VMware DVS 또는 Cisco Nexus 1000v로 프라이빗 VLAN 및 UCS 구성

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[배경 정보](#)
[구성](#)
[네트워크 다이어그램](#)
[VMware DVS를 사용하는 UCS](#)
[VMware DVS](#)
[업스트림 N5k 스위치](#)
[UCS 버전 3.1(3)의 동작 변경](#)
[업스트림 4900 스위치](#)
[다음을 확인합니다.](#)
[문제 해결](#)
[업스트림 N5k에서 프로미스큐어스 포트가 포함된 Nexus 1000v를 사용한 컨피그레이션](#)
[UCS 컨피그레이션](#)
[N1k 컨피그레이션](#)
[N1K 업링크 포트 프로필에서 프로미스큐어스 포트가 포함된 Nexus 1000v 구성](#)
[UCS 컨피그레이션](#)
[업스트림 디바이스 컨피그레이션](#)
[N1K 구성](#)

소개

이 문서에서는 2.2(2c) 릴리스 이상에서 Cisco UCS(Unified Computing System)에 대한 PVLAN(Private VLAN) 지원에 대해 설명합니다.

> **주의:**UCS **버전 3.1(3)** 이상 섹션의 **동작 변경**에 설명된 대로 UCS 펌웨어 버전 3.1(3a)**부터** 동작**이** 변경됩니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

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

- VMware
- 레이어 2(L2) 스위칭

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

프라이빗 VLAN은 동일한 프라이빗 VLAN 내의 다른 포트와 L2 격리를 위해 구성된 VLAN입니다 .PVLAN에 속하는 포트는 PVLAN 구조를 생성하는 데 사용되는 공통 지원 VLAN 집합과 연결됩니다.

PVLAN 포트에는 세 가지 유형이 있습니다.

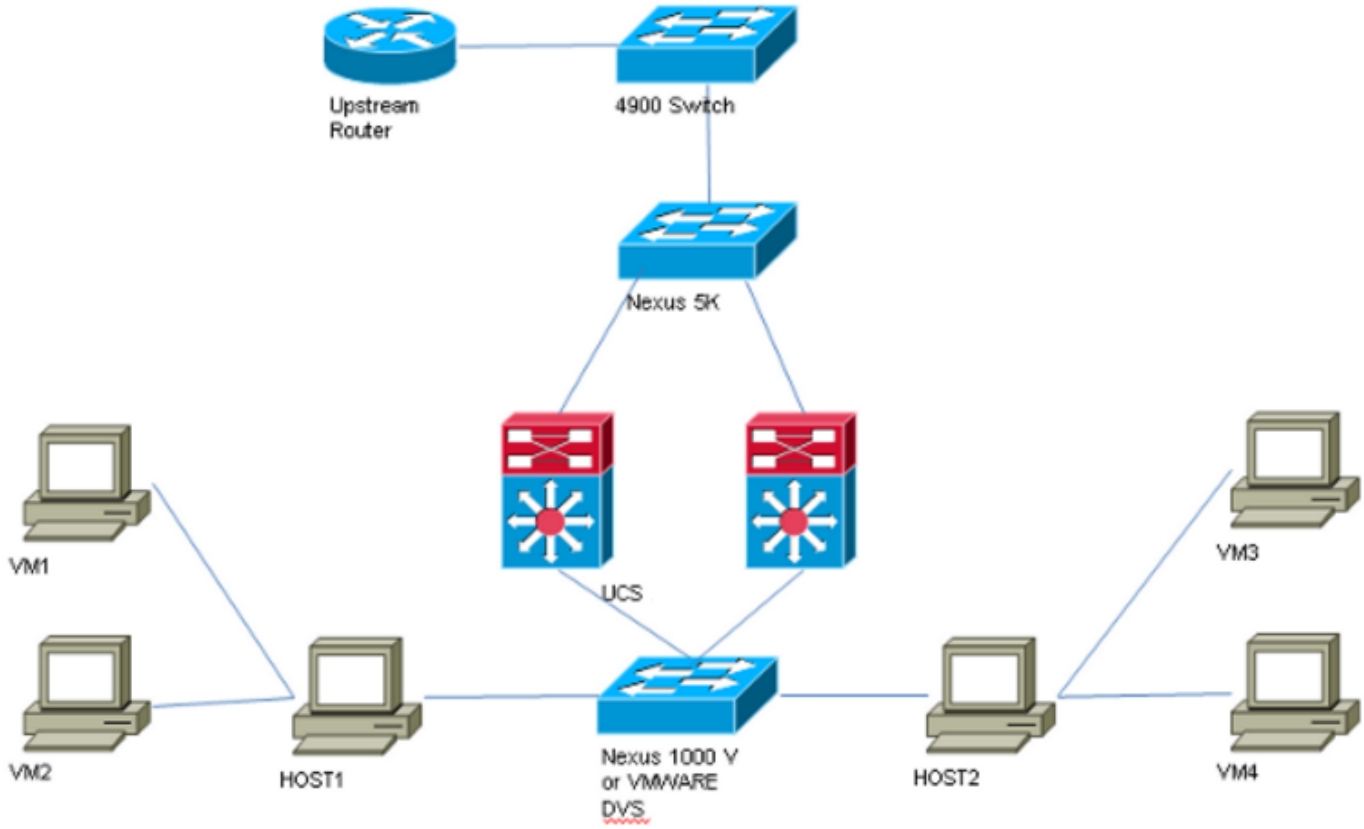
- 프로미스큐어스 포트는 다른 모든 PVLAN 포트와 통신하며 PVLAN 외부의 디바이스와 통신하는 데 사용되는 포트입니다.
- 격리된 포트는 프로미스큐어스 포트를 제외하고 동일한 PVLAN 내의 다른 포트에서 완전한 L2 분리(브로드캐스트 포함)를 수행합니다.
- 커뮤니티 포트는 프로미스큐어스 포트 뿐만 아니라 동일한 PVLAN의 다른 포트와 통신할 수 있습니다.커뮤니티 포트는 L2에서 다른 커뮤니티의 포트 또는 격리된 PVLAN 포트에서 격리됩니다.브로드캐스트는 커뮤니티의 다른 포트 및 프로미스큐어스 포트에만 전파됩니다.

Cisco Systems의 프라이빗 VLAN인 RFC 5517을 참조하십시오.PVLAN의 이론, 운영 및 개념을 이해하기 위한 멀티 클라이언트 환경의 확장 가능한 보안

구성

네트워크 다이어그램

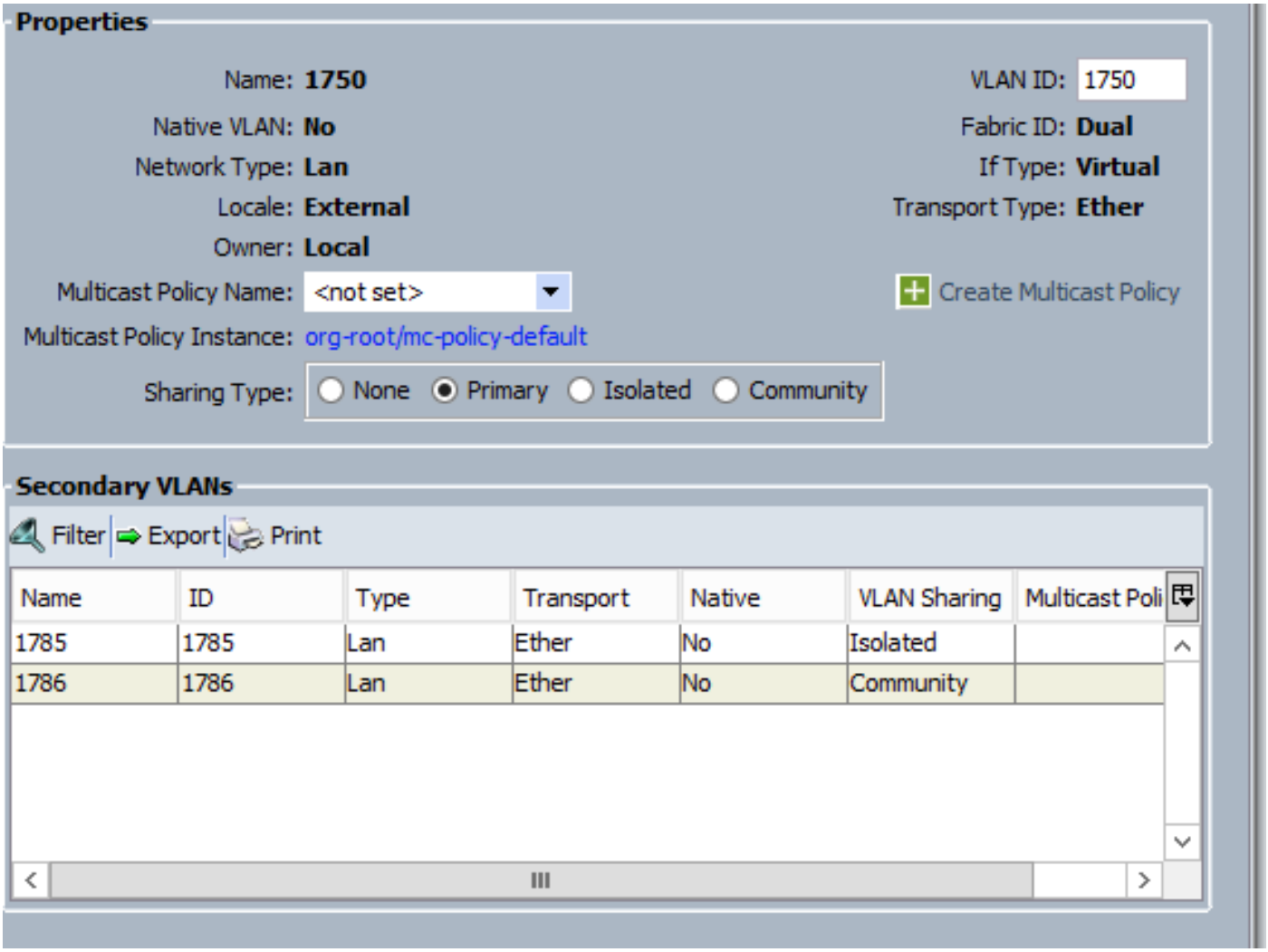
Nexus 1000v 또는 VMware DVS 사용



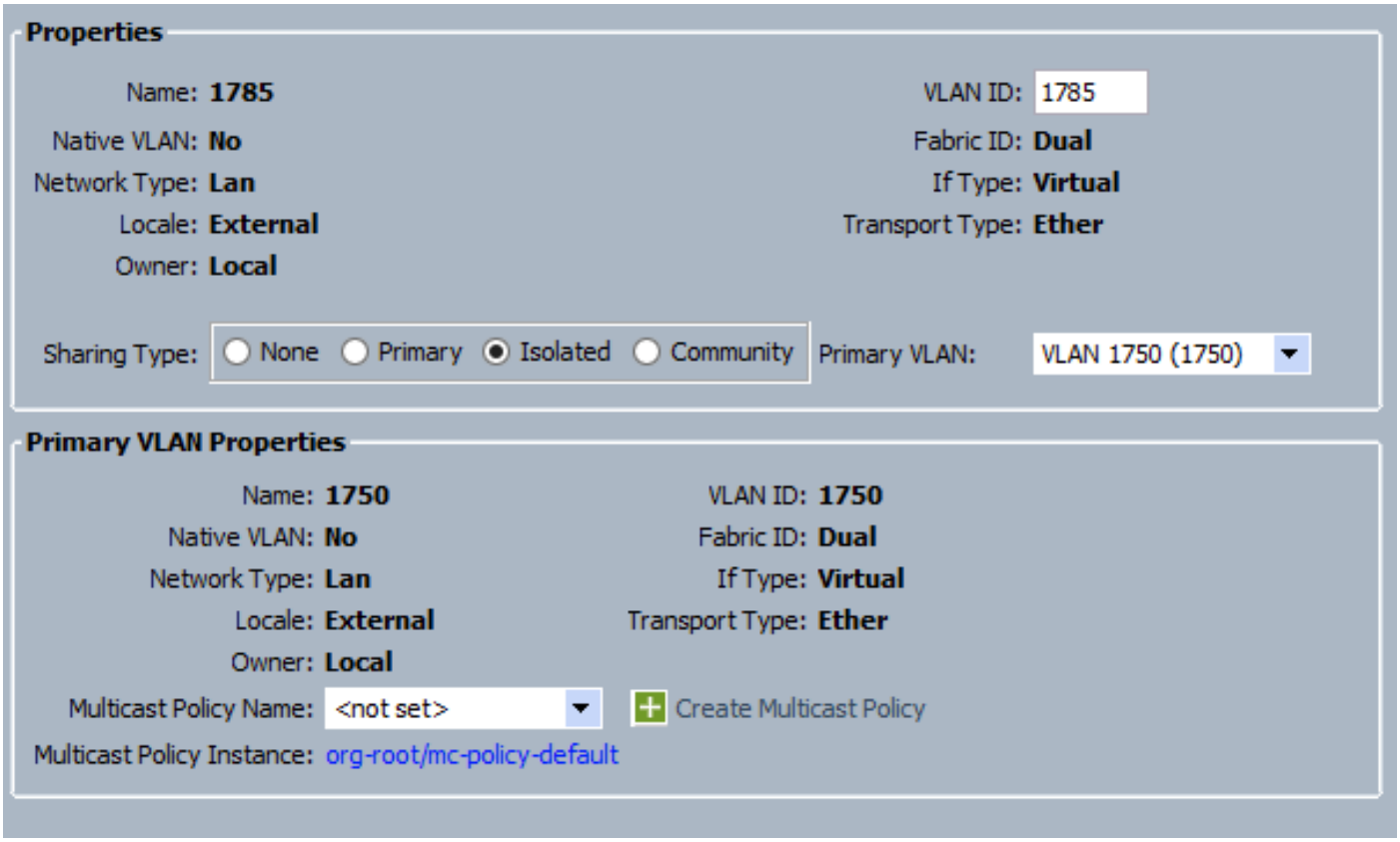
참고:이 예에서는 VLAN 1750을 기본으로, 1785를 격리됨으로, 1786을 커뮤니티 VLAN으로 사용합니다.

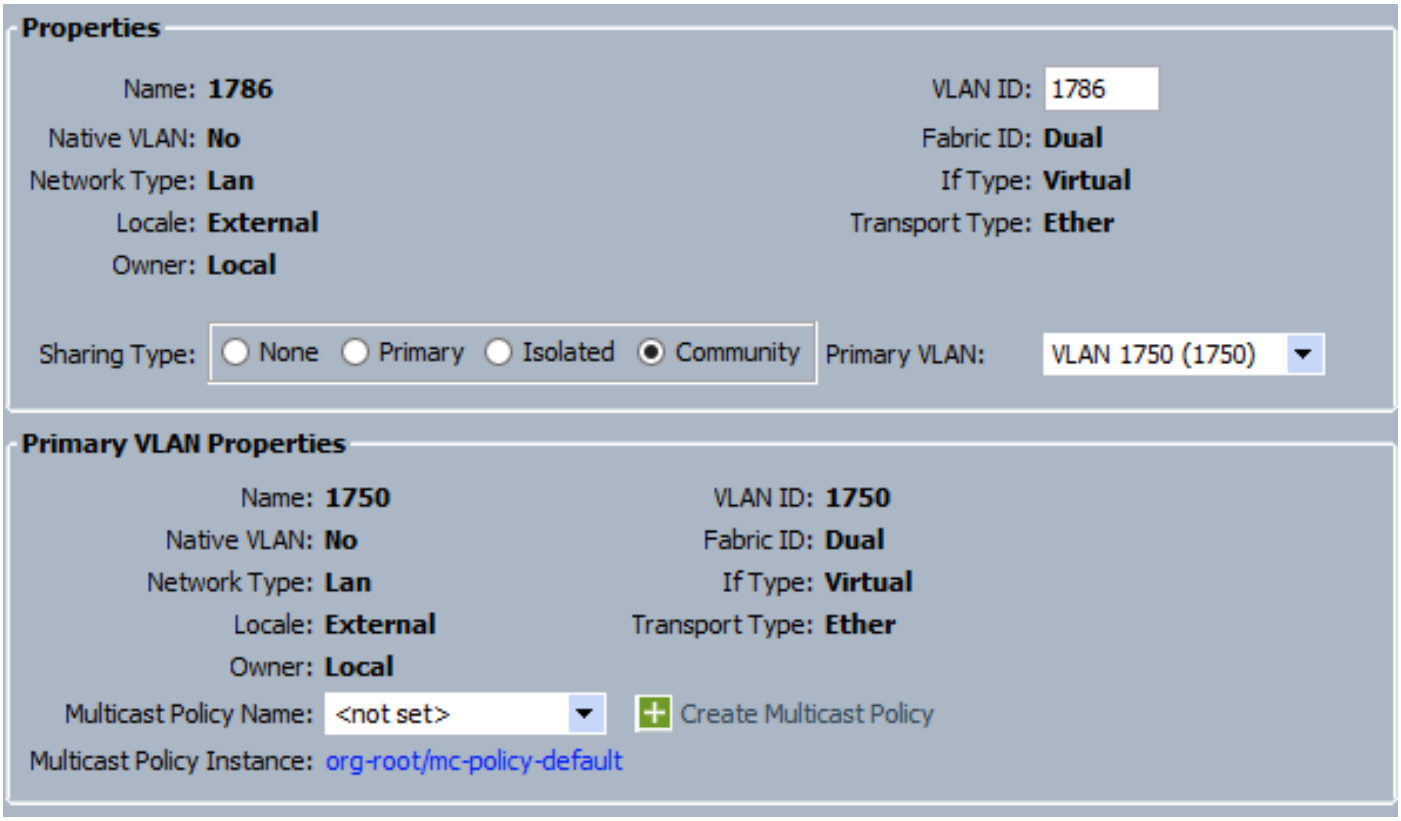
VMware DVS를 사용하는 UCS

1. 기본 VLAN을 생성하려면 Primary(**기본**) 라디오 버튼을 Sharing Type(공유 유형)으로 클릭하고 이미지에 표시된 대로 **VLAN ID** 1750을 입력합니다.

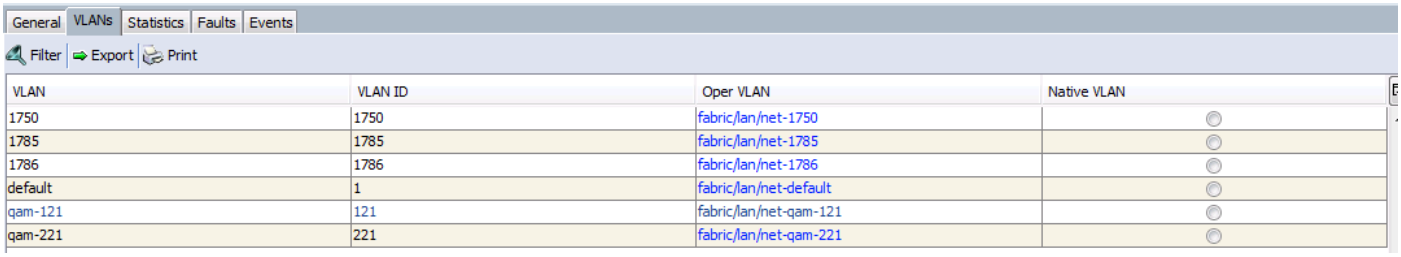


2. 이미지에 표시된 대로 격리 및 **커뮤니티** VLAN을 생성합니다.이 중 어느 것도 네이티브 VLAN일 필요는 없습니다.





3. 서비스 프로필의 vNIC(Virtual Network Interface Card)는 일반 VLAN 및 PVLAN을 전달합니다(이미지에 표시됨).

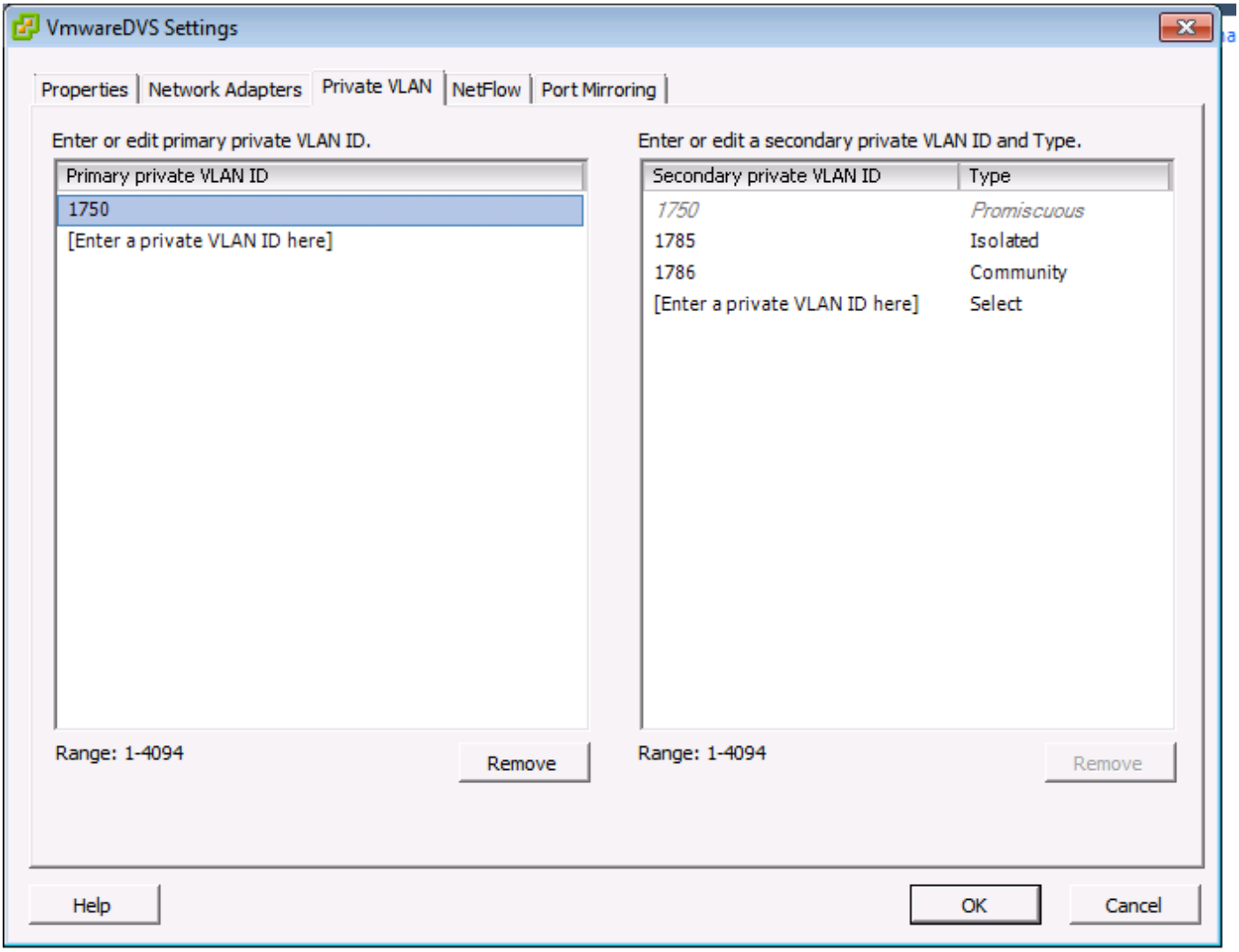


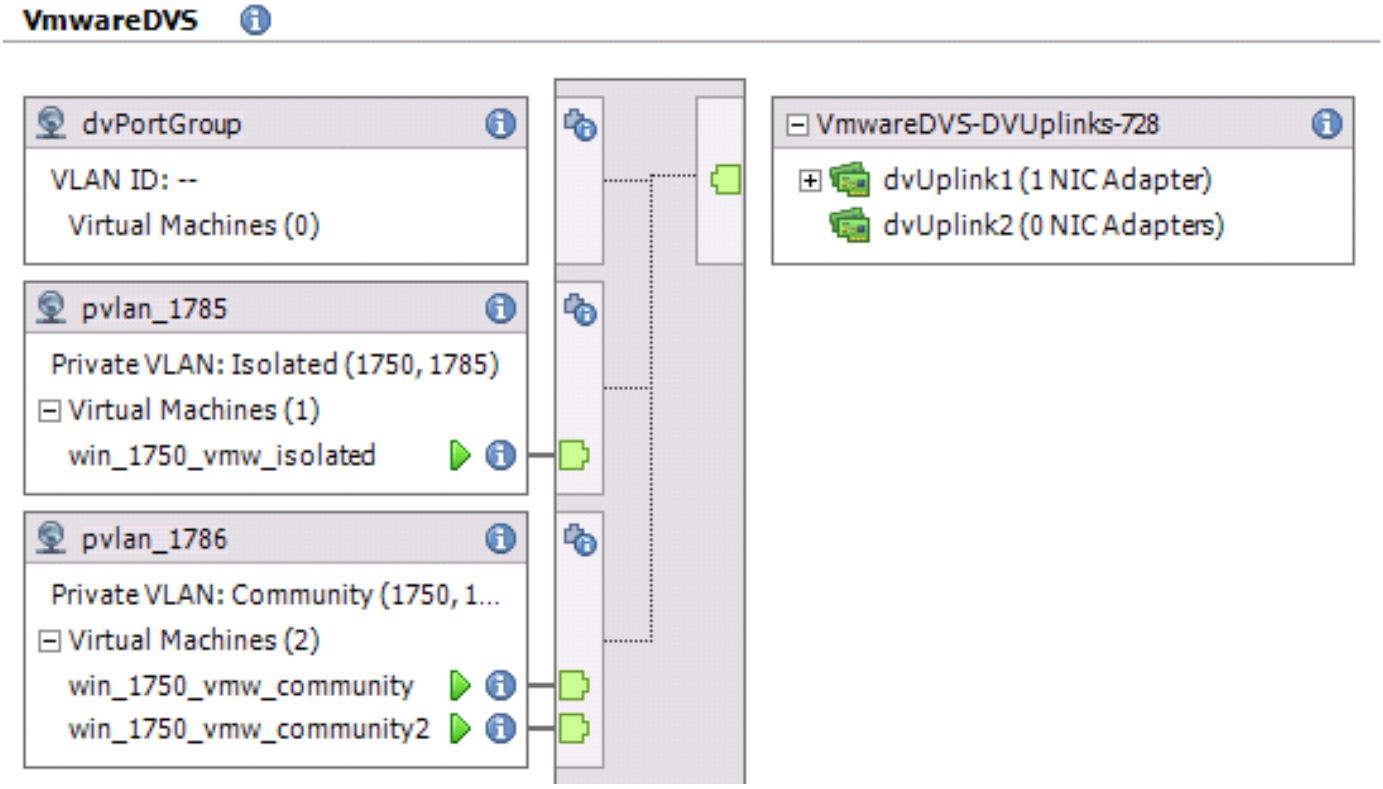
VLAN	VLAN ID	Oper VLAN	Native VLAN
1750	1750	fabric/lan/net-1750	
1785	1785	fabric/lan/net-1785	
1786	1786	fabric/lan/net-1786	
default	1	fabric/lan/net-default	
qam-121	121	fabric/lan/net-qam-121	
qam-221	221	fabric/lan/net-qam-221	

4. UCS의 업링크 포트 채널은 일반 VLAN 및 PVLAN을 전송합니다.

```
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 Settings
Properties
Network Adapters
Private VLAN
NetFlow
Port Mirroring
Enter or edit primary private VLAN ID.
Primary private VLAN ID
1750
[Enter a private VLAN ID here]
Range: 1-4094
Remove
Enter or edit a secondary private VLAN ID and Type.
Secondary private VLAN ID
Type
1750
Promiscuous
1785
Isolated
1786
Community
[Enter a private VLAN ID here]
Select
Range: 1-4094
Remove
Help
OK
Cancel


VmwareDVS
dvPortGroup
VLAN ID: --
Virtual Machines (0)
pvlan_1785
Private VLAN: Isolated (1750, 1785)
Virtual Machines (1)
win_1750_vmw_isolated
pvlan_1786
Private VLAN: Community (1750, 1...
Virtual Machines (2)
win_1750_vmw_community
win_1750_vmw_community2
VmwareDVS-DVUplinks-728
dvUplink1 (1 NIC Adapter)
dvUplink2 (0 NIC Adapters)

업스트림 N5k 스위치

```
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
```

UCS 버전 3.1(3)의 동작 변경

UCS 버전 3.1(3) 이전 버전에서는 커뮤니티 VLAN의 VM이 UCS 내에 기본 VLAN VM이 상주하는 VMware DVS의 기본 VLAN의 VM과 통신하도록 할 수 있습니다.기본 VM은 항상 노스바운드(northbound) 또는 UCS 외부에 있어야 하므로 이 동작은 올바르지 않습니다.이 동작은 결함 ID CSCvh87378을 통해 문서화됩니다. .

UCS 버전 2.2(2)부터 코드의 결함 때문에 커뮤니티 VLAN은 FI 뒤에 있던 기본 VLAN과 통신할 수 있었습니다.하지만 Isolated는 FI 뒤에 있는 기본 디바이스와 통신할 수 없었습니다.(격리 및 커뮤니티) VM 모두 여전히 FI 외부의 기본 VM과 통신할 수 있습니다.

3.1(3)부터 이 결함은 커뮤니티가 FI 뒤의 기본 VM과 통신할 수 있게 해주므로 커뮤니티 VM이 UCS 내에 상주하는 기본 VLAN의 VM과 통신할 수 없게 됩니다.

이 문제를 해결하려면 기본 VM을 UCS 외부로 이동(노스바운드)해야 합니다.옵션이 아닌 경우 기본 VM을 프라이빗 VLAN이 아닌 일반 VLAN인 다른 VLAN으로 이동해야 합니다.

예를 들어, 펌웨어 3.1(3) 이전 버전의 커뮤니티 VLAN 1786의 VM은 UCS 내에 상주하는 기본 VLAN 1750의 VM과 통신할 수 있지만, 이미지에 표시된 것처럼 이 통신은 펌웨어 3.1(3) 이상에서 중단됩니다.

참고:

—

CSCvh87378은 3.2(3l) 및 4.0.4e 이상에서 처리되었으므로 UCS 뒤에 기본 VLAN이 있을 수 있습니다.그러나 UCS 내부의 격리 VLAN은 UCS 내부의 기본 VLAN과 통신할 수 없습니다.커뮤니티 VLAN과 기본 VLAN만 둘 다 UCS를 지원하는 경우 서로 통신할 수 있습니다.

```
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)#
```

업스트림 4900 스위치

> **참고:**이 예에서 4900은 외부 네트워크에 대한 L3 인터페이스입니다.L3에 대한 토폴로지가 다른 경우 그에 따라 변경하십시오.

4900 스위치에서 다음 단계를 수행하고 프로미스큐어스 포트를 설정합니다.PVLAN은 프로미스큐어스 포트에서 끝납니다.

1. 필요한 경우 PVLAN 기능을 설정합니다.
2. Nexus 5K에서 수행한 대로 VLAN을 생성하고 연결합니다.
3. 4900 스위치의 이그레스 포트에 프로미스큐어스 포트를 생성합니다.이 시점부터 VLAN 1785 및 1786의 패킷이 VLAN 1750에서 표시됩니다.

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

업스트림 라우터에서 VLAN 1750에 대해서만 하위 인터페이스를 생성합니다.이 수준에서 요구 사항은 사용하는 네트워크 구성에 따라 달라집니다.

```
interface GigabitEthernet0/1.1

encapsulation dot1Q 1750

IP address10.10.175.254/24
```

다음을 확인합니다.

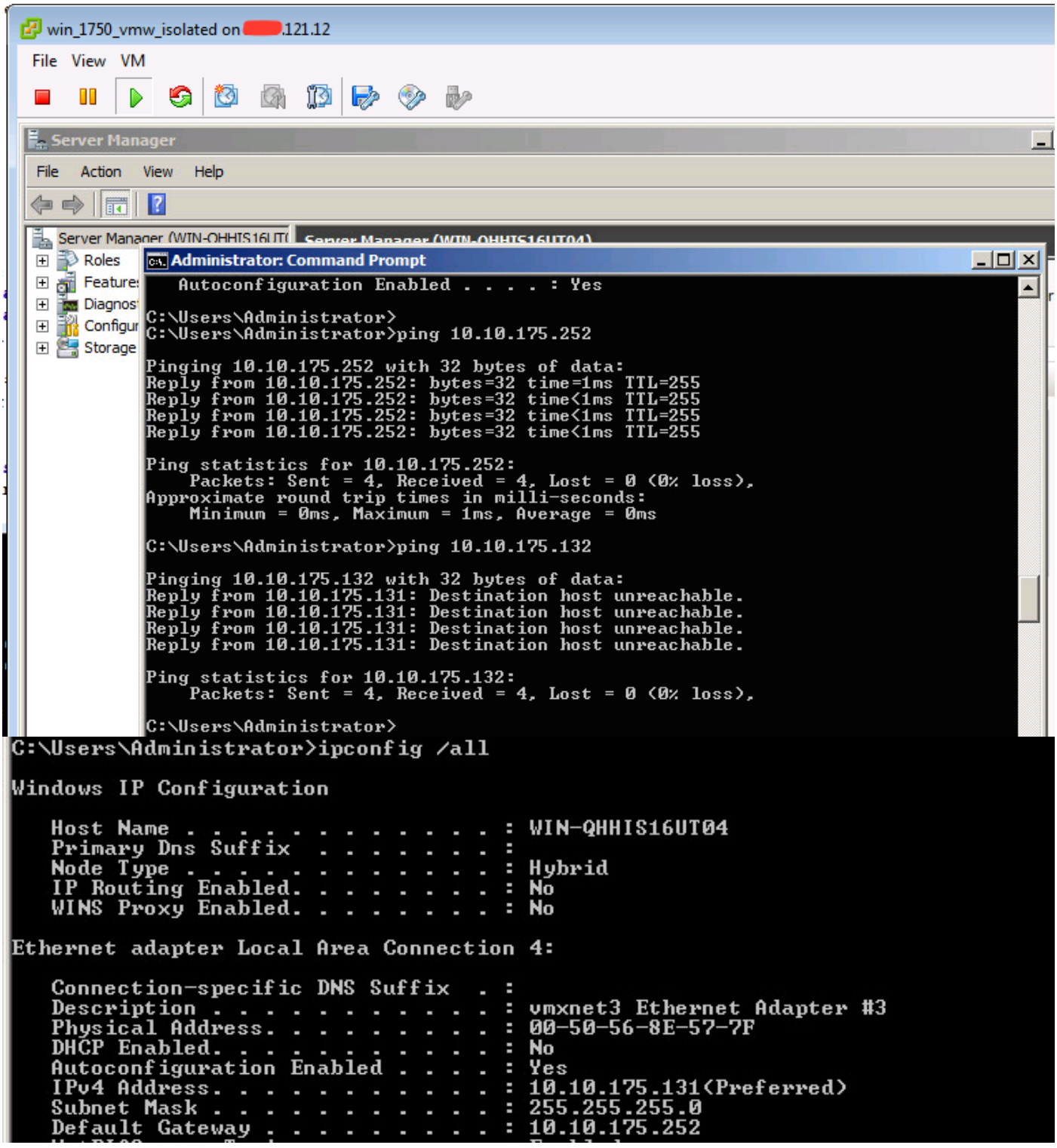
현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

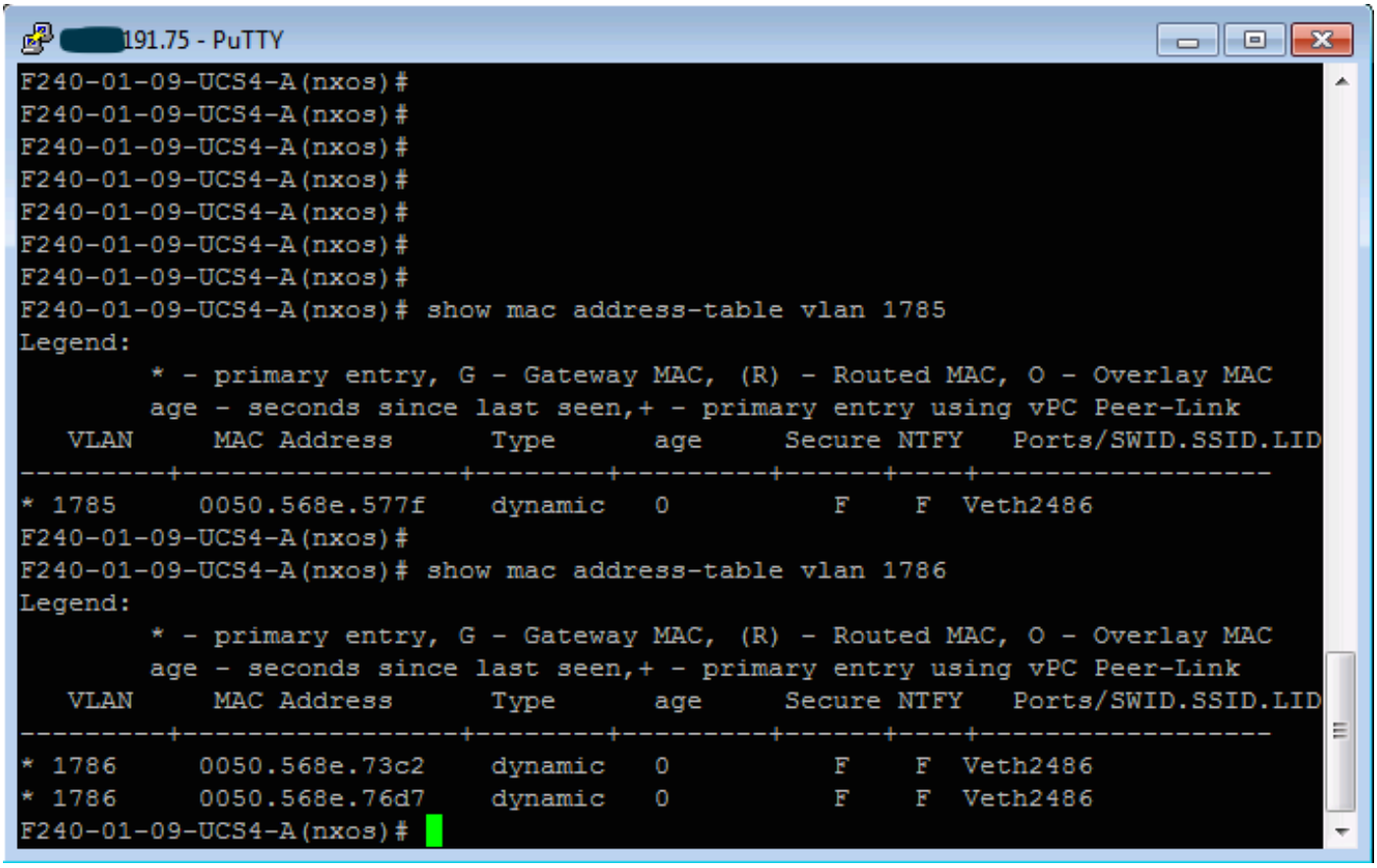
이 절차에서는 PVLAN을 사용하여 VMware DVS 컨피그레이션을 테스트하는 방법에 대해 설명합니다.

1. 포트 그룹에 구성된 다른 시스템 및 프로미스큐어스 포트에서 라우터 또는 기타 장치에 대한 ping을 실행합니다.프로미스큐어스 포트를 지나 디바이스에 대한 ping은 작동해야 하며, 격리된 VLAN의 다른 디바이스에 대한 ping은 이미지에 표시된 대로 실패해야 합니다.



MAC의 학습 위치를 확인하려면 MAC 주소 테이블을 확인합니다.모든 스위치에서 MAC은 프로미스큐어스 포트가 있는 스위치를 제외한 격리된 VLAN에 있어야 합니다.프로미스큐어스 스위치에서 MAC은 기본 VLAN에 있어야 합니다.

2. 이미지에 표시된 UCS



3. 업스트림 n5k에서 동일한 MAC을 확인합니다. 이전 출력과 유사한 출력이 n5k에 있어야 하고 이미지에 표시된 대로 있어야 합니다.

```
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#
```

업스트림 N5k에서 프로미스큐어스 포트가 포함된 Nexus 1000v를 사용한 컨피그레이션

UCS 컨피그레이션

UCS 컨피그레이션(서비스 프로파일 vNIC 컨피그레이션 포함)은 VMware DVS의 예와 동일하게 유지됩니다.

N1k 컨피그레이션

```
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
```

이 절차에서는 컨피그레이션을 테스트하는 방법을 설명합니다.

1. 포트 그룹에 구성된 다른 시스템 및 프로미스큐어스 포트에서 라우터 또는 기타 장치에 대한 ping을 실행합니다.프로미스큐어스 포트를 지나 디바이스에 대한 ping은 작동해야 하지만, 이전 섹션과 이미지에 표시된 것처럼 격리된 VLAN의 다른 디바이스에 대한 ping은 실패해야 합니다.