

Private VLAN und UCS mit VMware DVS oder Cisco Nexus 1000v konfigurieren

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[UCS mit VMware DVS](#)

[VMware-DVS](#)

[Upstream-Nexus 5000-Switch](#)

[Verhaltensänderungen mit UCS Version 3.1\(3\)](#)

[Upstream-Switch der Serie 4900](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Konfiguration mit Nexus 1000v mit Promiscuous Port im Upstream \(Nexus 500\)](#)

[UCS-Konfiguration](#)

[N1k-Konfiguration](#)

[Konfiguration mit Nexus 1000v mit Promiscuous Port im N1K Uplink-Portprofil](#)

[UCS-Konfiguration](#)

[Konfiguration von Upstream-Geräten](#)

[Konfiguration von N1K](#)

Einführung

Dieses Dokument beschreibt die private VLAN-Unterstützung (PVLAN) für das Cisco Unified Computing System (UCS) ab Version 2.2(2c).

Vorsicht: Die UCS-Firmware Version 3.1(3a) beginnt ab einer Änderung des Verhaltens, wie im Abschnitt **Verhaltensänderung mit UCS Version 3.1(3) und höher** beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

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

- 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

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:

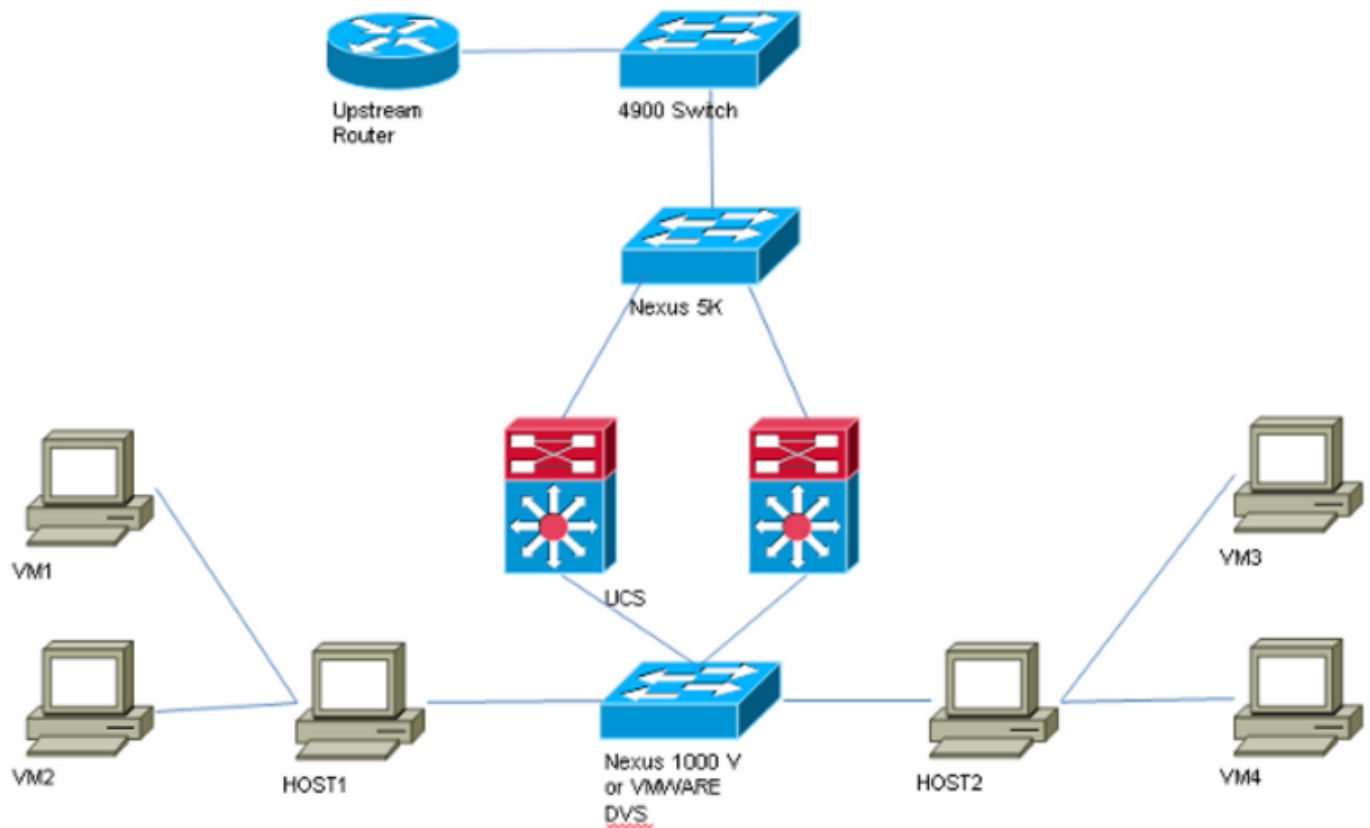
- Ein Promiscuous-Port kommuniziert mit allen anderen PVLAN-Ports und ist der Port, der für die Kommunikation mit Geräten außerhalb des PVLAN verwendet wird.
- Ein isolierter Port verfügt über eine vollständige L2-Trennung (einschließlich Broadcasts) von anderen Ports innerhalb desselben PVLAN, mit Ausnahme 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.

Konfigurieren

Netzwerkdiagramm

Mit Nexus 1000v oder VMware DVS



Hinweis: In diesem Beispiel wird VLAN 1750 als primäres, 1785 als isoliertes und 1786 als Community-VLAN verwendet.

UCS mit VMware DVS

1. Um das primäre VLAN zu erstellen, klicken Sie auf das Optionsfeld **Primär** als Freigabebetyp, und geben Sie eine **VLAN-ID** von 1750 ein, wie im Bild gezeigt.

Properties

Name: **1750** VLAN ID:
 Native VLAN: **No** Fabric ID: **Dual**
 Network Type: **Lan** If Type: **Virtual**
 Locale: **External** Transport Type: **Ether**
 Owner: **Local**

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

Sharing Type: None Primary Isolated Community

Secondary VLANs

Filter | Export | Print

Name	ID	Type	Transport	Native	VLAN Sharing	Multicast Poli	
1785	1785	Lan	Ether	No	Isolated		^
1786	1786	Lan	Ether	No	Community		

< ||| >

2. Erstellen Sie **isolierte** und **Community**-VLANs entsprechend, wie in den Bildern gezeigt. Keines dieser Elemente muss ein natives VLAN sein.

Properties

Name: **1785** VLAN ID:
 Native VLAN: **No** Fabric ID: **Dual**
 Network Type: **Lan** If Type: **Virtual**
 Locale: **External** Transport Type: **Ether**
 Owner: **Local**

Sharing Type: None Primary Isolated Community Primary VLAN:

Primary VLAN Properties

Name: **1750** VLAN ID: **1750**
 Native VLAN: **No** Fabric ID: **Dual**
 Network Type: **Lan** If Type: **Virtual**
 Locale: **External** Transport Type: **Ether**
 Owner: **Local**

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

Properties

Name: **1786** VLAN ID: **1786**
 Native VLAN: **No** Fabric ID: **Dual**
 Network Type: **Lan** If Type: **Virtual**
 Locale: **External** Transport Type: **Ether**
 Owner: **Local**

Sharing Type: None Primary Isolated Community Primary VLAN: **VLAN 1750 (1750)**

Primary VLAN Properties

Name: **1750** VLAN ID: **1750**
 Native VLAN: **No** Fabric ID: **Dual**
 Network Type: **Lan** If Type: **Virtual**
 Locale: **External** Transport Type: **Ether**
 Owner: **Local**

Multicast Policy Name: **<not set>**
 Multicast Policy Instance: [org-root/mc-policy-default](#)

3. Die virtuelle Netzwerkschnittstellenkarte (vNIC) im Serviceprofil überträgt reguläre VLANs sowie PVLANS, wie im Bild dargestellt.

VLAN	VLAN ID	Oper VLAN	Native VLAN
1750	1750	fabric/lan/net-1750	<input type="radio"/>
1785	1785	fabric/lan/net-1785	<input type="radio"/>
1786	1786	fabric/lan/net-1786	<input type="radio"/>
default	1	fabric/lan/net-default	<input type="radio"/>
qam-121	121	fabric/lan/net-qam-121	<input type="radio"/>
qam-221	221	fabric/lan/net-qam-221	<input type="radio"/>

4. Uplink-Port-Channel auf dem UCS überträgt reguläre VLANs sowie PVLANS:

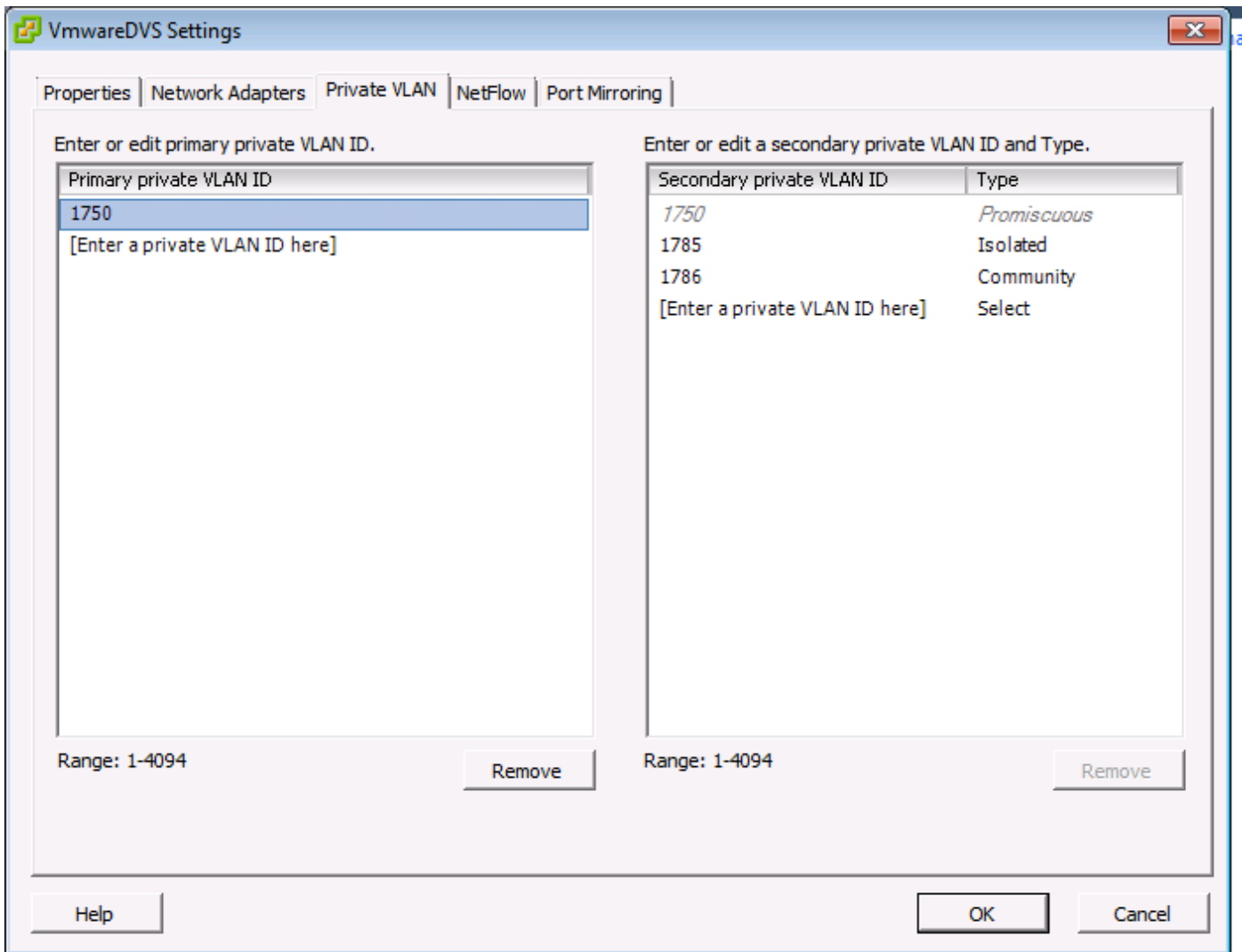
```
interface port-channel1
description U: Uplink
switchport mode trunk
pinning border
switchport trunk allowed vlan 1,121,221,321,1750,1785-1786
speed 10000
```

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

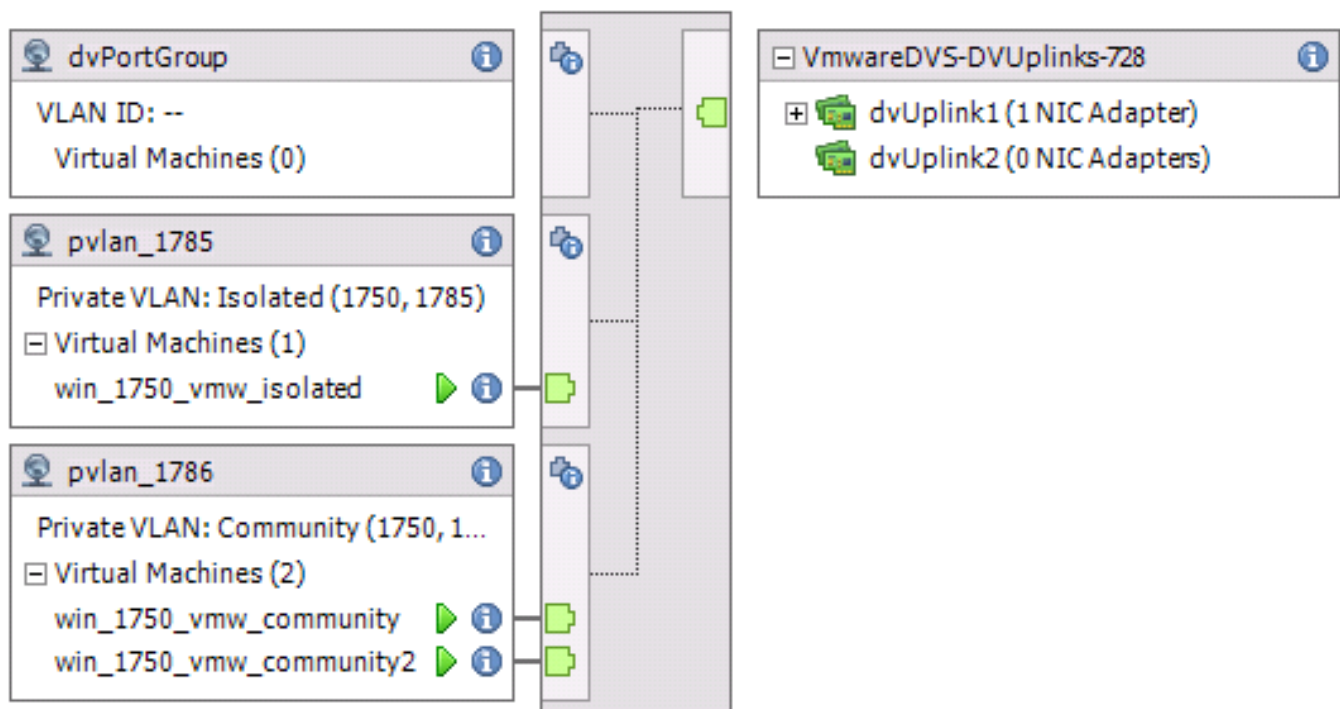
```
F240-01-09-UCS4-A (nxos) # show vlan private-vlan
Primary Secondary Type Ports
```

```
-----
1750    1785        isolated
1750    1786        community
```

VMware-DVS



VMwareDVS i



Upstream-Nexus 5000-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
```

Verhaltensänderungen mit UCS Version 3.1(3)

Vor der UCS-Version 3.1(3) kann eine VM in einem Community-VLAN mit einer VM im primären VLAN auf VMware-DVS kommunizieren, wobei sich die primäre VLAN-VM im UCS befindet. Dieses Verhalten war falsch, da die primäre VM immer Northbound oder außerhalb des UCS sein muss. Dieses Verhalten wird mithilfe der Defekt-ID [CSCvh87378](#) dokumentiert. .

Ab UCS Version 2.2(2) konnte das Community-VLAN aufgrund eines Codefehlers mit dem primären VLAN kommunizieren, das sich hinter dem FI befand. Isolated konnte jedoch niemals mit dem primären hinter dem FI kommunizieren. Beide (isolierten und Community-VMs) können weiterhin mit den primären Systemen außerhalb des FI kommunizieren.

Ab 3.1(3) ermöglicht dieser Defekt der Community die Kommunikation mit dem primären hinter dem FI, wurde beseitigt und Community VMs können daher nicht mit einem VM im primären VLAN kommunizieren, das innerhalb des UCS ansässig ist.

Um dieses Problem zu beheben, muss die primäre VM entweder (Northbound) außerhalb des UCS verschoben werden. Wenn dies nicht möglich ist, muss die primäre VM in ein anderes VLAN verschoben werden, das ein reguläres VLAN und kein privates VLAN ist.

Beispielsweise konnte ein VM im Community-VLAN 1786 vor Firmware 3.1(3) mit einem VM im primären VLAN 1750, das sich innerhalb des UCS befindet, kommunizieren. Allerdings würde diese Kommunikation in der Firmware 3.1(3) und später brechen, wie im Image gezeigt.

HINWEIS:

[CSCvh87378](#) wurde in Version 3.2(3l) und Version 4.0.4e und höher adressiert, sodass das primäre VLAN für das UCS verfügbar sein kann. Beachten Sie jedoch, dass isolierte VLANs innerhalb des UCS nicht mit primärem VLAN innerhalb des UCS kommunizieren können. Nur Community-VLAN und primäre VLANs können miteinander kommunizieren, wenn beide hinter dem UCS liegen.

```
F240-01-09-UCS4-A(nxos)# show mac address-table | inc 76d7
* 1786      0050.568e.76d7      dynamic      440          F          F          Veth3148
F240-01-09-UCS4-A(nxos)#
```

```

VLAN      MAC Address      Type      age      Secure NTFY      Ports/SWID.SSID.LID
-----+-----+-----+-----+-----+-----
* 1750      0050.568e.476f      dynamic      0          F          F          Veth3240
F240-01-09-UCS4-B(nxos)#
```

Upstream-Switch der Serie 4900

Hinweis: In diesem Beispiel ist 4900 eine L3-Schnittstelle für ein externes Netzwerk. Wenn Ihre Topologie für L3 anders ist, nehmen Sie bitte entsprechende Änderungen vor.

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 von VLAN 1785 und 1786 in diesem Fall im VLAN 1750 angezeigt.

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

Erstellen Sie auf dem Upstream-Router nur eine Subschnittstelle für das VLAN 1750. Auf dieser Ebene hängen die Anforderungen von der verwendeten Netzwerkkonfiguration ab:

```
interface GigabitEthernet0/1.1
encapsulation dot1Q 1750
IP address 10.10.175.254/24
```

Überprüfen

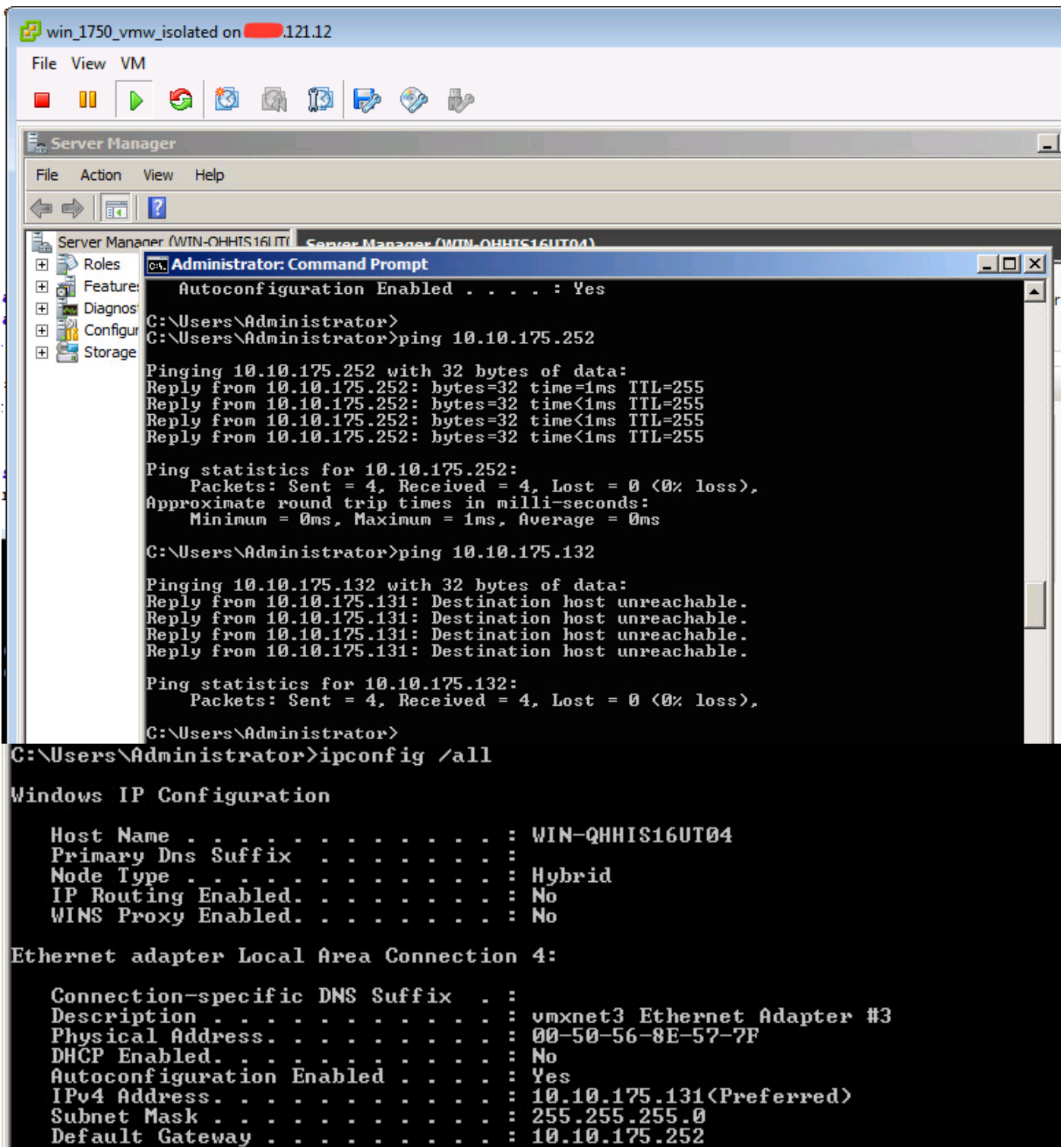
Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Dieses Verfahren beschreibt, wie die Konfiguration für VMware DVS mit PVLAN getestet wird.

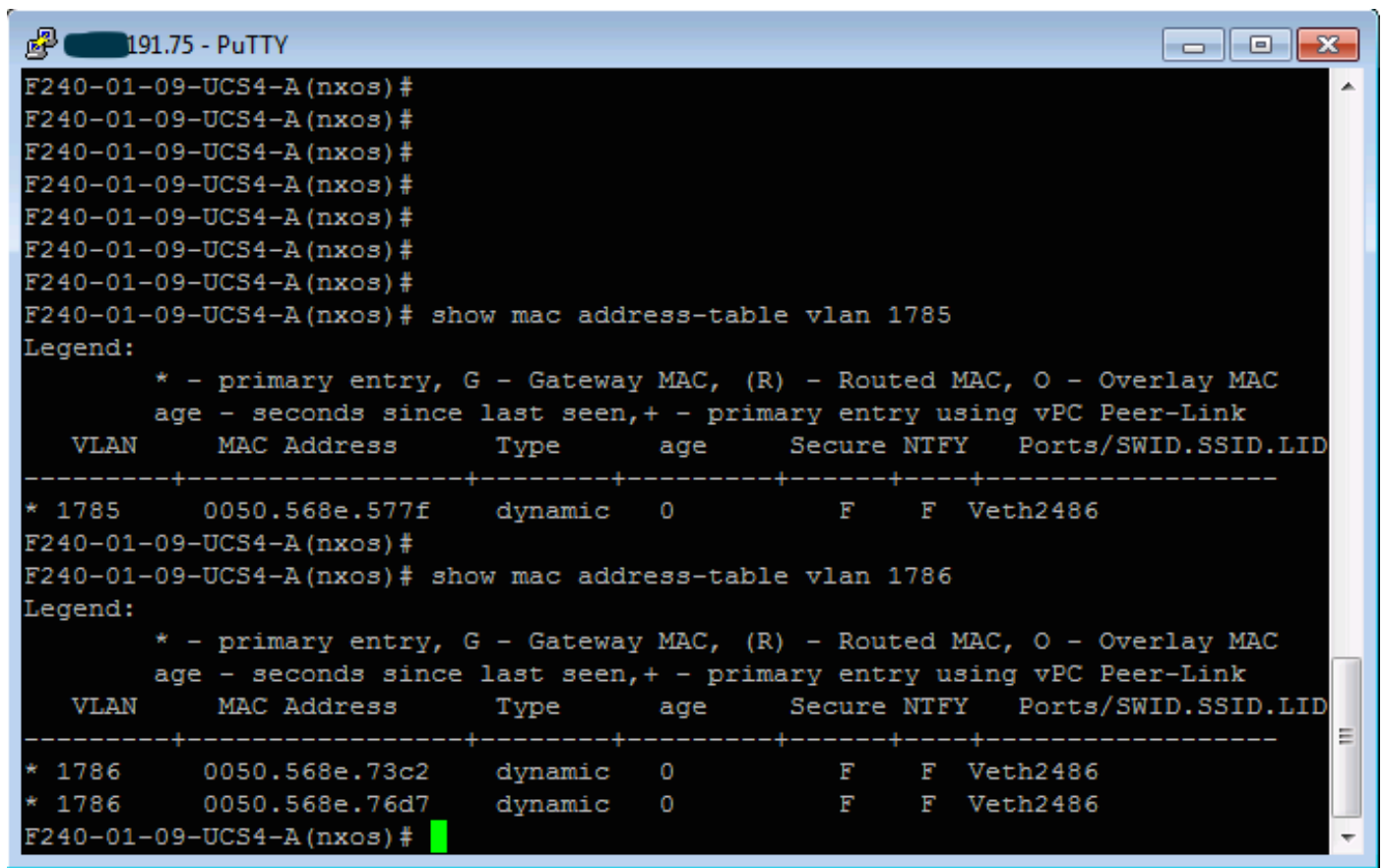
1. Führen Sie Pings zu anderen Systemen aus, die in der Port-Gruppe konfiguriert wurden, sowie zum Router oder anderen Gerät am Promiscuous-Port. Pings an das Gerät, das den Promiscuous-Port überschritten hat, müssen funktionieren, während Pings an andere Geräte im isolierten VLAN fehlschlagen müssen,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



Überprüfen Sie die MAC-Adresstabellen, um zu sehen, wo Ihre MAC-Adresse erfasst wird. Auf allen Switches muss sich die MAC-Adresse im isolierten VLAN befinden, außer auf dem Switch mit dem Promiscuous-Port. Auf dem Promiscuous-Switch muss sich die MAC-Adresse im

primären VLAN befinden.

2. UCS wie im Bild gezeigt.



```
191.75 - PuTTY
F240-01-09-UCS4-A(nxos)#
F240-01-09-UCS4-A(nxos)#
F240-01-09-UCS4-A(nxos)#
F240-01-09-UCS4-A(nxos)#
F240-01-09-UCS4-A(nxos)#
F240-01-09-UCS4-A(nxos)#
F240-01-09-UCS4-A(nxos)#
F240-01-09-UCS4-A(nxos)# show mac address-table vlan 1785
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/SWID.SSID.LID
-----+-----+-----+-----+-----+-----
* 1785     0050.568e.577f   dynamic   0        F      F      Veth2486
F240-01-09-UCS4-A(nxos)#
F240-01-09-UCS4-A(nxos)# show mac address-table vlan 1786
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/SWID.SSID.LID
-----+-----+-----+-----+-----+-----
* 1786     0050.568e.73c2   dynamic   0        F      F      Veth2486
* 1786     0050.568e.76d7   dynamic   0        F      F      Veth2486
F240-01-09-UCS4-A(nxos)#
```

3. Aktivieren Sie auf Upstream n5k, um dieselbe MAC-Adresse zu erhalten. Die Ausgabe, die der früheren Ausgabe ähnelt, muss auf Nexus 500 vorliegen und im Bild dargestellt werden.

```
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#
```

Konfiguration mit Nexus 1000v mit Promiscuous Port im Upstream (Nexus 500)

UCS-Konfiguration

Die UCS-Konfiguration (die auch die vNIC-Konfiguration für Serviceprofile enthält) bleibt mit der VMware DVS-Konfiguration identisch.

N1k-Konfiguration

```
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
```

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, müssen funktionieren, während Pings an andere Geräte im isolierten VLAN fehlschlagen müssen, wie im vorherigen Abschnitt und in den Images gezeigt.

