使用VMware DVS或Cisco Nexus 1000v配置专用VLAN和UCS

目录

简介

本文档介绍2.2(2c)版及更高版本中对思科统一计算系统(UCS)的专用VLAN(PVLAN)支持。

> **警告：**从UCS固件版本3.1(3a)开始的行为发生更改，如**UCS版本3.1(3)和更高版本的行为更改**一节所述。

先决条件

要求

Cisco 建议您了解以下主题：

- UCS
- Cisco Nexus 1000V(N1K)或VMware分布式虚拟交换机(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是配置为与同一专用VLAN中的其他端口进行L2隔离的VLAN。属于PVLAN的端口与一组通用的支持VLAN关联，这些VLAN用于创建PVLAN结构。

有三种类型的 PVLAN 端口：

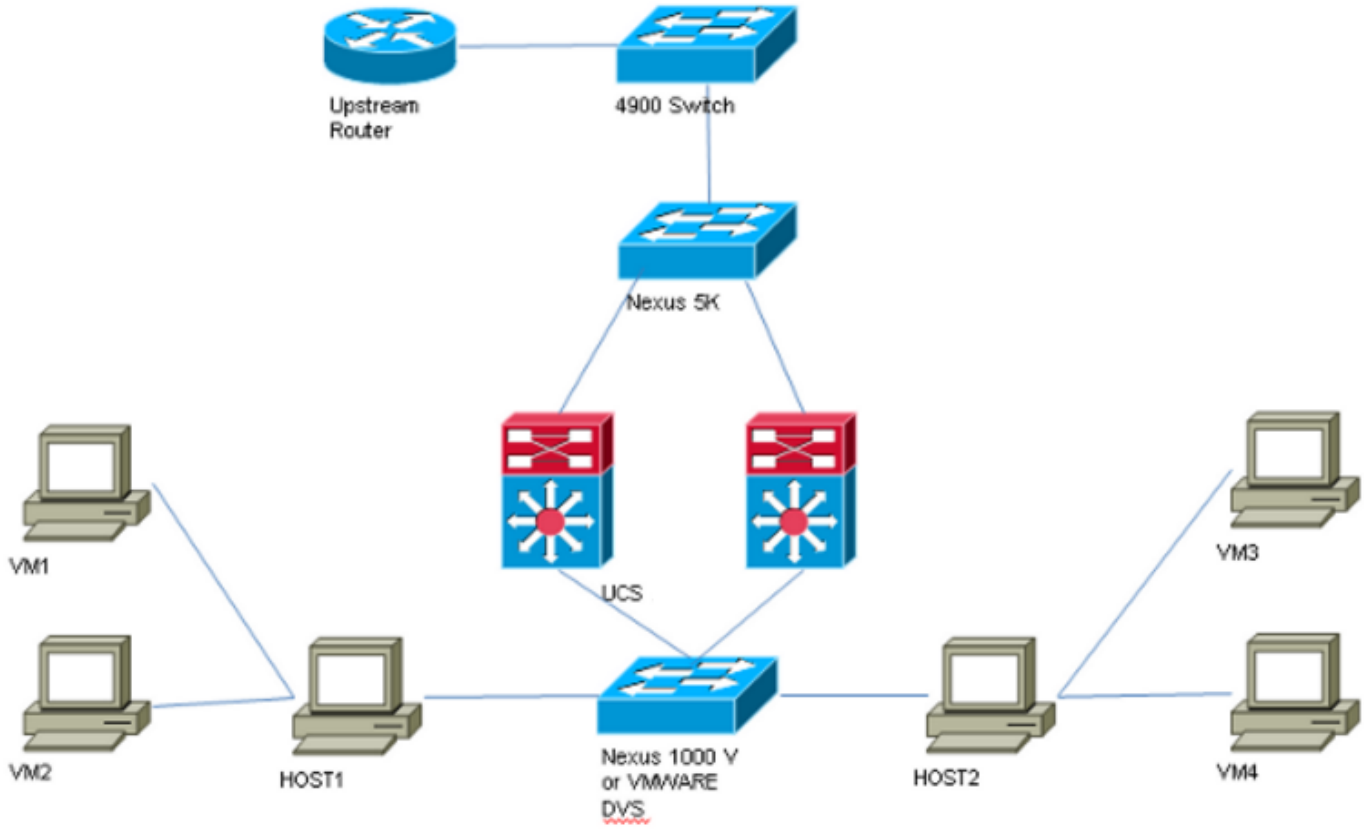
- 混杂端口与所有其他PVLAN端口通信，是用于与PVLAN外部设备通信的端口。
- 隔离端口与同一PVLAN中的其他端口（包括广播）有完全的L2分离（混合端口除外）。
- 社区端口可以与同一PVLAN中的其他端口以及混杂端口通信。在L2上，社区端口与其他社区或隔离PVLAN端口的端口隔离。广播仅传播到团体中的其他端口和混杂端口。

请参阅RFC 5517,Cisco Systems的专用VLAN:多客户端环境中的可扩展安全性，以便了解PVLAN的理论、操作和概念。

配置

网络图

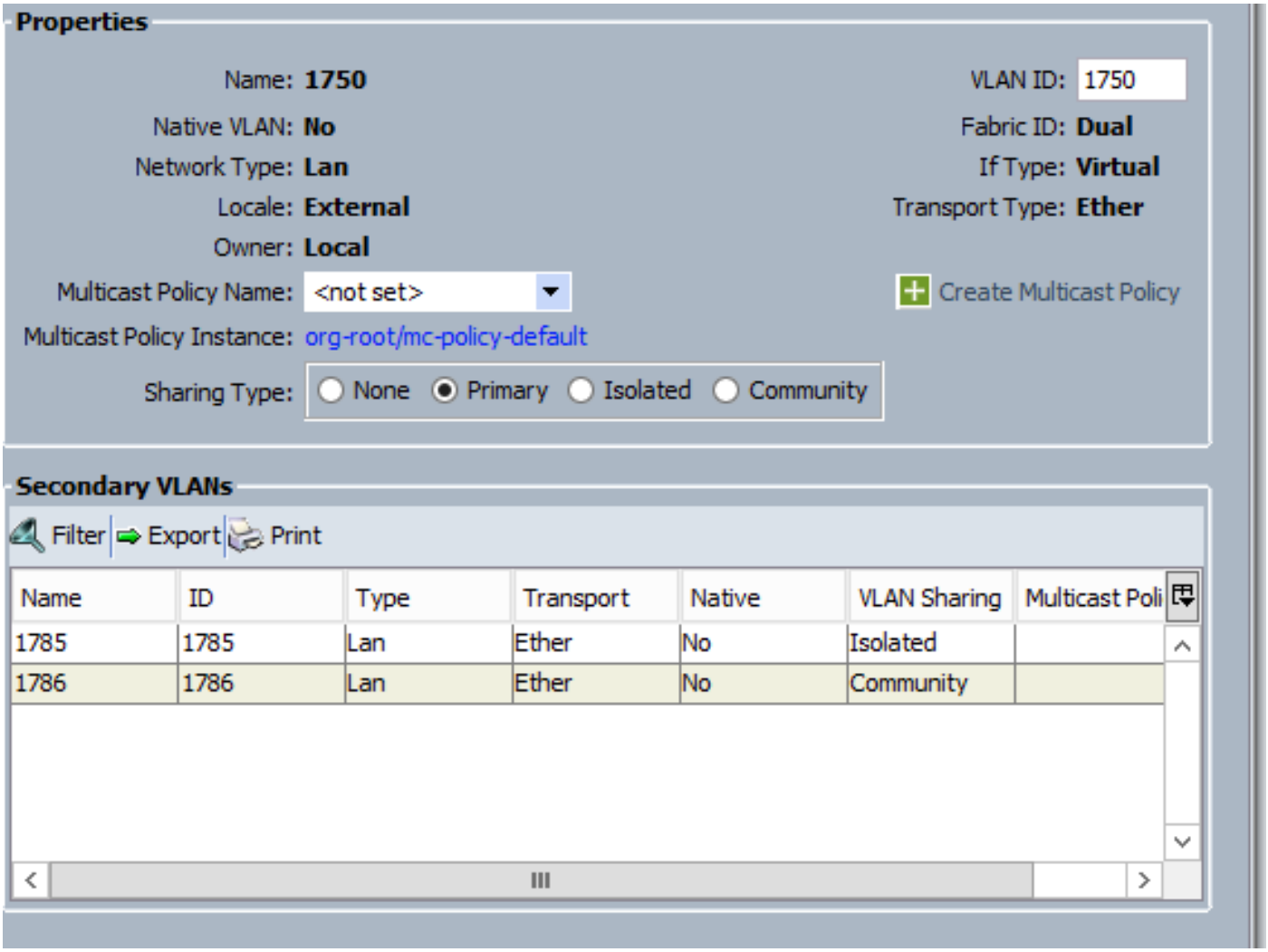
使用Nexus 1000v或VMware DVS



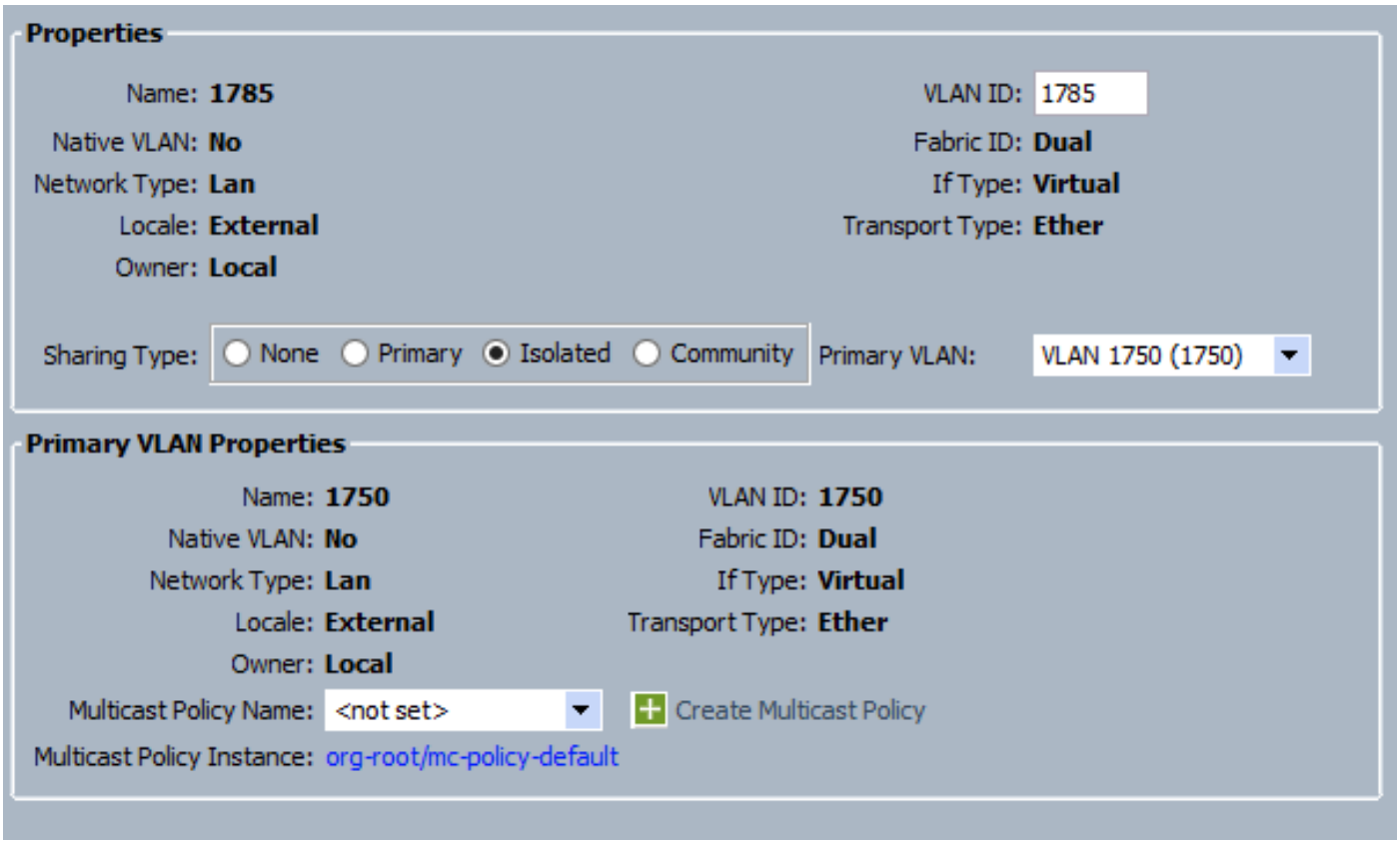
注意：本示例使用VLAN 1750作为主VLAN，1785作为隔离VLAN，1786作为社区VLAN。

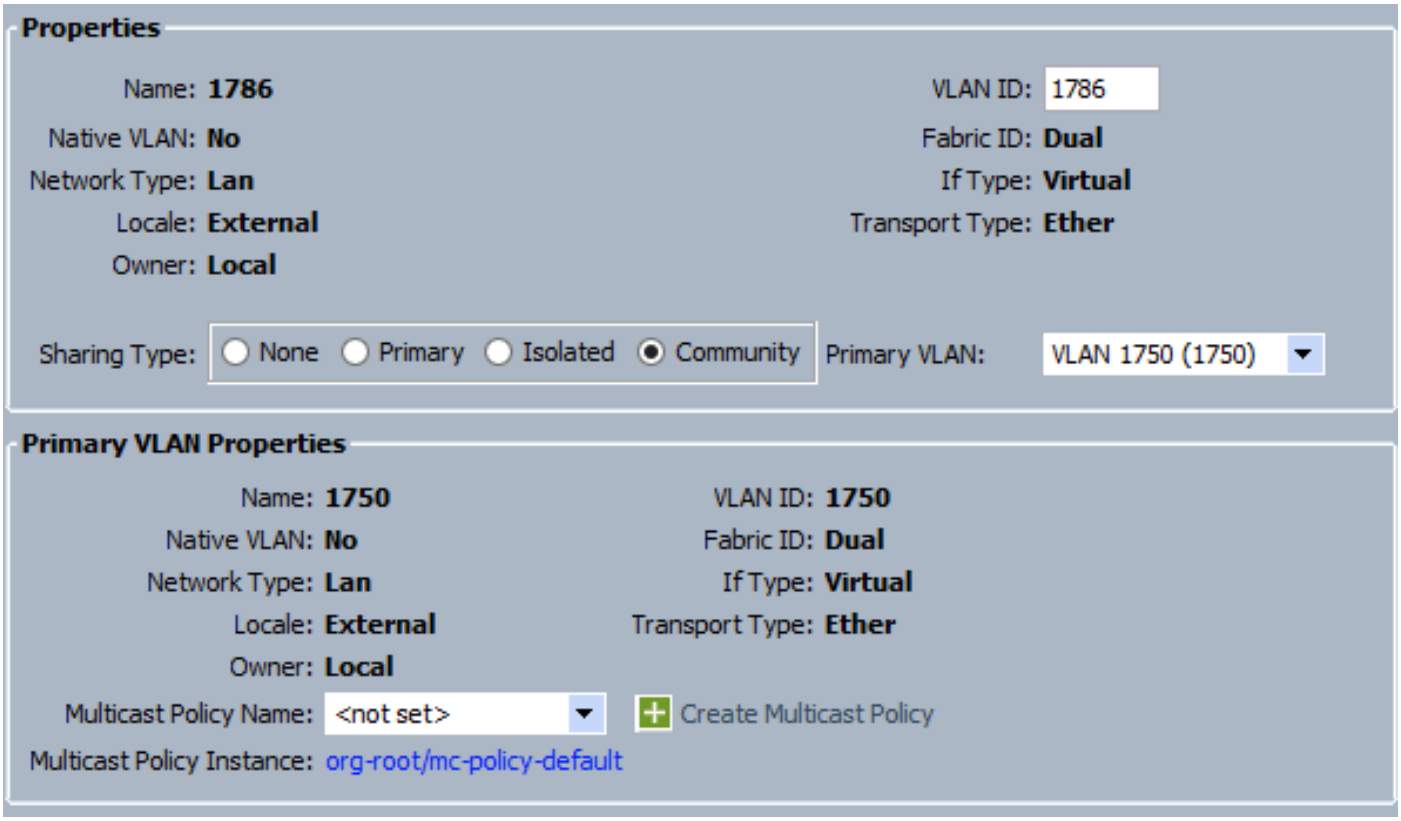
带VMware DVS的UCS

1. 要创建主VLAN，请单击**主**单选按钮作为共享类型，并输入**VLAN ID** 1750，如图所示。

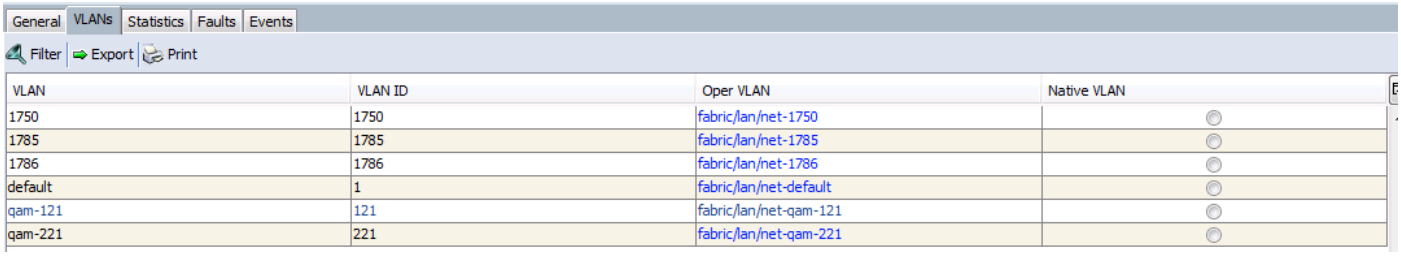


2.如图**所示**，相**应创**建隔离和社区VLAN。这些都不必是本征VLAN。





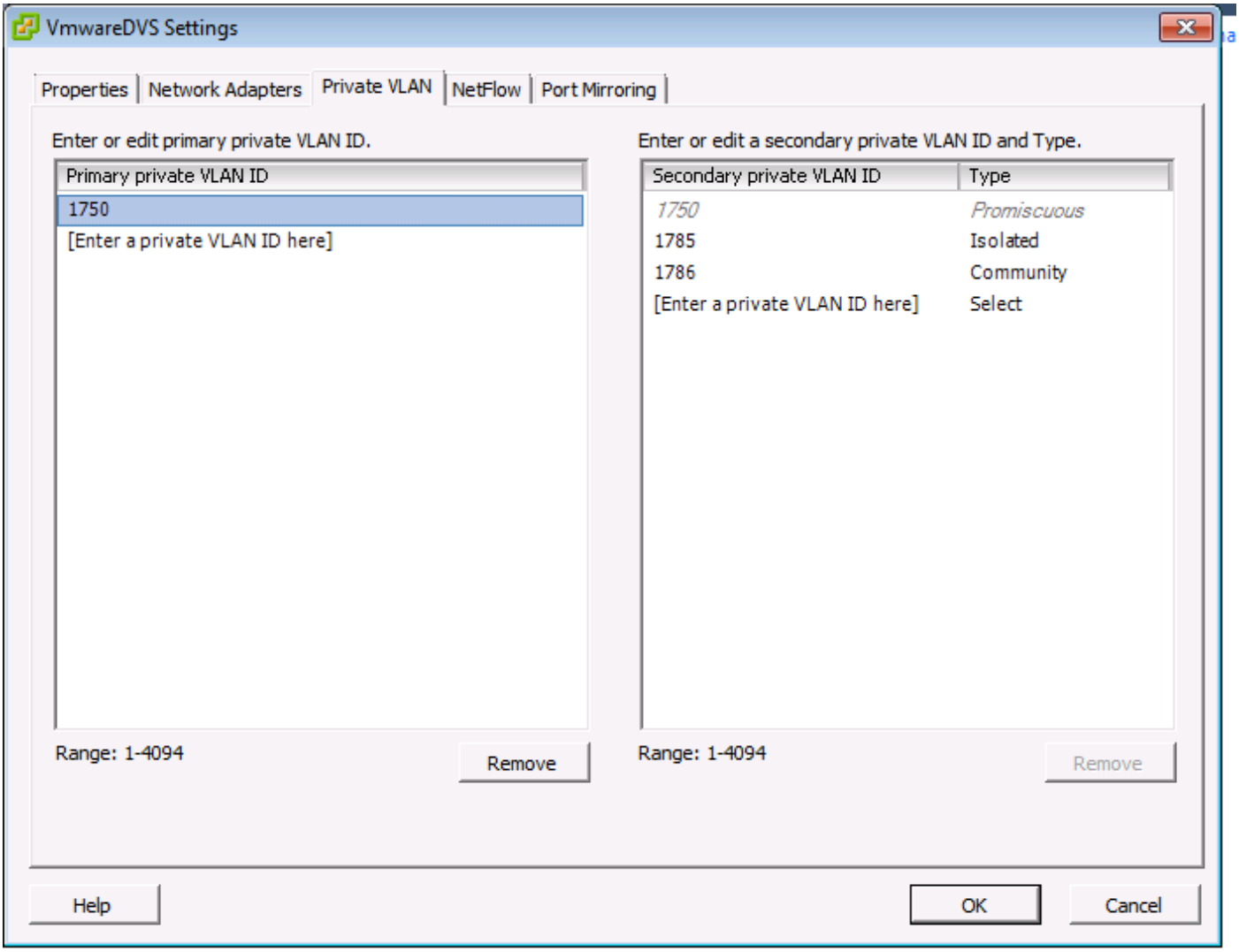
3.服务配置文件上的虚拟网络接口卡(vNIC)传输常规VLAN和PVLAN，如图所示。

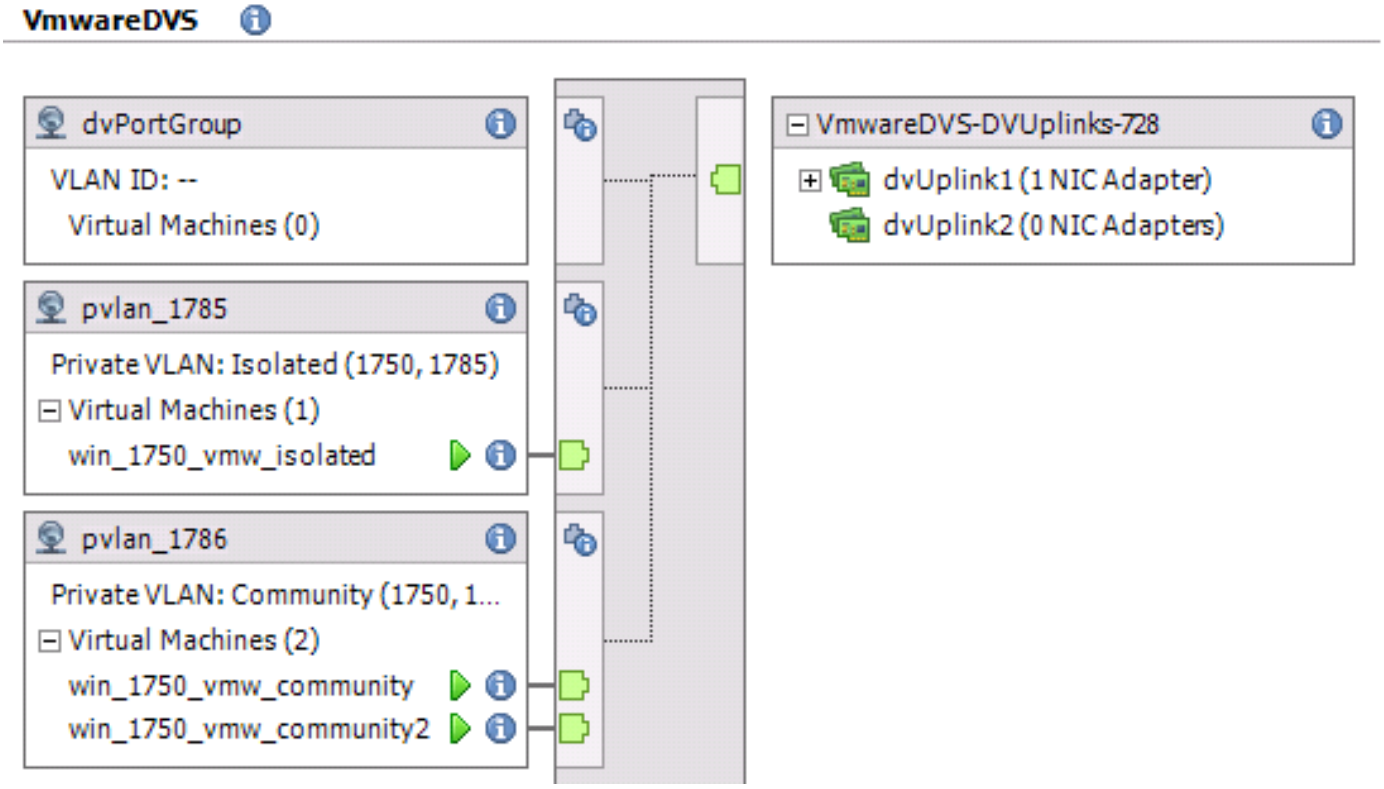


4. UCS上的上行链路端口通道传输常规VLAN和PVLAN:

```
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)

上游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
```

UCS版本3.1(3)的行为更改

在UCS版本3.1(3)之前，您可以在VMware DVS上的社区VLAN中的VM与主VLAN中的VM通信，主VLAN VM驻留在UCS内。此行为不正确，因为主VM必须始终是北向或UCS外部。此行为通过缺陷ID CSCvh87378记录 。

从UCS版本2.2(2)开始，由于代码有缺陷，社区VLAN能够与FI后的主VLAN通信。但Isolated永远无法与FI后的主通信。两个（隔离和社区）虚拟机仍能与FI外的主机通信。

从3.1(3)开始，此缺陷允许社区与FI后的主VM通信，已进行修正，因此社区VM将无法与驻留在UCS内的主VLAN中的VM通信。

要解决此情况，需要将主VM移到UCS之外（北向）。如果不能，则需要将主VM移入另一个VLAN，该VLAN是常规VLAN，而不是专用VLAN。

例如，在固件3.1(3)之前，团体VLAN 1786中的VM可以与驻留在UCS中的主要VLAN 1750中的VM通信，但是，如图所示，此通信会在固件3.1(3)及更高版本中中断。

NOTE:

—

CSCvh87378在3.2(3l)和4.0.4e及更高版本中已编址，因此我们可以在UCS后面设置主VLAN。但请注意，UCS内的隔离VLAN将无法与UCS内的主VLAN通信。当两个UCS后面都处于UCS之后时

，只有社区VLAN和主VLAN可以相互通信。

```
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)#
```

上游4900交换机

注意：在本例中，4900是到外部网络的L3接口。如果第3层的拓扑不同，请相应地进行更改

在4900交换机上，执行以下步骤，并设置混杂端口。PVLAN在混杂端口结束。

1. 根据需要打开PVLAN功能。
2. 按照Nexus 5K上的操作创建并关联VLAN。
3. 在4900交换机的出口端口上创建混杂端口。从此时开始，VLAN 1785和1786的数据包在VLAN 1750上出现。

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

在上游路由器上，仅为VLAN 1750创建子接口。在此级别，要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

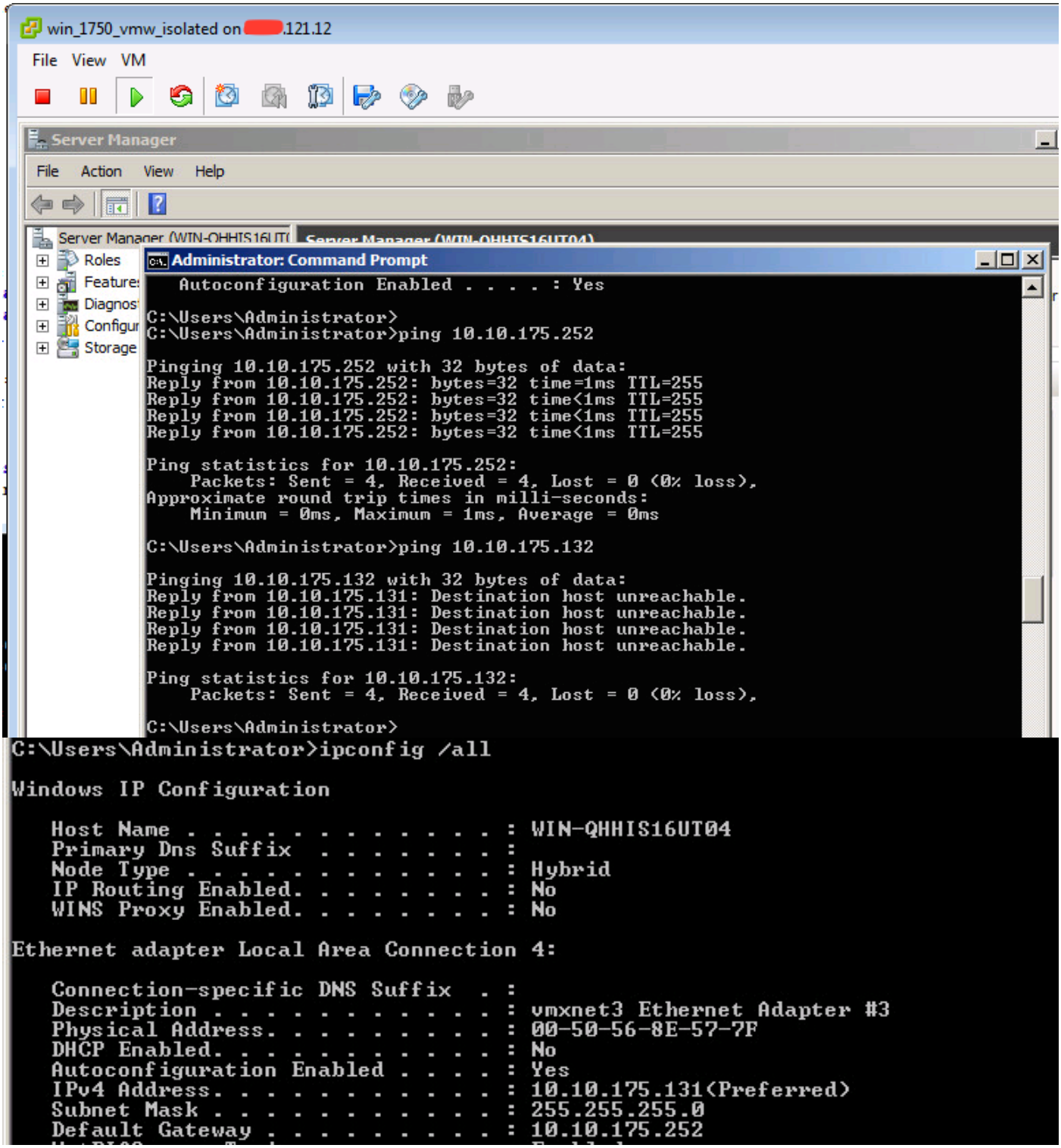
当前没有可用于此配置的验证过程。

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。

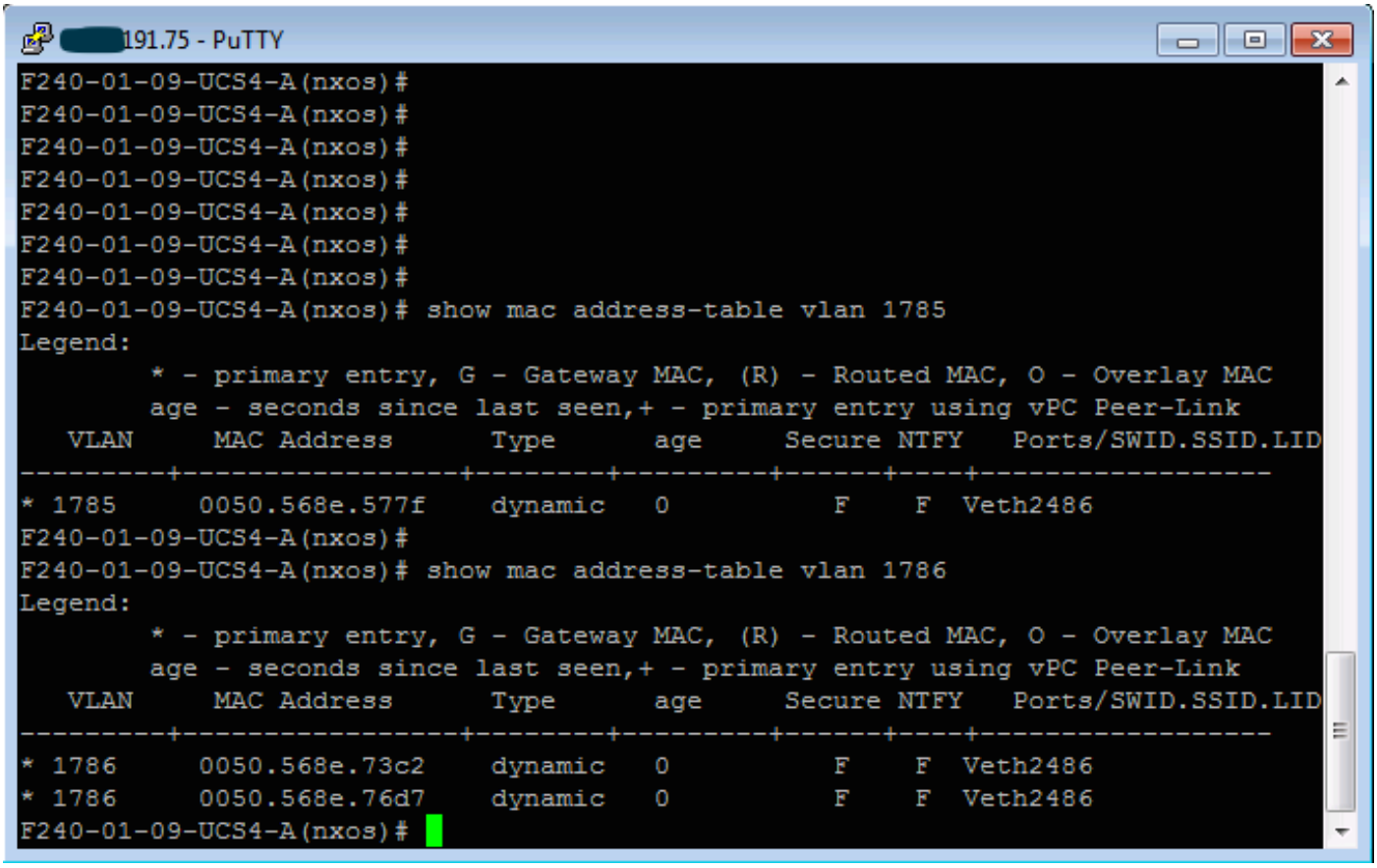
此过程介绍如何使用PVLAN测试VMware DVS的配置。

1.对端口组中配置的其他系统以及混杂端口上的路由器或其他设备执行ping操作。对经过混杂端口的设备执行ping操作必须有效，而对隔离VLAN中其他设备执行ping操作必须失败，如图所示。



检查MAC地址表，以查看MAC的学习位置。在所有交换机上，MAC必须位于隔离VLAN中，但具有混杂端口的交换机除外。在混杂交换机上，MAC必须位于主VLAN中。

2.如图所示的UCS。



3.检查上游n5k上是否有相同的MAC，n5k上必须存在与早期输出类似的输出，如图所示。

```
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#
```

在上游N5k上配置Nexus 1000v和混杂端口

UCS配置

UCS配置（包括服务配置文件vNIC配置）与VMware DVS的示例相同。

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
```

此步骤介绍如何测试配置。

1.对端口组中配置的其他系统以及混杂端口上的路由器或其他设备执行ping操作。对经过混杂端口的设备执行ping操作必须有效，而对隔离VLAN中的其他设备执行ping操作必须失败，如上一节和映像所示。