端口。对设备的Ping通过混乱端口必须工作，而那些对在隔离VLAN的其它设备必须发生故障，如前面的部分所显示和在镜像。