VMware DVSまたはCisco Nexus 1000vによるプライベートVLANおよびUCSの設定

内容

概要

このドキュメントでは、2.2(2c)リリース以降でのCisco Unified Computing System(UCS)のプライベートVLAN(PVLAN)サポートについて説明します。

> **注意**：UCSファームウェアバージョン3.1(3a)以降での動作の変更については、**「UCSバージョン3.1(3)以降での動作の変更」の項で説明されているように変更されて**います。

前提条件

要件

次の項目に関する知識があることが推奨されます。

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

- VMware
- レイヤ 2 (L2) スイッチング

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

プライベート VLAN (PVLAN) とは、同じプライベート VLAN 内の他のポートから L2 で隔離するように設定された VLAN です。PVLAN に所属するポートは、その PVLAN 構造を作成するために使用される共通のサポート VLAN のセットに関連付けられます。

PVLAN ポートには次の 3 種類があります。

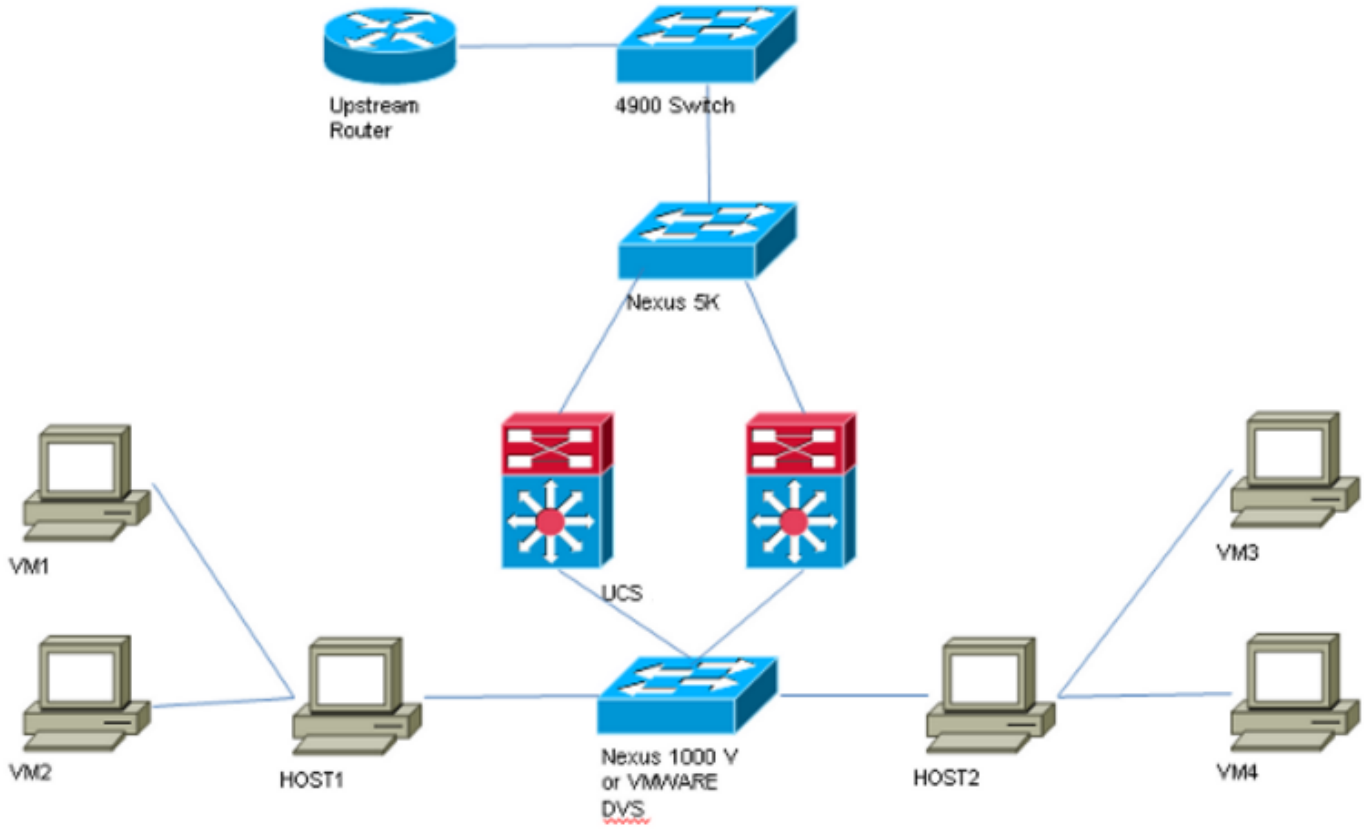
- 無差別ポートとは他のすべての PVLAN ポートと通信を行うポートであり、PVLAN 外部のデバイスと通信するために使用されます。
- 隔離ポートは、無差別ポートを除き、同じPVLAN内の他のポートから完全にL2分離 (ブロードキャストを含む) されています。
- コミュニティ ポートは、同じ PVLAN 内の他のポートならびに無差別ポートと通信できます。コミュニティ ポートは、隔離モードの PVLAN ポートと通信するために、L2 で隔離されています。ブロードキャストが伝搬されるのは、関連するコミュニティ内の他のポートおよび無差別ポートのみです。

PVLAN の理論、動作、概念については、RFC 5517、シスコのプライベート VLAN：マルチクライアント環境におけるスケーラブルなセキュリティ』を参照してください。

設定

ネットワーク図

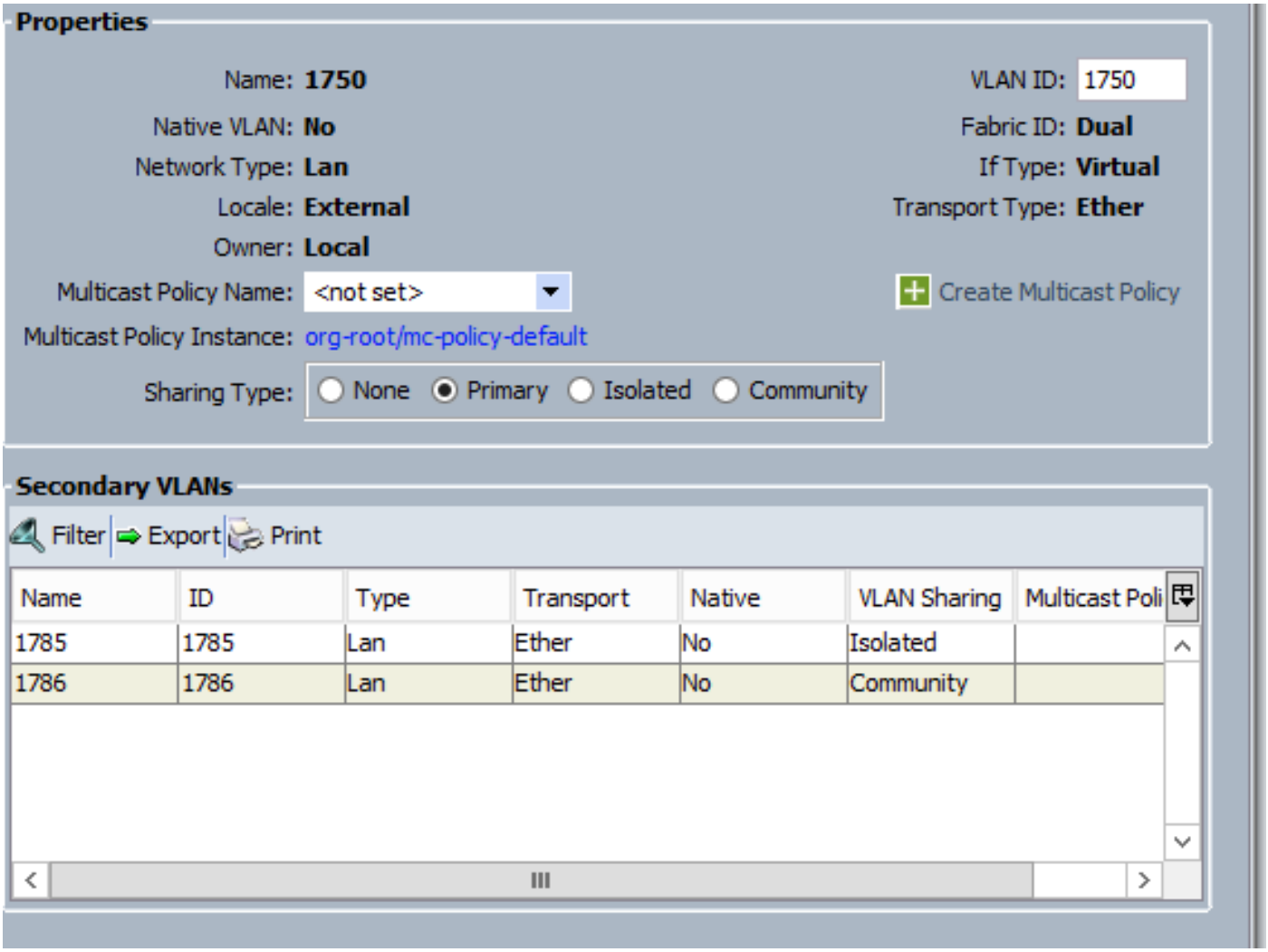
Nexus 1000vまたはVMware DVS



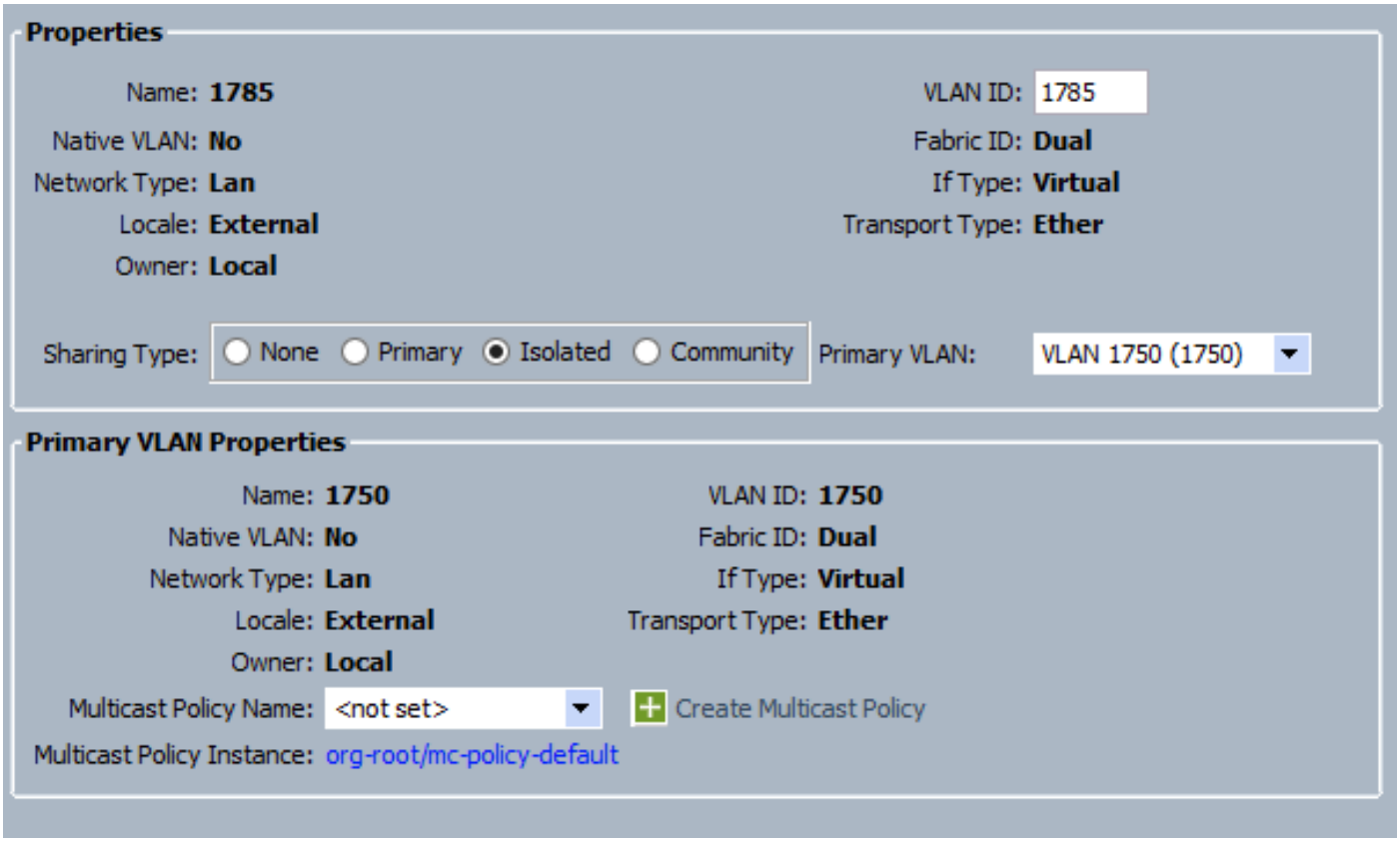
注：この例では、プライマリとしてVLAN 1750、隔離VLANとして1785、コミュニティVLANとして1786を使用しています。

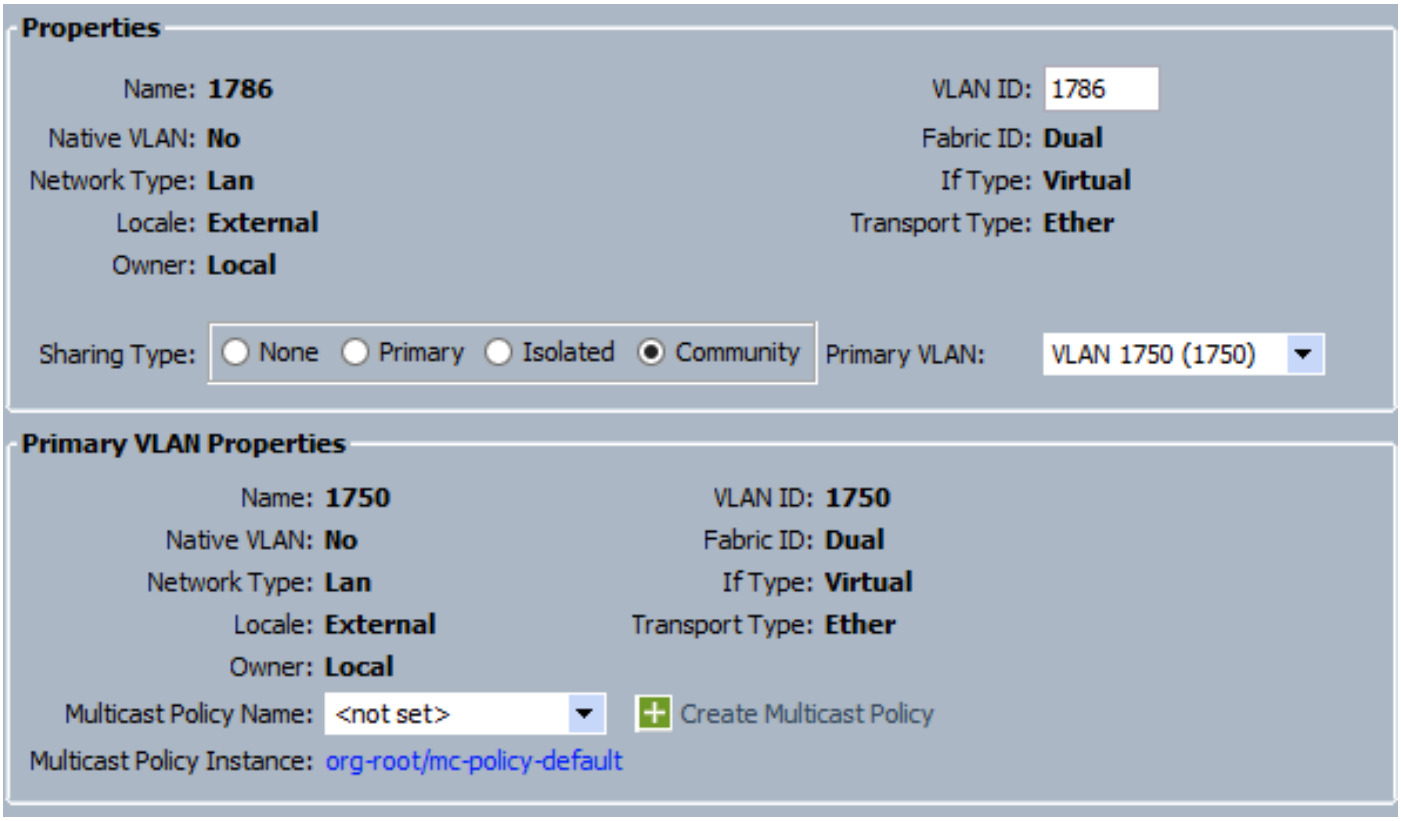
UCSとVMware DVS

1. プライマリVLANを作成するには、[Sharing Type]として[**Primary**]オプションボタンをクリックし、図に示すように**VLAN ID**に1750を入力します。

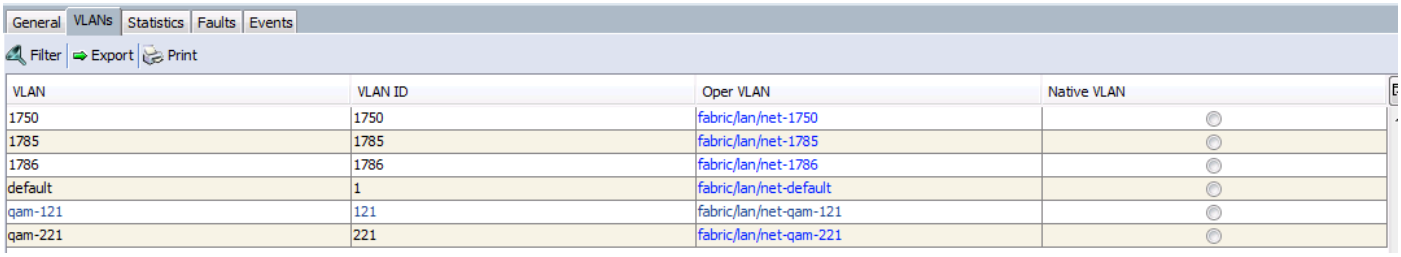


2.図に示すように、**隔離**VLANと**コミュニティ**VLANを作成します。これらはいずれもネイティブVLANである必要はありません。





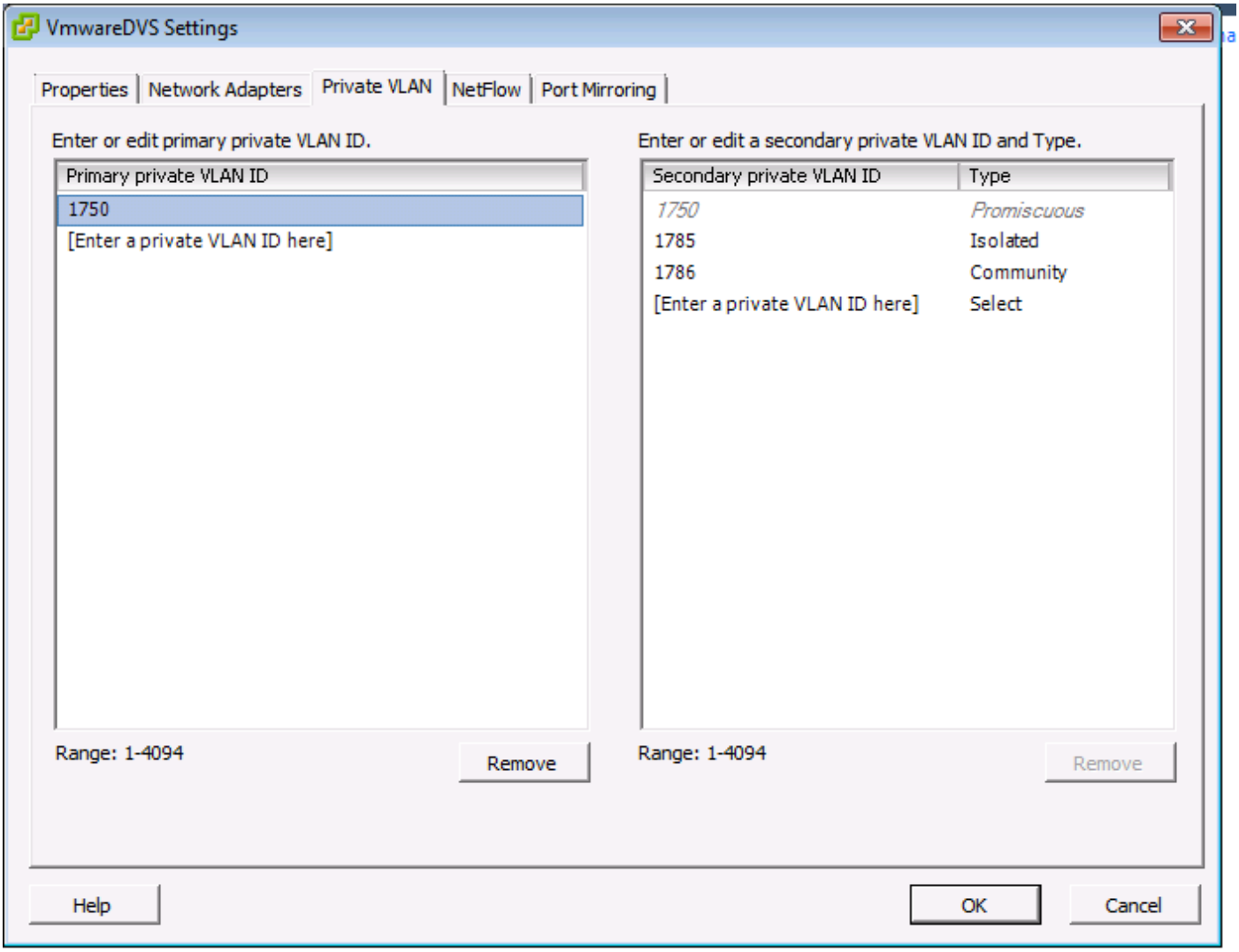
3.サービスプロファイルの仮想ネットワークインターフェイスカード(vNIC)は、図に示すように、通常のVLANとPVLANを伝送します。

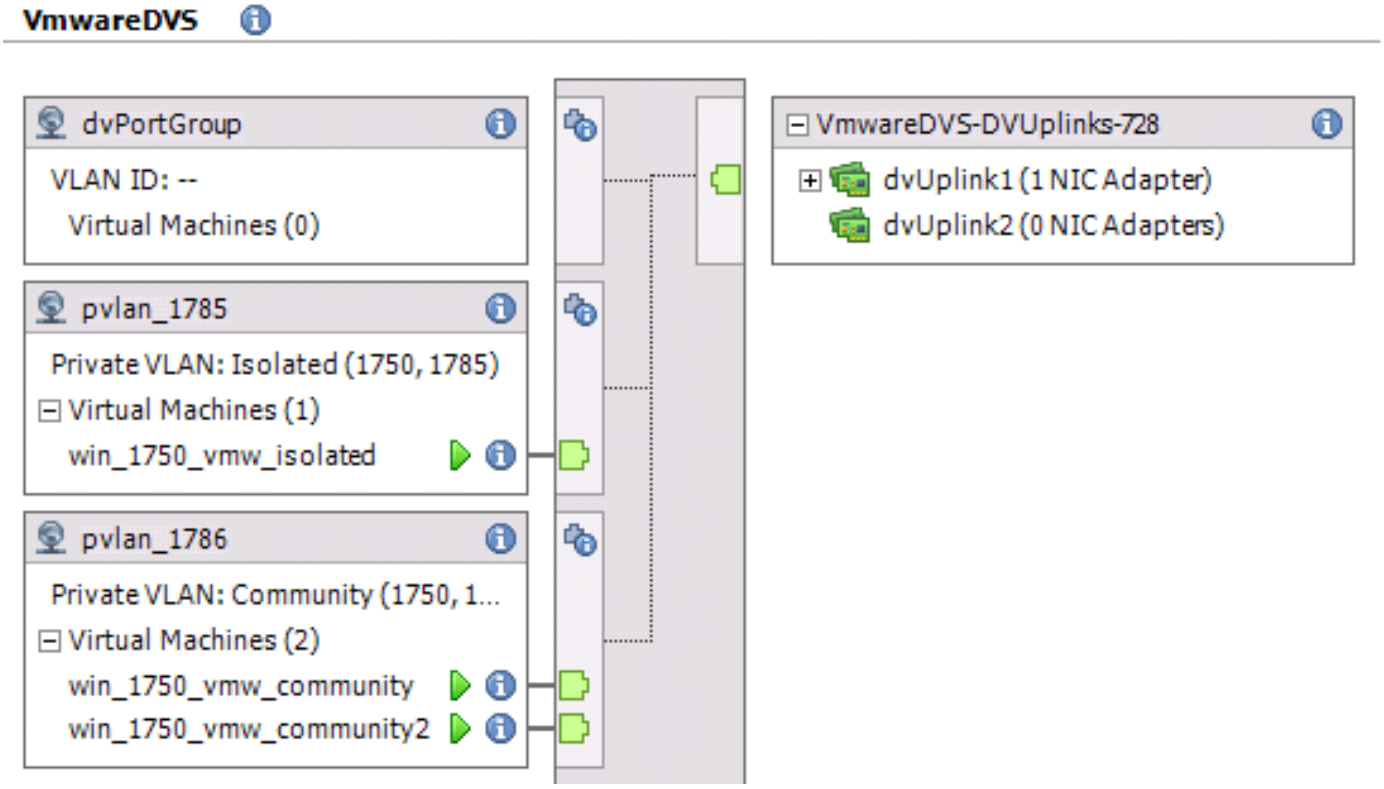


4. UCSのアップリンクポートチャネルは、通常のVLANとPVLANを伝送します。

```
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





アップストリームN5kスイッチ

```
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バージョン3.1(3)での動作変更

UCSバージョン3.1(3)より前のバージョンでは、コミュニティVLAN内のVMが、プライマリVLAN VMがUCS内に存在するVMware DVS上のプライマリVLAN内のVMと通信できます。プライマリVMは常にノースバウンドまたはUCSの外部である必要があるため、この動作は正しくありません。この動作は、不具合ID CSCvh87378で文書化されています .

UCSバージョン2.2(2)以降では、コードの不具合により、コミュニティVLANはFIの背後にあるプライマリVLANと通信できました。しかし、IsolatedはFIの背後にあるプライマリと通信できません。(隔離VMとコミュニティVMの両方が、FI外部のプライマリと通信できます。

3.1(3)以降、この不具合により、コミュニティはFIの背後にあるプライマリと通信できるようになり、修正されたため、コミュニティVMはUCS内にあるプライマリVLAN内のVMと通信できなくなります。

この状況を解決するには、プライマリVMをUCSの外部に移動（ノースバウンド）する必要があります。これがオプションではない場合、プライマリVMを、プライベートVLANではなく通常のVLANである別のVLANに移動する必要があります。

たとえば、ファームウェア3.1(3)よりも前では、コミュニティVLAN 1786のVMは、UCS内のプライマリVLAN 1750のVMと通信できますが、図に示すように、この通信はファームウェア3.1(3)以降で中断されます。

注：

—

CSCvh87378は、3.2(3l)および4.0.4e以降で対応されているため、UCSの背後にプライマリVlanを配置できます。ただし、UCS内部の隔離VLANは、UCS内部のプライマリVLANと通信できないことに注意してください。両方がUCSの背後にある場合、コミュニティVLANとプライマリVLANだけが相互に通信できます。

```
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)#
```

アップストリーム4900スイッチ

> **注**：この例では、4900は外部ネットワークへのL3インターフェイスです。L3のトポロジが異なる場合は、適宜変更を加えてください

4900 スイッチで、次の手順に従って無差別ポートを設定します。PVLAN は無差別ポートで終端します。

1. 必要に応じて PVLAN 機能をオンにします。
2. Nexus 5K で行ったように、VLAN を作成して関連付けます。
3. 4900 スイッチの出力ポートで無差別ポートを作成します。この時点から、VLAN 1785および1786からのパケットは、この場合はVLAN 1750で表示されます。

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

アップストリーム ルータで、VLAN 1750 専用のサブインターフェイスを作成します。このレベルの要件は、使用するネットワーク設定によって異なります。

```
interface GigabitEthernet0/1.1

encapsulation dot1Q 1750

IP address10.10.175.254/24
```

確認

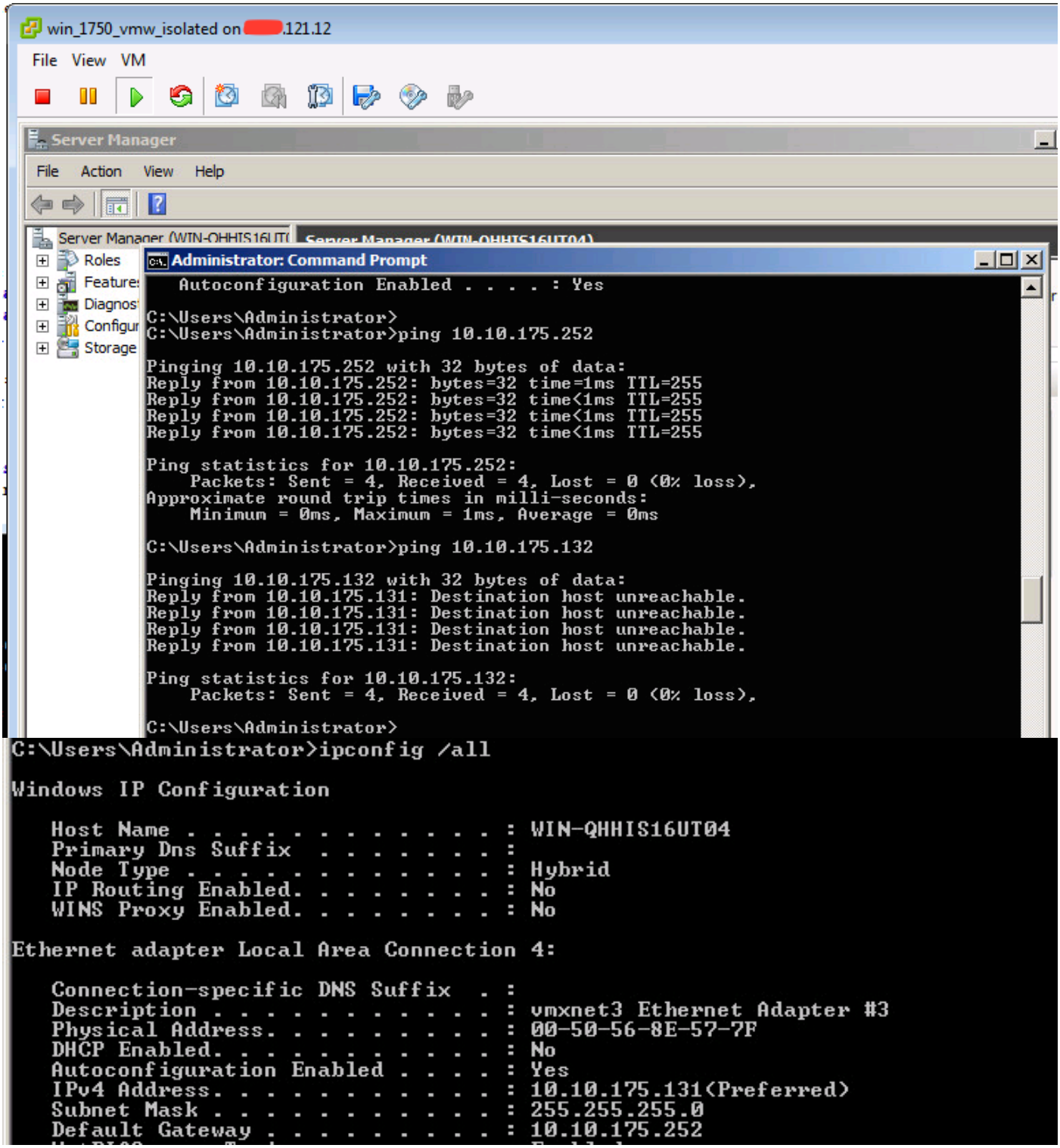
現在、この設定に使用できる確認手順はありません。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

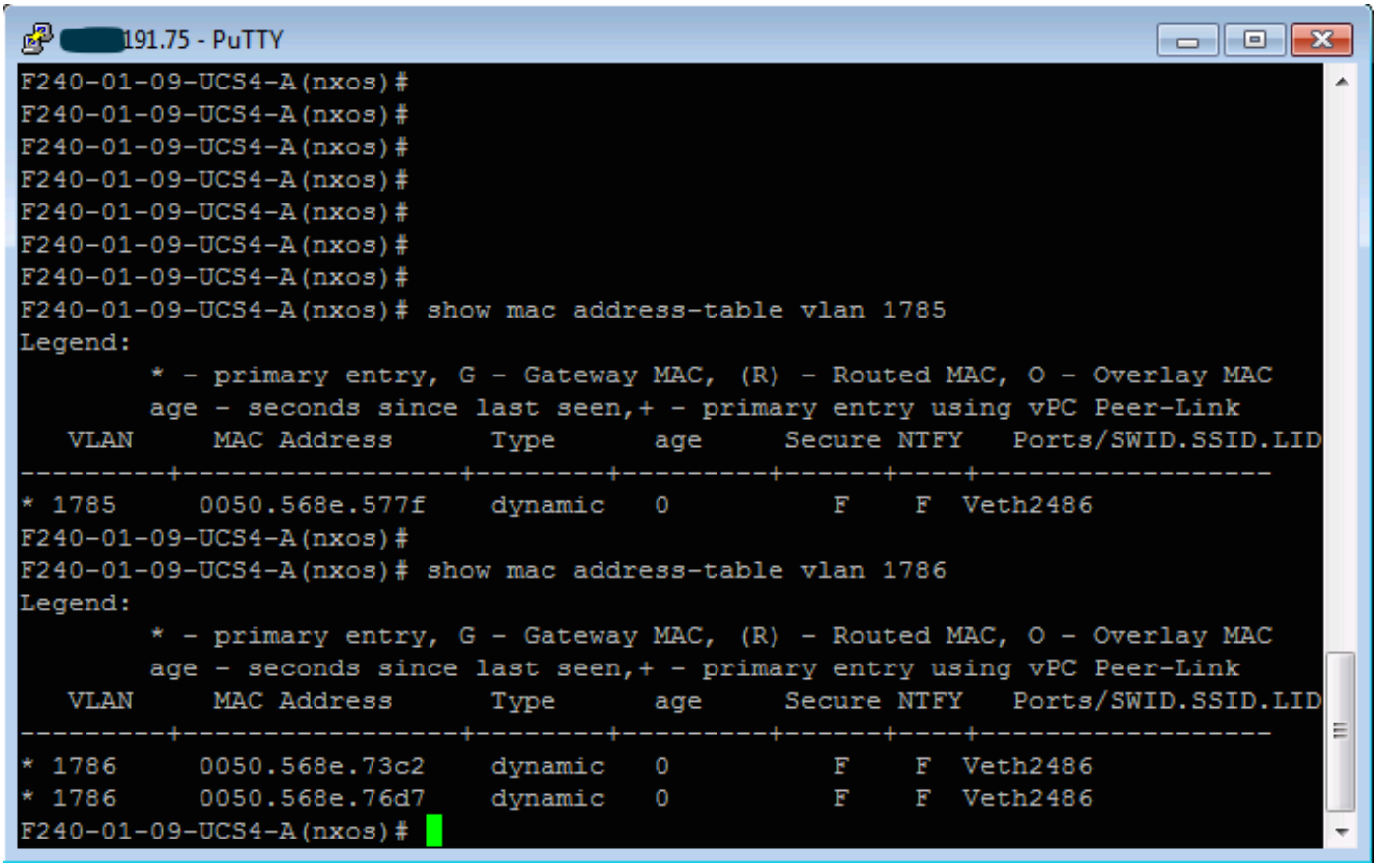
この手順では、PVLANを使用してVMware DVSの設定をテストする方法について説明します。

1.ポートグループに設定されている他のシステム、およびルータや混合モードポートのその他のデバイスに対してpingを実行します。無差別ポートを通過するデバイスへのpingは動作する必要がありますが、図に示すように、隔離VLAN内の他のデバイスへのpingは失敗する必要があります。



MAC アドレス テーブルを調べて、MAC が学習されている場所を確認します。すべてのスイッチで、混合ポートを備えたスイッチを除き、MACは隔離VLAN内にある必要があります。無差別スイッチでは、MACはプライマリVLAN内にある必要があります。

2.図に示すようにUCS。



3.アップストリームのn5kで同じMACを確認します。前の出力と同様の出力がn5k上にあり、次の図に示すように必要です。

```
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#
```

アップストリームN5kの無差別ポートを使用したNexus 1000vの設定

UCSの設定

UCS構成（サービスプロファイルvNIC構成を含む）は、VMware DVSの例と同じです。

N1kの設定

```
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
```

この手順では、設定のテスト方法について説明します。

1.ポートグループに設定されている他のシステム、およびルータや混合モードポートのその他のデバイスに対してpingを実行します。前のセクションと図に示すように、無差別ポートを経由したデバイスへのpingは動作し、隔離VLAN内の他のデバイスへのpingは失敗する必要があります。