

# Private VLAN und Cisco UCS-Konfiguration vor 2.2(2C)

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Theorie](#)

[PVLAN-Implementierung in UCS](#)

[Ziel](#)

[Konfigurieren](#)

[Netzwerkdigramme](#)

[PVLAN auf vSwitch: Isolated-PVLAN mit Promiscuous-Port auf einem Upstream-Gerät](#)

[Konfiguration in UCS](#)

[Konfiguration von Upstream-Geräten](#)

[Fehlerbehebung](#)

[Isolated-PVLAN auf N1K mit Promiscuous-Port auf einem Upstream-Gerät](#)

[Konfiguration in UCS](#)

[Konfiguration von Upstream-Geräten](#)

[Konfiguration von N1K](#)

[Fehlerbehebung](#)

[Isolated-PVLAN auf N1K mit Promiscuous-Port im N1K-Uplink-Portprofil](#)

[Konfiguration in UCS](#)

[Konfiguration von Upstream-Geräten](#)

[Konfiguration von N1K](#)

[Fehlerbehebung](#)

[Community PVLAN auf N1K mit Promiscuous Port im N1K Uplink-Portprofil](#)

[Fehlerbehebung](#)

[Isolated PVLAN und Community PVLAN auf VMware DVS Promiscuous Port auf dem DVS](#)

[Überprüfen](#)

[Fehlerbehebung](#)

## Einführung

In diesem Dokument wird die PVLAN-Unterstützung (Private VLAN) im Cisco Unified Computing System (UCS) beschrieben, eine Funktion, die in Version 1.4 des Cisco UCS Manager (UCSM) eingeführt wurde. Darüber hinaus werden die Funktionen, die Probleme und die Konfiguration beschrieben, wenn in einer UCS-Umgebung PVLANS verwendet werden.

**DIESES DOKUMENT IST ZUR VERWENDUNG MIT UCSM VERSION 2.2(2C) UND FRÜHEREN VERSIONEN BESTIMMT. In Versionen nach Version 2.2(2C) wurden Änderungen an UCSM**

vorgenommen, und ESXi DVS wird unterstützt. Auch die Funktionsweise von Tagging für die PVLAN-NIC wurde geändert.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- UCS
- Cisco Nexus 1000 V (N1K)
- VMware
- Layer-2-Switching (L2)

### Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Hintergrundinformationen

### Theorie

Ein privates VLAN ist ein VLAN, das für die L2-Isolierung von anderen Ports innerhalb desselben privaten VLAN konfiguriert ist. Ports, die zu einem PVLAN gehören, sind mit einem gemeinsamen Satz von Support-VLANs verbunden, die zur Erstellung der PVLAN-Struktur verwendet werden.

Es gibt drei Arten von PVLAN-Ports:

- Ein **Promiscuous-Port** kommuniziert mit allen anderen PVLAN-Ports und ist der Port, der für die Kommunikation mit Geräten außerhalb des PVLAN verwendet wird.
- Ein **isolierter Port** verfügt über eine vollständige L2-Trennung (einschließlich Broadcasts) von anderen Ports innerhalb desselben PVLAN, mit Ausnahme des Promiscuous-Ports.
- Ein **Community-Port** kann sowohl mit anderen Ports im selben PVLAN als auch mit dem Promiscuous-Port kommunizieren. Community-Ports sind in L2 von Ports in anderen Communities oder isolierten PVLAN-Ports isoliert. Broadcasts werden nur an andere Ports in der Community und an den Promiscuous-Port weitergeleitet.

Siehe [RFC 5517, Private VLANs von Cisco Systems: Skalierbare Sicherheit in einer Multi-Client-Umgebung](#), um Theorie, Betrieb und Konzepte von PVLANs zu verstehen.

### PVLAN-Implementierung in UCS

Das UCS ähnelt der Nexus 5000/2000-Architektur, in der der Nexus 5000 mit dem UCS 6100 und

der Nexus 2000 mit den UCS 2104 Fabric Extendern vergleichbar ist.

Viele Einschränkungen der PVLAN-Funktionalität im UCS sind auf die Einschränkungen der Nexus 5000/2000-Implementierung zurückzuführen.

Wichtige Punkte:

- Im UCS werden nur einzelne Ports unterstützt. Wenn das N1K integriert ist, können Sie Community-VLANs verwenden, aber der Promiscuous-Port muss sich auch auf dem N1K befinden.
- Promiscuous-Ports/Trunks, Community-Ports/Trunks und isolierte Trunks werden nicht unterstützt.
- Promiscuous-Ports müssen sich außerhalb der UCS-Domäne befinden, z. B. ein Upstream-Switch/Router oder ein Downstream-N1K.

## Ziel

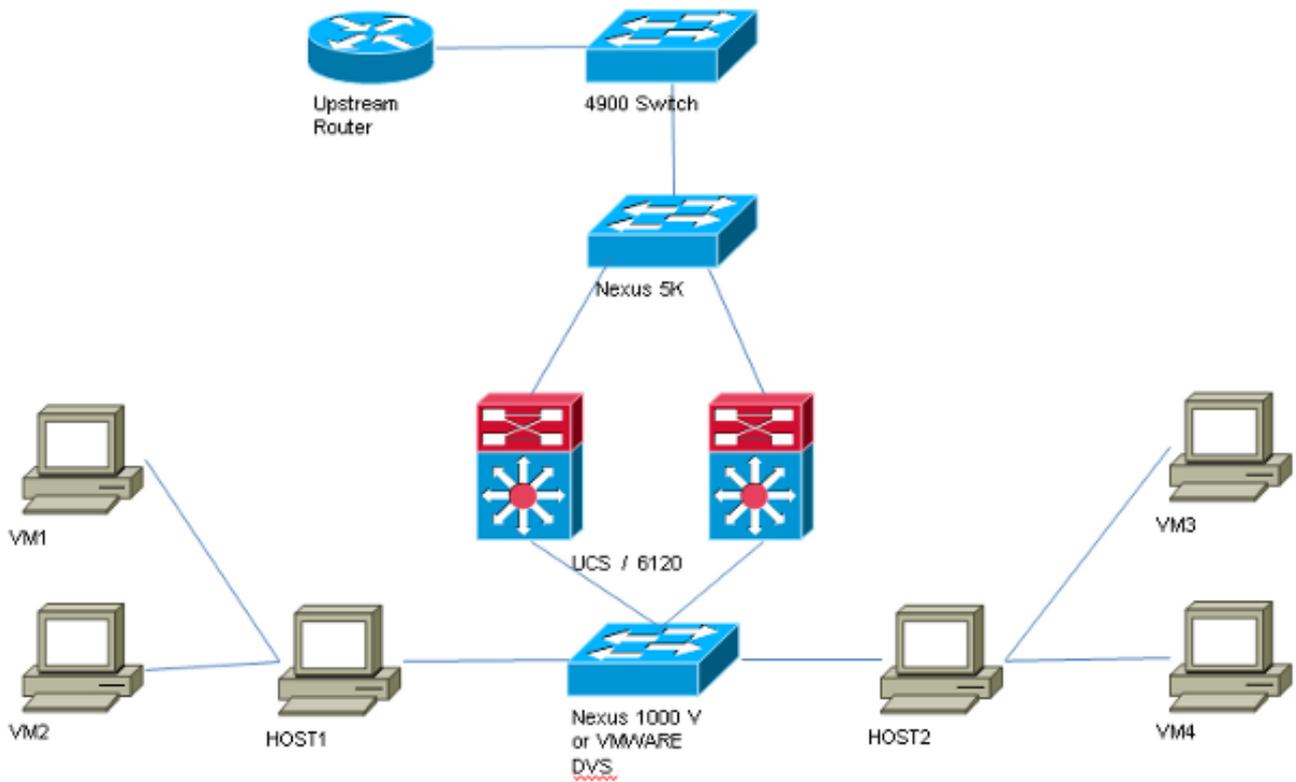
In diesem Dokument werden verschiedene Konfigurationen erläutert, die für PVLAN mit UCS verfügbar sind:

1. Isolated-PVLAN mit Promiscuous-Port auf einem Upstream-Gerät.
2. Isolated-PVLAN auf N1K mit Promiscuous-Port auf einem Upstream-Gerät.
3. Isolated-PVLAN auf N1K mit Promiscuous-Port im N1K-Uplink-Portprofil
4. Community PVLAN auf N1K mit Promiscuous-Port im N1K-Uplink-Portprofil.
5. Isolated PVLAN auf VMware Distributed Virtual Switch (DVS) Promiscuous Port auf dem DVS.
6. Community PVLAN auf VMware DVS-Switch Promiscuous-Port auf dem DVS.

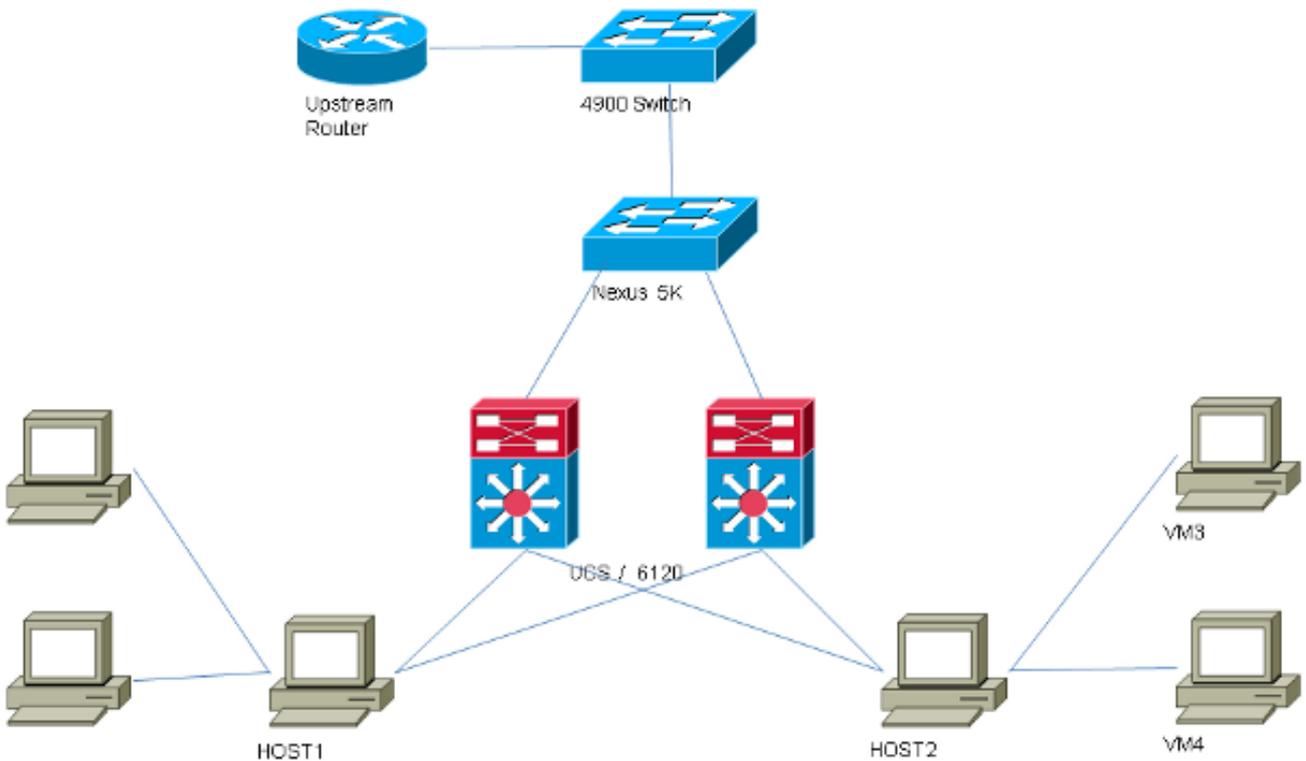
## Konfigurieren

### Netzwerkdiagramme

Die Topologie für alle Beispiele mit einem verteilten Switch ist:



Die Topologie für alle Beispiele ohne verteilten Switch ist:



## PVLAN auf vSwitch: Isolated-PVLAN mit Promiscuous-Port auf einem Upstream-Gerät

In dieser Konfiguration leiten Sie PVLAN-Datenverkehr über das UCS an einen Promiscuous-Port

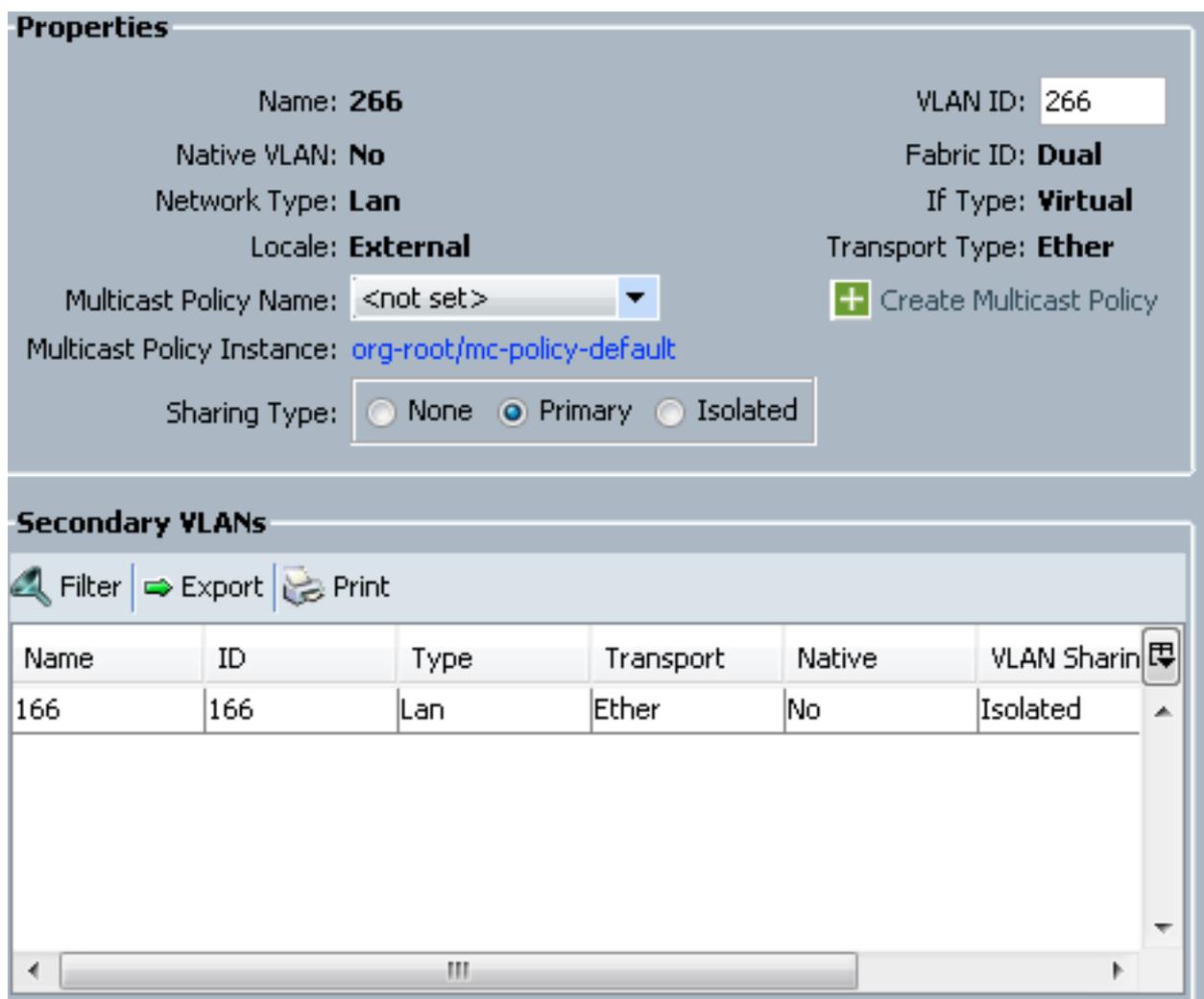
weiter, der Upstream ist. Da Sie nicht sowohl primäre als auch sekundäre VLANs auf derselben vNIC senden können, benötigen Sie für jeden Blade für jedes PVLAN eine vNIC, um den PVLAN-Datenverkehr zu übertragen.

## Konfiguration in UCS

In diesem Verfahren wird beschrieben, wie sowohl das primäre als auch alle isolierten VLANs erstellt werden.

**Hinweis:** In diesem Beispiel wird 266 als primäres und 166 als isoliertes Element verwendet. Die VLAN-IDs werden vom Standort bestimmt.

1. Um das primäre VLAN zu erstellen, klicken Sie als Freigabebetyp auf **Primär**, und geben Sie eine **VLAN-ID** von 266 ein:



The screenshot displays the configuration interface for a VLAN. The top section, titled "Properties", shows the following settings:

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

The bottom section, titled "Secondary VLANs", contains a table with the following data:

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

2. Um das isolierte VLAN zu erstellen, klicken Sie als Freigabebetyp auf **Isolated**, geben Sie eine **VLAN-ID** von 166 ein, und wählen Sie **VLAN 266 (266)** als primäres VLAN aus:



Nur das isolierte VLAN wird hinzugefügt. Es muss als primär festgelegt werden, und es kann nur ein VLAN für jede vNIC vorhanden sein. Da das native VLAN hier definiert ist, sollten Sie VLAN Tagging nicht für die VMware-Portgruppen konfigurieren.

## Konfiguration von Upstream-Geräten

Diese Verfahren beschreiben, wie ein Nexus 5K so konfiguriert wird, dass das PVLAN an einen Upstream-Switch der Serie 4900 weitergeleitet wird, bei dem sich der Promiscuous-Port befindet. Dies ist möglicherweise nicht in allen Umgebungen erforderlich. Verwenden Sie diese Konfiguration jedoch für den Fall, dass Sie das PVLAN über einen anderen Switch weiterleiten müssen.

Geben Sie auf dem Nexus 5K diese Befehle ein, und überprüfen Sie die Uplink-Konfiguration:

1. Aktivieren Sie die PVLAN-Funktion:

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

2. Fügen Sie die VLANs als primäre und isolierte VLANs hinzu:

```
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. Ordnen Sie VLAN 266 dem isolierten VLAN 166 zu:

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

4. Stellen Sie sicher, dass alle Uplinks so konfiguriert sind, dass sie die VLANs trunk:

Schnittstelle Ethernet1/1 Beschreibung Verbindung zu 4900 Trunk im Switch-Port-Modus Geschwindigkeit 1000  
Schnittstelle Ethernet1/3 Beschreibung Verbindung mit FIB-Port 5 Trunk im Switch-Port-Modus Geschwindigkeit 1000  
Schnittstelle Ethernet1/4 Beschreibung Verbindung mit FIA-Port 5 Trunk im Switch-Port-Modus Geschwindigkeit 1000

Gehen Sie auf dem Switch der Serie 4900 wie folgt vor, und richten Sie den Promiscuous-Port ein. Das PVLAN endet am Promiscuous-Port.

1. Aktivieren Sie ggf. die PVLAN-Funktion.
2. Erstellen und Zuordnen der VLANs wie auf dem Nexus 5K ausgeführt
3. Erstellen Sie den Promiscuous-Port am Ausgangs-Port des 4900-Switches. Ab diesem Punkt werden die Pakete aus VLAN 166 in diesem Fall auf VLAN 266 angezeigt.

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

Erstellen Sie auf dem Upstream-Router nur eine Subschnittstelle für das VLAN 266. Auf dieser Ebene hängen die Anforderungen von der verwendeten Netzwerkkonfiguration ab:

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

## Fehlerbehebung

Dieses Verfahren beschreibt, wie die Konfiguration getestet wird.

1. Konfigurieren Sie die virtuelle Switch-Schnittstelle (SVI) auf jedem Switch, sodass Sie die SVI vom PVLAN aus pingen können:

```
(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. Überprüfen Sie die MAC-Adresstabellen, um zu sehen, wo Ihre MAC-Adresse erfasst wird. Auf allen Switches sollte sich die MAC-Adresse im isolierten VLAN befinden, außer auf dem Switch mit dem Promiscuous-Port. Beachten Sie auf dem Promiscuous-Switch, dass sich die MAC-Adresse im primären VLAN befindet.

Auf dem Fabric Interconnect wird die MAC-Adresse 0050.56bd.7bef auf Veth1491 gelernt:

```
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--
```

Auf dem Nexus 5K wird die MAC-Adresse 0050.56bd.7bef auf Eth1/4 gelernt:

```

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#

```

Auf dem 4900-Switch wird die MAC-Adresse 0050.56bd.7bef auf GigabitEthernet1/1 gelernt:

```

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.ffff.ffff       system      Gi1/1
15    ffff.ffff.ffff       system      Gi1/1
16    ffff.ffff.ffff       system      Gi1/1
17    ffff.ffff.ffff       system      Gi1/1
18    ffff.ffff.ffff       system      Gi1/1
--More--

```

In dieser Konfiguration können die Systeme in diesem isolierten VLAN nicht miteinander kommunizieren, sondern über den Promiscuous-Port des 4900-Switches mit anderen Systemen kommunizieren. Ein Problem ist die Konfiguration von Downstream-Geräten. In diesem Fall verwenden Sie VMware und zwei Hosts.

Denken Sie daran, dass Sie für jedes PVLAN eine vNIC verwenden müssen. Diese vNICs werden VMware vSphere ESXi präsentiert. Anschließend können Sie Portgruppen erstellen und Gäste zu

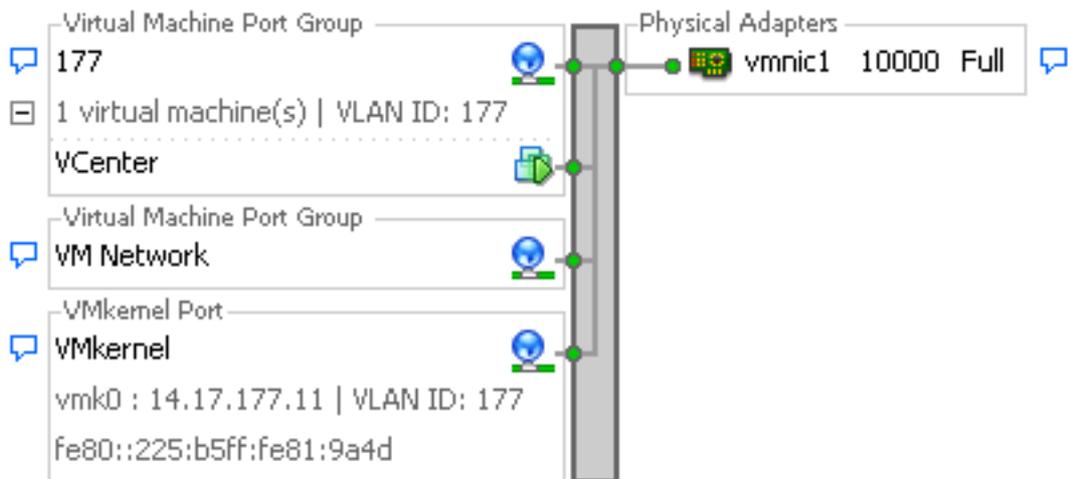
diesen Portgruppen hinzufügen.

Wenn zwei Systeme derselben Portgruppe auf demselben Switch hinzugefügt werden, können sie miteinander kommunizieren, da ihre Kommunikation lokal auf dem vSwitch geschaltet wird. In diesem System gibt es zwei Blades mit jeweils zwei Hosts.

Auf dem ersten System wurden zwei verschiedene Portgruppen erstellt - eine mit dem Namen 166 und eine mit dem Namen 166A. Jede ist mit einer einzelnen NIC verbunden, die im isolierten VLAN im UCS konfiguriert wird. Es gibt derzeit nur einen Gast für jede Portgruppe. Da diese auf ESXi getrennt sind, können sie in diesem Fall nicht miteinander sprechen.

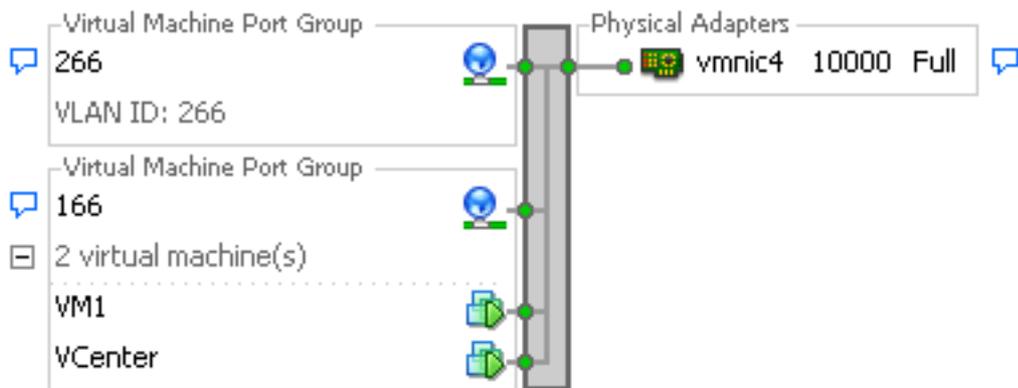
### Standard Switch: vSwitch0

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



### Standard Switch: vSwitch1

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



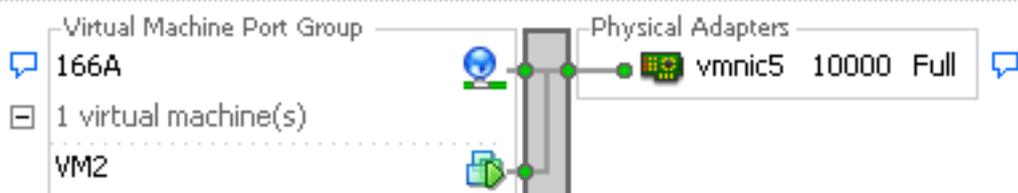
### Standard Switch: vSwitch2

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



### Standard Switch: vSwitch3

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

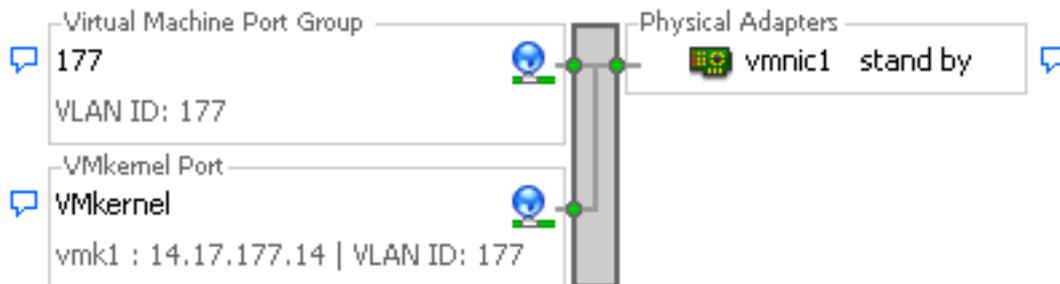


Auf dem zweiten System gibt es nur eine Port-Gruppe namens 166. Diese Portgruppe besteht aus zwei Gästen. In dieser Konfiguration können VM3 und VM4 miteinander kommunizieren, auch wenn Sie dies nicht zulassen möchten. Um dies zu korrigieren, müssen Sie eine einzelne NIC für jedes virtuelle System (VM) im isolierten VLAN konfigurieren und dann eine Port-Gruppe erstellen, die mit dieser vNIC verbunden ist. Nach der Konfiguration sollte nur ein Gast in die Portgruppe

aufgenommen werden. Dies ist kein Problem mit einer reinen Windows-Installation, da Sie diese zugrunde liegenden vSwitches nicht haben.

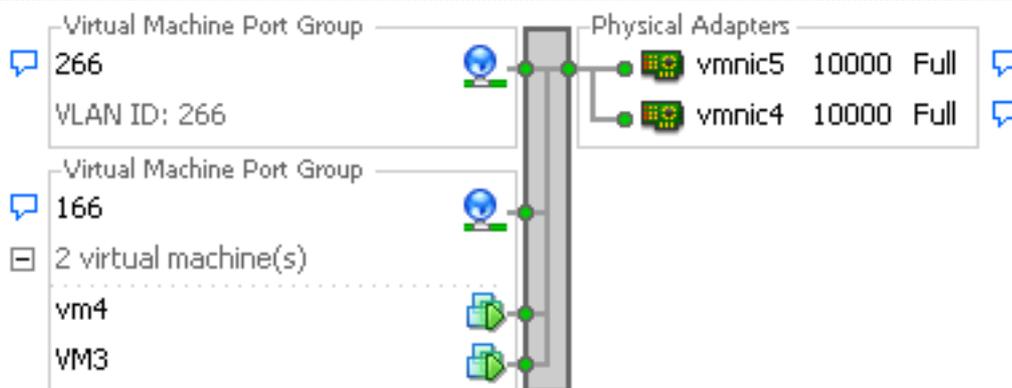
#### Standard Switch: vSwitch0

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



#### Standard Switch: vSwitch1

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



#### Standard Switch: vSwitch2

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



## Isolated-PVLAN auf N1K mit Promiscuous-Port auf einem Upstream-Gerät

In dieser Konfiguration leiten Sie PVLAN-Datenverkehr über N1K und dann das UCS an einen Promiscuous-Port weiter, der Upstream ist. Da Sie nicht sowohl primäre als auch sekundäre VLANs auf derselben vNIC senden können, benötigen Sie für jeden PVLAN-Uplink eine vNIC, um den PVLAN-Datenverkehr zu übertragen.

### Konfiguration in UCS

In diesem Verfahren wird beschrieben, wie sowohl das primäre als auch alle isolierten VLANs erstellt werden.

**Hinweis:** In diesem Beispiel wird 266 als primäres und 166 als isoliertes Element verwendet. Die VLAN-IDs werden vom Standort bestimmt.



**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:

---

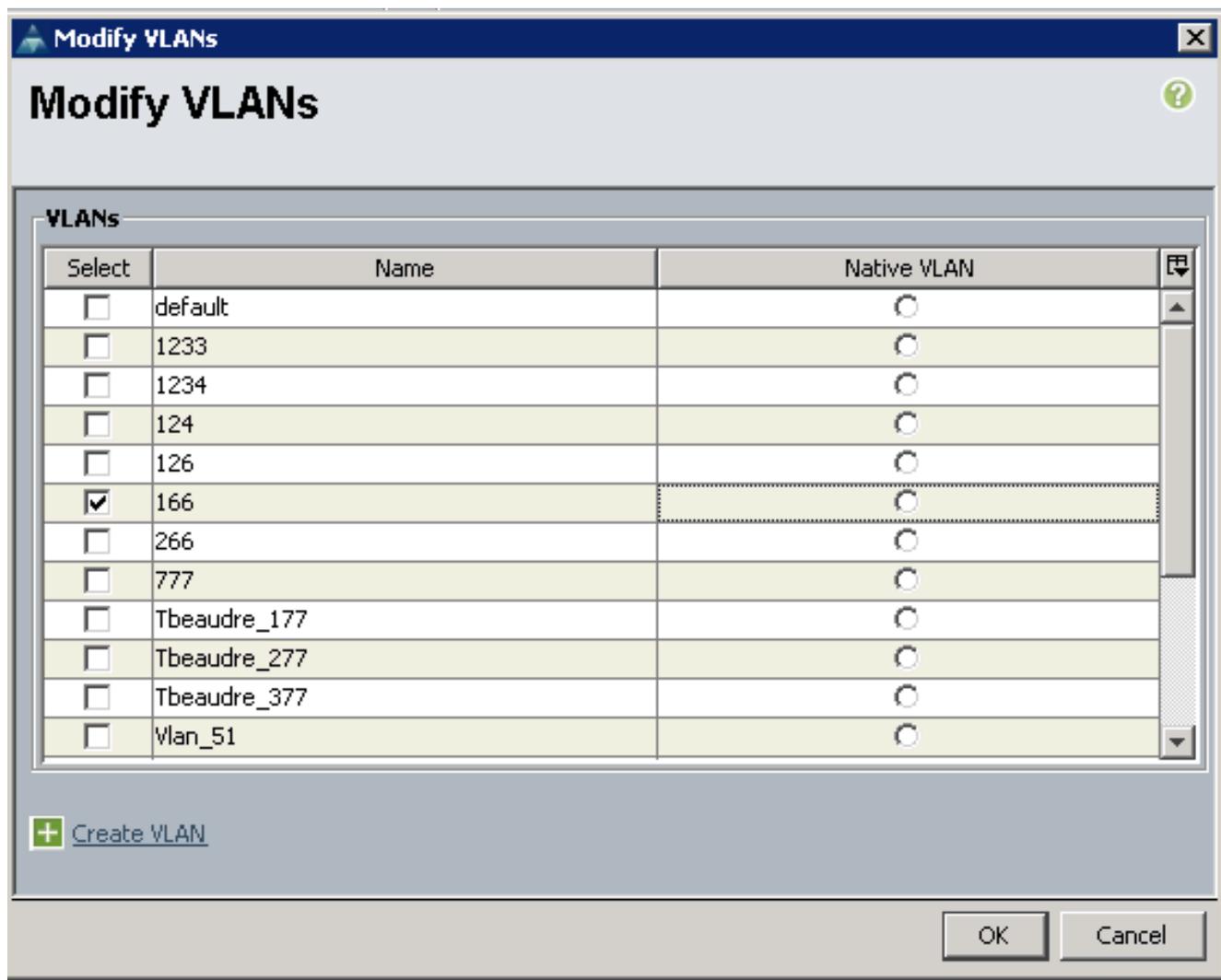
**Primary VLAN Properties**

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](#)

- Um das VLAN der vNIC hinzuzufügen, aktivieren Sie das Kontrollkästchen **Select (Auswählen)** für VLAN 166. Für VLAN 166 wurde kein natives VLAN ausgewählt.



Nur das isolierte VLAN wird hinzugefügt. Es darf nicht als nativ festgelegt werden, und es kann nur ein VLAN für jede vNIC vorhanden sein. Da das native VLAN hier nicht definiert ist, kennzeichnen Sie das native VLAN auf dem N1K. Die Option zum Taggen eines nativen VLAN ist im VMware-DVS nicht verfügbar, daher wird dies auf dem DVS nicht unterstützt.

## Konfiguration von Upstream-Geräten

Diese Verfahren beschreiben, wie ein Nexus 5K konfiguriert wird, um das PVLAN an einen Upstream-Switch der Serie 4900 weiterzuleiten, an dem sich der Promiscuous-Port befindet. Dies ist möglicherweise nicht in allen Umgebungen erforderlich. Verwenden Sie diese Konfiguration jedoch für den Fall, dass Sie das PVLAN über einen anderen Switch weiterleiten müssen.

Geben Sie auf dem Nexus 5K diese Befehle ein, und überprüfen Sie die Uplink-Konfiguration:

1. Aktivieren Sie die PVLAN-Funktion:

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

2. Fügen Sie die VLANs als primäre und isolierte VLANs hinzu:

```
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. Ordnen Sie VLAN 266 dem isolierten VLAN 166 zu:

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

### 4. Stellen Sie sicher, dass alle Uplinks so konfiguriert sind, dass sie die VLANs trunk:

Schnittstelle Ethernet1/1 Beschreibung Verbindung zu 4900 Trunk im Switch-Port-Modus Geschwindigkeit 1000  
Schnittstelle Ethernet1/3 Beschreibung Verbindung mit FIB-Port 5 Trunk im Switch-Port-Modus Geschwindigkeit 1000  
Schnittstelle Ethernet1/4 Beschreibung Verbindung mit FIA-Port 5 Trunk im Switch-Port-Modus Geschwindigkeit 1000

Gehen Sie auf dem Switch der Serie 4900 wie folgt vor, und richten Sie den Promiscuous-Port ein. Das PVLAN endet am Promiscuous-Port.

1. Aktivieren Sie ggf. die PVLAN-Funktion.
2. Erstellen und Zuordnen der VLANs wie auf dem Nexus 5K ausgeführt
3. Erstellen Sie den Promiscuous-Port am Ausgangs-Port des 4900-Switches. Ab diesem Punkt werden die Pakete aus VLAN 166 in diesem Fall auf VLAN 266 angezeigt.

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

Erstellen Sie auf dem Upstream-Router nur eine Subschnittstelle für das VLAN 266. Auf dieser Ebene hängen die Anforderungen von der Netzwerkkonfiguration ab, die Sie verwenden:

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

## Konfiguration von N1K

Dieses Verfahren beschreibt, wie das N1K als Standard-Trunk und nicht als PVLAN-Trunk konfiguriert wird.

1. Erstellen und Zuordnen der VLANs wie auf dem Nexus 5K ausgeführt Weitere Informationen finden Sie im Abschnitt [Konfiguration von Upstream-Geräten](#).
2. Erstellen Sie ein Uplink-Port-Profil für den PVLAN-Datenverkehr:

```
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. Erstellen Sie die Port-Gruppe für das isolierte VLAN. Erstellen Sie einen PVLAN-Host-Port mit der Hostzuordnung für die primären und isolierten VLANs:

```

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

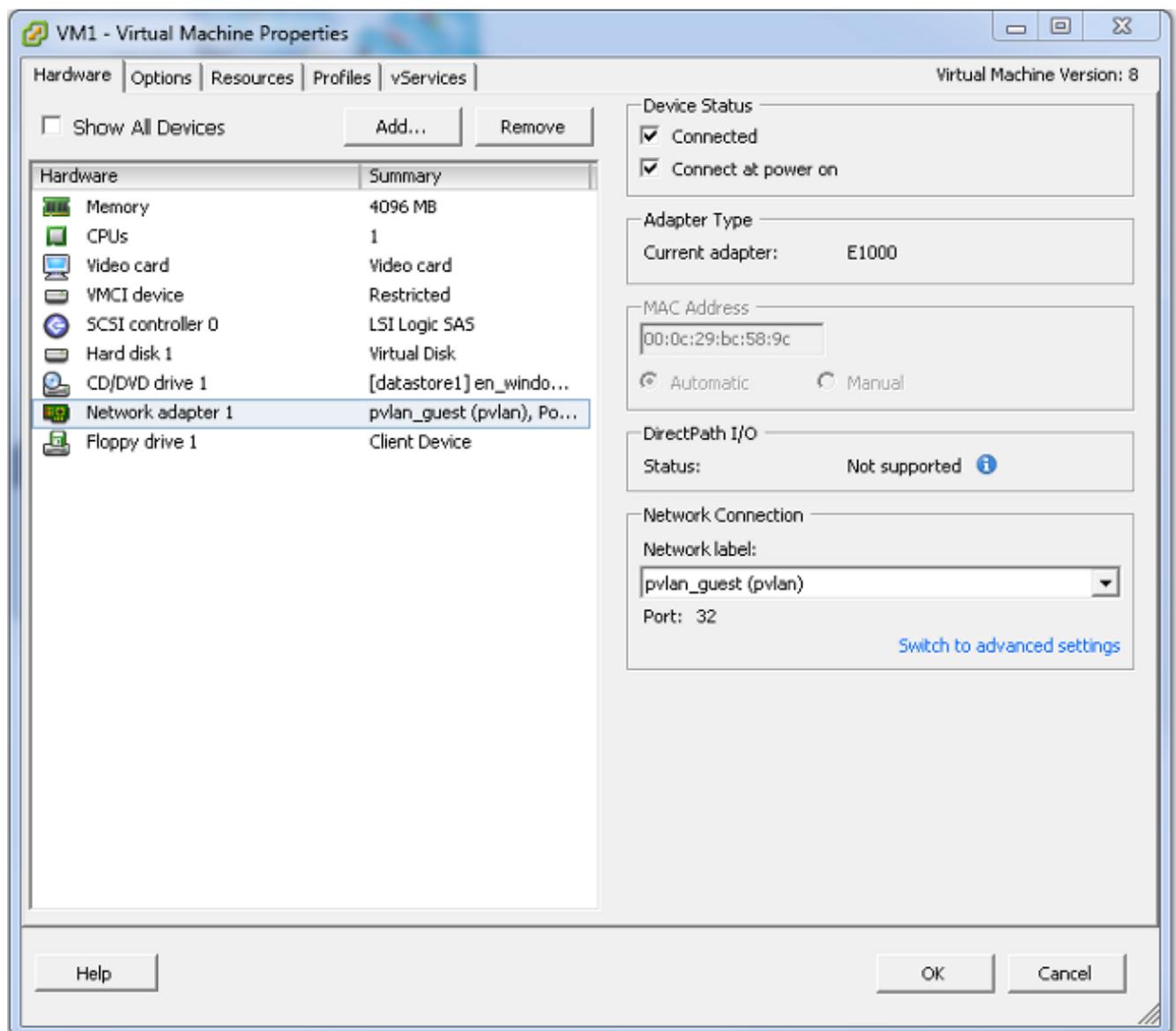
```

4. Fügen Sie im vCenter dem PVLAN-Uplink die entsprechende vNIC hinzu. Dies ist die vNIC, zu der Sie in den UCS-Einstellungen unter der Konfiguration das isolierte VLAN hinzugefügt haben.

<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. Fügen Sie das virtuelle System der richtigen Portgruppe hinzu:

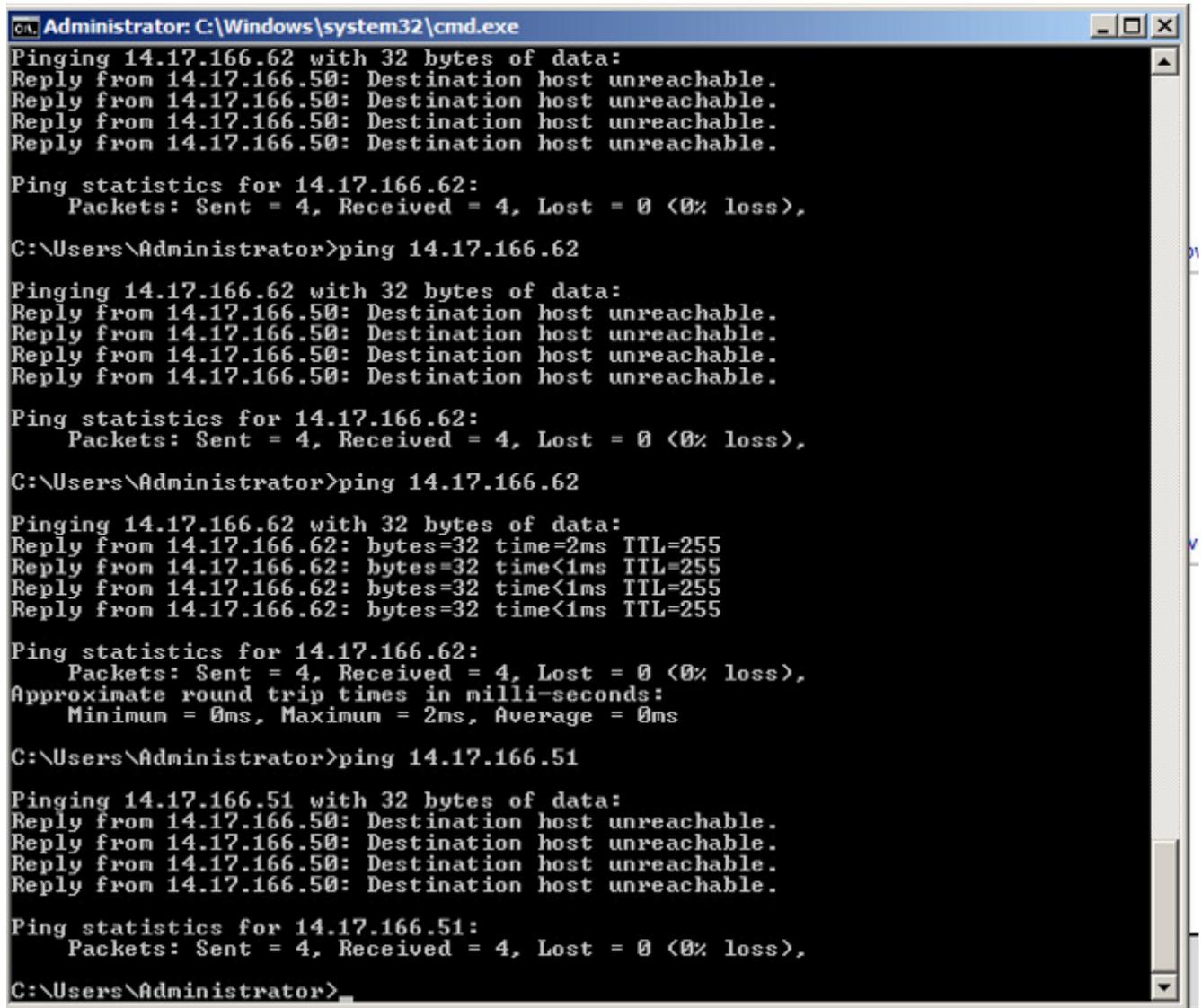
Klicken Sie auf der Registerkarte Hardware auf **Netzwerkadapter 1**. Wählen Sie unter Netzwerkverbindung **pvlan\_guest (pvlan)** für das Netzwerklabel aus:



## Fehlerbehebung

Dieses Verfahren beschreibt, wie die Konfiguration getestet wird.

1. Führen Sie Pings zu anderen Systemen aus, die in der Port-Gruppe konfiguriert wurden, sowie zum Router oder anderen Gerät am Promiscuous-Port. Pings an das Gerät, das den Promiscuous-Port überschritten hat, sollten funktionieren, während Pings an andere Geräte im isolierten VLAN fehlschlagen sollten.



```
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.

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.

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.

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

C:\Users\Administrator>
```

2. Auf dem N1K sind die VMs im primären VLAN aufgeführt. Dies liegt daran, dass Sie sich in PVLAN-Host-Ports befinden, die dem PVLAN zugeordnet sind. Achten Sie darauf, dass Sie das PVLAN nicht als natives PVLAN im UCS-System festlegen, da die virtuellen Systeme gelernt werden. Beachten Sie außerdem, dass Sie das Upstream-Gerät vom Port-Channel erlernen und dass das Upstream-Gerät auch im primären VLAN erfasst wird. Dies muss bei dieser Methode erlernt werden. Daher ist das primäre VLAN auf dem PVLAN-Uplink das native VLAN.

In diesem Screenshot sind die beiden Geräte auf Veth3 und Veth 4 die VMs. Das Gerät auf Po1 ist der Upstream-Router, der über den Promiscuous-Port verläuft.

```

pvlan# show mac address-table
VLAN      MAC Address      Type      Age      Port
-----+-----+-----+-----+-----+-----+-----
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. Auf dem UCS-System sollten Sie alle MACs für diese Kommunikation im isolierten VLAN erlernen. Hier sollten Sie die Upstream-Dateien nicht sehen:

```

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. Auf dem Nexus 5K befinden sich die beiden VMs im isolierten VLAN, während sich das Upstream-Gerät im primären VLAN befindet:

```

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. Auf dem 4900-Switch, wo sich der Promiscuous-Port befindet, befindet sich alles im primären VLAN:

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

## Isolated-PVLAN auf N1K mit Promiscuous-Port im N1K-Uplink-Portprofil

In dieser Konfiguration enthalten Sie PVLAN-Datenverkehr zum N1K, wobei nur das primäre VLAN für den Upstream verwendet wird.

### Konfiguration in UCS

In diesem Verfahren wird beschrieben, wie das primäre VLAN der vNIC hinzugefügt wird. Eine PVLAN-Konfiguration ist nicht erforderlich, da Sie nur das primäre VLAN benötigen.

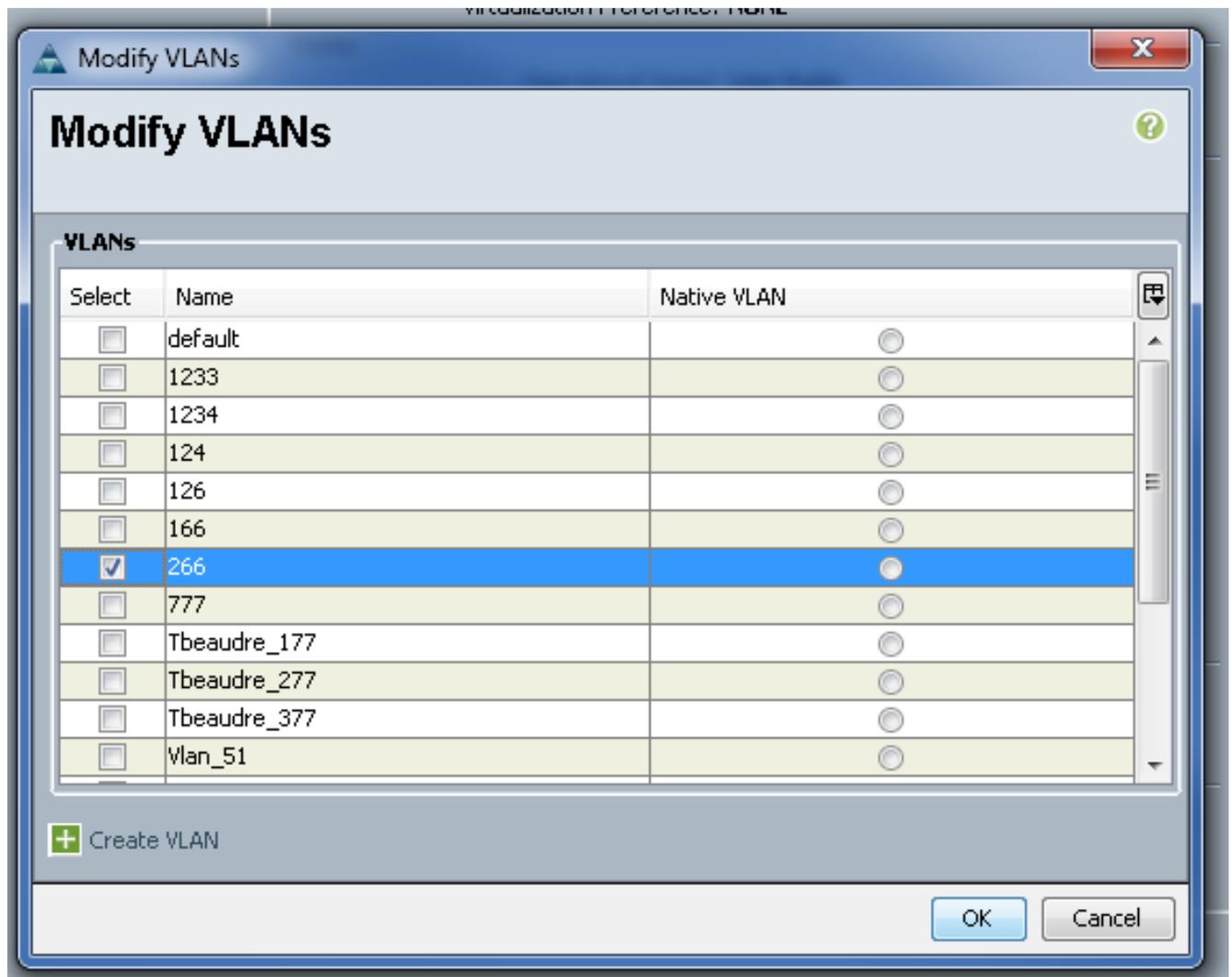
**Hinweis:** In diesem Beispiel wird 266 als primäres und 166 als isoliertes Element verwendet. Die VLAN-IDs werden vom Standort bestimmt.

1. Beachten Sie, dass der Freigabetyp **None** ist.

The screenshot shows the UCS Management GUI for VLAN 266. The 'Properties' section is expanded, showing the following configuration:

- 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. Aktivieren Sie das Kontrollkästchen **Select (Auswählen)** für VLAN 266, um das primäre VLAN der vNIC hinzuzufügen. Legen Sie ihn nicht als nativ fest.



## Konfiguration von Upstream-Geräten

Diese Verfahren beschreiben, wie die Upstream-Geräte konfiguriert werden. In diesem Fall benötigen die Upstream-Switches nur Trunk-Ports und müssen nur das VLAN 266 Trunk-Trunks durchführen, da es das einzige VLAN ist, das die Upstream-Switches sehen.

Geben Sie auf dem Nexus 5K diese Befehle ein, und überprüfen Sie die Uplink-Konfiguration:

1. Fügen Sie das VLAN als primäres VLAN hinzu:

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

2. Stellen Sie sicher, dass alle Uplinks so konfiguriert sind, dass sie die VLANs trunk:

Schnittstelle Ethernet1/1 Beschreibung Verbindung zu 4900 Trunk im Switch-Port-Modus Geschwindigkeit 1000 Schnittstelle Ethernet1/3 Beschreibung Verbindung mit FIB-Port 5 Trunk im Switch-Port-Modus Geschwindigkeit 1000 Schnittstelle Ethernet1/4 Beschreibung Verbindung mit FIA-Port 5 Trunk im Switch-Port-Modus Geschwindigkeit 1000

Gehen Sie auf dem Switch 4900 wie folgt vor:

1. Erstellen Sie die als primäres VLANs auf dem N1K.
2. Trunk aller Schnittstellen zum und vom 4900-Switch, sodass das VLAN übergeben wird

Erstellen Sie auf dem Upstream-Router nur eine Subschnittstelle für das VLAN 266. Auf dieser Ebene hängen die Anforderungen von der verwendeten Netzwerkkonfiguration ab.

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

## Konfiguration von N1K

Dieses Verfahren beschreibt die Konfiguration des N1K.

1. Erstellen und Zuordnen der VLANs:

```
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. Erstellen Sie ein Uplink-Port-Profil für den PVLAN-Datenverkehr mit dem Promiscuous-Port.  
Hinweis:

```
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. Erstellen Sie die Port-Gruppe für das isolierte VLAN. Erstellen Sie einen PVLAN-Host-Port mit der Hostzuordnung für die primären und isolierten VLANs:

```
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
```

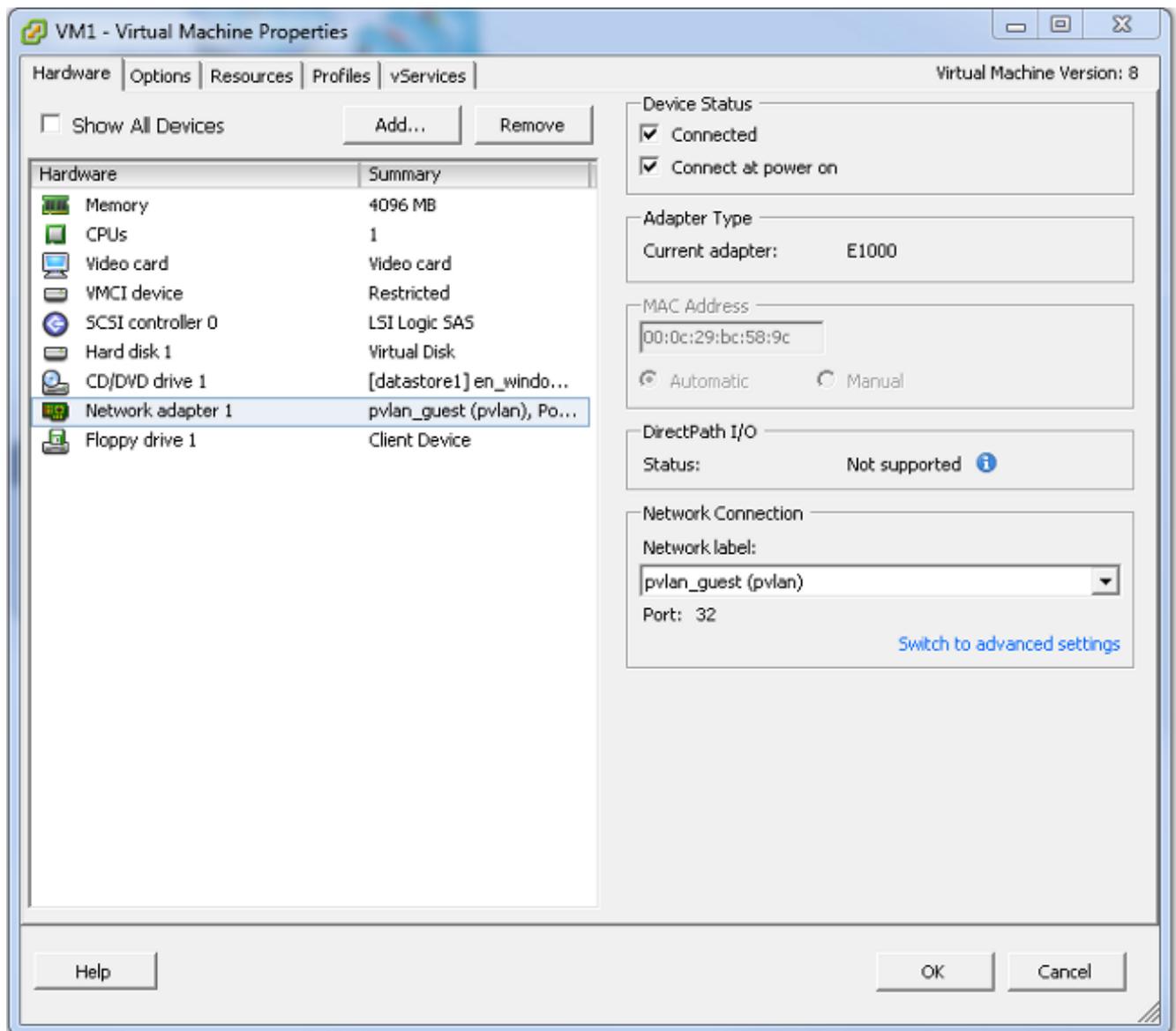
4. Fügen Sie im vCenter dem PVLAN-Uplink die entsprechende vNIC hinzu. Dies ist die vNIC, zu der Sie in den UCS-Einstellungen unter der Konfiguration das isolierte VLAN hinzugefügt haben.

<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. Fügen Sie die VM der richtigen Port-Gruppe hinzu.

Klicken Sie auf der Registerkarte Hardware auf **Netzwerkadapter 1**. Wählen Sie **pvlan\_guest**

(pvlan) für das Netzwerklabel unter Netzwerkverbindung aus.



## Fehlerbehebung

Dieses Verfahren beschreibt, wie die Konfiguration getestet wird.

1. Führen Sie Pings zu anderen Systemen aus, die in der Port-Gruppe konfiguriert wurden, sowie zum Router oder anderen Gerät am Promiscuous-Port. Pings an das Gerät, das den Promiscuous-Port überschritten hat, sollten funktionieren, während Pings an andere Geräte im isolierten VLAN fehlschlagen sollten.

```

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.

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

```

2. Auf dem N1K sind die VMs im primären VLAN aufgeführt. Dies liegt daran, dass Sie sich in PVLAN-Host-Ports befinden, die dem PVLAN zugeordnet sind. Beachten Sie außerdem, dass Sie das Upstream-Gerät vom Port-Channel erlernen und dass das Upstream-Gerät auch im primären VLAN erfasst wird.

In diesem Screenshot sind die beiden Geräte auf Veth3 und Veth 4 die VMs. Das Gerät auf Po1 ist das Upstream-Gerät, das den Promiscuous-Port hinter sich hat.

```

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. Auf dem UCS-System sollten Sie alle MACs für diese Kommunikation im primären VLAN erlernen, das Sie auf dem N1K verwenden. Hier sollten Sie die Upstream-Informationen nicht kennen:

```
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. Auf dem Nexus 5K befinden sich alle MACs im von Ihnen ausgewählten primären VLAN:

```
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. Auf dem 4900-Switch befindet sich alles im von Ihnen ausgewählten primären VLAN:

```
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#
```

## Community PVLAN auf N1K mit Promiscuous Port im N1K Uplink-Portprofil

Dies ist die einzige unterstützte Konfiguration für Community-VLAN mit dem UCS.

Diese Konfiguration entspricht der Konfiguration im [isolierten PVLAN auf N1K mit Promiscuous Port im N1K Uplink-Portprofil](#)-Abschnitt. Der einzige Unterschied zwischen Community und Isolated ist die Konfiguration des PVLANS.

Um das N1K zu konfigurieren, müssen Sie die VLANs wie beim Nexus 5K erstellen und zuordnen:

```
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
```

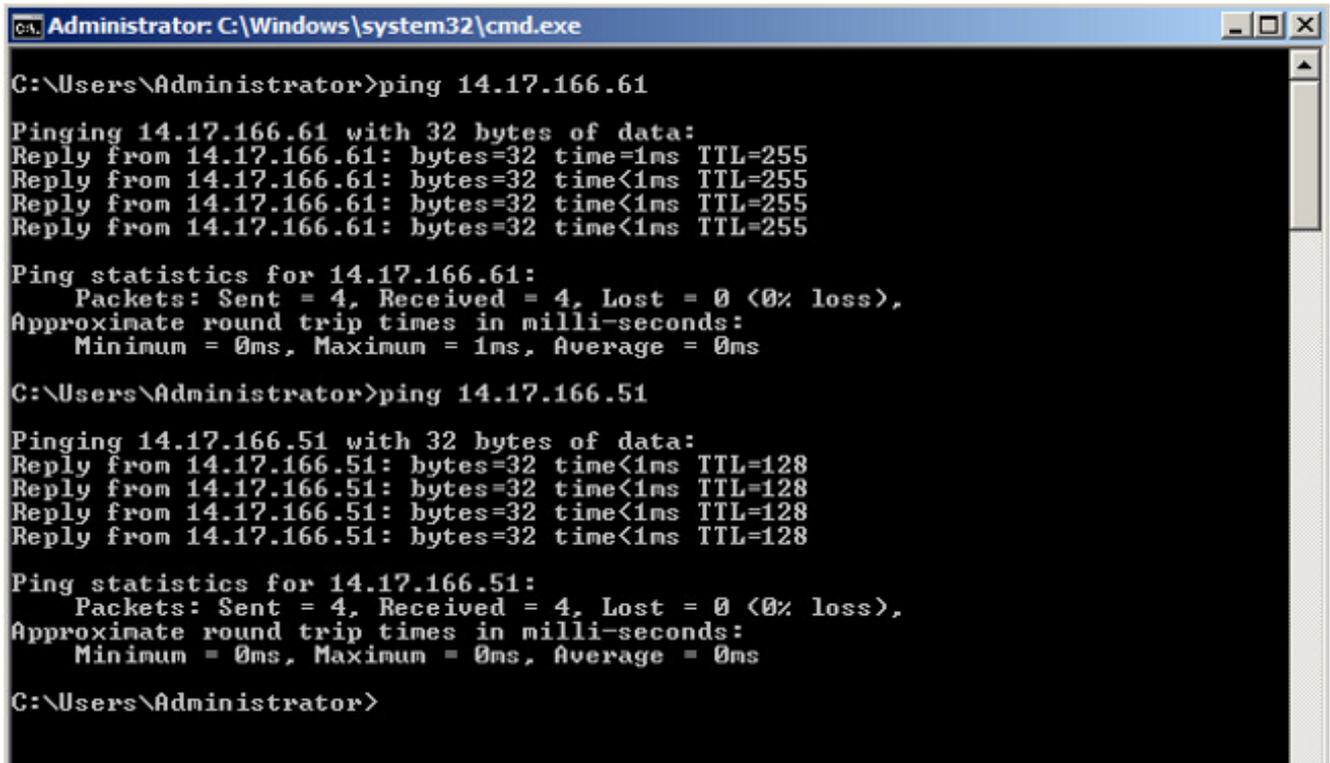
Alle anderen Konfigurationen sind identisch mit dem isolierten PVLAN auf dem N1K-Modul mit Promiscuous-Port im N1K-Uplink-Portprofil.

Nach der Konfiguration können Sie mit allen VMs kommunizieren, die mit dem für Ihr PVLAN verwendeten vEthernet-Portprofil verbunden sind.

## Fehlerbehebung

Dieses Verfahren beschreibt, wie die Konfiguration getestet wird.

1. Führen Sie Pings zu anderen Systemen aus, die in der Port-Gruppe konfiguriert wurden, sowie zum Router oder anderen Gerät am Promiscuous-Port. Pings über den Promiscuous-Port und zu anderen Systemen in der Community sollten funktionieren.



```
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

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. Alle anderen Fehlerbehebungen sind mit dem [isolierten PVLAN](#) identisch.

## Isolated PVLAN und Community PVLAN auf VMware DVS Promiscuous Port auf dem DVS

Aufgrund der Konfigurationsprobleme sowohl auf dem DVS als auch auf dem UCS-System werden PVLANS mit DVS und UCS vor Version 2.2(2c) nicht unterstützt.

## Überprüfen

Für diese Konfigurationen sind derzeit keine Überprüfungsverfahren verfügbar.

## Fehlerbehebung

Die vorherigen Abschnitte enthalten Informationen, die Sie zur Fehlerbehebung in Ihren Konfigurationen verwenden können.

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des Befehls show** anzuzeigen.