Configurar o VLAN privado e o UCS com VMware DV ou nexo 1000v de Cisco

Índice

Introdução

Este documento descreve o apoio do VLAN privado (PVLAN) para o Cisco Unified Computing System (UCS) 2.2(2c) na liberação e mais tarde.

> Cuidado: Há uma mudança no comportamento que começa com versão de firmware UCS 3.1(3a) como descrito na **mudança do comportamento com** seção da **versão 3.1(3) e mais recente UCS**.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- UCS

- O nexo 1000V (N1K) ou VMware de Cisco distribuiu o virtual switch (os DV)
- VMware
- Interruptor da camada 2 (L2)

Componentes Utilizados

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Um VLAN privado é um VLAN configurado para o isolamento L2 de outras portas dentro do mesmo VLAN privado. As portas que pertencem a um PVLAN são associadas com um grupo comum do apoio VLAN, que são usados a fim criar a estrutura PVLAN.

Há três tipos de portas PVLAN:

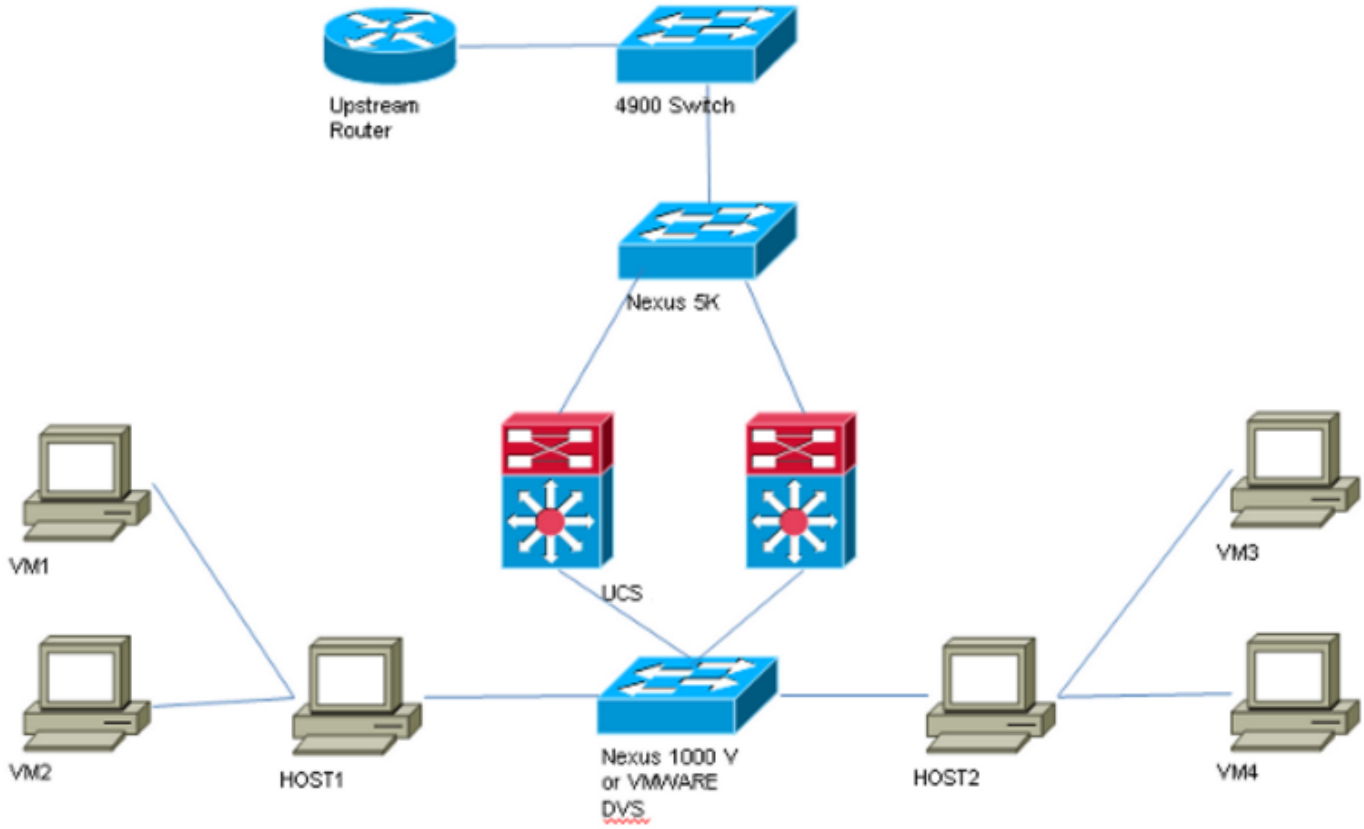
- Uma porta misturada comunica-se com todas portas restantes PVLAN e é-se a porta usada a fim comunicar-se com os dispositivos fora do PVLAN.
- Uma porta isolada tem a separação L2 completa (que inclui transmissões) de outras portas dentro do mesmo PVLAN à excecpção da porta misturada.
- Uma porta da comunidade pode comunicar-se com outras portas no mesmo PVLAN assim como na porta misturada. As portas da comunidade são isoladas no L2 das portas em outras comunidades ou portas isoladas PVLAN. As transmissões são propagadas somente a outras portas na comunidade e na porta misturada.

Refira o RFC 5517, os VLAN privados dos Cisco Systems: Segurança escalável em um ambiente do Multi-cliente a fim compreender a teoria, a operação, e os conceitos dos PVLAN.

Configurar

Diagrama de Rede

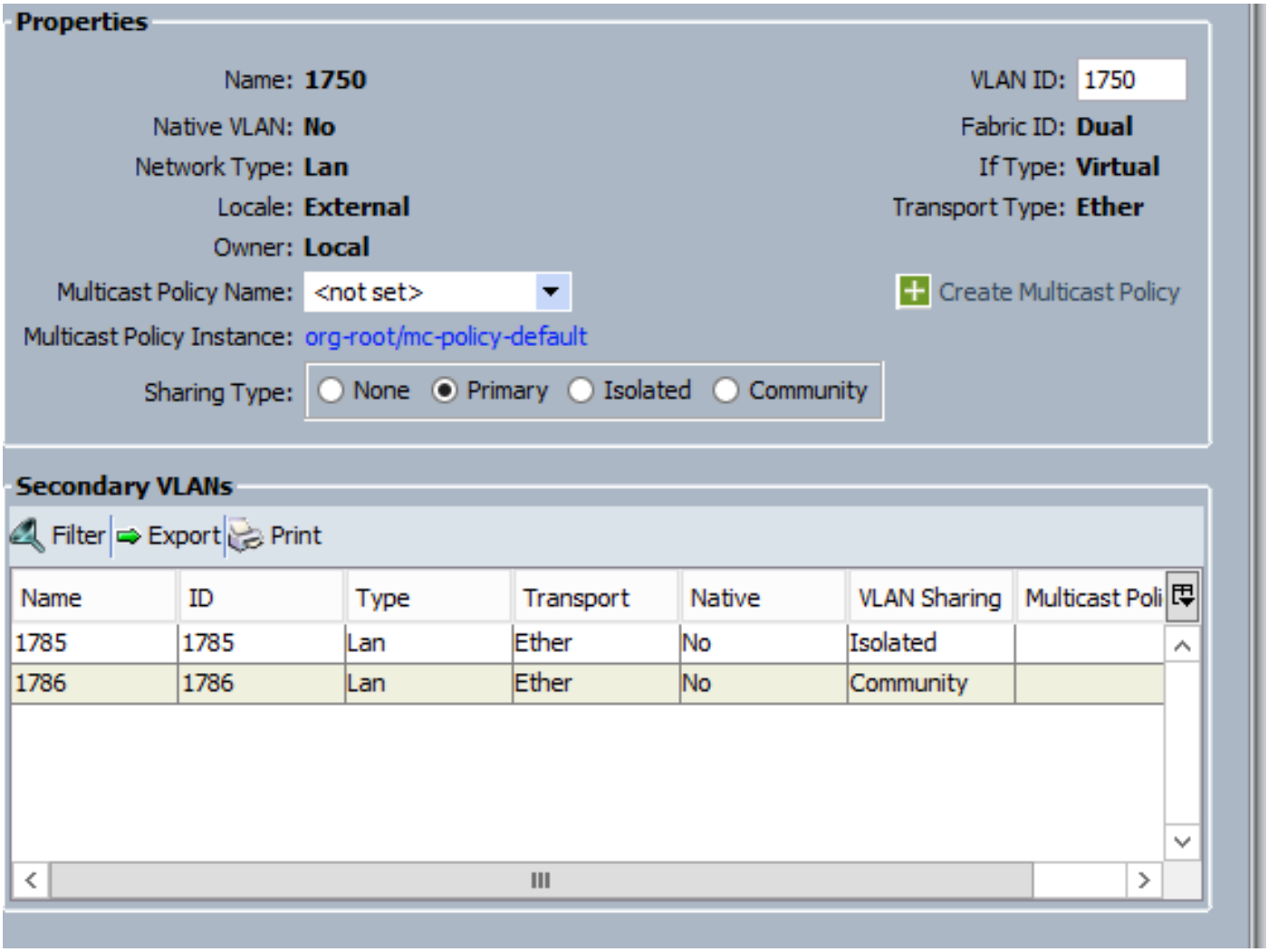
Com nexo 1000v ou VMware DV



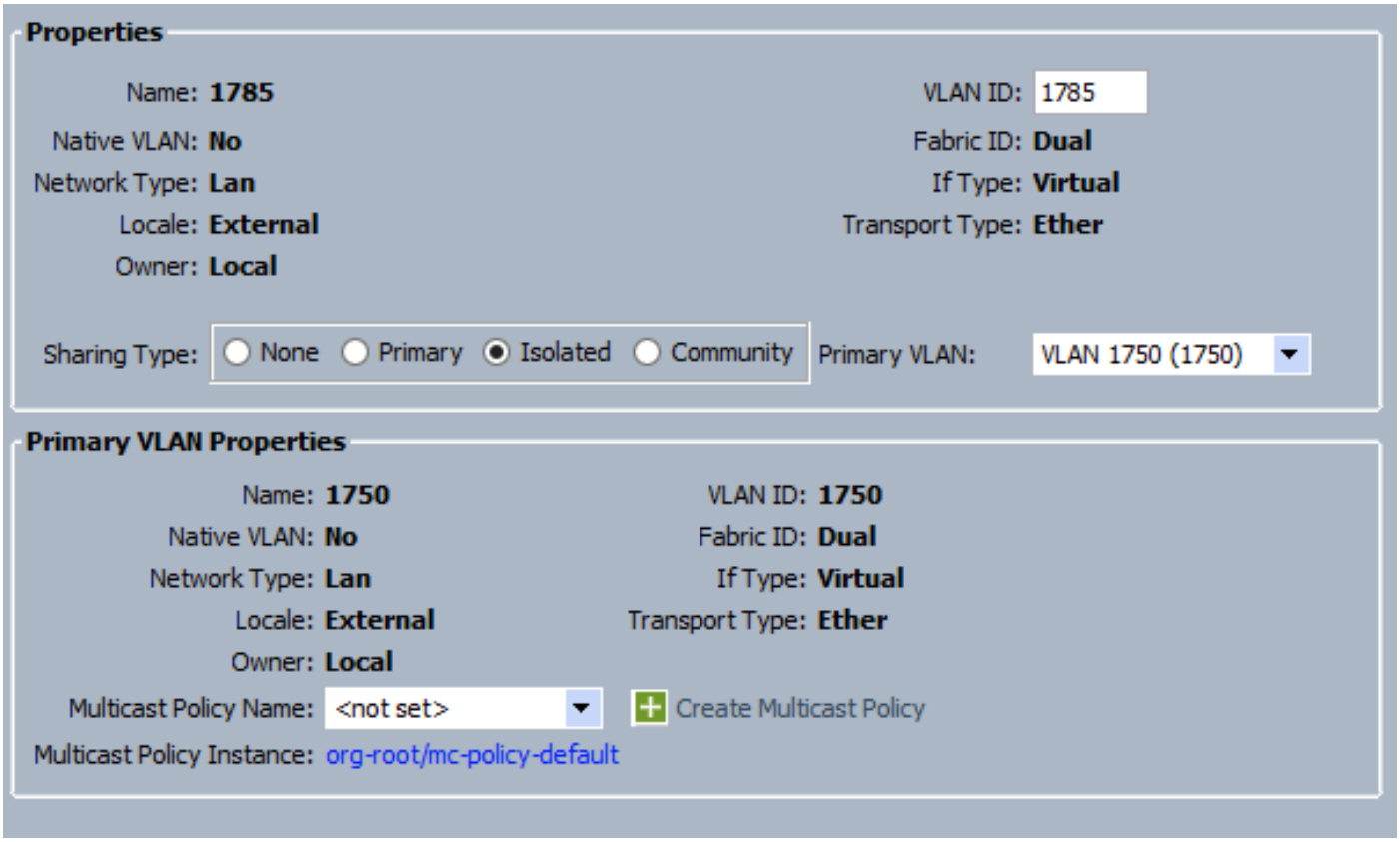
Nota: Este exemplo usa VLAN 1750 como o preliminar, 1785 como isolados e 1786 como o VLAN de comunidade.

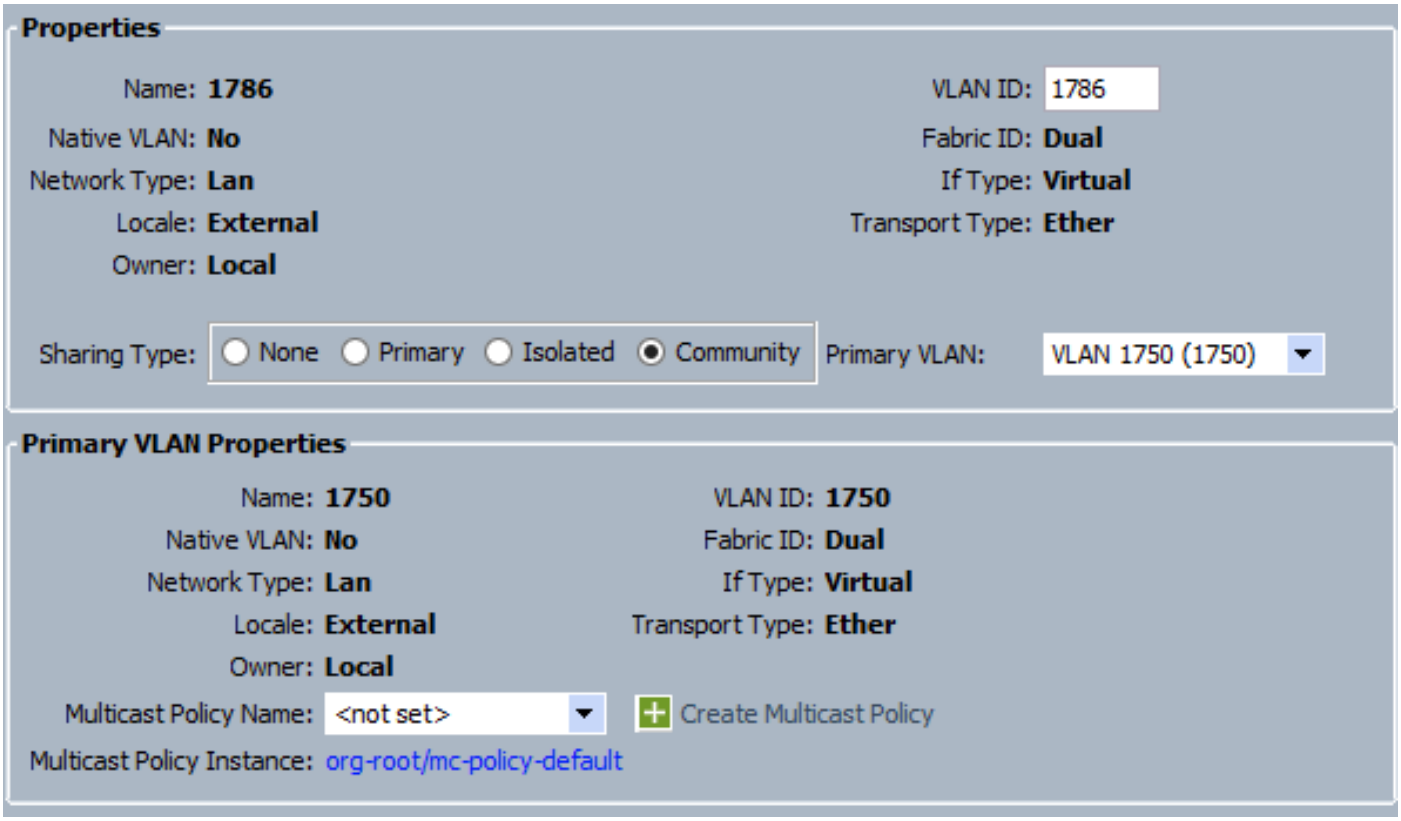
UCS com VMware DV

1. A fim criar o VLAN principal, clique o botão de rádio **preliminar** como o tipo de partilha, e incorpore um **ID de VLAN de** 1750 segundo as indicações da imagem.

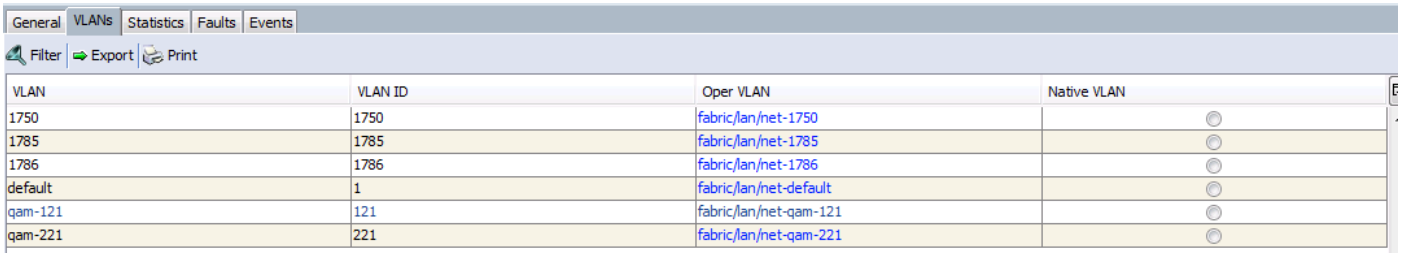


2. Crie **isolado** e **VLAN de comunidade** em conformidade segundo as indicações das imagens. Nenhuma destes tem que ser um VLAN nativo.





3. A placa de interface da rede virtual (vNIC) no serviço-perfil leva VLAN assim como PVLAN regulares, como visto na imagem.

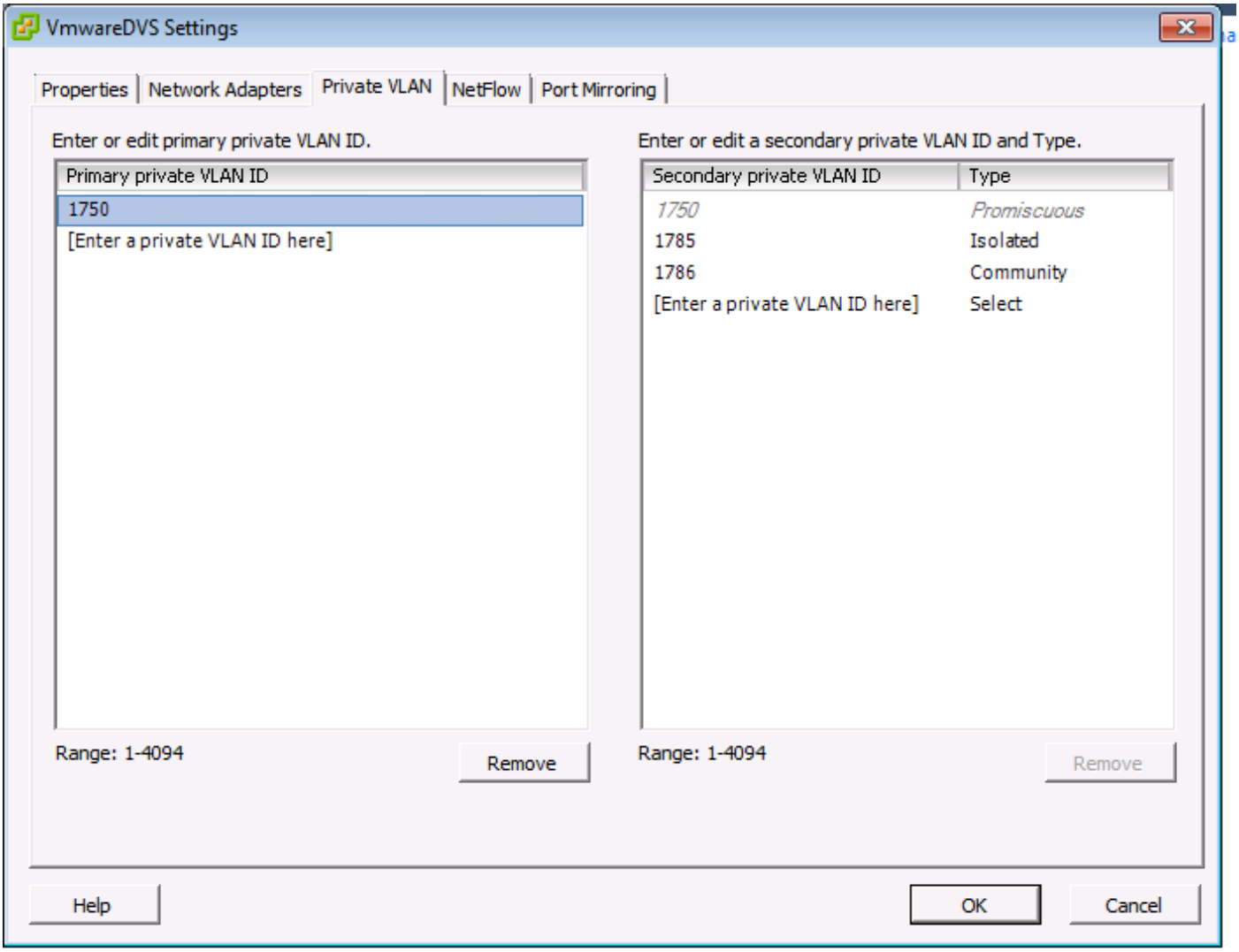


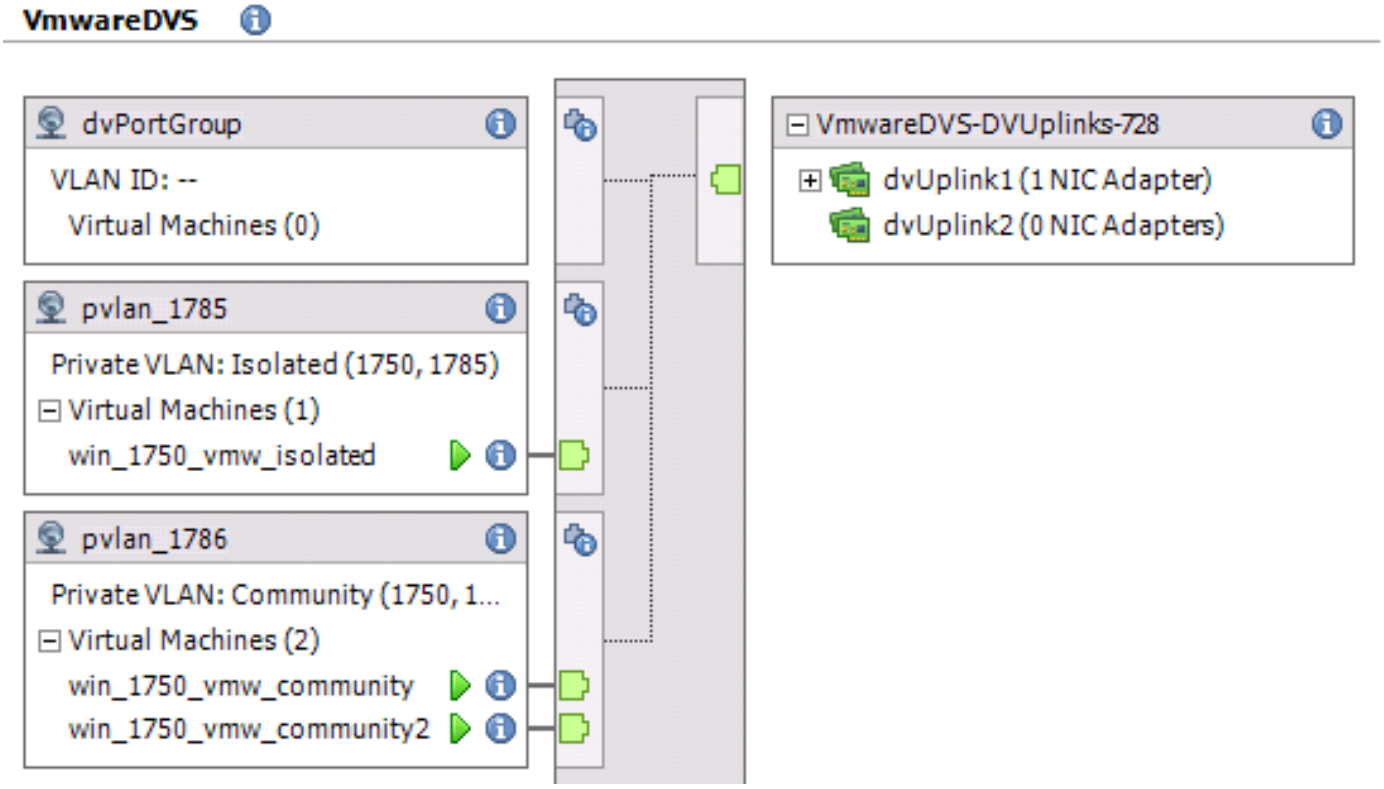
VLAN	VLAN ID	Oper VLAN	Native VLAN
1750	1750	fabric/lan/net-1750	
1785	1785	fabric/lan/net-1785	
1786	1786	fabric/lan/net-1786	
default	1	fabric/lan/net-default	
qam-121	121	fabric/lan/net-qam-121	
qam-221	221	fabric/lan/net-qam-221	

4. O canal de porta do uplink no UCS leva VLAN assim como PVLAN regulares:

```
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 DV





Interruptor ascendente N5k

```
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 do comportamento com versão 3.1(3) UCS

Antes da versão 3.1(3) UCS, você poderia mandar um VM no VLAN de comunidade comunicar-se com um VM no VLAN principal em VMware DV onde o VLAN principal VM reside dentro do UCS. Este comportamento estava por mais incorreto que o VM preliminar deva sempre estar northbound ou exterior do UCS. Este comportamento é documentado através do ID de defeito CSCvh87378 .

Da versão 2.2(2) UCS avante, devido a um defeito no código, o VLAN de comunidade podia comunicar-se com o VLAN principal que estou presente atrás do FI. Mas isolado podia nunca comunicar-se com o preliminar atrás do FI. Ambos os (isolado e a comunidade) VM podem ainda comunicar-se com o preliminar fora do FI.

De 3.1(3) avante, este defeito permite que a comunidade comunique-se com o preliminar atrás do FI, foi retificado e assim a comunidade VM não poderá comunicar-se com um VM no VLAN principal que reside dentro do UCS.

A fim resolver esta situação, o VM preliminar uma ou outra necessidade de ser movido (northbound) fora do UCS. Se aquela não é uma opção, a seguir o VM preliminar precisaria de ser movido em um outro VLAN que fosse um VLAN regular e não um VLAN privado.

Por exemplo, antes do firmware 3.1(3), um VM no VLAN de comunidade 1786 poderia comunicar-se a um VM no VLAN principal 1750 que reside dentro do UCS, contudo, esta comunicação quebraria no firmware 3.1(3) e mais atrasado, segundo as indicações da imagem.

NOTA:

CSCvh87378 foi endereçado em 3.2(3l) e em 4.0.4e & mais altamente assim que nós podemos ter Vlan preliminar atrás do UCS. Satisfaça de qualquer modo notam que o vlan isolada dentro do UCS não poderá falar ao UCS interno vlan preliminar. Vlan vlan & preliminar somente da comunidade pode falar entre si quando ambos são atrás 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)#
```

4900 Switch ascendente

> Nota: Neste exemplo, 4900 são a relação L3 à rede externa. Se sua topologia para o L3 é diferente, a seguir faça amavelmente mudanças em conformidade

No 4900 Switch, tome estas etapas, e estabelece a porta misturada. As extremidades PVLAN na porta misturada.

1. Gire sobre recursos de PVLAN se for necessário.
2. Crie e associe os VLAN como feitos no nexo 5K.
3. Crie a porta misturada na porta de saída do 4900 Switch. A partir daqui, os pacotes de VLAN 1785 & 1786 são vistos em VLAN 1750 neste caso.

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

No roteador fluxo acima, crie uma subinterface para o VLAN 1750 somente. Neste nível, as exigências dependem em cima da configuração de rede que você se usa:

```
interface GigabitEthernet0/1.1

encapsulation dot1Q 1750

IP address10.10.175.254/24
```

Verificar

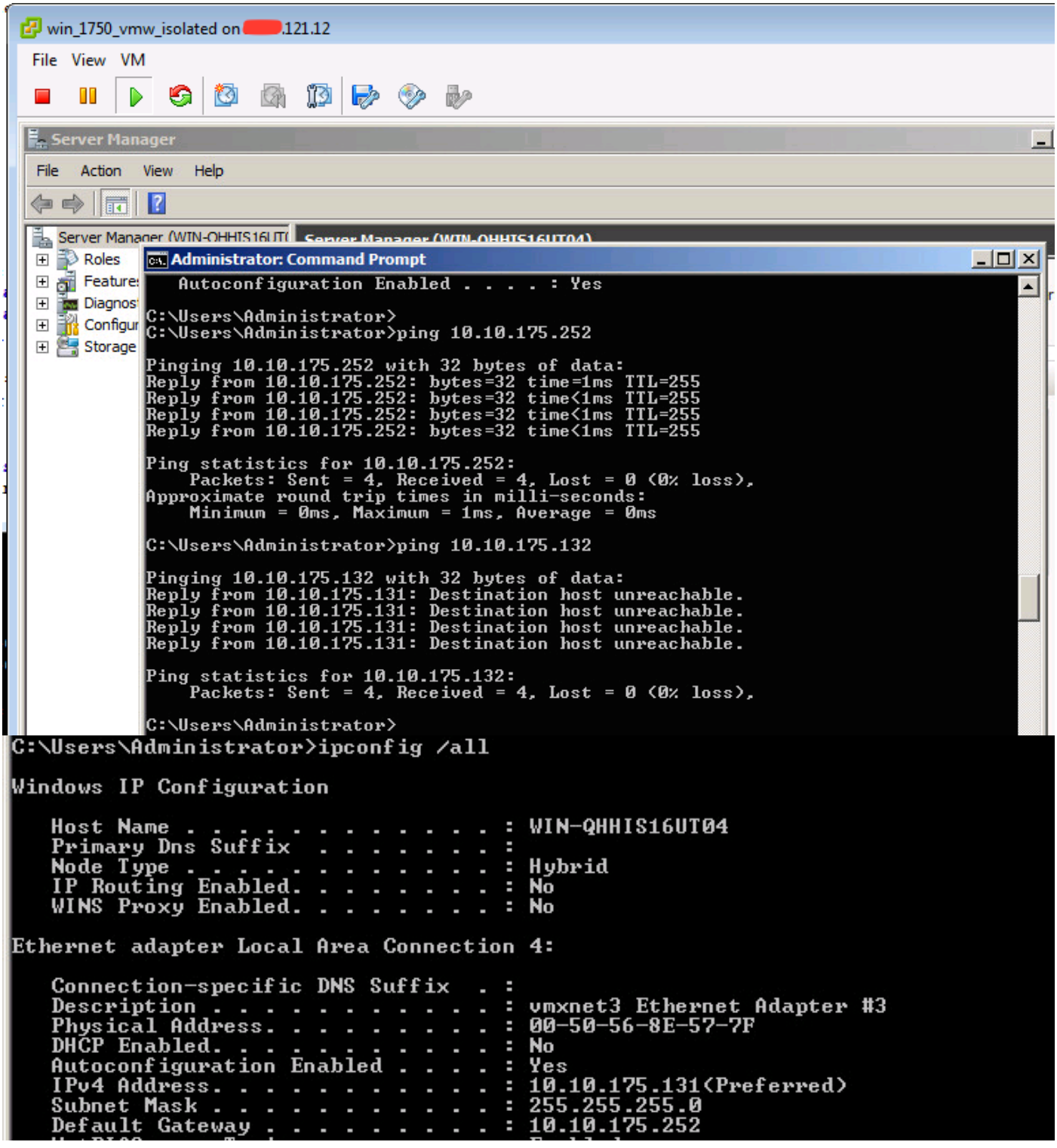
No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Esta seção fornece informações que você pode usar na solução de problemas de sua configuração.

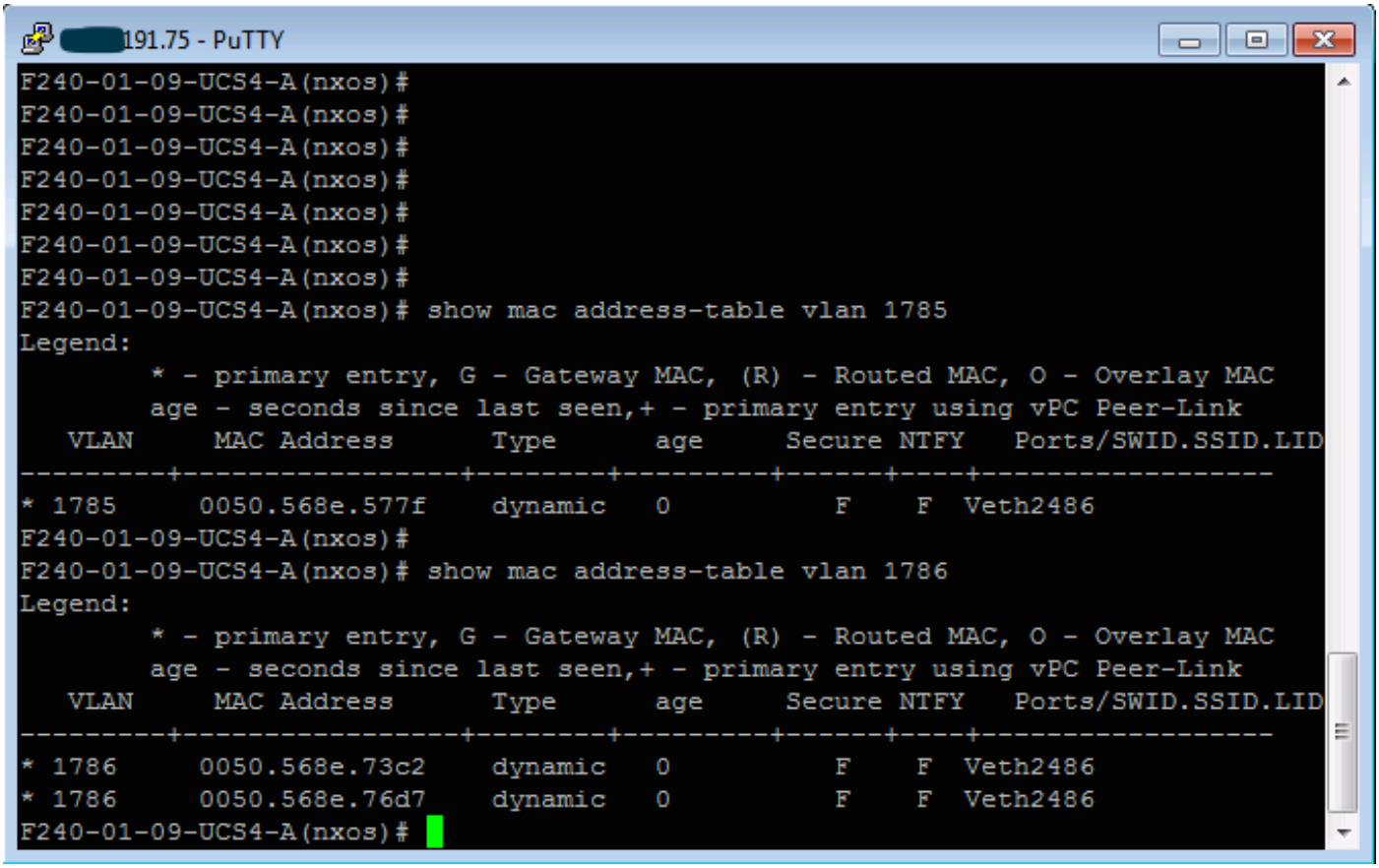
Este procedimento descreve como testar a configuração para VMware DV com o uso do PVLAN.

1. Execute sibilos a outros sistemas configurados no grupo de porta assim como o roteador ou o outro dispositivo na porta misturada. Os sibilos ao dispositivo após a porta misturada devem trabalhar, quando aqueles aos outros dispositivos no vlan isolada deverem falhar segundo as indicações das imagens.



Verifique as tabelas de endereços MAC a fim ver onde seu MAC está sendo instruído. Em todo o Switches, o MAC deve estar no vlan isolada exceto no interruptor com a porta misturada. No interruptor promíscuo, o MAC deve estar no VLAN principal.

2. UCS segundo as indicações da imagem.



3. Verifique em n5k ascendente para ver se há o mesmo MAC, saída similar para output mais cedo deve estam presente em n5k e segundo as indicações da 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 nexo 1000v com porta misturada em N5k ascendente

Configuração UCS

A configuração UCS (que inclui a configuração do vNIC do serviço-perfil) fica o mesmos conforme o exemplo com VMware DV.

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 & 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
```

Este procedimento descreve como testar a configuração.

1. Execute sibilos a outros sistemas configurados no grupo de porta assim como o roteador ou o outro dispositivo na porta misturada. Os sibilos ao dispositivo após a porta misturada devem trabalhar, quando aqueles aos outros dispositivos no vlan isolada deverem falhar, segundo as indicações da seção anterior e nas imagens.