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

Contents

Introduction

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

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- UCS
- Cisco Nexus 1000 V (N1K) or Vmware DVS
- VMware
- Layer 2 (L2) switching

Components Used

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

Theory

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.

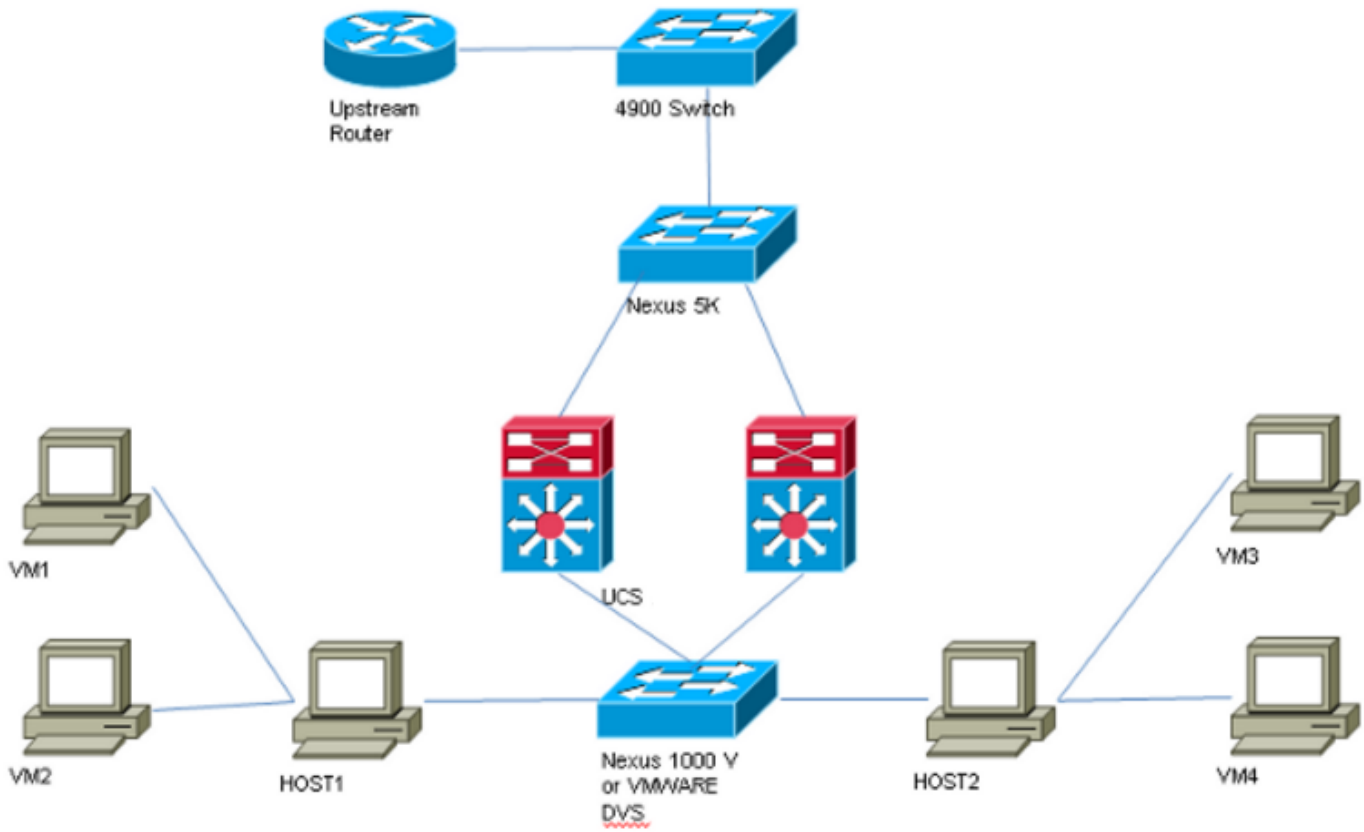
There are three types of PVLAN ports:

- 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 (including 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

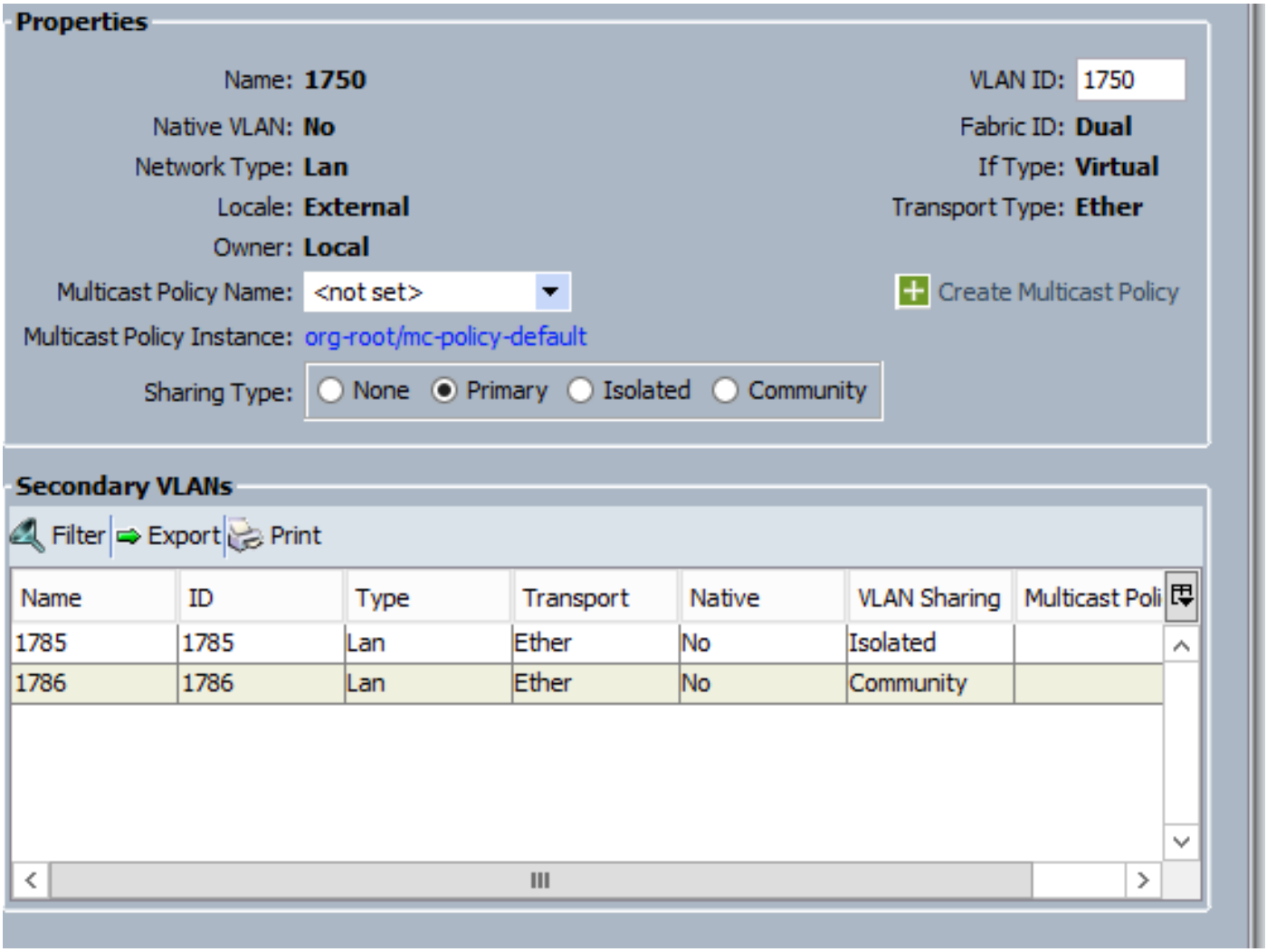
with Nexus 1000v or Vmware DVS



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

UCS Configuration with VMware DVS

1. In order to create the primary VLAN, click **Primary** as the Sharing Type, and enter a **VLAN ID** of 1750:



2. Create Isolated & Community Vlans accordingly as below. None of these has to be a Native Vlan

Properties

Name: **1785**
Native VLAN: **No**
Network Type: **Lan**
Locale: **External**
Owner: **Local**

VLAN ID: 1785
Fabric ID: **Dual**
If Type: **Virtual**
Transport Type: **Ether**

Sharing Type: ○ None ○ Primary ◉ Isolated ○ Community
Primary VLAN: VLAN 1750 (1750)

Primary VLAN Properties

Name: **1750**
Native VLAN: **No**
Network Type: **Lan**
Locale: **External**
Owner: **Local**

VLAN ID: **1750**
Fabric ID: **Dual**
If Type: **Virtual**
Transport Type: **Ether**

Multicast Policy Name: <not set> + Create Multicast Policy
Multicast Policy Instance: org-root/mc-policy-default

Properties

Name: **1786**
Native VLAN: **No**
Network Type: **Lan**
Locale: **External**
Owner: **Local**

VLAN ID: 1786
Fabric ID: **Dual**
If Type: **Virtual**
Transport Type: **Ether**

Sharing Type: ○ None ○ Primary ○ Isolated ◉ Community
Primary VLAN: VLAN 1750 (1750)

Primary VLAN Properties

Name: **1750**
Native VLAN: **No**
Network Type: **Lan**
Locale: **External**
Owner: **Local**

VLAN ID: **1750**
Fabric ID: **Dual**
If Type: **Virtual**
Transport Type: **Ether**

Multicast Policy Name: <not set> + Create Multicast Policy
Multicast Policy Instance: org-root/mc-policy-default

3. vnic on service-profile is carrying regular vlans as well as pvlans

General | VLANs | Statistics | Faults | Events

Filter | Export | Print

VLAN	VLAN ID	Oper VLAN	Native VLAN
1750	1750	fabric/lan/net-1750	
1785	1785	fabric/lan/net-1785	
1786	1786	fabric/lan/net-1786	
default	1	fabric/lan/net-default	
qam-121	121	fabric/lan/net-qam-121	
qam-221	221	fabric/lan/net-qam-221	

4.

Uplink port-channel on UCS is carrying regular vlans as well as pvlans

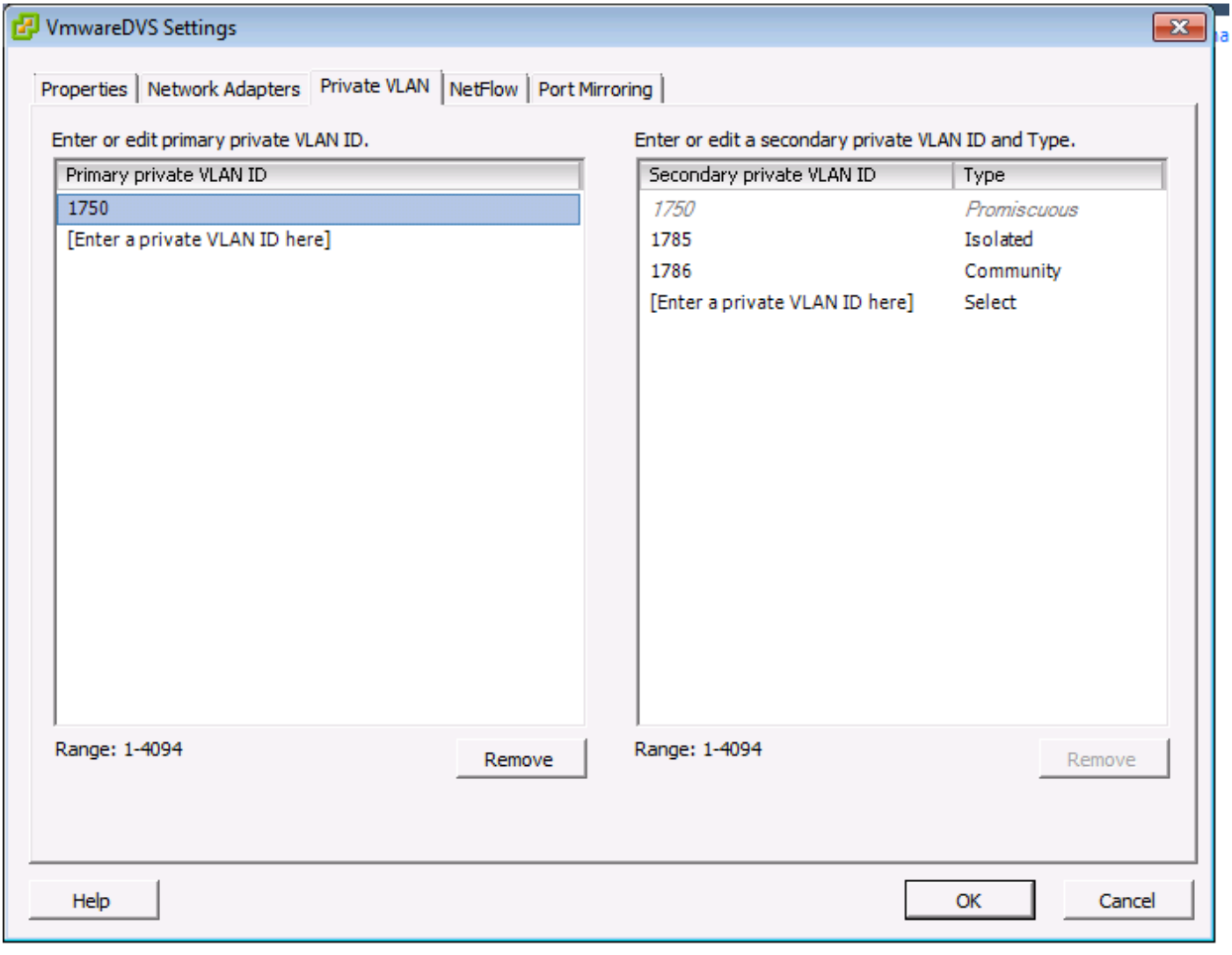
interface port-channel1
description U: Uplink
switchport mode trunk
pinning border
switchport trunk allowed vlan 1,121,221,321,1750,1785-1786
speed 10000

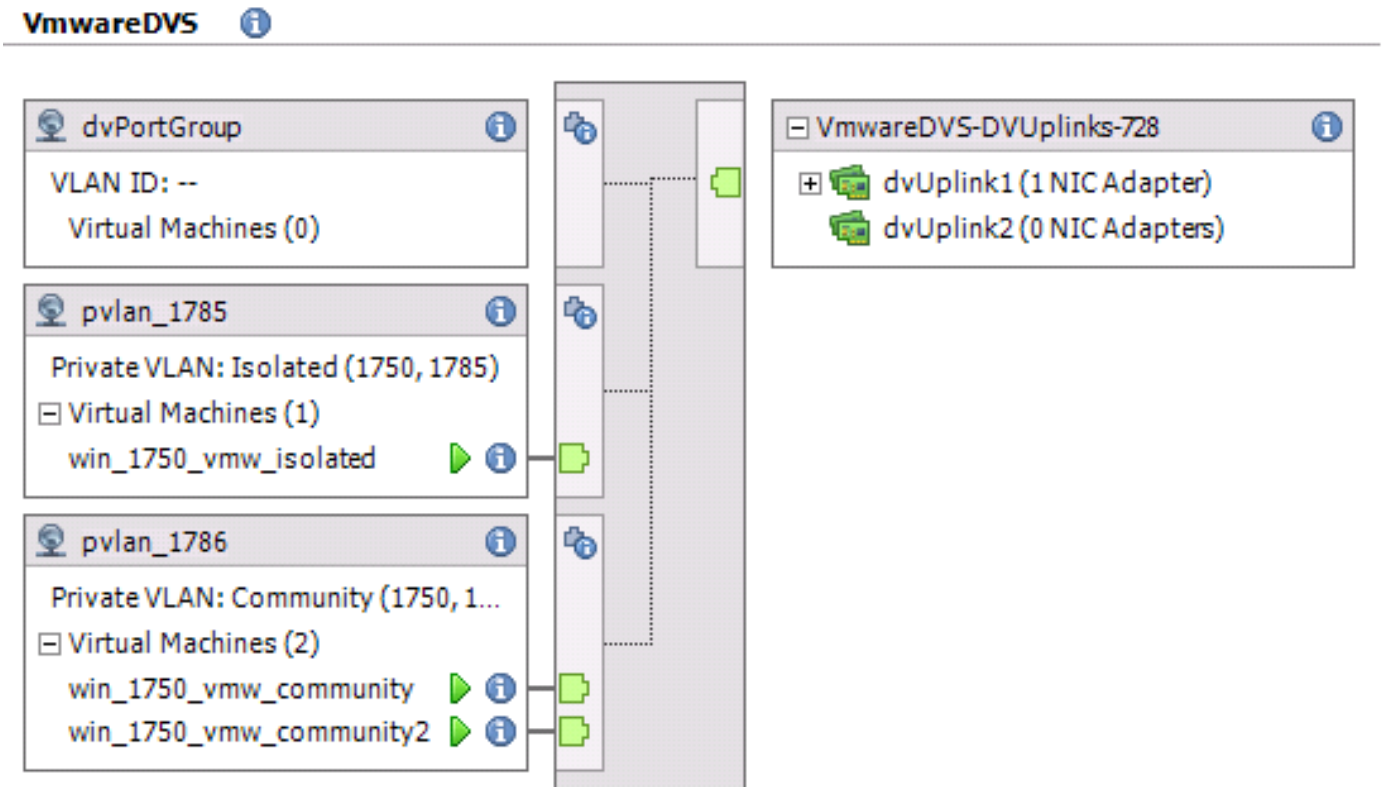
F240-01-09-UCS4-A(nxos)#

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

1750 1785 isolated
1750 1786 community

Configuration on VMware DVS





Configuration of 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

Configuration of Upstream 4900 Switch

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
```

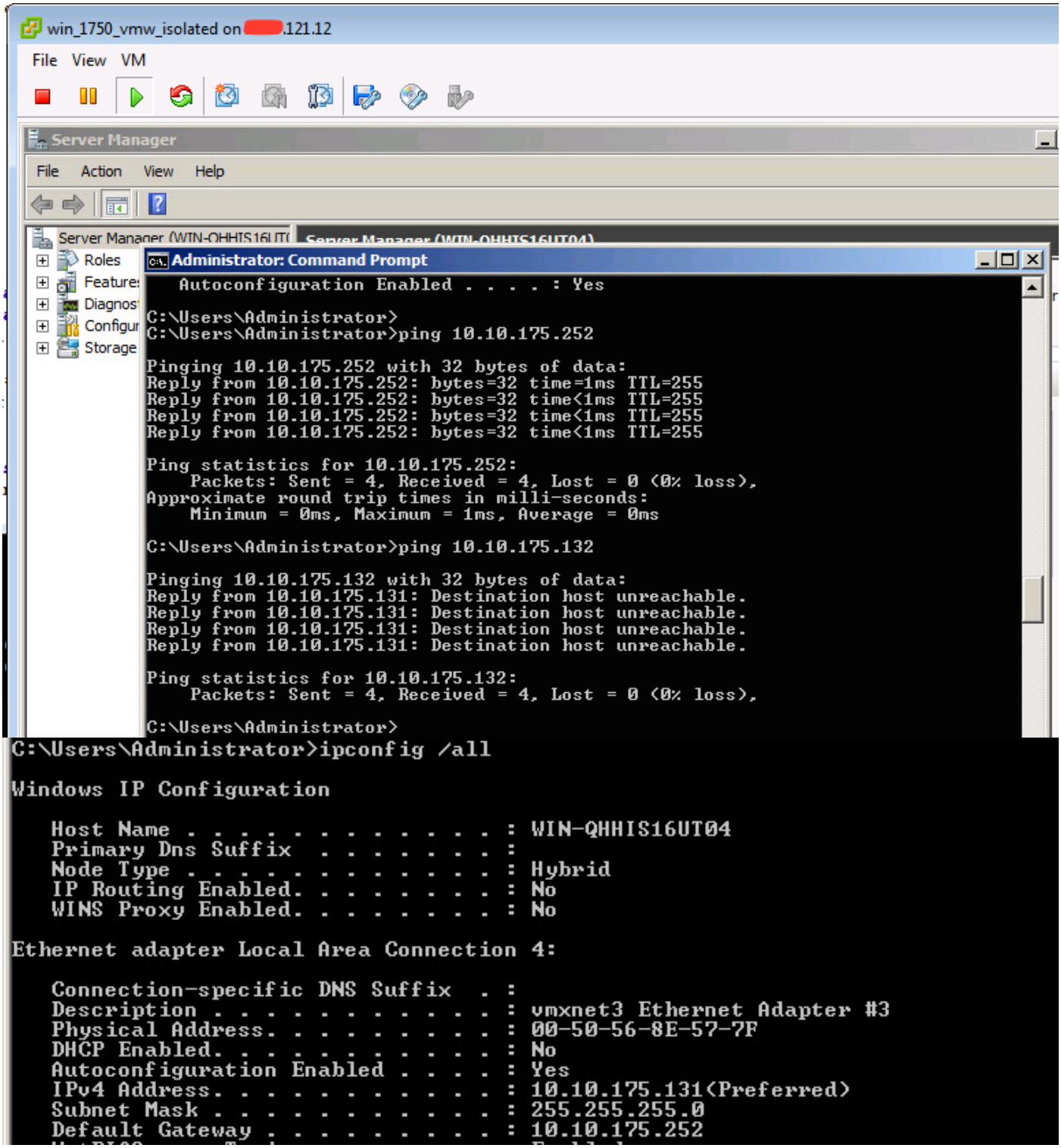
On the upstream router, create a subinterface for the VLAN 1750 only. At this level, the requirements depend upon the network configuration you are using:

1. interface GigabitEthernet0/1.1
2. encapsulation dot1Q 1750
3. IP address10.10.175.254/24

Troubleshooting

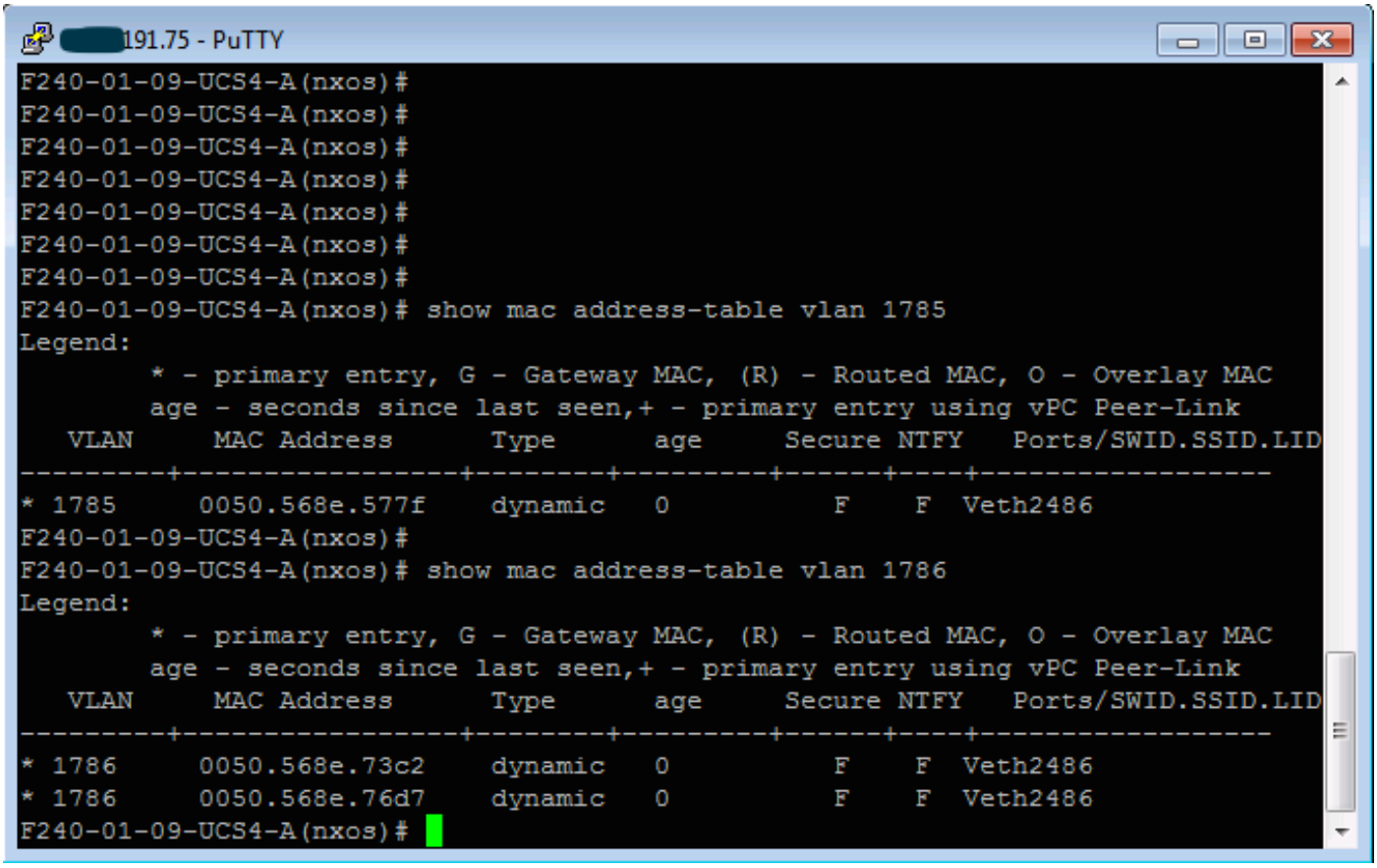
This procedure describes how to test the configuration for vmware dvs using pvlan.

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 should work, while those to other devices in the isolated VLAN should fail.



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

2. UCS



3. check on upstream n5k for same mac, output similar to above output should be present on n5k

```
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 using Nexus 1000v with Promiscous Port on Upstream N5k

UCS Configuration

UCS configuration (inclusing service-profile vnic config) will stay the same as per above 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

Troubleshooting

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 should work, while those to other devices in the isolated VLAN should fail, as shown in previous section