

# 2.2 ( 2C ) 以前のプライベート VLAN および Cisco UCS 構成

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[理論](#)

[UCS での PVLAN 実装](#)

[目標](#)

[設定](#)

[ネットワーク図](#)

[vSwitch 上の PVLAN アップストリーム デバイス上の無差別ポートを使用した隔離 PVLAN](#)

[UCS での設定](#)

[アップストリーム デバイスの設定](#)

[トラブルシューティング](#)

[アップストリーム デバイス上の無差別ポートを使用した、N1K 上の隔離 PVLAN](#)

[UCS での設定](#)

[アップストリーム デバイスの設定](#)

[N1K の設定](#)

[トラブルシューティング](#)

[N1K アップリンク ポート プロファイルの無差別ポートを使用した、N1K 上の隔離 PVLAN](#)

[UCS での設定](#)

[アップストリーム デバイスの設定](#)

[N1K の設定](#)

[トラブルシューティング](#)

[N1K アップリンク ポート プロファイルの無差別ポートを使用した、N1K 上のコミュニティ PVLAN](#)

[トラブルシューティング](#)

[DVS 上の VMware DVS 無差別ポートでの隔離 PVLAN およびコミュニティ PVLAN](#)

[確認](#)

[トラブルシューティング](#)

## 概要

このドキュメントでは、Cisco UCS Manager(UCSM)リリース1.4で導入された機能であるCisco Unified Computing System(UCS)でのプライベートVLAN(PVLAN)のサポートについて説明します。また、UCS環境でPVLANを使用する場合の機能、警告、設定についても詳しく説明します。

このドキュメントは、UCSMバージョン2.2(2C)以前のバージョンで使用します。バージョン2.2(2C)以降では、UCSMおよびESXi DVSに対する変更がサポートされています。PVLAN NICの

タギングの動作にも変更があります。

## 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 1000 V ( N1K )
- 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

### 理論

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。
- 隔離モードのポートは、同じ PVLAN 内の他のポートから完全に L2 で隔離 ( ブロードキャストを含む ) されています ( 無差別ポートはこれにはあてはまりません ) 。
- 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。

### UCS での PVLAN 実装

UCS は Nexus 5000/2000 のアーキテクチャに非常によく似ており、Nexus 5000 は UCS 6100 に

、Nexus 2000 は UCS 2104 ファブリック エクステンダに相当します。

UCS における PVLAN 機能の多くの制約事項は、Nexus 5000/2000 実装に見られる制約事項によるものです。

注意すべき点は次のとおりです。

- UCS では隔離モードのポートのみがサポートされます。N1K が統合されている場合、コミュニティ VLAN を使用することはできますが、無差別ポートが N1K 上にもなければなりません。
- 無差別ポート/トランク、コミュニティ ポート/トランク、隔離トランクはいずれもサポートされていません。
- 無差別ポートはドメイン外部 ( アップストリーム スイッチ/ルータまたはダウンロードストリーム N1K など ) になければなりません。

## 目標

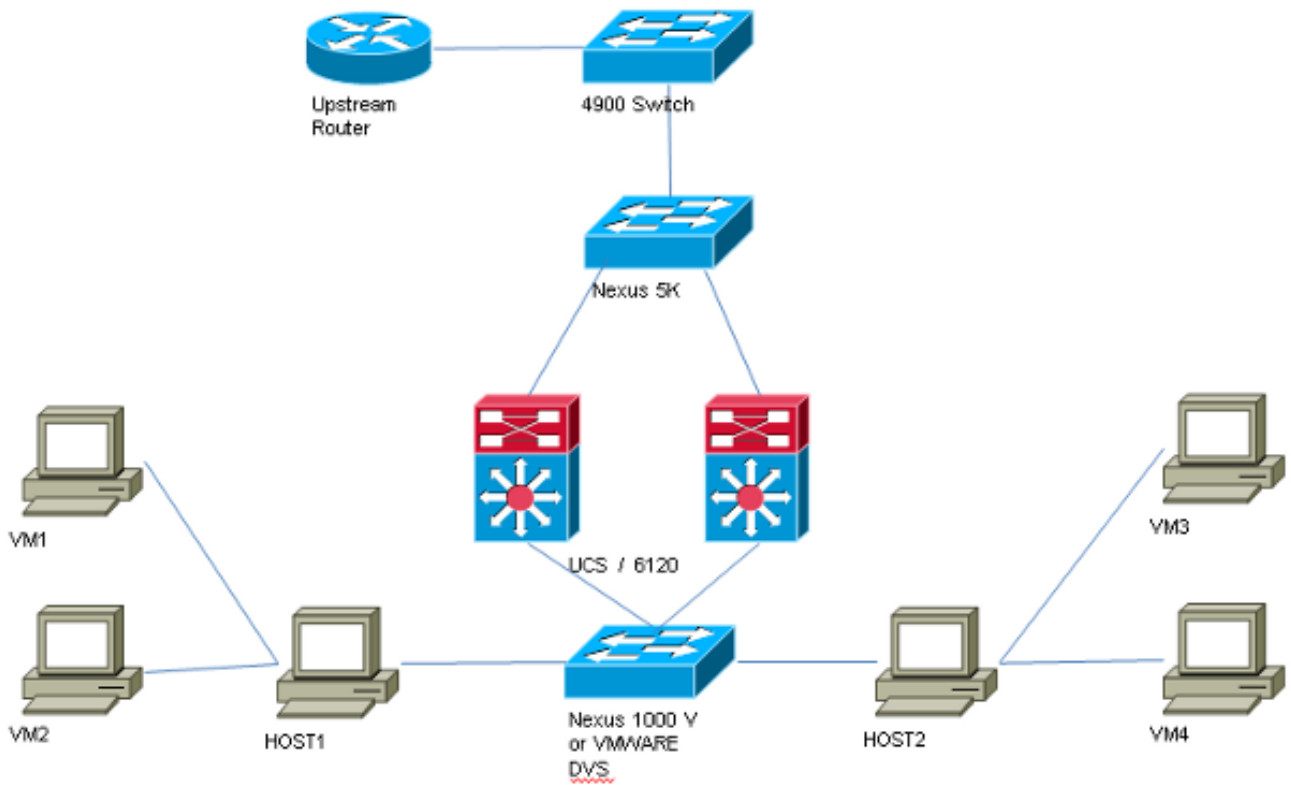
このドキュメントでは、UCS を使用した PVLAN に有効な以下の設定を取り上げます。

1. アップストリーム デバイス上の無差別ポートを使用した隔離 PVLAN。
2. アップストリーム デバイス上の無差別ポートを使用した、N1K 上の隔離 PVLAN。
3. N1K アップリンク ポート プロファイルの無差別ポートを使用した、N1K 上の隔離 PVLAN
4. N1K アップリンク ポート プロファイルの無差別ポートを使用した、N1K 上のコミュニティ PVLAN。
5. DVS 上の VMware 分散仮想スイッチ ( DVS ) 無差別ポートでの隔離 PVLAN。
6. DVS 上の VMware DVS 無差別ポートでのコミュニティ PVLAN。

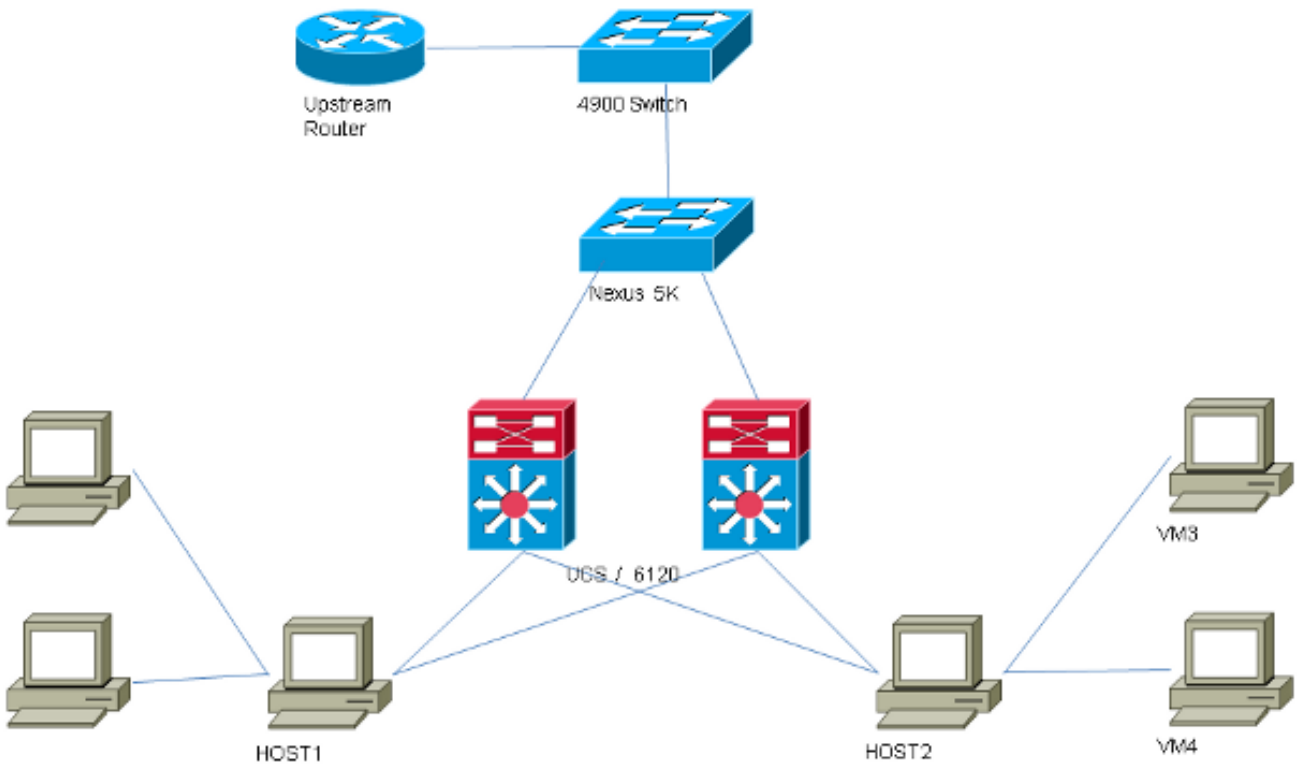
## 設定

### ネットワーク図

分散スイッチを使用したすべての例のトポロジは、次のようになります。



分散スイッチを使用しないすべての例のトポロジは、次のようになります。



## vSwitch 上の PVLAN アップストリーム デバイス上の無差別ポートを使用した隔離 PVLAN

この設定では、PVLAN トラフィックを UCS 経由でアップストリームの無差別ポートに渡します

。同じ vNIC でプライマリ VLAN とセカンダリ VLAN の両方を送信することはできないため、PVLAN トラフィックを伝送するには、各 PVLAN のブレードごとに 1 つの vNIC が必要になります。

## UCS での設定

この手順では、プライマリ VLAN と隔離 VLAN の両方を作成する方法について説明します。

注：次の例では、VLAN 266 をプライマリ VLAN として使用し、VLAN 166 を隔離 VLAN として使用します。VLAN ID は、サイトによって決まります。

1. プライマリ VLAN を作成するために、[Sharing Type] として [Primary] をクリックし、[VLAN ID] に 266 と入力します。

The screenshot shows the configuration interface for a VLAN. The 'Properties' section is at the top, and the 'Secondary VLANs' section is below it.

**Properties**

Name: 266  
Native VLAN: No  
Network Type: Lan  
Locale: External  
Multicast Policy Name: <not set>  
Multicast Policy Instance: org-root/mc-policy-default  
Sharing Type:  None  Primary  Isolated

VLAN ID: 266  
Fabric ID: Dual  
If Type: Virtual  
Transport Type: Ether  
+ Create Multicast Policy

**Secondary VLANs**

Filter | Export | Print

Name	ID	Type	Transport	Native	VLAN Sharing
166	166	Lan	Ether	No	Isolated

2. 隔離 VLAN を作成するために、[Sharing Type] として [Isolated] をクリックし、[VLAN ID] に 166 と入力します。プライマリ VLAN には [VLAN 266 (266)] を選択します。

### Properties

Name: **166** VLAN ID:

Native VLAN: **No** Fabric ID: **Dual**

Network Type: **Lan** If Type: **Virtual**

Locale: **External** Transport Type: **Ether**

Sharing Type:  None  Primary  Isolated Primary VLAN:

---

### Primary VLAN Properties

Name: **266** VLAN ID: **266**

Native VLAN: **No** Fabric ID: **Dual**

Network Type: **Lan** If Type: **Virtual**

Locale: **External** Transport Type: **Ether**

Multicast Policy Name:

Multicast Policy Instance: [org-root/mc-policy-default](#)

3. VLAN を vNIC に追加するために、[VLAN 166] の [Select] チェックボックスをオンにしてから、対応する [Native VLAN] オプション ボタンをクリックします。

### Modify VLANs

Select	Name	Native VLAN
<input type="checkbox"/>	default	<input type="radio"/>
<input type="checkbox"/>	1233	<input type="radio"/>
<input type="checkbox"/>	1234	<input type="radio"/>
<input type="checkbox"/>	124	<input type="radio"/>
<input type="checkbox"/>	126	<input type="radio"/>
<input checked="" type="checkbox"/>	166	<input checked="" type="radio"/>
<input type="checkbox"/>	266	<input type="radio"/>
<input type="checkbox"/>	777	<input type="radio"/>
<input type="checkbox"/>	Tbeaudre_177	<input type="radio"/>
<input type="checkbox"/>	Tbeaudre_277	<input type="radio"/>
<input type="checkbox"/>	Tbeaudre_377	<input type="radio"/>
<input type="checkbox"/>	vlan_51	<input type="radio"/>

OK Cancel

隔離 VLAN のみを追加して、プライマリとして設定する必要があります。vNIC ごとに許容されるプライマリは 1 つだけです。ここではネイティブ VLAN が定義されているため、VMware ポート グループに VLAN タギングを設定しないでください。

## アップストリーム デバイスの設定

次の手順では、無差別ポートがあるアップストリームの 4900 スイッチ経由で PVLAN を渡すように Nexus 5K を設定する方法について説明します。これは、すべての環境で必要なわけではありませんが、PVLAN を別のスイッチに渡す必要がある場合には、この設定を使用してください。

Nexus 5K で、次のコマンドを入力してアップリンクの設定を確認します。

1. PVLAN 機能をオンにします。

```
Nexus5000-5(config)# feature private-vlan
```

2. VLAN をプライマリ VLAN および隔離 VLAN として追加します。

```
Nexus5000-5(config)# vlan 166
Nexus5000-5(config-vlan)# private-vlan isolated
Nexus5000-5(config-vlan)# vlan 266
Nexus5000-5(config-vlan)# private-vlan primary
```

3. VLAN 166 を隔離 VLAN 266 に関連付けます。

```
Nexus5000-5(config-vlan)# private-vlan association 166
```

4. VLAN をトランキングするために、すべてのアップリンクが設定されていることを確認します。

```
interface Ethernet1/1description Connection to 4900switchport mode trunkspeed
1000interface Ethernet1/3description Connection to FIB Port 5switchport mode trunkspeed
1000interface Ethernet1/4description Connection to FIA port 5switchport mode trunkspeed
1000
```

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了します。

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 166 からのパケットが VLAN 266 (この例の場合) で確認されるようになります。

```
Switch(config-if)#switchport mode trunk
switchport private-vlan mapping 266 166
switchport mode private-vlan promiscuous
```

アップストリーム ルータで、VLAN 266 専用のサブインターフェイスを作成します。このレベルでの要件は、使用しているネットワークによって決まります。

1. interface GigabitEthernet0/1.1

2. encapsulation dot1Q 266
3. IP address 209.165.200.225 255.255.255.224

## トラブルシューティング

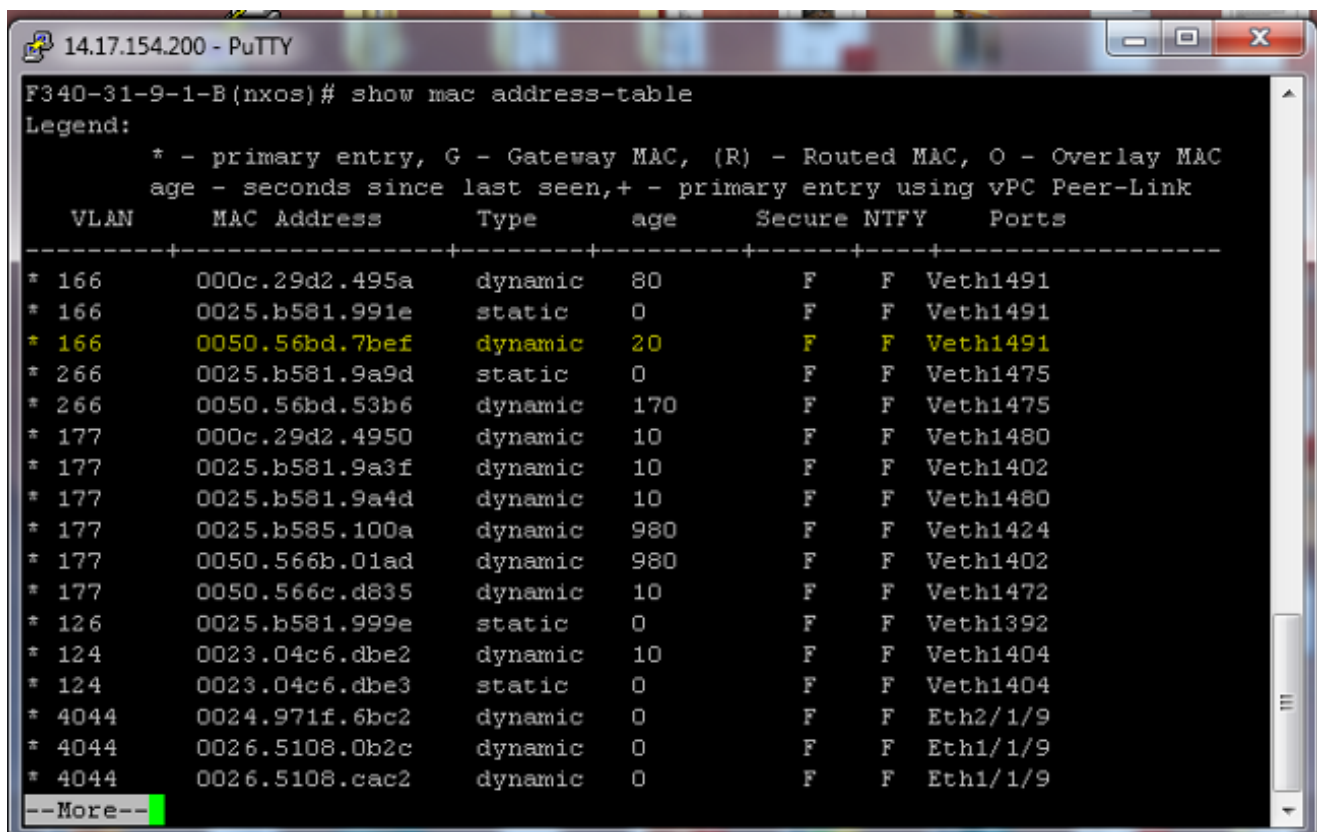
この手順では、設定のテスト方法について説明します。

1. 各スイッチでスイッチ仮想インターフェイス (SVI) を設定し、PVLAN から SVI への ping を実行できるようにします。

```
(config)# interface vlan 266
(config-if)# ip address 209.165.200.225 255.255.255.224
(config-if)# private-vlan mapping 166
(config-if)# no shut
```

2. 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。無差別ポートがあるスイッチを除くすべてのスイッチで、MAC は隔離 VLAN 内になければなりません。無差別ポートがあるスイッチでは、MAC はプライマリ VLAN 内にあることに注意してください。

ファブリック インターコネクトでは、MAC アドレス 0050.56bd.7bef が Veth1491 で学習されます。



```
14.17.154.200 - PuTTY
F340-31-9-1-B (nxos)# show mac address-table
Legend:
 * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
 age - seconds since last seen, + - primary entry using vPC Peer-Link
 VLAN      MAC Address      Type      age      Secure NTFY      Ports
-----
 * 166      000c.29d2.495a   dynamic   80       F      F      Veth1491
 * 166      0025.b581.991e   static    0        F      F      Veth1491
 * 166      0050.56bd.7bef   dynamic   20       F      F      Veth1491
 * 266      0025.b581.9a9d   static    0        F      F      Veth1475
 * 266      0050.56bd.53b6   dynamic   170      F      F      Veth1475
 * 177      000c.29d2.4950   dynamic   10       F      F      Veth1480
 * 177      0025.b581.9a3f   dynamic   10       F      F      Veth1402
 * 177      0025.b581.9a4d   dynamic   10       F      F      Veth1480
 * 177      0025.b585.100a   dynamic   980      F      F      Veth1424
 * 177      0050.566b.01ad   dynamic   980      F      F      Veth1402
 * 177      0050.566c.d835   dynamic   10       F      F      Veth1472
 * 126      0025.b581.999e   static    0        F      F      Veth1392
 * 124      0023.04c6.dbe2   dynamic   10       F      F      Veth1404
 * 124      0023.04c6.dbe3   static    0        F      F      Veth1404
 * 4044     0024.971f.6bc2   dynamic   0        F      F      Eth2/1/9
 * 4044     0026.5108.0b2c   dynamic   0        F      F      Eth1/1/9
 * 4044     0026.5108.cac2   dynamic   0        F      F      Eth1/1/9
--More--
```

Nexus 5K では、MAC アドレス 0050.56bd.7bef が Eth1/4 で学習されます。



```

F340-11-12-COMM.cisco.com - PuTTY
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
F340.11.13-Nexus5000-5# show mac
mac          mac-list
F340.11.13-Nexus5000-5# show mac
mac          mac-list
F340.11.13-Nexus5000-5# show mac address-table
Legend:
    * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
    age - seconds since last seen,+ - primary entry using vPC Peer-Link
VLAN      MAC Address      Type      age      Secure NTFY      Ports
-----+-----+-----+-----+-----+-----
* 266     0050.56aa.0a63     dynamic   260      F      F      Eth1/3
* 266     0050.56bd.53b6     dynamic   10       F      F      Eth1/4
* 166     000c.29d2.495a     dynamic   160      F      F      Eth1/4
* 166     0050.56bd.6fd2     dynamic   100      F      F      Eth1/3
* 166     0050.56bd.7bef     dynamic   60       F      F      Eth1/4
F340.11.13-Nexus5000-5#

```

4900 スイッチでは、MAC アドレス 0050.56bd.7bef が GigabitEthernet1/1 で学習されます。

```

F340-11-05-COMM.cisco.com - PuTTY
Unicast Entries
vlan      mac address      type      protocols      port
-----+-----+-----+-----+-----
266      000c.29d2.495a     dynamic   ip,ipx,assigned,other GigabitEthernet1/1
266      0050.56bd.53b6     dynamic   ip,ipx,assigned,other GigabitEthernet1/1
266      0050.56bd.6fd2     dynamic   ip,ipx,assigned,other GigabitEthernet1/1
266      0050.56bd.7bef     dynamic   ip,ipx,assigned,other GigabitEthernet1/1
266      c84c.75f6.013f     static    ip,ipx,assigned,other Switch

Multicast Entries
vlan      mac address      type      ports
-----+-----+-----+-----
1         0100.0ccc.cccc     system    Gi1/1
1         ffff.ffff.ffff     system    Gi1/1
2         ffff.ffff.ffff     system    Gi1/1
11        ffff.ffff.ffff     system    Gi1/1
12        ffff.ffff.ffff     system    Gi1/1
13        ffff.ffff.ffff     system    Gi1/1
14        ffff.fff.fff       system    Gi1/1
15        ffff.fff.fff       system    Gi1/1
16        ffff.fff.fff       system    Gi1/1
17        ffff.fff.fff       system    Gi1/1
18        ffff.fff.fff       system    Gi1/1
--More--

```

この設定では、この隔離 VLAN 内のシステムが互いに通信することはできませんが、4900 スイッチ上の無差別ポートを介して他のシステムと通信することができます。1つの問題は、ダウンストリーム デバイスを設定する方法です。この例では、VMware と 2つのホストを使用します。

PVLANごとに1つのvNICを使用する必要があることに注意してください。これらのvNICがVMware vSphere ESXi に提示されるようになった後、ポートグループを作成して、作成したポ

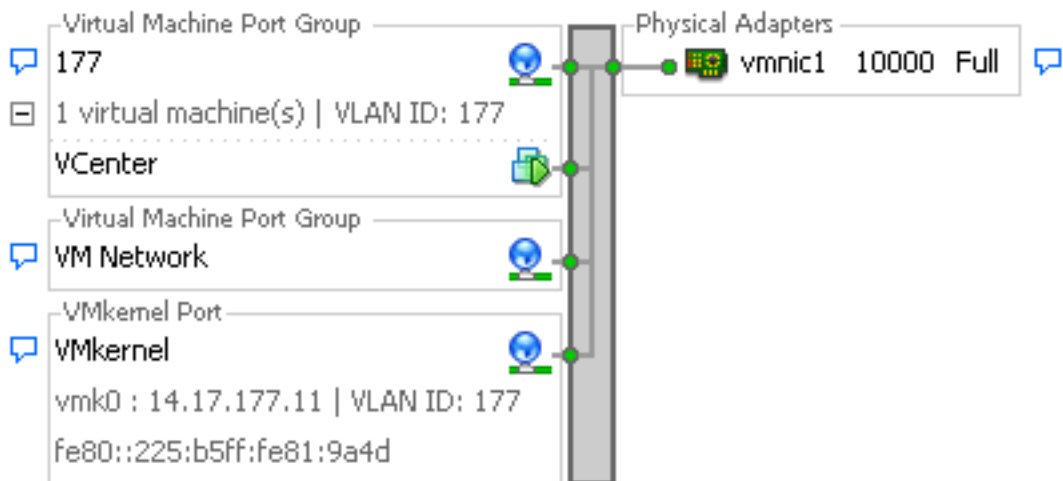
ートグループに対するゲストを使用できます。

2つのシステムが同じスイッチ上の同じポートグループに追加されていれば、その2つのシステムの通信がvSwitch上でローカルに切り替えられるため、システム間での通信が可能になります。このシステムには2つのブレードがあり、それぞれのブレードに2つのホストがあります。

最初のシステムには、166と166Aという2つの異なるポートグループが作成されています。それぞれのポートグループは、UCS上の隔離VLAN内に設定された単一のNICに接続されています。現在、ゲストはポートグループごとに1つだけあります。この場合、ESXi上で分離されるため、互いに対話することはできません。

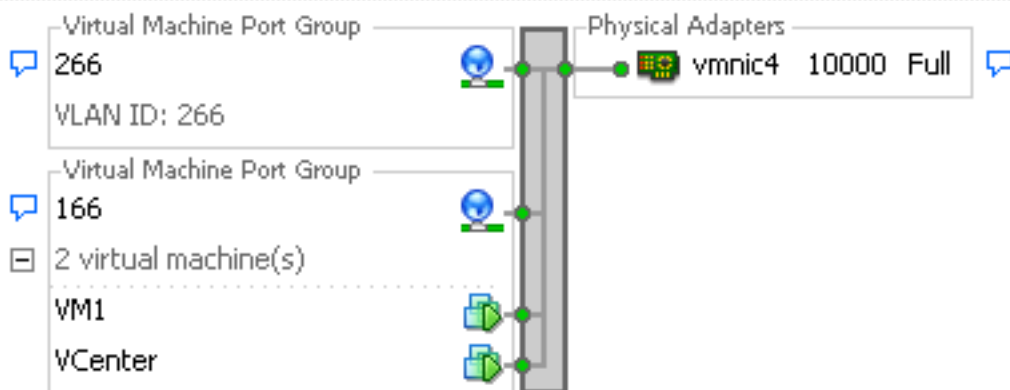
### Standard Switch: vSwitch0

[Remove...](#) [Properties...](#)



### Standard Switch: vSwitch1

[Remove...](#) [Properties...](#)



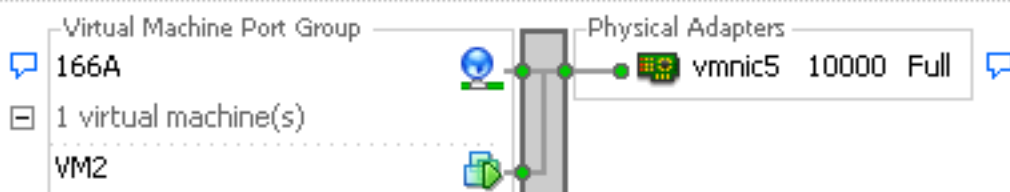
### Standard Switch: vSwitch2

[Remove...](#) [Properties...](#)



### Standard Switch: vSwitch3

[Remove...](#) [Properties...](#)

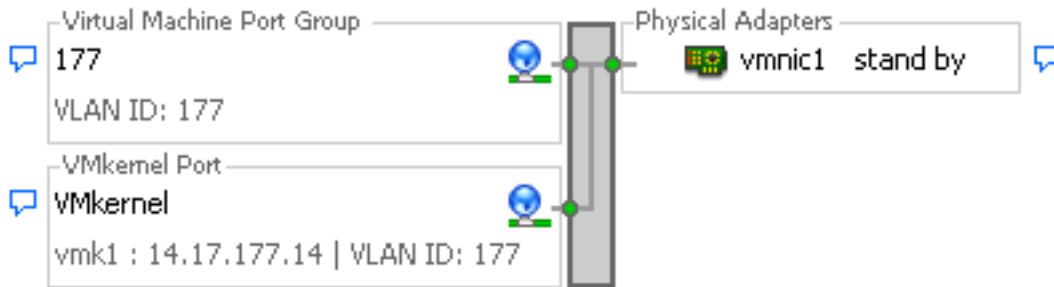


2つ目のシステムでは、166と呼ばれる1つのポートグループしかありません。このポートグループには2人のゲストがいます。この設定では、不本意であっても VM3 と VM4 が互いに通信できてしまいます。この状態を修正するには、隔離 VLAN 内にある仮想マシン ( VM ) ごとに単一の NIC を設定してから、その vNIC に接続するポートグループを作成します。このように設定した後、1つのゲストだけをポートグループに含めます。これらの基本 vSwitch を使用しないペアメ

タル Windows インストールでは、これは問題になりません。

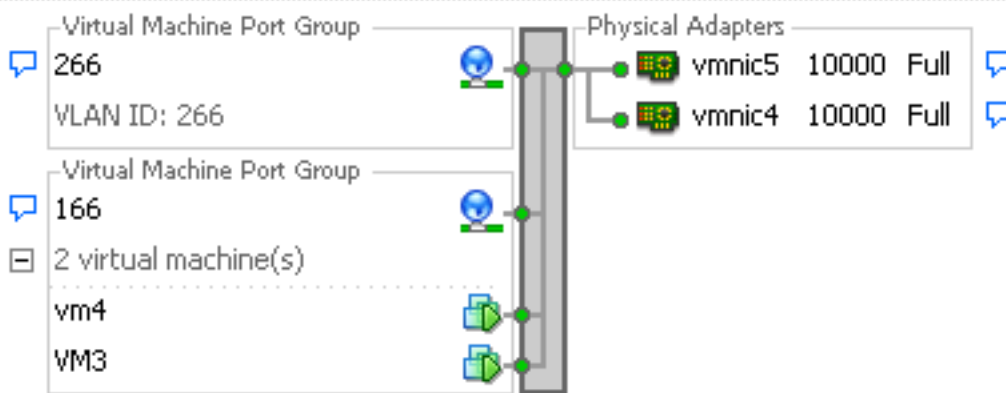
Standard Switch: vSwitch0

[Remove...](#) [Properties...](#)



Standard Switch: vSwitch1

[Remove...](#) [Properties...](#)



Standard Switch: vSwitch2

[Remove...](#) [Properties...](#)



## アップストリーム デバイス上の無差別ポートを使用した、N1K 上の隔離 PVLAN

この設定では、PVLAN トラフィックを N1K 経由、次に UCS 経由でアップストリームの無差別ポートに渡します。同じ vNIC でプライマリ VLAN とセカンダリ VLAN の両方を送信することはできないため、PVLAN トラフィックを伝送するには、PVLAN アップリンクごとに 1 つの vNIC が必要になります。

### UCS での設定

この手順では、プライマリ VLAN と隔離 VLAN の両方を作成する方法について説明します。

注：次の例では、VLAN 266 をプライマリ VLAN として使用し、VLAN 166 を隔離 VLAN として使用します。VLAN ID は、サイトによって決まります。

1. プライマリ VLAN を作成するために、[Sharing Type] として [Primary] をクリックします。


**Properties**

Name: **266**      VLAN ID:

Native VLAN: **No**      Fabric ID: **Dual**

Network Type: **Lan**      If Type: **Virtual**

Locale: **External**      Transport Type: **Ether**




Multicast Policy Name:        Create Multicast Policy


Multicast Policy Instance: [org-root/mc-policy-default](#)

Sharing Type:  None  Primary  Isolated

---

**Secondary VLANs**

 Filter |  Export |  Print

Name	ID	Type	Transport	Native	VLAN Sharing	
166	166	Lan	Ether	No	Isolated	

2. 隔離 VLAN を作成するために、[Sharing Type] として [Isolated] をクリックします。

**Properties**

Name: <b>166</b>	VLAN ID: <input type="text" value="166"/>
Native VLAN: <b>No</b>	Fabric ID: <b>Dual</b>
Network Type: <b>Lan</b>	If Type: <b>Virtual</b>
Locale: <b>External</b>	Transport Type: <b>Ether</b>

Sharing Type:  None  Primary  Isolated Primary VLAN:

---

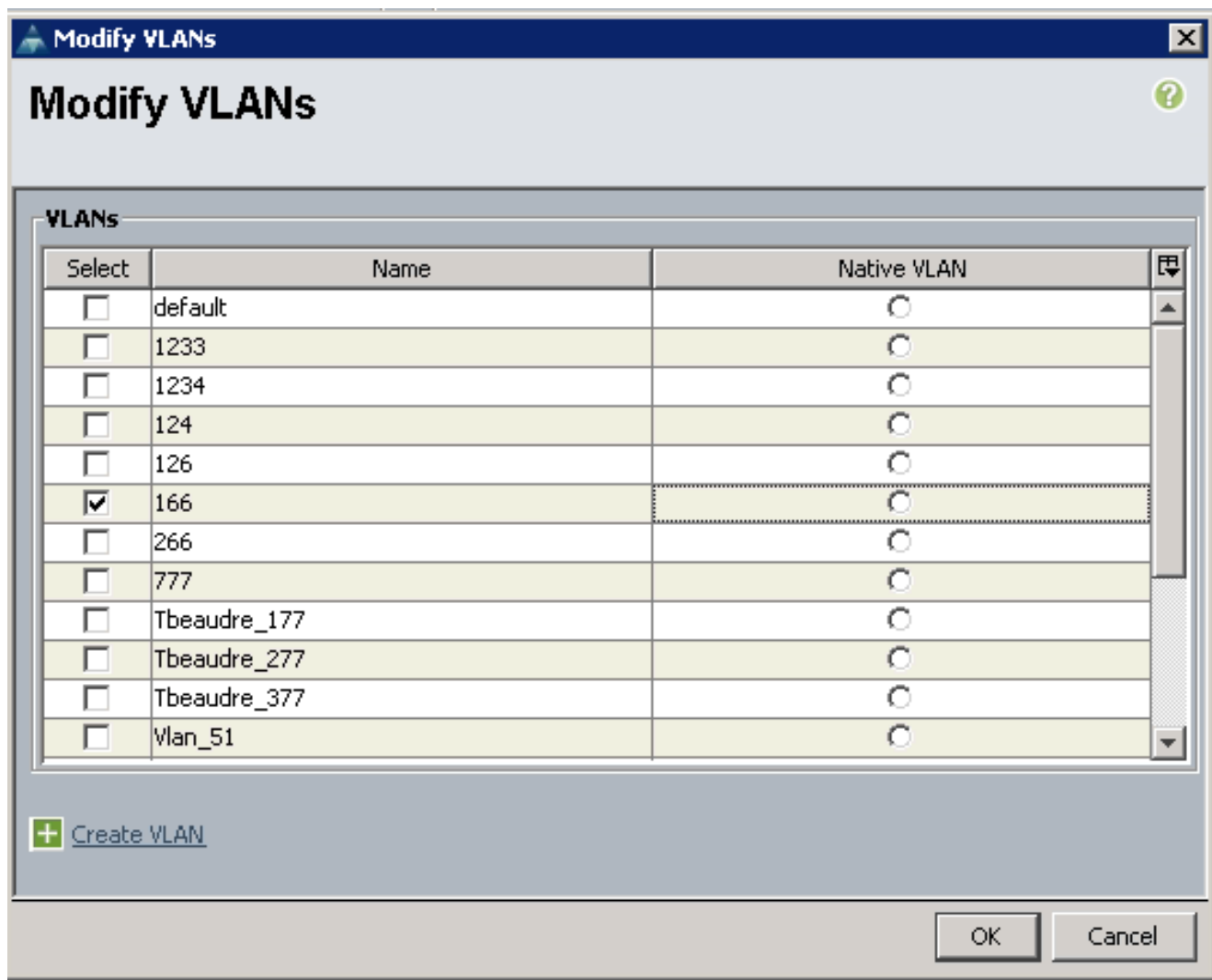
**Primary VLAN Properties**

Name: <b>266</b>	VLAN ID: <b>266</b>
Native VLAN: <b>No</b>	Fabric ID: <b>Dual</b>
Network Type: <b>Lan</b>	If Type: <b>Virtual</b>
Locale: <b>External</b>	Transport Type: <b>Ether</b>

Multicast Policy Name:

Multicast Policy Instance: [org-root/mc-policy-default](#)

3. VLANをvNICに追加するには、VLAN 166の[Select]チェックボックスをオンにします。  
VLAN 166では[Native VLAN]が選択されていません。



隔離 VLAN のみを追加して、ネイティブとして設定する必要があります。vNIC ごとに許容されるネイティブは 1 つだけです。ここではネイティブ VLAN が定義されていないため、N1K 上のネイティブ VLAN にタグを付けます。ネイティブ VLAN にタグを付けるオプションは VMware DVS では使用できないため、DVS ではサポートされません。

## アップストリーム デバイスの設定

次の手順では、無差別ポートがあるアップストリームの 4900 スイッチ経由で PVLAN を渡すように Nexus 5K を設定する方法について説明します。これは、すべての環境で必要なわけではありませんが、PVLAN を別のスイッチに渡す必要がある場合には、この設定を使用してください。

Nexus 5K で、次のコマンドを入力してアップリンクの設定を確認します。

1. PVLAN 機能をオンにします。

```
Nexus5000-5(config)# feature private-vlan
```

2. VLAN をプライマリ VLAN および隔離 VLAN として追加します。

```
Nexus5000-5(config)# vlan 166
Nexus5000-5(config-vlan)# private-vlan isolated
Nexus5000-5(config-vlan)# vlan 266
```

```
Nexus5000-5(config-vlan)# private-vlan primary
```

### 3. VLAN 166 を隔離 VLAN 266 に関連付けます。

```
Nexus5000-5(config-vlan)# private-vlan association 166
```

### 4. VLAN をランキングするために、すべてのアップリンクが設定されていることを確認します。

```
interface Ethernet1/1description Connection to 4900switchport mode trunkspeed 1000interface Ethernet1/3description Connection to FIB Port 5switchport mode trunkspeed 1000interface Ethernet1/4description Connection to FIA port 5switchport mode trunkspeed 1000
```

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了します。

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 166 からのパケットが VLAN 266 (この例の場合) で確認されるようになります。

```
Switch(config-if)#switchport mode trunk  
switchport private-vlan mapping 266 166  
switchport mode private-vlan promiscuous
```

アップストリーム ルータで、VLAN 266 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。

1. interface GigabitEthernet0/1.1
2. encapsulation dot1Q 266
3. IP address 209.165.200.225 255.255.255.224

## N1K の設定

この手順では、N1K を PVLAN トランクとしてではなく、標準トランクとして設定する方法について説明します。

1. Nexus 5K で行ったように、VLAN を作成して関連付けます。詳細については、「[アップストリーム デバイスの設定](#)」の項を参照してください。
2. PVLAN トラフィックのアップリンク ポート プロファイルを作成します。

```
Switch(config)#port-profile type ethernet pvlan_uplink  
Switch(config-port-prof)# vmware port-group  
Switch(config-port-prof)# switchport mode trunk  
Switch(config-port-prof)# switchport trunk allowed vlan 166,266  
Switch(config-port-prof)# switchport trunk native vlan 266 <-- This is necessary to handle  
traffic coming back from the promiscuous port.  
Switch(config-port-prof)# channel-group auto mode on mac-pinning  
Switch(config-port-prof)# no shut  
Switch(config-port-prof)# state enabled
```

3. 隔離 VLAN のポート グループを作成します。PVLAN ホスト ポートを作成し、プライマリ VLAN と隔離 VLAN のホスト関係を設定します。



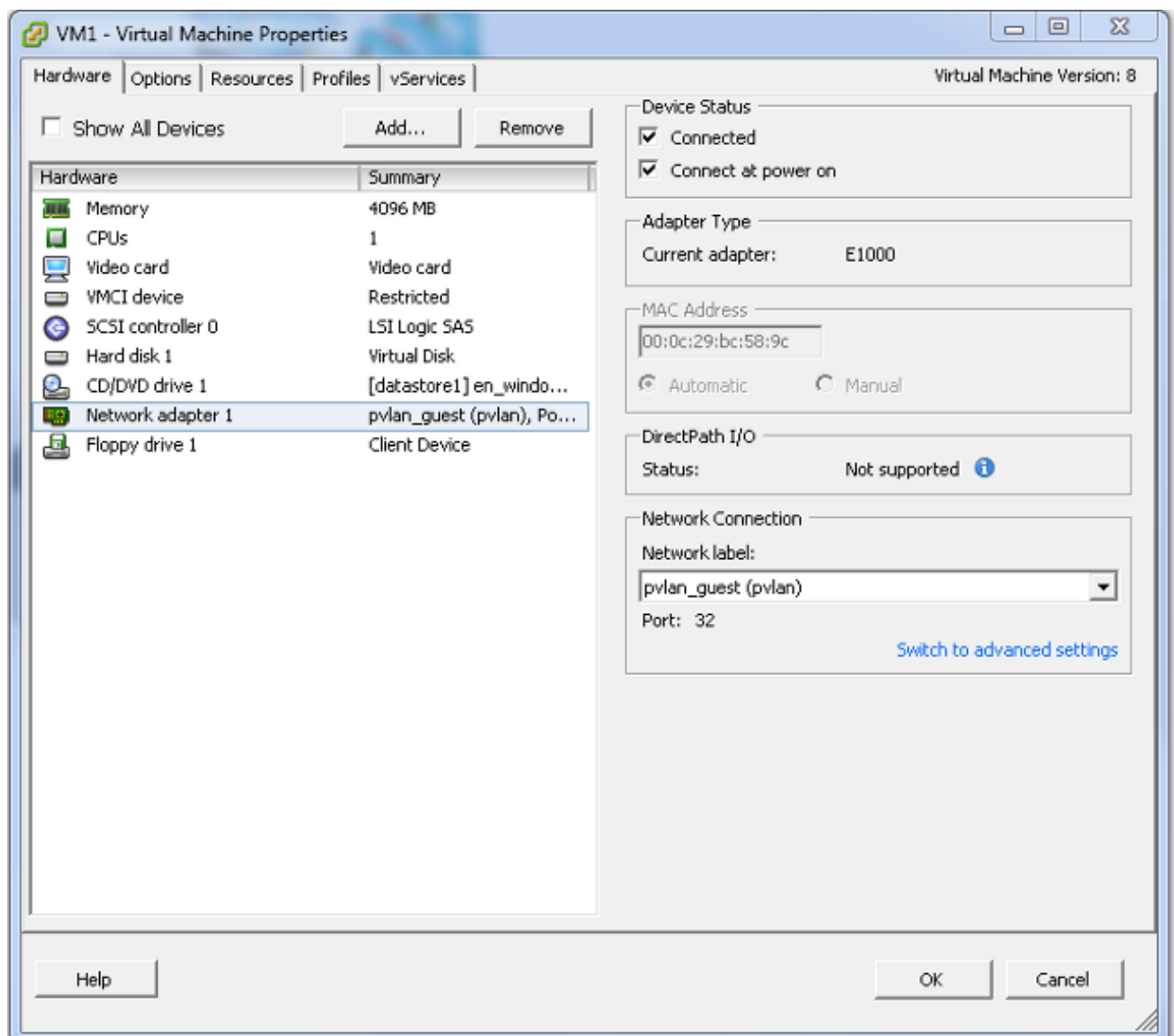
```
Switch(config)# port-profile type vethernet pvlan_guest
Switch(config-port-prof)# vmware port-group
Switch(config-port-prof)# switchport mode private-vlan host
Switch(config-port-prof)# switchport private-vlan host-association 266 166
Switch(config-port-prof)# no shut
Switch(config-port-prof)# state enabled
```

4. vCenter で、適切な vNIC を PVLAN アップリンクに追加します。適切な vNIC とは、UCS での設定で隔離 VLAN を追加した vNIC です。

<input type="checkbox"/>		vmnic3	--	<a href="#">View Details...</a>	Select an uplink port gr...
<input checked="" type="checkbox"/>		vmnic4	pvlan	<a href="#">View Details...</a>	pvlan_uplink
<input type="checkbox"/>		vmnic5	--	<a href="#">View Details...</a>	Select an uplink port gr...

5. VM を適切なポート グループに追加します。

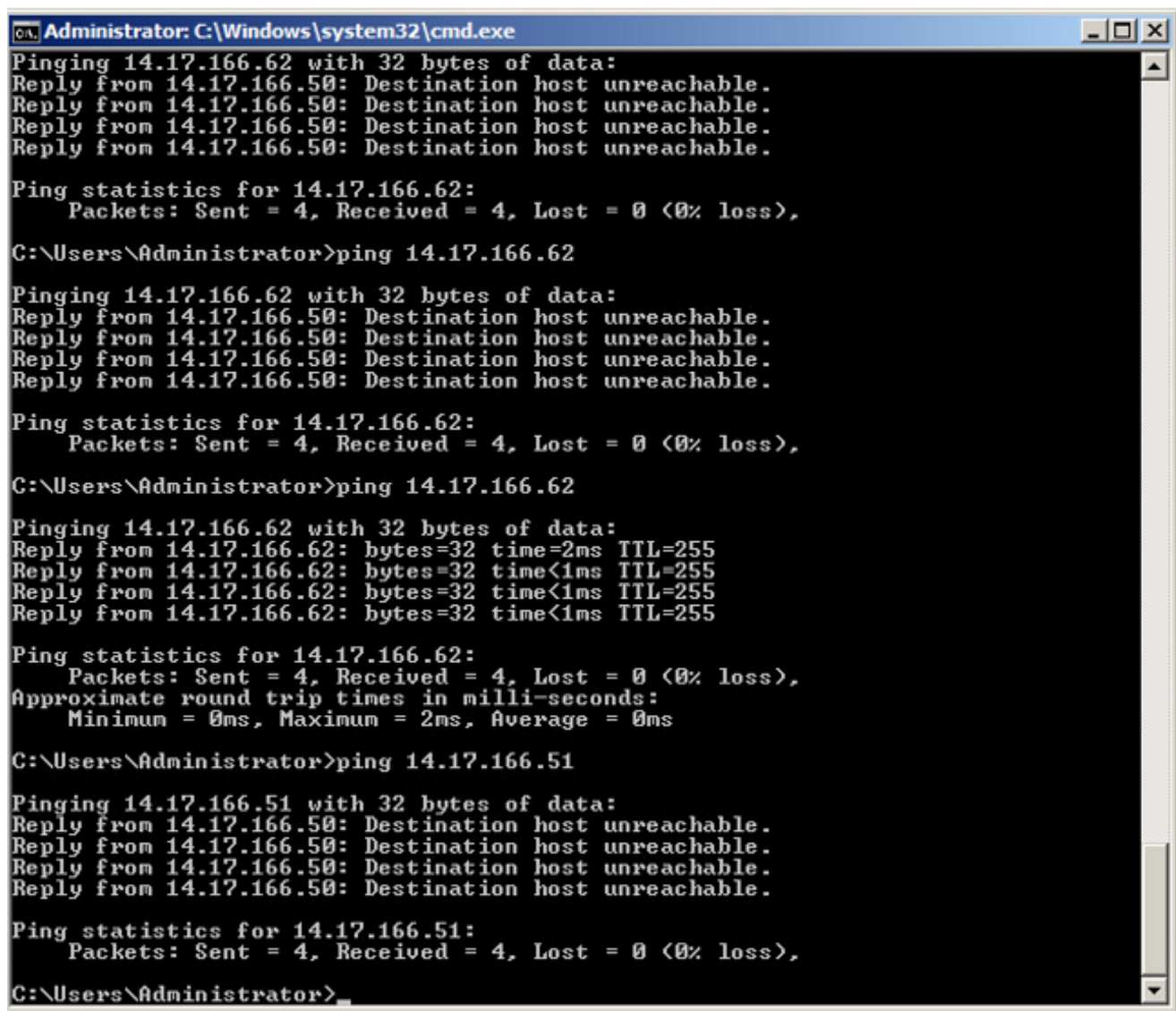
[Hardware] タブで、[Network adapter 1] をクリックします。[Network Connection] で、ネットワーク ラベルとして [pvlan\_guest (pvlan)] を選択します。



## トラブルシューティング

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した他のシステムおよび無差別ポートにあるルータおよび他のデバイスに対して ping を実行します。無差別ポート経由でのデバイスへの ping は成功する一方、隔離 VLAN 内の他のデバイスへの ping は失敗するはずですが。



```
Administrator: C:\Windows\system32\cmd.exe
Pinging 14.17.166.62 with 32 bytes of data:
Reply from 14.17.166.50: Destination host unreachable.
Reply from 14.17.166.50: Destination host unreachable.
Reply from 14.17.166.50: Destination host unreachable.
Reply from 14.17.166.50: Destination host unreachable.

Ping statistics for 14.17.166.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Administrator>ping 14.17.166.62

Pinging 14.17.166.62 with 32 bytes of data:
Reply from 14.17.166.50: Destination host unreachable.
Reply from 14.17.166.50: Destination host unreachable.
Reply from 14.17.166.50: Destination host unreachable.
Reply from 14.17.166.50: Destination host unreachable.

Ping statistics for 14.17.166.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Administrator>ping 14.17.166.62

Pinging 14.17.166.62 with 32 bytes of data:
Reply from 14.17.166.62: bytes=32 time=2ms TTL=255
Reply from 14.17.166.62: bytes=32 time<1ms TTL=255
Reply from 14.17.166.62: bytes=32 time<1ms TTL=255
Reply from 14.17.166.62: bytes=32 time<1ms TTL=255

Ping statistics for 14.17.166.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\Administrator>ping 14.17.166.51

Pinging 14.17.166.51 with 32 bytes of data:
Reply from 14.17.166.50: Destination host unreachable.
Reply from 14.17.166.50: Destination host unreachable.
Reply from 14.17.166.50: Destination host unreachable.
Reply from 14.17.166.50: Destination host unreachable.

Ping statistics for 14.17.166.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Administrator>
```

2. N1K では、プライマリ VLAN にある VM がリストされます。これは、PVLAN に関連付けられる PVLAN ホストポートで操作しているためです。VM を学習する方法とかが異なるため、UCS システムで PVLAN をネイティブとして設定しないでください。また、アップストリーム デバイスはポートチャネルから学習すること、アップストリーム デバイスはプライマリ VLAN で学習されることにも注意してください。これは、この方式で学習する必要があります。PVLAN アップリンクにプライマリ VLAN とネイティブ VLAN の両方を設定するのは、そのためです。

このスクリーンショットでは、Veth3 および Veth4 上にある 2 台のデバイスが VM です。Po1 上のデバイスはアップストリーム ルータであり、無差別ポートを経由します。

```

pvlan# show mac address-table
VLAN      MAC Address      Type      Age      Port      Mod
-----+-----+-----+-----+-----+-----
1         0002.3d10.b102   static    0        N1KV Internal Port  3
1         0002.3d20.b100   static    0        N1KV Internal Port  3
1         0002.3d30.b102   static    0        N1KV Internal Port  3
1         0002.3d40.0002   static    0        N1KV Internal Port  3
1         0002.3d60.b100   static    0        N1KV Internal Port  3
177      0002.3d20.b102   static    0        N1KV Internal Port  3
177      0002.3d40.b102   static    0        N1KV Internal Port  3
177      0050.5686.4fe8   static    0        Veth2            3
177      0050.5686.7787   static    0        Veth1            3
177      0002.3d40.2100   dynamic   3        Po3              3
177      000c.29c2.d1ba   dynamic   15       Po3              3
177      0050.5686.3bc0   dynamic   56       Po3              3
177      0050.56bc.5eea   dynamic   1        Po3              3
177      0050.56bc.761d   dynamic   1        Po3              3
266      000c.2996.9a1d   static    0        Veth4            3
266      000c.29bc.589c   static    0        Veth3            3
266      0012.8032.86a9   dynamic   214     Po1              3
Total MAC Addresses: 17
pvlan#

```

3. UCS システムでは、この通信に使用する隔離 VLAN 内のすべての MAC を学習する必要があります。ここにはアップストリームが表示されません。

```

F340-31-9-1-B(nxos)# show mac address-table
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link
VLAN      MAC Address      Type      age      Secure NTFY  Ports
-----+-----+-----+-----+-----+-----
* 166     000c.2996.9a1d   dynamic   10       F    F    Veth1491
* 166     000c.29bc.589c   dynamic   270     F    F    Veth1491
* 166     0025.b581.991e   static    0        F    F    Veth1491

```

4. Nexus 5K では、2 台の VM が隔離 VLAN にあり、アップストリーム デバイスはプライマリ VLAN にあります。

```

F340.11.13-Nexus5000-5# show mac address-table
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link
VLAN      MAC Address      Type      age      Secure NTFY  Ports
-----+-----+-----+-----+-----+-----
* 266     0012.8032.86a9   dynamic   0        F    F    Eth1/1
* 166     000c.2996.9a1d   dynamic   40       F    F    Eth1/4
* 166     000c.29bc.589c   dynamic   60       F    F    Eth1/4

```

5. 無差別ポートがある 4900 スイッチでは、すべてがプライマリ VLAN にあります。

Unicast Entries					
vlan	mac address	type	protocols	port	
266	000c.2996.9a1d	dynamic	ip,ipx,assigned,other	GigabitEthernet1/1	
266	000c.29bc.589c	dynamic	ip,ipx,assigned,other	GigabitEthernet1/1	
266	0012.8032.86a9	dynamic	ip,ipx,assigned,other	GigabitEthernet1/2	

Multicast Entries			
vlan	mac address	type	ports
1	0100.0ccc.cccc	system	Gi1/1
1	ffff.ffff.ffff	system	Gi1/1
266	ffff.ffff.ffff	system	Gi1/1,Gi1/2

## N1K アップリンク ポート プロファイルの無差別ポートを使用した、N1K 上の隔離 PVLAN

この設定では、アップストリームで使用されるプライマリVLANのみを使用して、N1KへのPVLANトラフィックを含めます。

### UCS での設定

この手順では、vNIC にプライマリ VLAN を追加する方法について説明します。必要なのはプライマリ VLAN だけなので、PVLAN の設定は不要です。

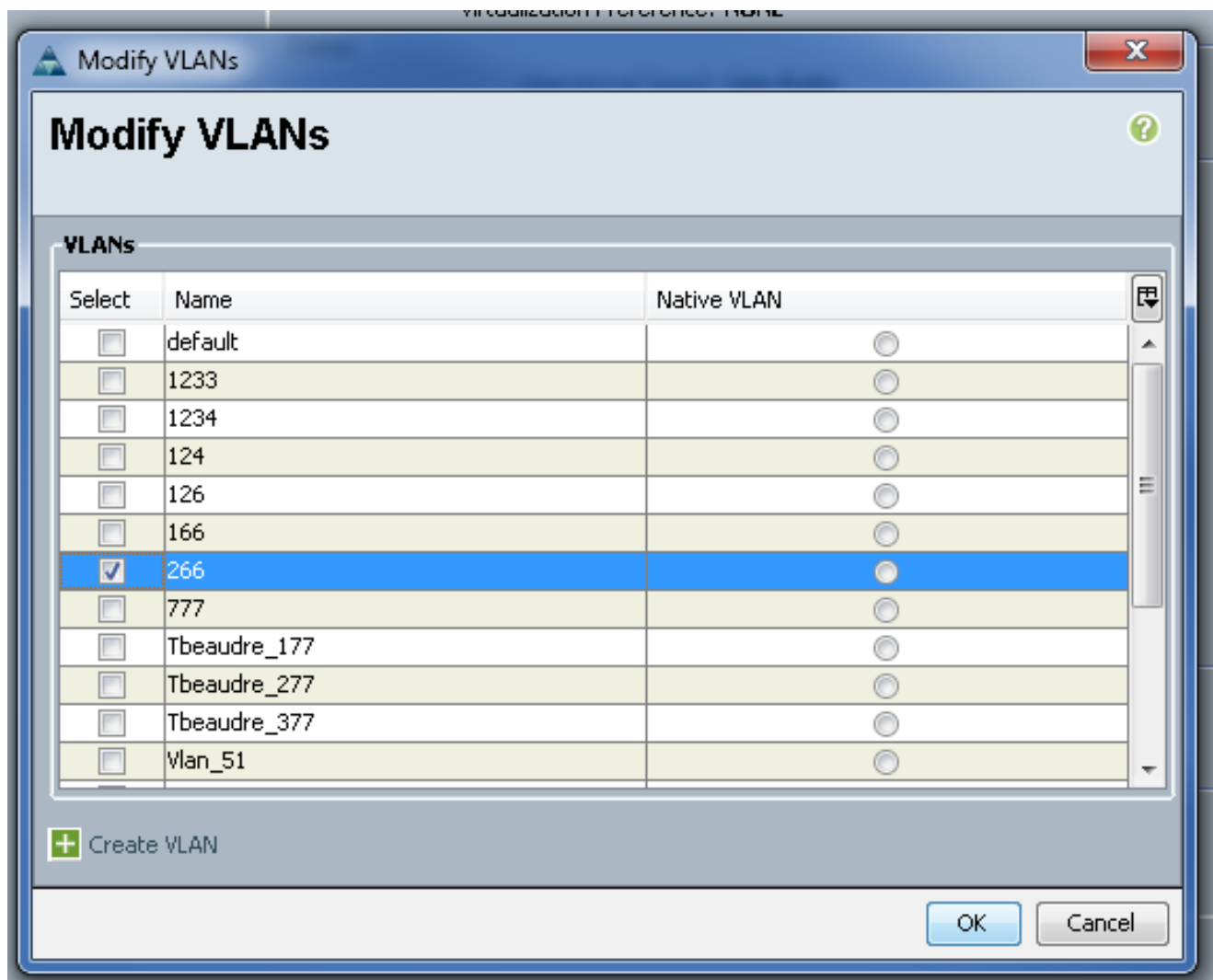
注：次の例では、VLAN 266 をプライマリ VLAN として使用し、VLAN 166 を隔離 VLAN として使用します。VLAN ID は、サイトによって決まります。

1. [Sharing Type] は [None] であることに注意してください。

The screenshot shows the configuration page for VLAN 266 in the UCS Network Management GUI. The 'Properties' section is expanded, displaying the following settings:

- Name: 266
- VLAN ID: 266
- Native VLAN: No
- Fabric ID: Dual
- Network Type: Lan
- If Type: Virtual
- Locale: External
- Transport Type: Ether
- Multicast Policy Name: <not set>
- Multicast Policy Instance: org-root/mc-policy-default
- Sharing Type:  None  Primary  Isolated

2. プライマリ VLAN を vNIC に追加するために、VLAN 266 の [Select] チェックボックスをクリックします。ネイティブとして設定しないでください。



## アップストリーム デバイスの設定

この手順では、アップストリーム デバイスを設定する方法について説明します。この場合、アップストリーム スイッチに必要なのはトランク ポートだけです。アップストリーム スイッチに可視になる VLAN は VLAN 266 だけなので、VLAN 266 のトランキングだけが必要となります。

Nexus 5K で、次のコマンドを入力してアップリンクの設定を確認します。

1. VLAN をプライマリとして追加します。

```
Nexus5000-5(config-vlan)# vlan 266
```

2. VLAN をトランキングするために、すべてのアップリンクが設定されていることを確認します。

```
interface Ethernet1/1description Connection to 4900switchport mode trunkspeed 1000interface Ethernet1/3description Connection to FIB Port 5switchport mode trunkspeed 1000interface Ethernet1/4description Connection to FIA port 5switchport mode trunkspeed 1000
```

4900 スイッチで、次の手順を実行します。

1. N1K でプライマリとして使用する VLAN を作成します。
2. VLAN が渡されるように、4900 スイッチとのインターフェイスのすべてをトランキングし

ます。

アップストリーム ルータで、VLAN 266 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。

1. interface GigabitEthernet0/1.1
2. encapsulation dot1Q 266
3. IP address 209.165.200.225 255.255.255.224

## N1K の設定

この手順では、N1K を設定する方法について説明します。

1. VLAN を作成して関連付けます。

```
Switch(config)# vlan 166
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# vlan 266
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association 166
```



2. 無差別ポートを指定した PVLAN トラフィックのアップリンク ポート プロファイルを作成します。

```
Switch(config)#port-profile type ethernet pvlan_uplink
Switch(config-port-prof)# vmware port-group
Switch(config-port-prof)# switchport mode private-vlan trunk promiscuous
Switch(config-port-prof)# switchport private-vlan trunk allowed vlan 266 <-- Only need to
allow the primary VLAN
Switch(config-port-prof)# switchport private-vlan mapping trunk 266 166 <-- The VLANs must
be mapped at this point
Switch(config-port-prof)# channel-group auto mode on mac-pinning
Switch(config-port-prof)# no shut
Switch(config-port-prof)# state enabled
```

3. 隔離 VLAN のポート グループを作成します。PVLAN ホスト ポートを作成し、プライマリ VLAN と隔離 VLAN のホスト関係を設定します。

```
Switch(config)# port-profile type vethernet pvlan_guest
Switch(config-port-prof)# vmware port-group
Switch(config-port-prof)# switchport mode private-vlan host
Switch(config-port-prof)# switchport private-vlan host-association 266 166
Switch(config-port-prof)# no shut
Switch(config-port-prof)# state enabled
```

4. vCenter で、適切な vNIC を PVLAN アップリンクに追加します。適切な vNIC とは、UCS での設定で隔離 VLAN を追加した vNIC です。

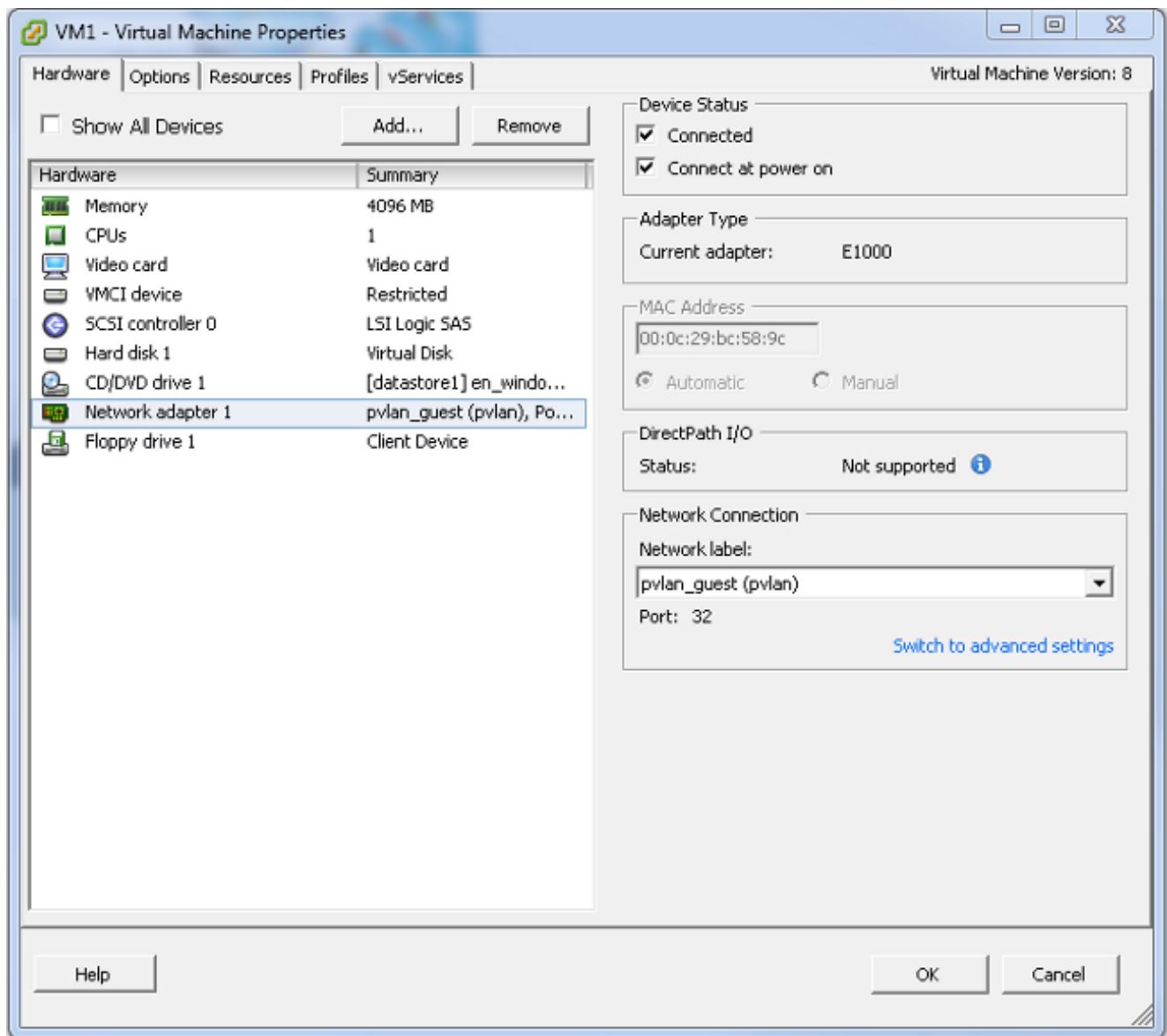
<input type="checkbox"/>	 vmnic3	--	<a href="#">View Details...</a>	Select an uplink port gr...
<input checked="" type="checkbox"/>	 vmnic4	pvlan	<a href="#">View Details...</a>	pvlan_uplink
<input type="checkbox"/>	 vmnic5	--	<a href="#">View Details...</a>	Select an uplink port gr...

5. VM を適切なポート グループに追加します。

[Hardware] タブで、[Network adapter 1] をクリックします。[Network Connection] で、ネッ



トワーク ラベルとして [pvlan\_guest (pvlan)] を選択します。



## トラブルシューティング

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 グループに設定した他のシステムおよび無差別ポートにあるルータおよび他のデバイスに対して ping を実行します。無差別ポート経由でのデバイスへの ping は成功する一方、隔離 VLAN 内の他のデバイスへの ping は失敗するはずです。

```

Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping 14.17.166.61
Pinging 14.17.166.61 with 32 bytes of data:
Reply from 14.17.166.61: bytes=32 time<1ms TTL=255
Reply from 14.17.166.61: bytes=32 time<1ms TTL=255

Ping statistics for 14.17.166.61:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\Administrator>ping 14.17.166.51
Pinging 14.17.166.51 with 32 bytes of data:
Reply from 14.17.166.50: Destination host unreachable.
Reply from 14.17.166.50: Destination host unreachable.
Reply from 14.17.166.50: Destination host unreachable.
Reply from 14.17.166.50: Destination host unreachable.

Ping statistics for 14.17.166.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
C:\Users\Administrator>_

```

2. N1K では、プライマリ VLAN にある VM がリストされます。これは、PVLAN に関連付けられる PVLAN ホスト ポートで操作しているためです。また、アップストリーム デバイスはポート チャネルから学習すること、アップストリーム デバイスはプライマリ VLAN で学習されることにも注意してください。

このスクリーン ショットでは、Veth3 および Veth4 上にある 2 台のデバイスが VM です。Po1 上のデバイスはアップストリーム デバイスであり、無差別ポートを経由します。

```

pvlan(config-port-prof)# show mac address-table
VLAN      MAC Address      Type      Age      Port      Mod
-----+-----+-----+-----+-----+-----
1         0002.3d10.b102   static    0        N1KV Internal Port  3
1         0002.3d20.b100   static    0        N1KV Internal Port  3
1         0002.3d30.b102   static    0        N1KV Internal Port  3
1         0002.3d40.0002   static    0        N1KV Internal Port  3
1         0002.3d60.b100   static    0        N1KV Internal Port  3
177       0002.3d20.b102   static    0        N1KV Internal Port  3
177       0002.3d40.b102   static    0        N1KV Internal Port  3
177       0050.5686.4fe8   static    0        Veth2       3
177       0050.5686.7787   static    0        Veth1       3
177       0002.3d40.2100   dynamic   1        Po3         3
177       000c.29c2.d1ba   dynamic   55       Po3         3
177       0050.5686.3bc0   dynamic   45       Po3         3
177       0050.56bc.5eea   dynamic   1        Po3         3
177       0050.56bc.761d   dynamic   1        Po3         3
266       000c.2996.9a1d   static    0        Veth4       3
266       000c.29bc.589c   static    0        Veth3       3
266       c84c.75f6.013f   dynamic   104     Po1         3
Total MAC Addresses: 17
pvlan(config-port-prof)#

```

3. UCS システムでは、この通信に使用する、N1K 上で使用するプライマリ VLAN 内のすべての MAC を学習する必要があります。ここではアップストリームを学習しません。



```
F340-31-9-1-B(nxos)# show mac address-table
Legend:
    * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
    age - seconds since last seen,+ - primary entry using vPC Peer-Link
VLAN    MAC Address    Type    age    Secure NTFY    Ports
-----+-----+-----+-----+-----+-----
* 266    000c.2996.9a1d    dynamic    100        F    F    Veth1491
* 266    000c.29bc.589c    dynamic    180        F    F    Veth1491
* 177    0025.b581.9a3f    dynamic    0          F    F    Veth1402
* 177    0025.b585.100a    dynamic    350        F    F    Veth1424
* 177    0050.566b.01ad    dynamic    380        F    F    Veth1402
* 126    0025.b581.999e    static    0          F    F    Veth1392
* 124    0023.04c6.dbe2    dynamic    0          F    F    Veth1404
```

4. Nexus 5K では、選択したプライマリ VLAN 内にすべての MAC があります。

```
F340.11.13-Nexus5000-5# show mac address-table
Legend:
    * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
    age - seconds since last seen,+ - primary entry using vPC Peer-Link
VLAN    MAC Address    Type    age    Secure NTFY    Ports
-----+-----+-----+-----+-----+-----
* 266    000c.2996.9a1d    dynamic    90        F    F    Eth1/4
* 266    000c.29bc.589c    dynamic    20        F    F    Eth1/4
* 266    c84c.75f6.013f    dynamic    100       F    F    Eth1/1
F340.11.13-Nexus5000-5#
```

5. 4900 スイッチでは、選択したプライマリ VLAN 内にすべてがあります。

```
Switch#show mac address-table
Unicast Entries
vlan    mac address    type    protocols    port
-----+-----+-----+-----+-----+-----
266     000c.2996.9a1d    dynamic    ip,ipx,assigned,other    GigabitEthernet1/1
266     000c.29bc.589c    dynamic    ip,ipx,assigned,other    GigabitEthernet1/1
266     c84c.75f6.013f    static    ip,ipx,assigned,other    Switch

Multicast Entries
vlan    mac address    type    ports
-----+-----+-----+-----+-----+-----
1       0100.0ccc.ccce    system    Gi1/1
1       ffff.ffff.ffff    system    Gi1/1
166     ffff.ffff.ffff    system    Gi1/1
266     ffff.ffff.ffff    system    Gi1/1,Gi1/2,Switch

Switch#
```

## N1K アップリンク ポート プロファイルの無差別ポートを使用した、N1K 上のコミュニティ PVLAN

この設定は、UCS を使用したコミュニティ VLAN にもサポートされます。

この設定は、「[N1K アップリンク ポート プロファイルの無差別ポートを使用した、N1K 上の隔離 PVLAN](#)」の項の設定と同じです。コミュニティと隔離の間の唯一の違いは、PVLAN の設定です。

N1Kを設定するには、Nexus 5Kで行ったようにVLANを作成して関連付けます。

```
Switch(config)# vlan 166
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# vlan 266
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association 16
```

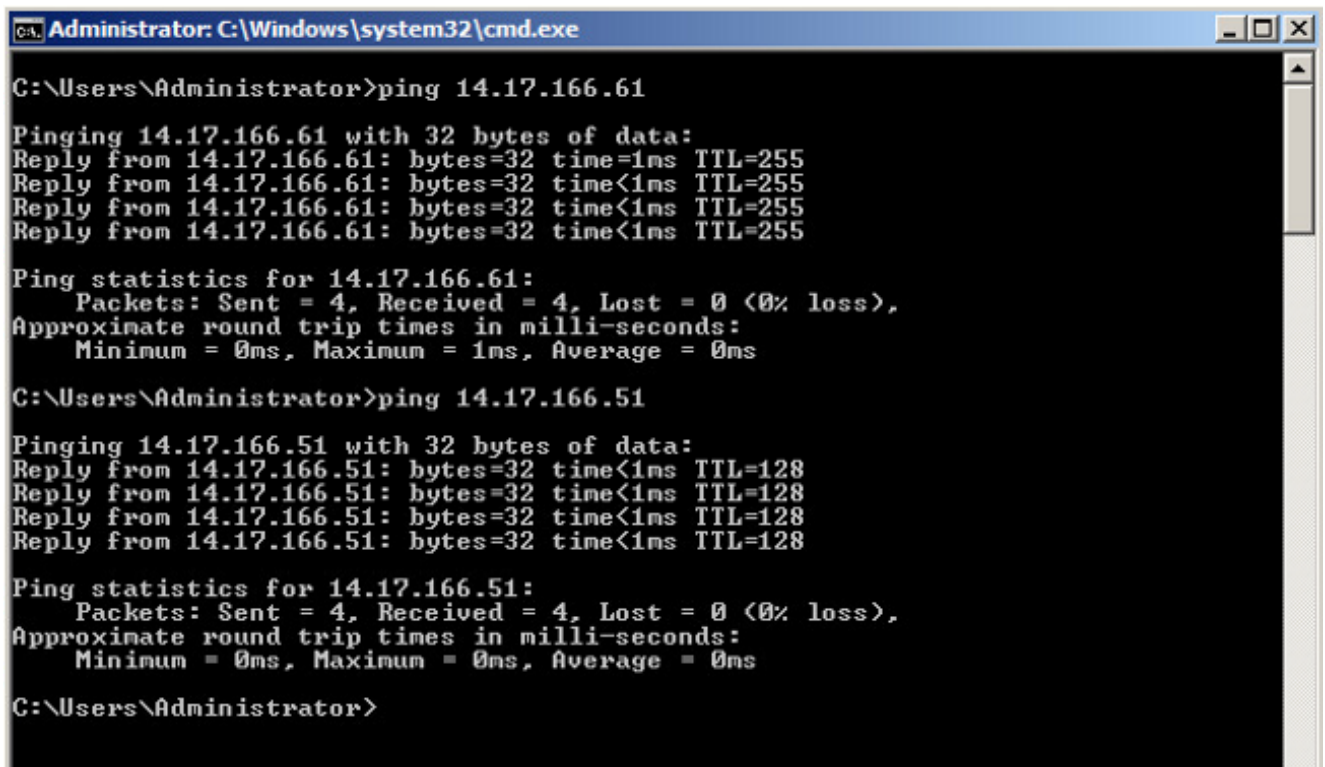
他のすべての設定は、N1K アップリンク ポート プロファイルの無差別ポートを使用した、N1K 上の隔離 PVLAN と同じです。

設定が完了すると、PVLAN に使用されている vEthernet ポート プロファイルに接続するすべての VM と通信できるようになります。

## トラブルシューティング

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 グループに設定した他のシステムおよび無差別ポートにあるルータおよび他のデバイスに対して ping を実行します。無差別ポートを経由してコミュニティ内の他のシステムに送信される ping は成功するはずですが、



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping 14.17.166.61

Pinging 14.17.166.61 with 32 bytes of data:
Reply from 14.17.166.61: bytes=32 time=1ms TTL=255
Reply from 14.17.166.61: bytes=32 time<1ms TTL=255
Reply from 14.17.166.61: bytes=32 time<1ms TTL=255
Reply from 14.17.166.61: bytes=32 time<1ms TTL=255

Ping statistics for 14.17.166.61:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>ping 14.17.166.51

Pinging 14.17.166.51 with 32 bytes of data:
Reply from 14.17.166.51: bytes=32 time<1ms TTL=128
Reply from 14.17.166.51: bytes=32 time<1ms TTL=128
Reply from 14.17.166.51: bytes=32 time<1ms TTL=128
Reply from 14.17.166.51: bytes=32 time<1ms TTL=128

Ping statistics for 14.17.166.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

2. その他すべてのトラブルシューティングは、[隔離 PVLAN](#) の場合と同じです。

## DVS 上の VMware DVS 無差別ポートでの隔離 PVLAN およびコミュニティ PVLAN

DVSとUCSシステムの両方の設定の問題により、DVSおよびUCSを使用するPVLANは、バージョン2.2(2c)より前ではサポートされません。

## 確認

現在、これらの設定に使用できる検証手順はありません。

## トラブルシューティング

ここまでの項で、設定のトラブルシューティングに役立つ情報を提供しました。

アウトプット インタープリタ ツール (登録ユーザ専用) は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。