

Configurar VLAN privada e UCS com VMware DVS ou Cisco Nexus 1000v

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[UCS com VMware DVS](#)

[VMware DVS](#)

[Switch N5k de upstream](#)

[Mudança de comportamento com o UCS versão 3.1\(3\)](#)

[Switch Upstream 4900](#)

[Verificar](#)

[Troubleshoot](#)

[Configuração com Nexus 1000v com porta promissora no upstream N5k](#)

[Configuração do UCS](#)

[Configuração N1k](#)

[Configuração com Nexus 1000v com porta confiável no perfil de porta de uplink N1K](#)

[Configuração do UCS](#)

[Configuração de dispositivos upstream](#)

[Configuração do N1K](#)

Introduction

Este documento descreve o suporte de VLAN privada (PVLAN) para o Cisco Unified Computing System (UCS) na versão 2.2(2c) e posterior.

Caution: Há uma alteração no comportamento a partir do firmware UCS versão 3.1(3a) conforme descrito na seção **Alteração do comportamento com UCS versão 3.1(3) e posterior**.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- UCS

- Cisco Nexus 1000V (N1K) ou VMware Distributed Virtual Switch (DVS)
- VMware
- Comutação da camada 2 (L2)

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

Uma VLAN privada é uma VLAN configurada para isolamento L2 de outras portas dentro da mesma VLAN privada. As portas que pertencem a uma PVLAN estão associadas a um conjunto comum de VLANs de suporte, que são usadas para criar a estrutura da PVLAN.

Há três tipos de portas PVLAN:

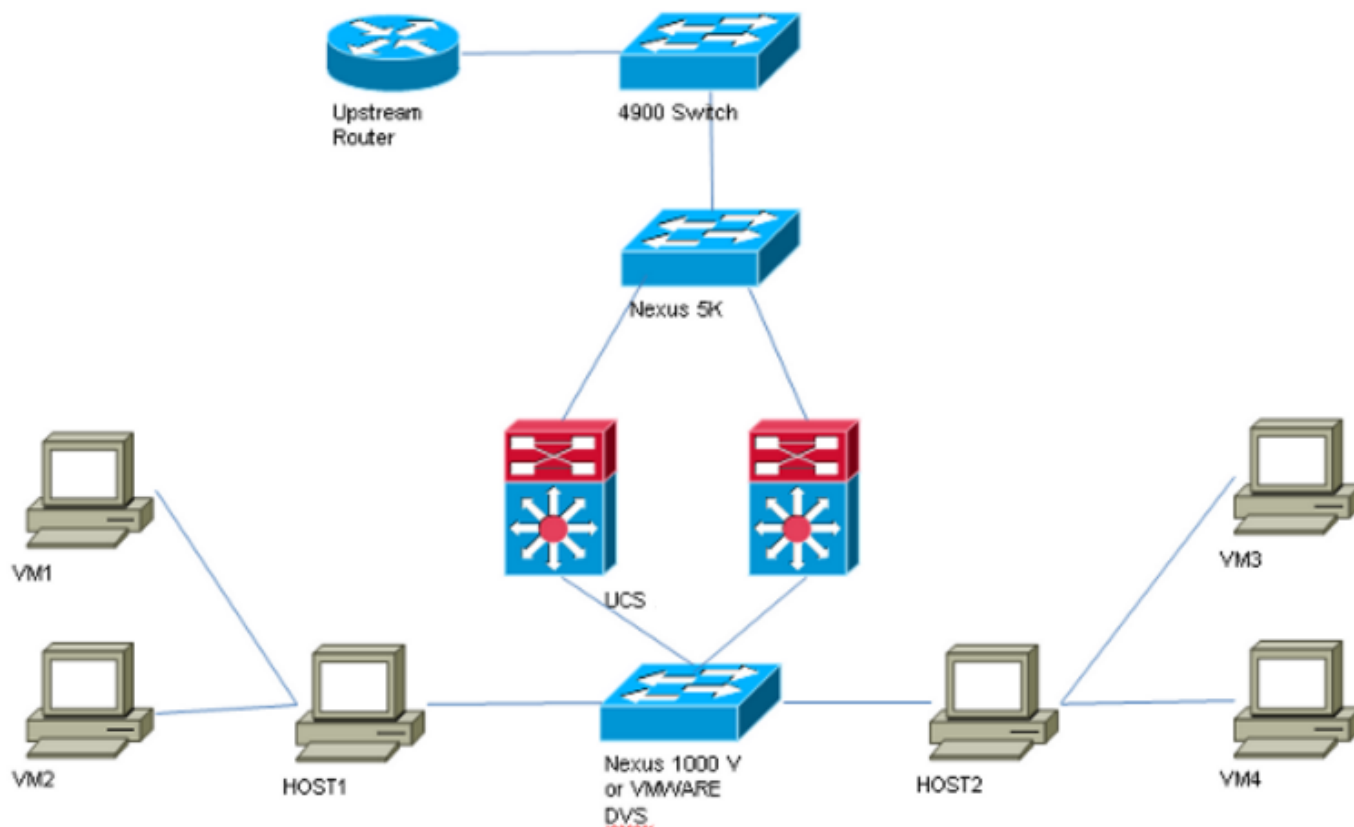
- Uma porta promíscua se comunica com todas as outras portas PVLAN e é a porta usada para se comunicar com dispositivos fora da PVLAN.
- Uma porta isolada tem separação L2 completa (que inclui broadcasts) de outras portas dentro do mesmo PVLAN, com exceção da porta promíscua.
- Uma porta da comunidade pode se comunicar com outras portas no mesmo PVLAN, bem como com a porta promíscua. As portas da comunidade são isoladas em L2 das portas de outras comunidades ou portas PVLAN isoladas. Os broadcasts só são propagados para outras portas na comunidade e na porta promíscua.

Consulte [RFC 5517, VLANs privadas da Cisco Systems: Segurança escalável em um ambiente multicliente](#) para entender a teoria, a operação e os conceitos de PVLANS.

Configurar

Diagrama de Rede

Com Nexus 1000v ou VMware DVS



Note: Este exemplo usa a VLAN 1750 como primária, 1785 como isolada e 1786 como VLAN de comunidade.

UCS com VMware DVS

1. Para criar a VLAN principal, clique no botão de opção **Primary** como Sharing Type (Tipo de compartilhamento) e insira um **ID de VLAN** de 1750 como mostrado na imagem.

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. Crie VLANs **isoladas** e **comunitárias** de acordo com as imagens. Nenhum desses deve ser uma VLAN nativa.

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

3. A Virtual Network Interface Card (vNIC) no perfil de serviço transporta VLANs regulares e PVLANS, como visto na imagem.

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. O uplink port-channel no UCS transporta VLANs regulares, bem como PVLANS:

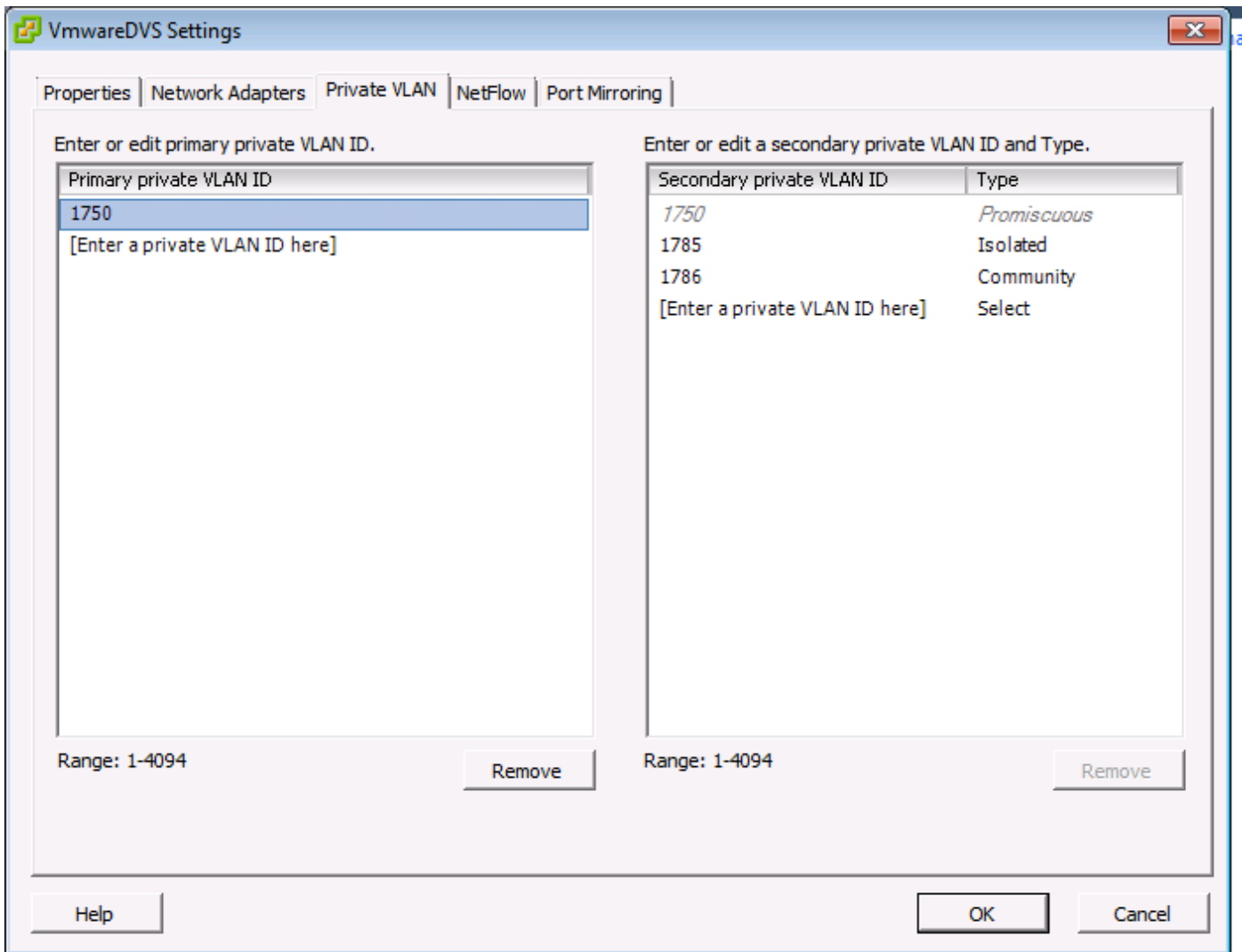
```
interface port-channel1
description U: Uplink
switchport mode trunk
pinning border
switchport trunk allowed vlan 1,121,221,321,1750,1785-1786
speed 10000
```

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

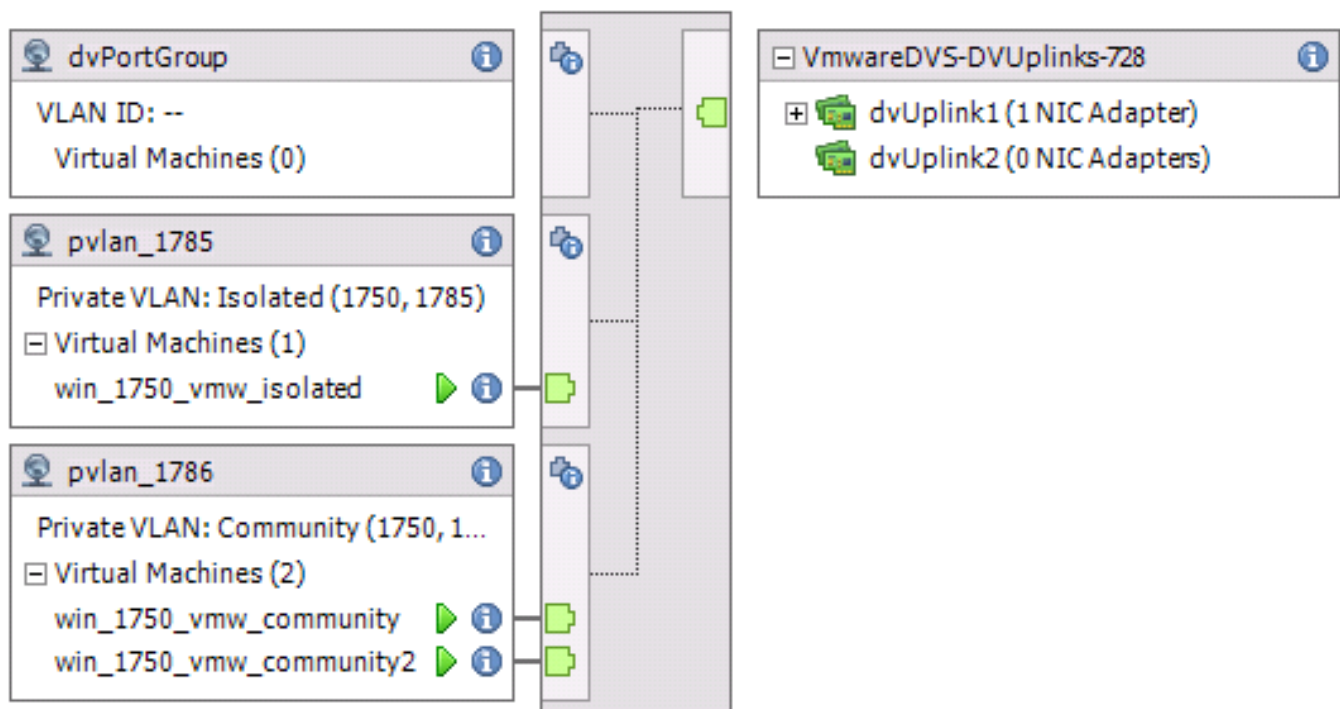
```
F240-01-09-UCS4-A(nxos)# show vlan private-vlan
Primary Secondary Type Ports
```

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

VMware DVS



VMwareDVS i



Switch N5k de upstream

```
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
```

Mudança de comportamento com o UCS versão 3.1(3)

Antes do UCS versão 3.1(3), você poderia ter uma VM na VLAN de comunidade se comunicando com uma VM na VLAN primária no VMware DVS, onde a VM da VLAN principal reside no UCS. Esse comportamento estava incorreto, pois a VM principal deve sempre ser northbound ou externa ao UCS. Esse comportamento é documentado por ID de defeito [CSCvh87378](#).

A partir da versão 2.2(2) do UCS, devido a um defeito no código, a VLAN da comunidade pôde se comunicar com a VLAN principal presente por trás do FI. Mas Isolado nunca poderia se comunicar com o principal por trás do FI. As VMs (isoladas e de comunidade) ainda podem se comunicar com o principal fora do FI.

A partir do 3.1(3), esse defeito permite que a comunidade se comunique com o principal por trás do FI, foi retificado e, portanto, as VMs da comunidade não poderão se comunicar com uma VM na VLAN principal que reside no UCS.

Para resolver essa situação, a VM principal precisaria ser movida (ascendente) para fora do UCS. Se essa não for uma opção, a VM principal precisará ser movida para outra VLAN que seja uma VLAN normal e não uma VLAN privada.

Por exemplo, antes do firmware 3.1(3), uma VM na VLAN 1786 da comunidade poderia se comunicar com uma VM na VLAN 1750 principal que reside no UCS, entretanto, essa comunicação quebraria o firmware 3.1(3) e posterior, como mostrado na imagem.

NOTE:

[O CSCvh87378](#) foi tratado em 3.2(3l) e 4.0.4e e mais recente para que possamos ter a Vlan primária atrás do UCS. No entanto, observe que a vlan isolada dentro do UCS não poderá falar com a vlan primária dentro do UCS. Somente a vlan da comunidade e a vlan primária podem se comunicar quando ambas estão por trás do UCS.

```
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)#
```

Switch Upstream 4900

Note: Neste exemplo, 4900 é a interface L3 para a rede externa. Se a topologia para L3 for diferente, faça as alterações de acordo

No switch 4900, siga estes passos e configure a porta promíscua. A PVLAN termina na porta promíscua.

1. Ative o recurso PVLAN, se necessário.
2. Crie e associe as VLANs como feito no Nexus 5K.
3. Crie a porta promíscua na porta de saída do switch 4900. A partir desse ponto, os pacotes da VLAN 1785 e 1786 são vistos na VLAN 1750 nesse caso.

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

No roteador upstream, crie uma subinterface somente para a VLAN 1750. Neste nível, os requisitos dependem da configuração de rede que você usa:

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

Verificar

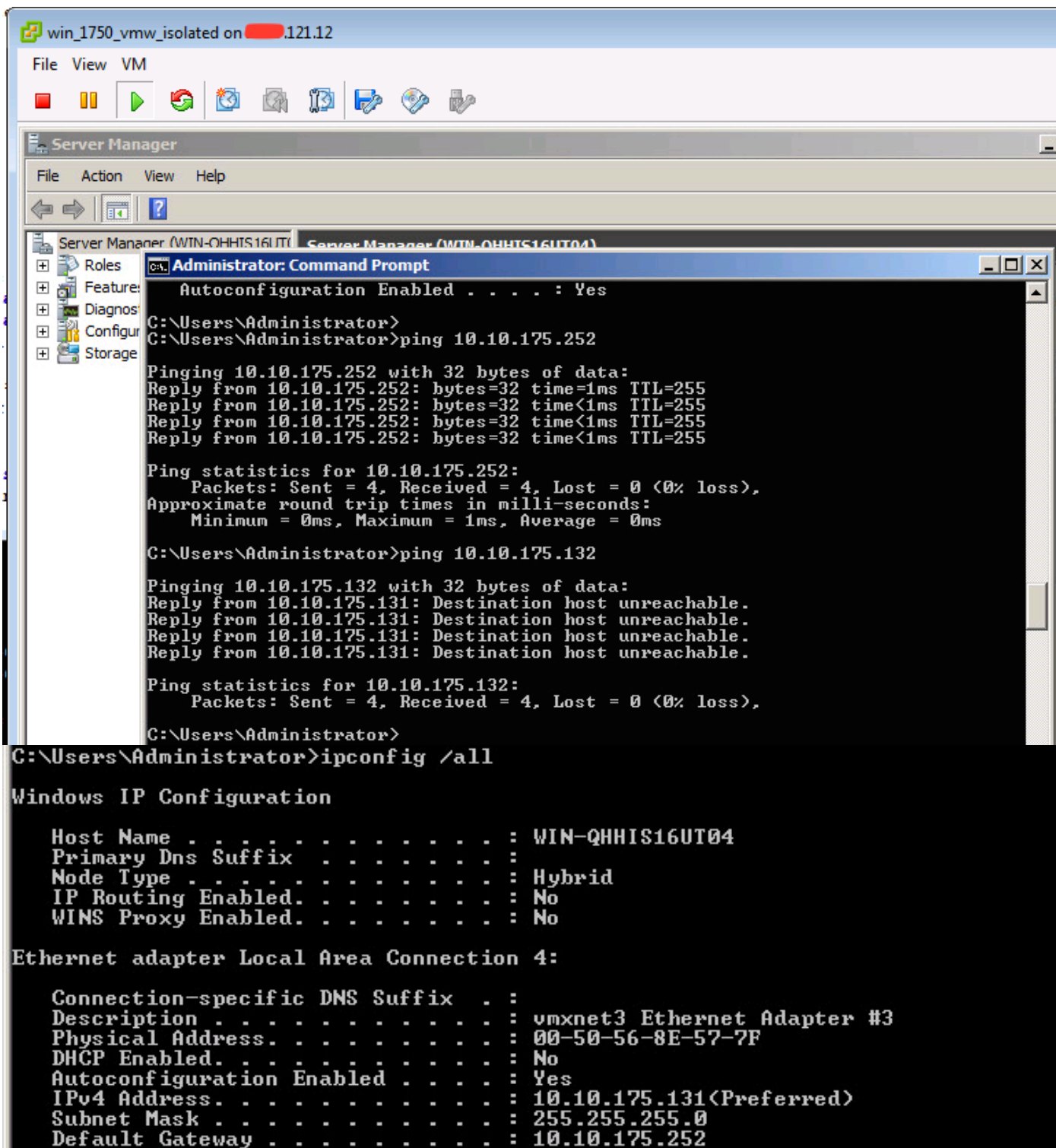
No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Este procedimento descreve como testar a configuração de VMware DVS com o uso de PVLAN.

1. Execute pings em outros sistemas configurados no grupo de portas, bem como no roteador ou em outro dispositivo na porta promíscua. Os pings para o dispositivo após a porta promíscua devem funcionar, enquanto os pings para outros dispositivos na VLAN isolada devem falhar, como mostrado nas imagens.



```
win_1750_vmw_isolated on 121.12
File View VM
Server Manager
File Action View Help
Server Manager (WIN-QHHIS16UT04) Server Manager (WIN-QHHIS16UT04)
Administrator: Command Prompt
Autoconfiguration Enabled . . . . : Yes
C:\Users\Administrator>
C:\Users\Administrator>ping 10.10.175.252
Pinging 10.10.175.252 with 32 bytes of data:
Reply from 10.10.175.252: bytes=32 time=1ms TTL=255
Reply from 10.10.175.252: bytes=32 time<1ms TTL=255
Reply from 10.10.175.252: bytes=32 time<1ms TTL=255
Reply from 10.10.175.252: bytes=32 time<1ms TTL=255
Ping statistics for 10.10.175.252:
    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 10.10.175.132
Pinging 10.10.175.132 with 32 bytes of data:
Reply from 10.10.175.131: Destination host unreachable.
Reply from 10.10.175.131: Destination host unreachable.
Reply from 10.10.175.131: Destination host unreachable.
Reply from 10.10.175.131: Destination host unreachable.
Ping statistics for 10.10.175.132:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
C:\Users\Administrator>
C:\Users\Administrator>ipconfig /all
Windows IP Configuration

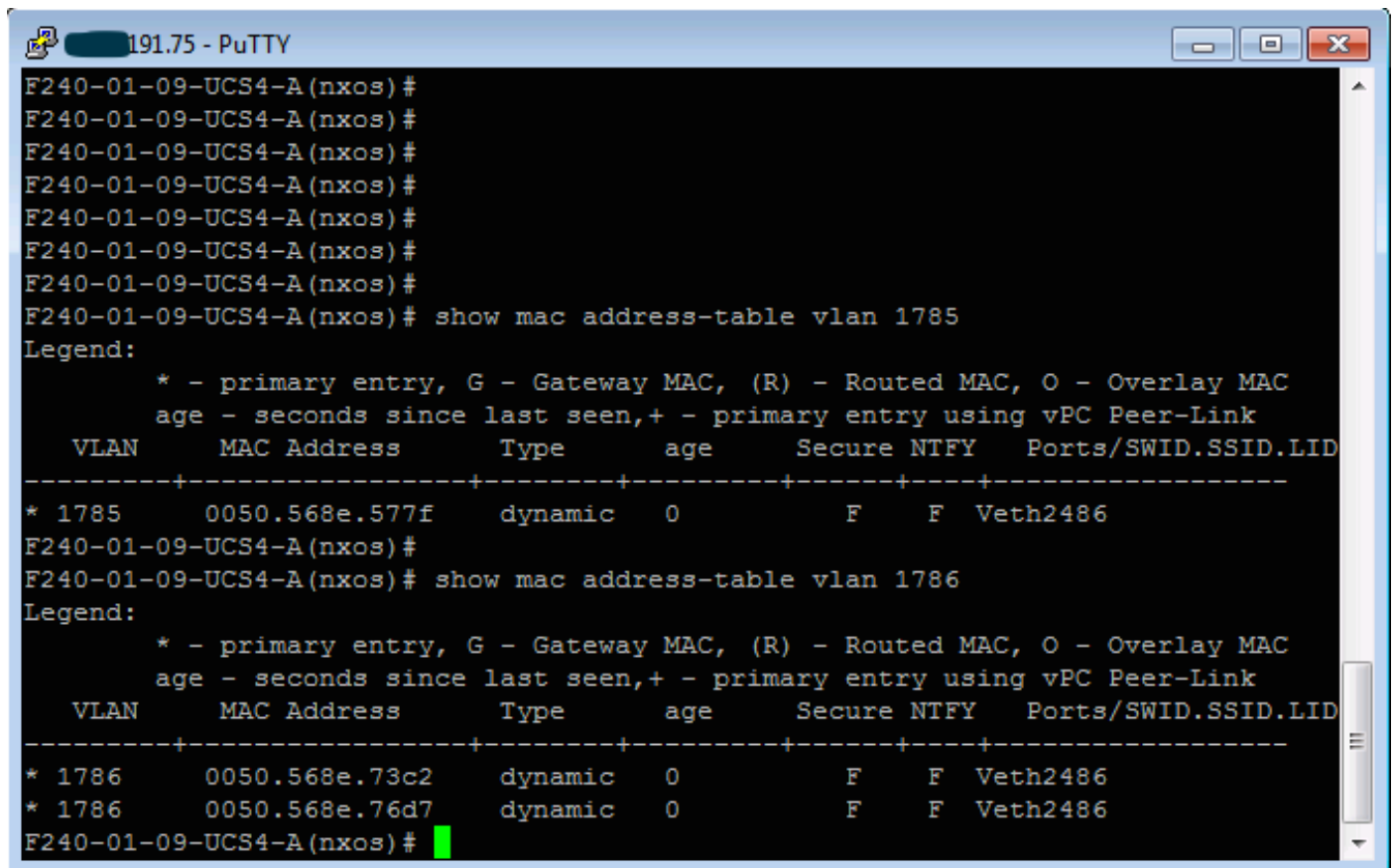
Host Name . . . . . : WIN-QHHIS16UT04
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection 4:

Connection-specific DNS Suffix . . :
Description . . . . . : vmxnet3 Ethernet Adapter #3
Physical Address. . . . . : 00-50-56-8E-57-7F
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
IPv4 Address. . . . . : 10.10.175.131(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.10.175.252
```

Verifique as tabelas de endereços MAC para ver onde seu MAC está sendo aprendido. Em todos os switches, o MAC deve estar na VLAN isolada, exceto no switch com a porta promíscua. No switch promíscuo, o MAC deve estar na VLAN principal.

2. UCS como mostrado na imagem.



```
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) #
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. Verifique no upstream n5k o mesmo MAC, a saída semelhante à saída anterior deve estar presente no n5k e conforme mostrado na imagem.

```
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#
```

Configuração com Nexus 1000v com porta promissora no upstream N5k

Configuração do UCS

A configuração do UCS (que inclui a configuração vNIC de perfil de serviço) permanece a mesma como no exemplo com o VMware DVS.

Configuração N1k

```
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 & pvlan. 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
```

Este procedimento descreve como testar a configuração.

1. Execute pings em outros sistemas configurados no grupo de portas, bem como no roteador ou em outro dispositivo na porta promíscua. Os pings para o dispositivo após a porta promíscua devem funcionar, enquanto os pings para outros dispositivos na VLAN isolada devem falhar, como mostrado na seção anterior e nas imagens.

