Configure Private VLAN and UCS with VMware DVS or Cisco Nexus 1000v

Contents

Introduction

This document describes the private VLAN (PVLAN) support for the Cisco Unified Computing System (UCS) in 2.2(2c) release and later.

> **Caution**: There is a change in behavior starting with UCS firmware version 3.1(3a) as described in the **Behavior Change with UCS Version 3.1(3) and Later** section.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- UCS
- Cisco Nexus 1000V (N1K) or VMware Distributed Virtual Switch (DVS)

- VMware
- Layer 2 (L2) switching

Components Used

This document is not restricted to specific software and hardware versions.

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.

Background Information

A private VLAN is a VLAN configured for L2 isolation from other ports within the same private VLAN. Ports that belong to a PVLAN are associated with a common set of support VLANs, which are used in order to create the PVLAN structure.

There are three types of PVLAN ports:

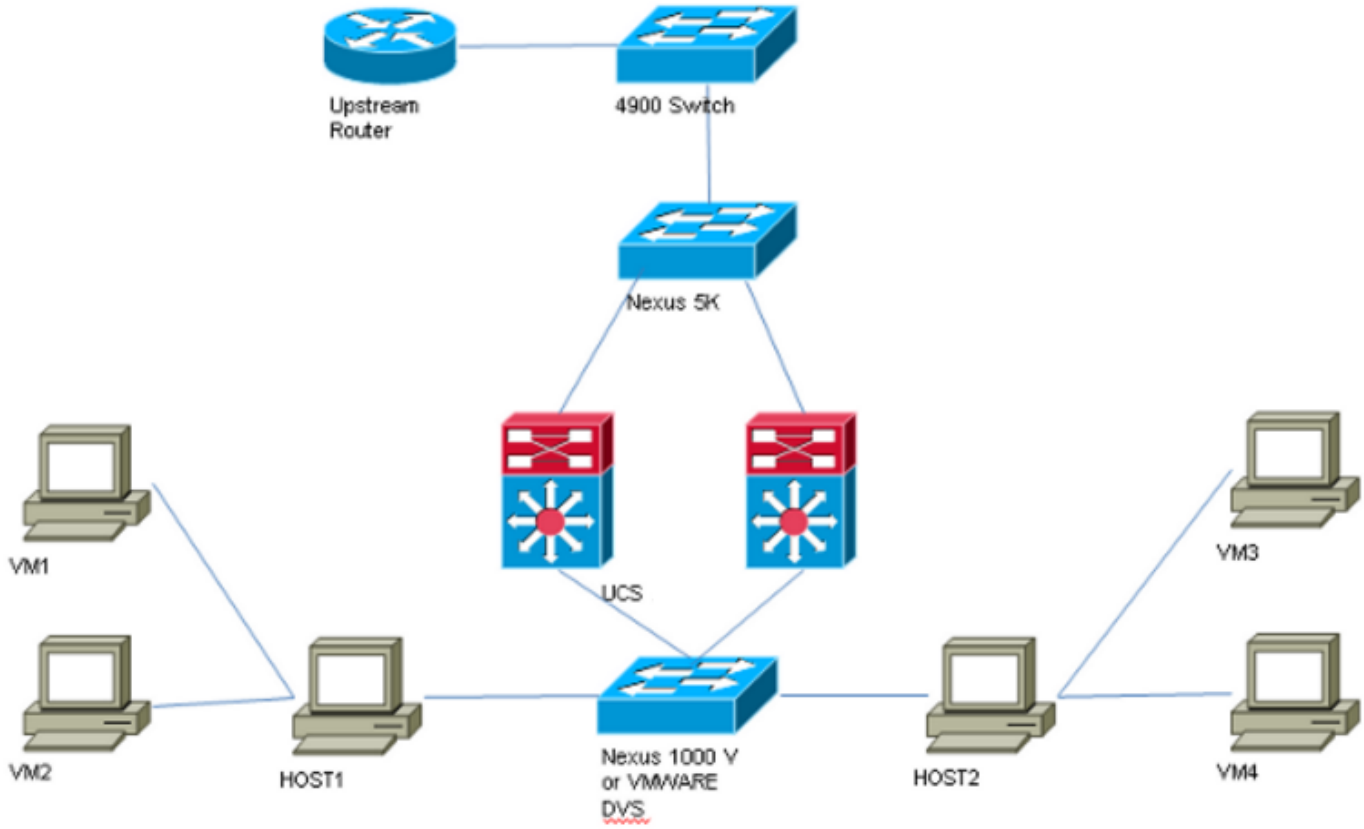
- A promiscuous port communicates with all other PVLAN ports and is the port used in order to communicate with devices outside of the PVLAN.
- An isolated port has complete L2 separation (which includes broadcasts) from other ports within the same PVLAN with the exception of the promiscuous port.
- A community port can communicate with other ports in the same PVLAN as well as the promiscuous port. Community ports are isolated at L2 from ports in other communities or isolated PVLAN ports. Broadcasts are only propagated to other ports in the community and the promiscuous port.

Refer to RFC 5517, Cisco Systems' Private VLANs: Scalable Security in a Multi-Client Environment in order to understand the theory, operation, and concepts of PVLANs.

Configure

Network Diagram

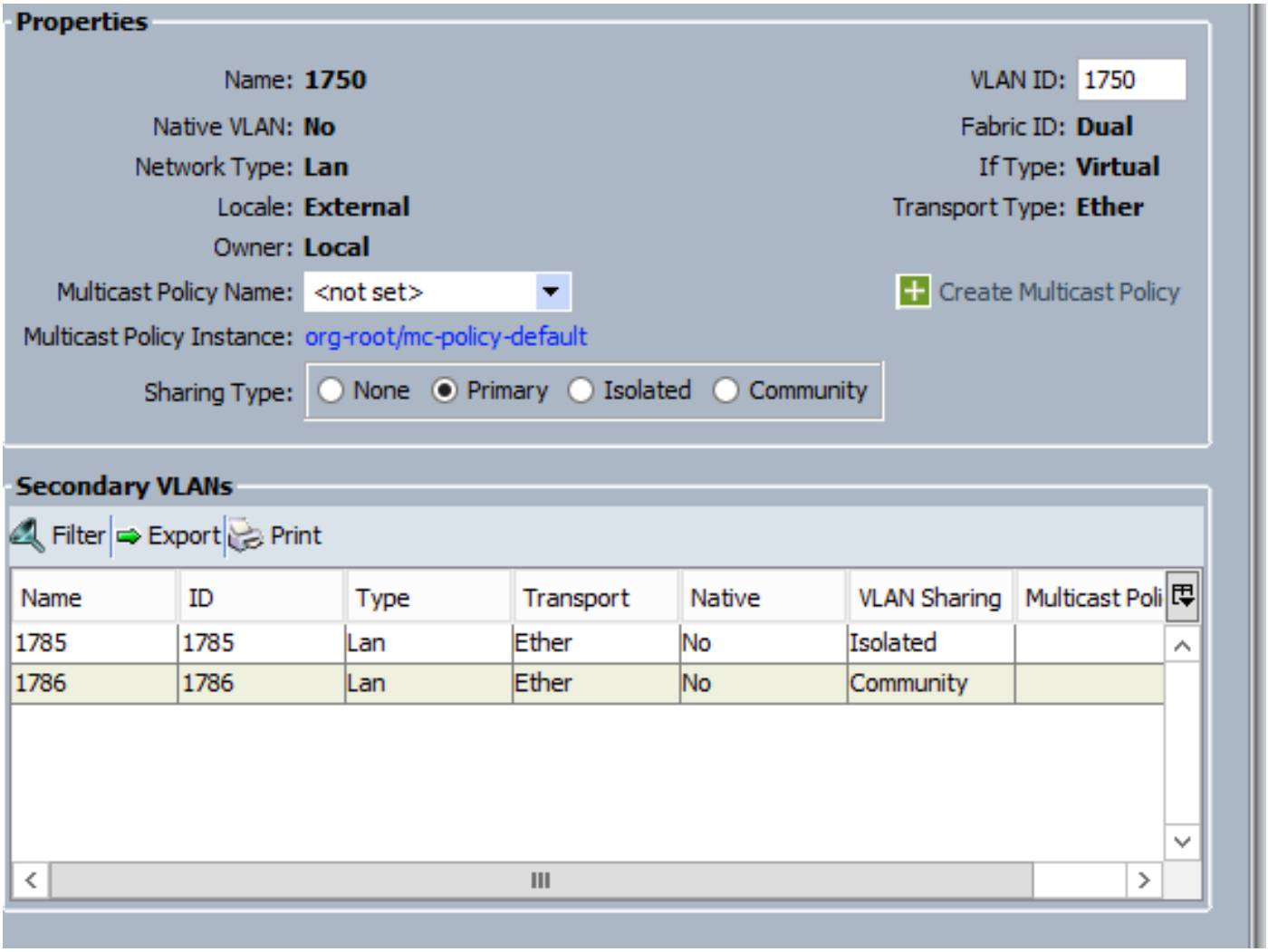
With Nexus 1000v or VMware DVS



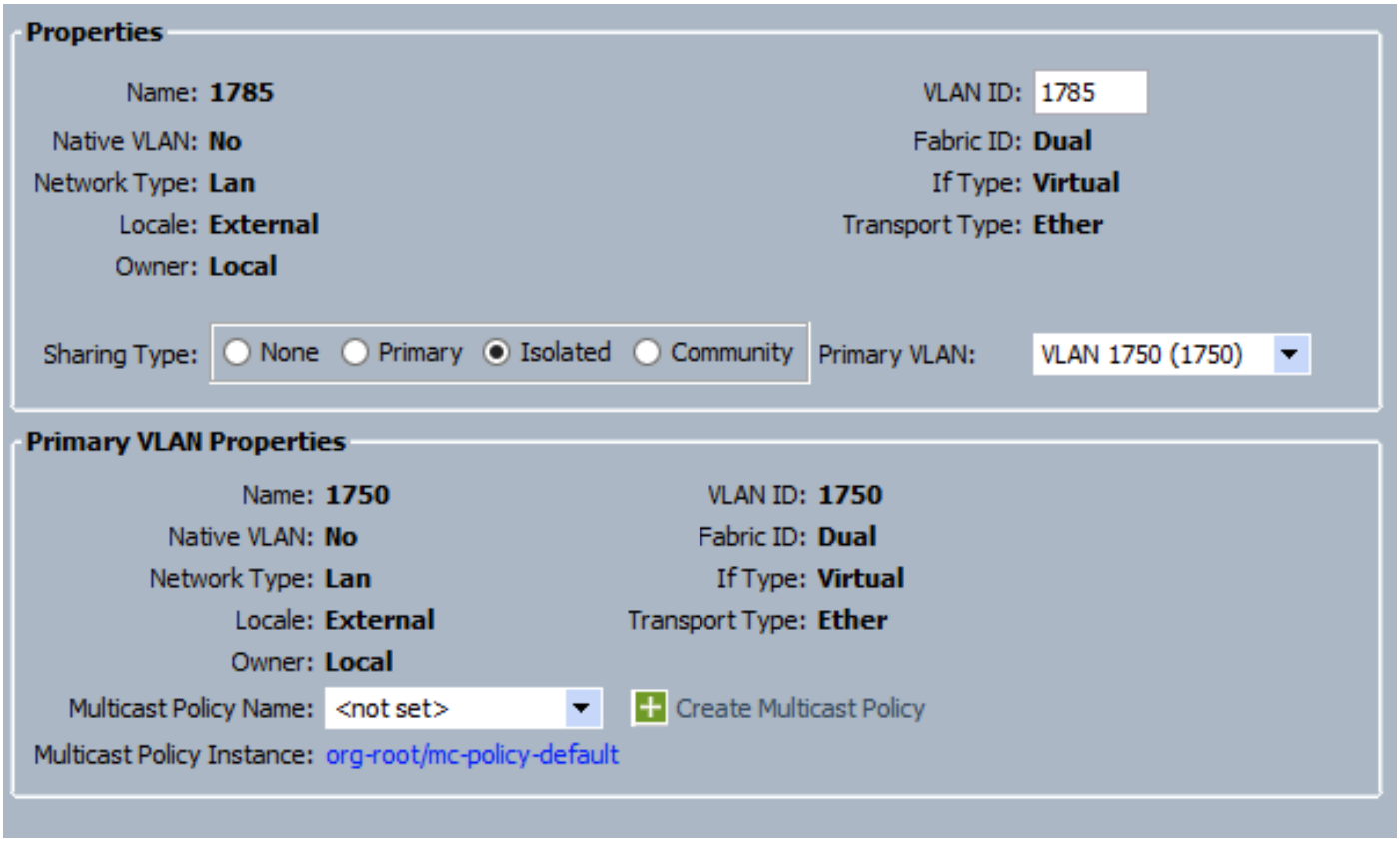
Note: This example uses VLAN 1750 as the primary, 1785 as isolated and 1786 as community VLAN.

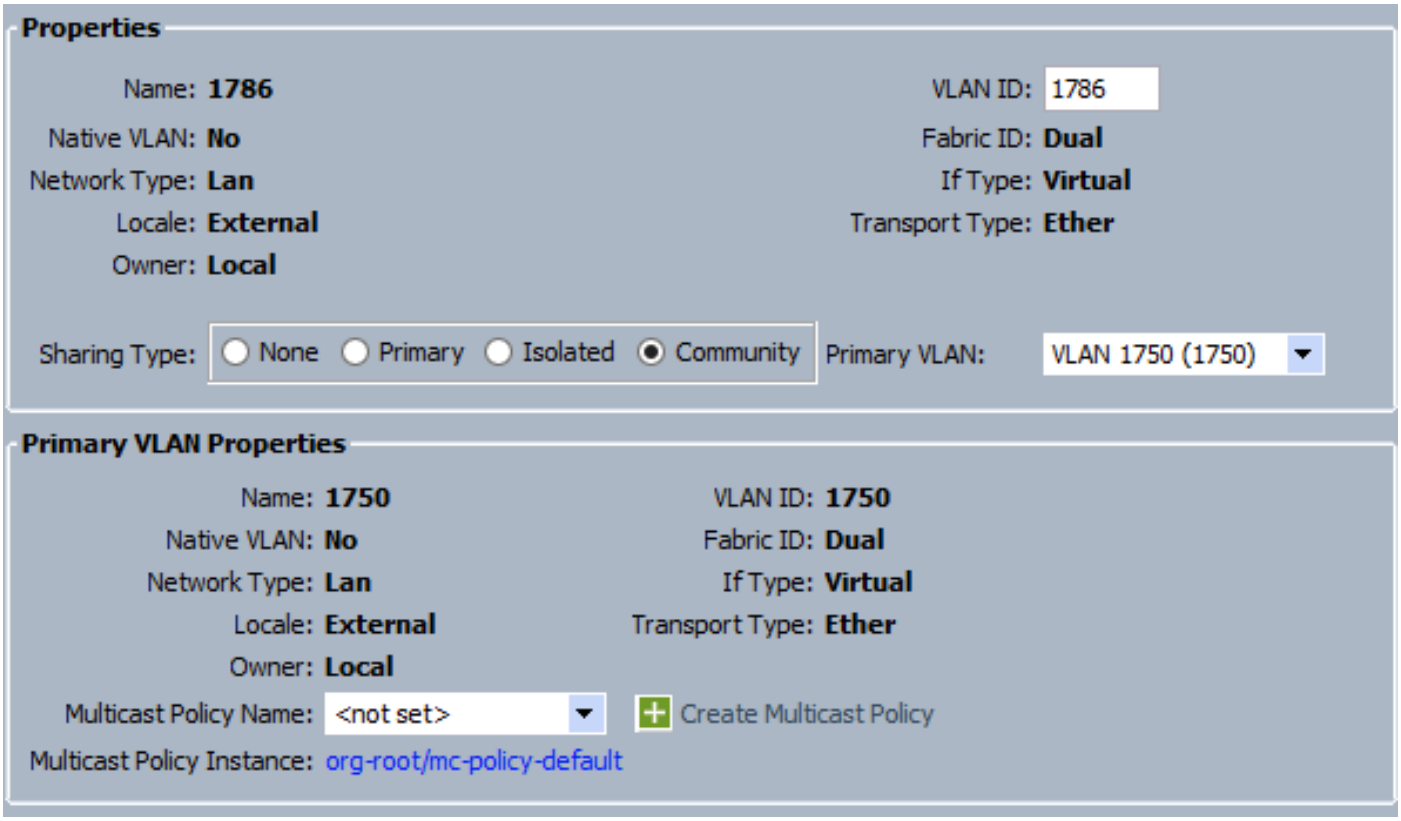
UCS with VMware DVS

1. In order to create the primary VLAN, click **Primary** radio button as the Sharing Type, and enter a **VLAN ID** of 1750 as shown in the image.

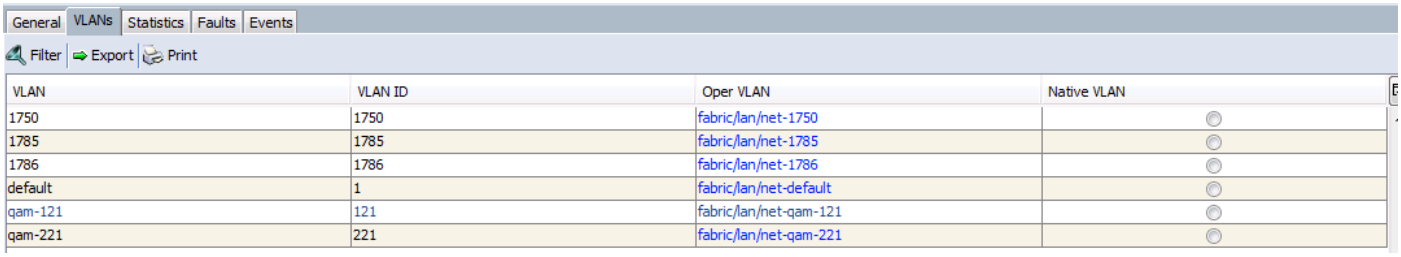


2. Create **Isolated** and **Community** VLANs accordingly as shown in the images. None of these has to be a Native VLAN.





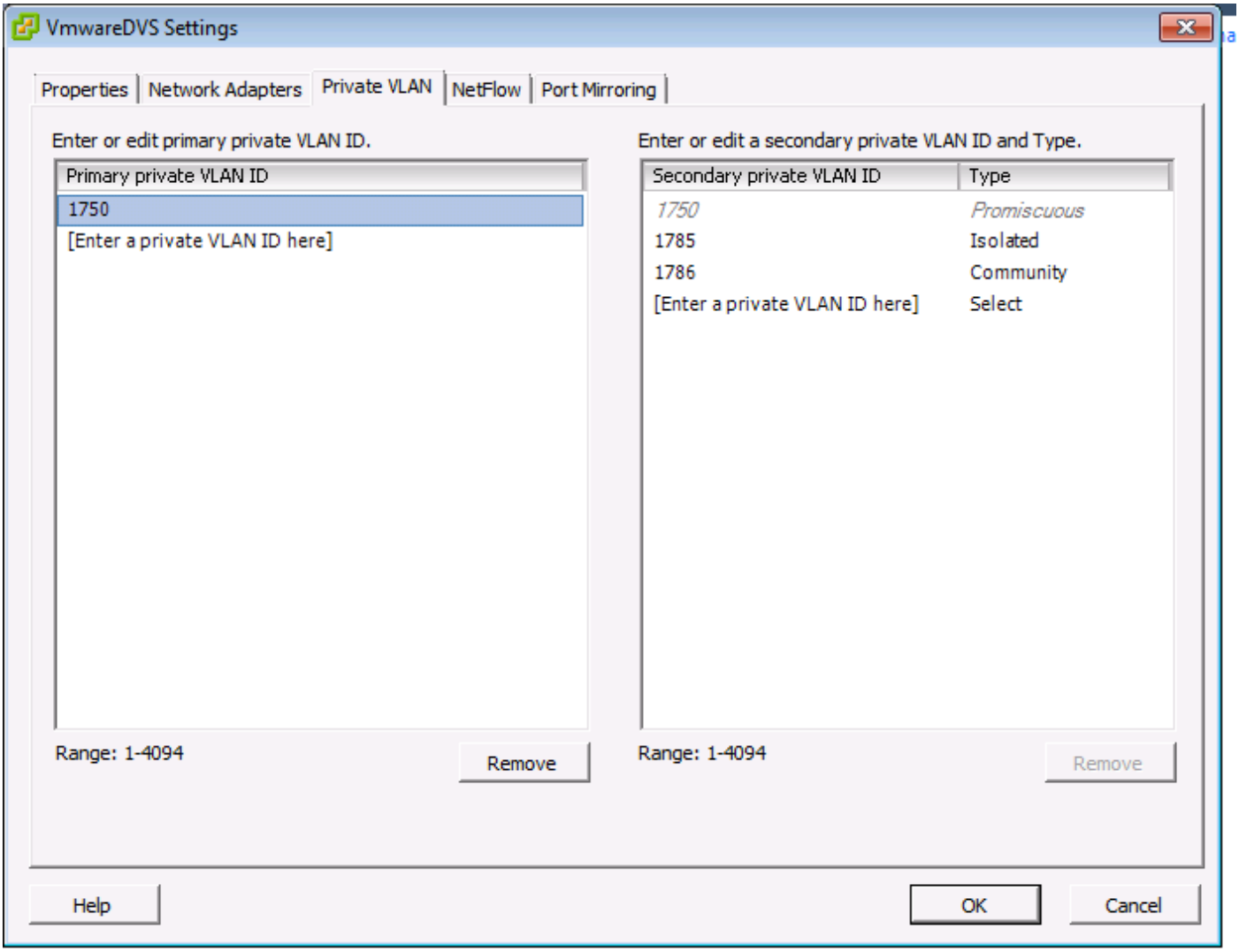
3. Virtual Network Interface Card (vNIC) on service-profile carries regular VLANs as well as PVLANs, as seen in the image.

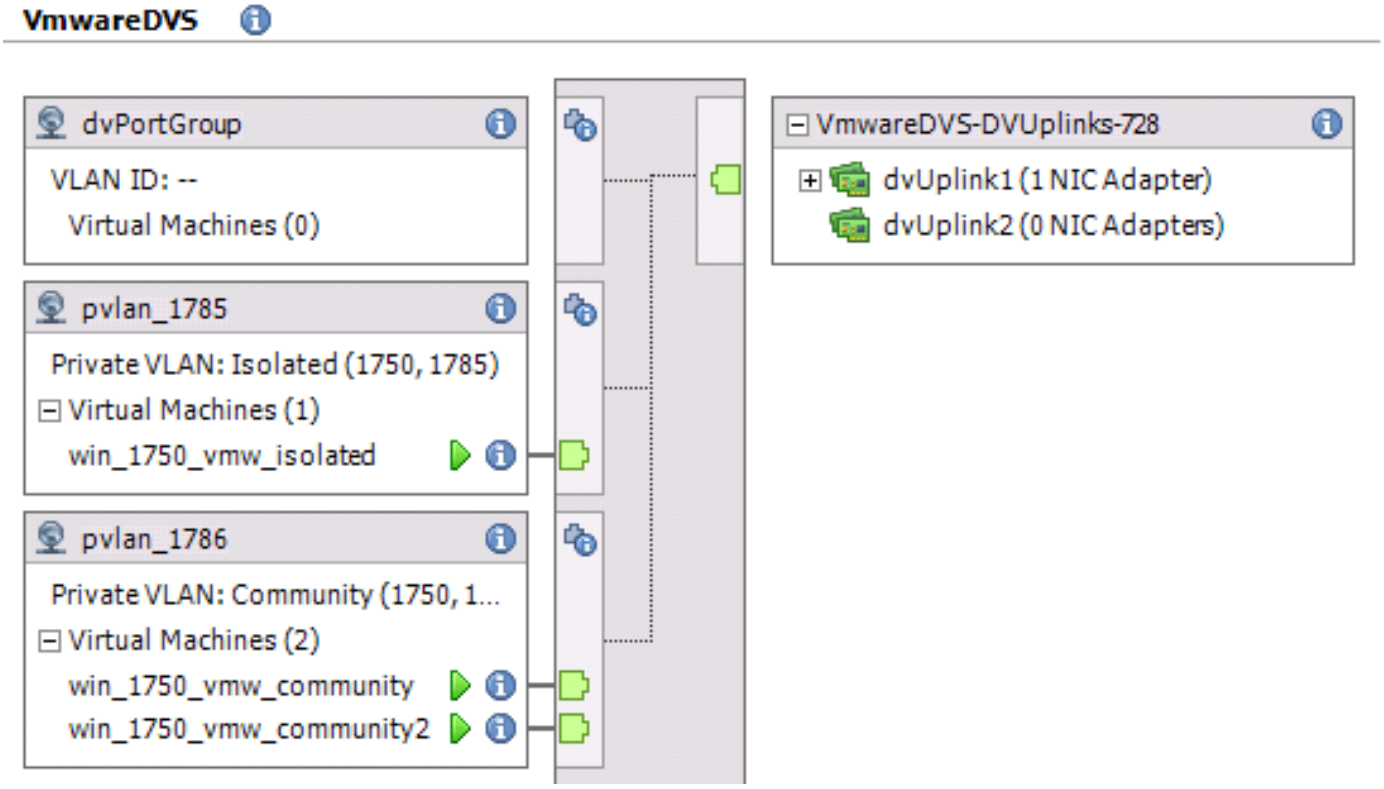


4. Uplink port-channel on UCS carries regular VLANs as well as PVLANs:

```
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





Upstream N5k Switch

```
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
```

Behavior Change with UCS Version 3.1(3)

Prior to UCS version 3.1(3), you could have a VM in community VLAN communicate with a VM in Primary VLAN on VMware DVS where the Primary VLAN VM resides inside the UCS. This behavior was incorrect as the primary VM must always be northbound or outside of the UCS. This behavior is documented via defect ID CSCvh87378 .

From UCS version 2.2(2) onwards, due to a defect in the code, community VLAN was able to communicate with primary VLAN that was present behind the FI. But Isolated could never communicate with the primary behind the FI. Both (isolated and community) VMs are still able to communicate with the primary outside the FI.

From 3.1(3) onwards, this defect allows community to communicate with primary behind the FI, was rectified and thus community VMs won't be able to communicate with a VM in primary VLAN which resides within UCS.

In order to resolve this situation, the primary VM would either need to be moved (northbound) outside of UCS. If that’s not an option, then the primary VM would need to be moved into another VLAN that is a regular VLAN and not a private VLAN.

For example, prior to firmware 3.1(3), a VM in community VLAN 1786 could communicate to a VM in primary VLAN 1750 which resides within UCS, however, this communication would break in firmware 3.1(3) and later, as shown in the image.

NOTE:

CSCvh87378 has been addressed in 3.2(3l) and 4.0.4e & higher so we can have Primary Vlan behind UCS. However please note that isolated vlan inside UCS won't be able to talk to primary vlan inside UCS. Only community vlan & primary vlan can talk to each other when both are behind UCS.

```
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)#
```

Upstream 4900 Switch

> **Note**: In this example, 4900 is L3 interface to outside network. If your topology for L3 is different, then kindly make changes accordingly

On the 4900 switch, take these steps, and set up the promiscuous port. The PVLAN ends at the promiscuous port.

1. Turn on PVLAN feature if required.
2. Create and associate the VLANs as done on the Nexus 5K.
3. Create the promiscuous port on the egress port of the 4900 switch. From this point on, the packets from VLAN 1785 & 1786 are seen on VLAN 1750 in this case.

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

On the upstream router, create a subinterface for the VLAN 1750 only. At this level, the requirements depend upon the network configuration you use:

```
interface GigabitEthernet0/1.1

encapsulation dot1Q 1750

IP address10.10.175.254/24
```

Verify

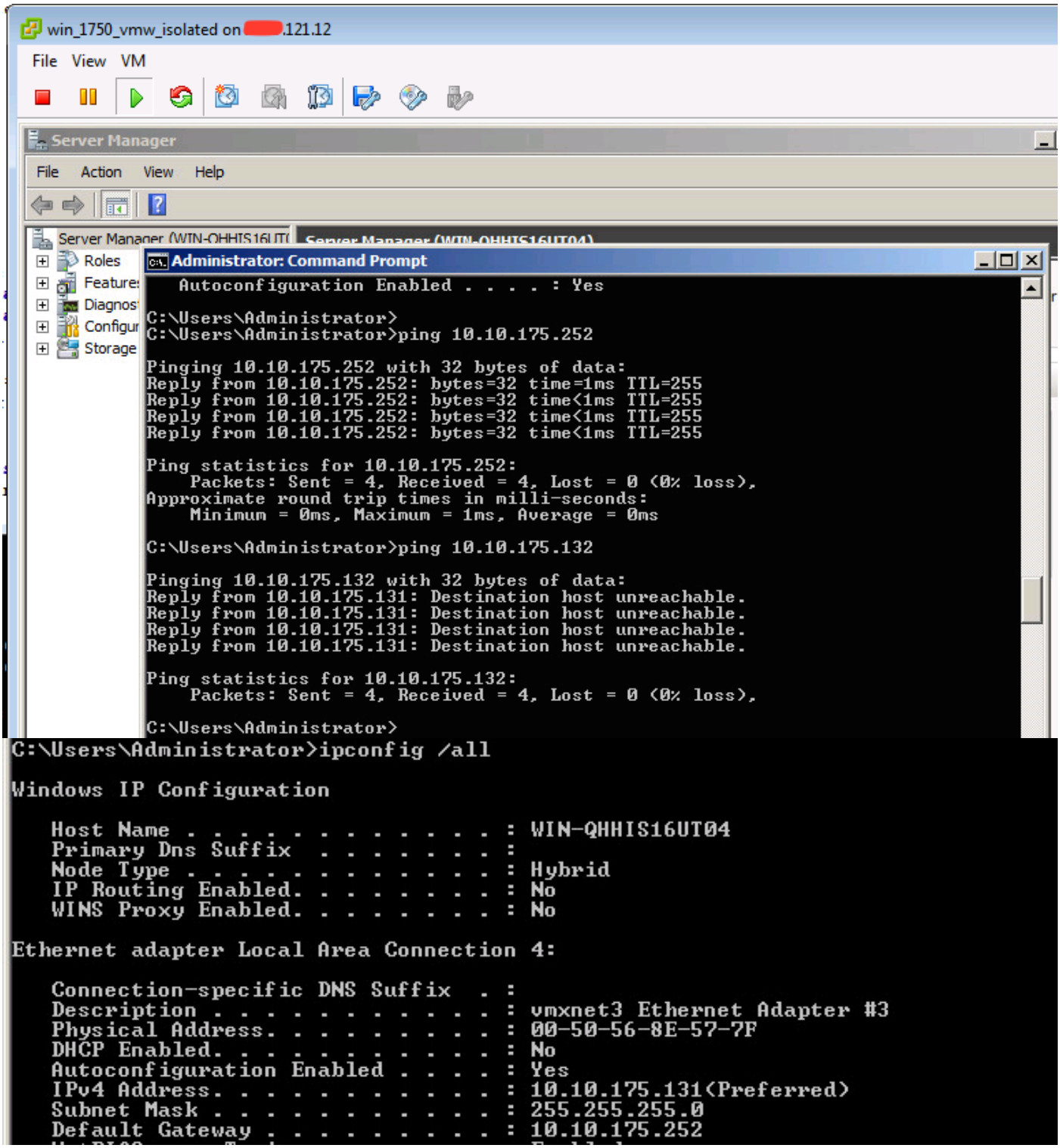
There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

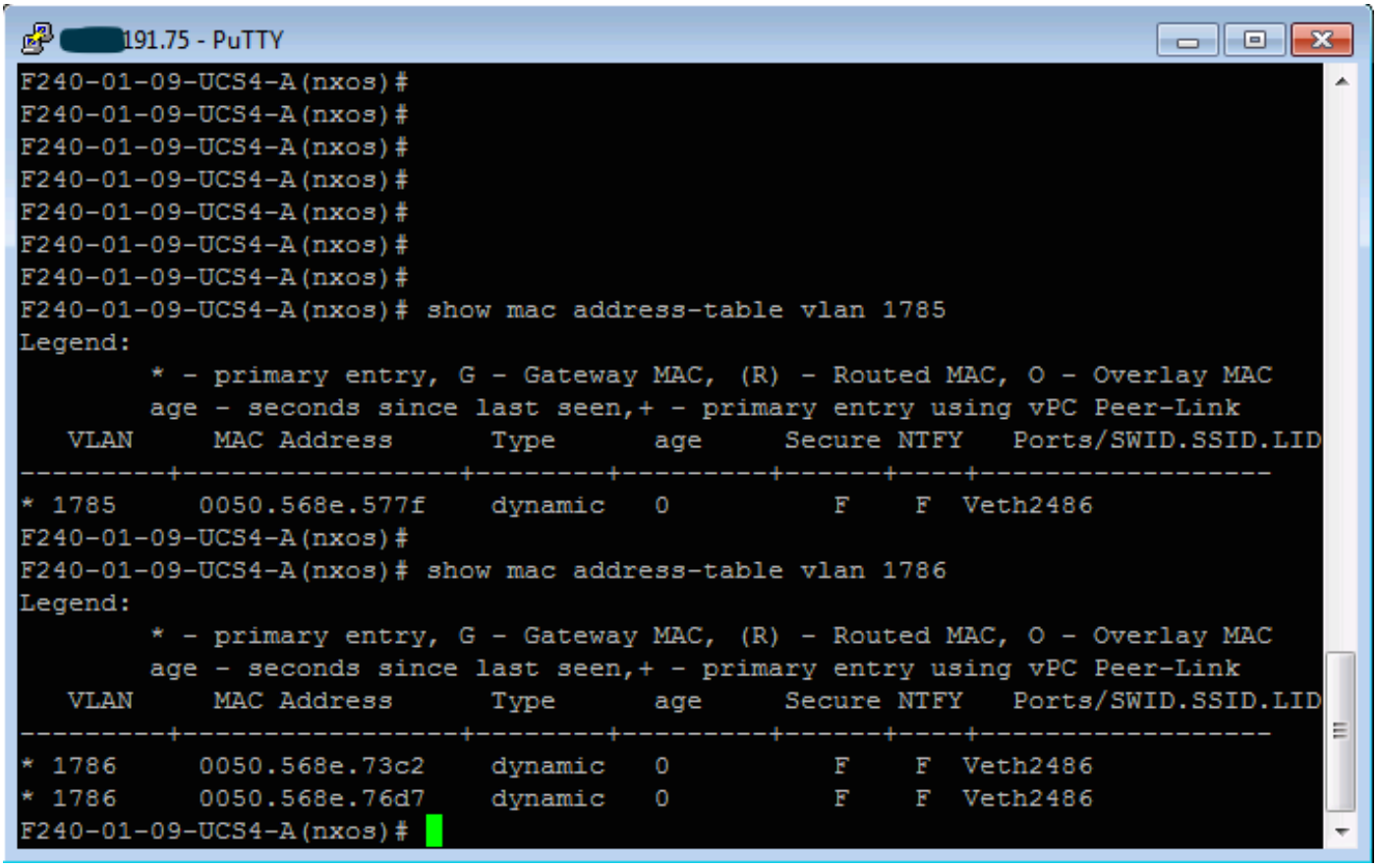
This procedure describes how to test the configuration for VMware DVS with the use of PVLAN.

1. Run pings to other systems configured in the port-group as well as the router or other device at the promiscuous port. Pings to the device past the promiscuous port must work, while those to other devices in the isolated VLAN must fail as shown in the images.



Check the MAC address tables in order to see where your MAC is being learned. On all switches, the MAC must be in the isolated VLAN except on the switch with the promiscuous port. On the promiscuous switch, the MAC must be in the primary VLAN.

2. UCS as shown in the image.



3. Check on upstream n5k for same MAC, output similar to earlier output must be present on n5k and as shown in the image.

```
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#
```

Configuration with Nexus 1000v with Promiscuous Port on Upstream N5k

UCS Configuration

UCS configuration (which includes service-profile vNIC configuration) stays the same as per the example with VMware DVS.

N1k Configuration

```
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
```

This procedure describes how to test the configuration.

1. Run pings to other systems configured in the port-group as well as the router or other device at the promiscuous port. Pings to the device past the promiscuous port must work, while those to other devices in the isolated VLAN must fail, as shown in previous section and in the images.