

Configurazione di VLAN private e Cisco UCS prima della versione 2.2(2C)

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Teoria](#)

[Implementazione di PVLAN in UCS](#)

[Obiettivo](#)

[Configurazione](#)

[Diagrammi di rete](#)

[PVLAN su vSwitch: PVLAN isolata con porta promiscua su un dispositivo upstream](#)

[Configurazione in UCS](#)

[Configurazione dei dispositivi upstream](#)

[Risoluzione dei problemi](#)

[PVLAN isolata su N1K con porta promiscua su un dispositivo upstream](#)

[Configurazione in UCS](#)

[Configurazione dei dispositivi upstream](#)

[Configurazione di N1K](#)

[Risoluzione dei problemi](#)

[PVLAN isolata su N1K con porta promiscua sul profilo della porta uplink N1K](#)

[Configurazione in UCS](#)

[Configurazione dei dispositivi upstream](#)

[Configurazione di N1K](#)

[Risoluzione dei problemi](#)

[Community PVLAN su N1K con porta promiscua sul profilo della porta uplink N1K](#)

[Risoluzione dei problemi](#)

[PVLAN isolata e PVLAN della community su porta promiscua VMware DVS su DVS](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

Questo documento descrive il supporto di VLAN private (PVLAN) nel Cisco Unified Computing System (UCS), una funzione introdotta nella release 1.4 di Cisco UCS Manager (UCS Manager). Descrive inoltre le funzionalità, le avvertenze e la configurazione quando si utilizzano le PVLAN in un ambiente UCS.

QUESTO DOCUMENTO DEVE ESSERE UTILIZZATO CON UCSM VERSIONE 2.2(2C) E VERSIONI PRECEDENTI. Nelle versioni successive alla 2.2(2C), sono state apportate modifiche

a UCSM e ESXi DVS è supportato. Sono inoltre state apportate modifiche al funzionamento dell'assegnazione di tag per la scheda di interfaccia di rete PVLAN.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Teoria

Una VLAN privata è una VLAN configurata per l'isolamento L2 da altre porte nell'ambito della stessa VLAN privata. Le porte che appartengono a una PVLAN sono associate a un set comune di VLAN di supporto, che vengono utilizzate per creare la struttura della PVLAN.

Sono disponibili tre tipi di porte PVLAN:

- Una **porta promiscua** comunica con tutte le altre porte PVLAN e è la porta utilizzata per comunicare con i dispositivi esterni alla PVLAN.
- Una **porta isolata** ha una separazione L2 completa (inclusi i broadcast) da altre porte nell'ambito della stessa PVLAN, ad eccezione della porta promiscua.
- Una **porta della community** può comunicare con altre porte della stessa PVLAN e della porta promiscua. Le porte della community sono isolate sull'L2 dalle porte di altre community o dalle porte PVLAN isolate. Le trasmissioni vengono propagate solo ad altri porti della comunità e alla porta promiscua.

Per ulteriori informazioni, fare riferimento alla [RFC 5517 - VLAN private di Cisco Systems: Sicurezza scalabile in un ambiente multi-client](#) per comprendere la teoria, il funzionamento e i concetti delle PVLAN.

Implementazione di PVLAN in UCS

UCS assomiglia molto all'architettura Nexus 5000/2000, dove Nexus 5000 è analogo a UCS 6100 e Nexus 2000 a UCS 2104 Fabric Extender.

Molte limitazioni della funzionalità PVLAN in UCS sono causate dalle limitazioni rilevate nell'implementazione di Nexus 5000/2000.

Punti importanti da ricordare sono:

- In UCS sono supportate solo porte isolate. Con il modello N1K incorporato, è possibile utilizzare VLAN di comunità, ma la porta promiscua deve trovarsi anche sul modello N1K.
- Non è disponibile il supporto per porte/trunk promiscui, porte/trunk di comunità o trunk isolati.
- Le porte promiscue devono essere esterne al dominio UCS, ad esempio uno switch/router a monte o un N1K a valle.

Obiettivo

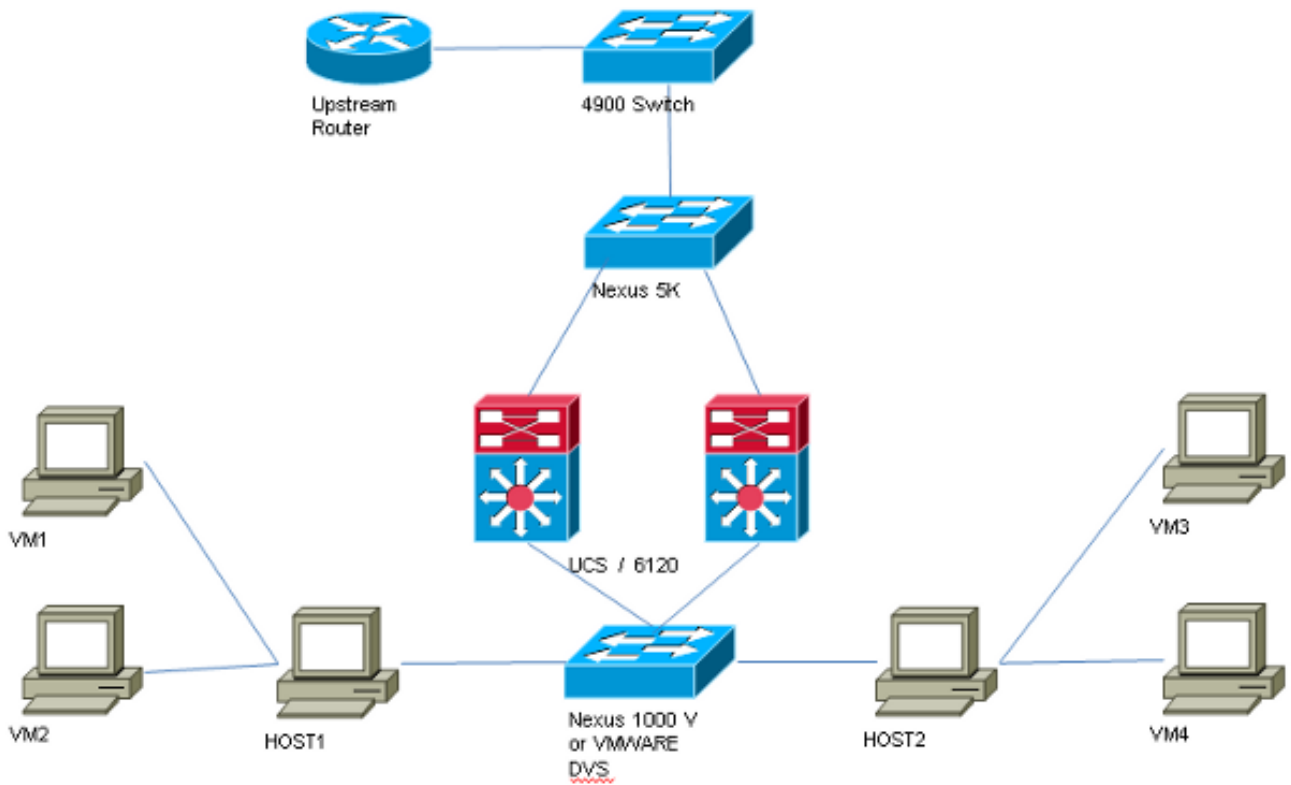
Questo documento descrive diverse configurazioni disponibili per le PVLAN con UCS:

1. PVLAN isolata con porta promiscua su un dispositivo upstream.
2. PVLAN isolata su N1K con porta promiscua su un dispositivo upstream.
3. PVLAN isolata su N1K con porta promiscua sul profilo della porta uplink N1K
4. Community PVLAN su N1K con porta promiscua sul profilo della porta uplink N1K.
5. PVLAN isolata su porta promiscua VMware Distributed Virtual Switch (DVS) su DVS.
6. PVLAN della community su porta promiscua dello switch VMware DVS su DVS.

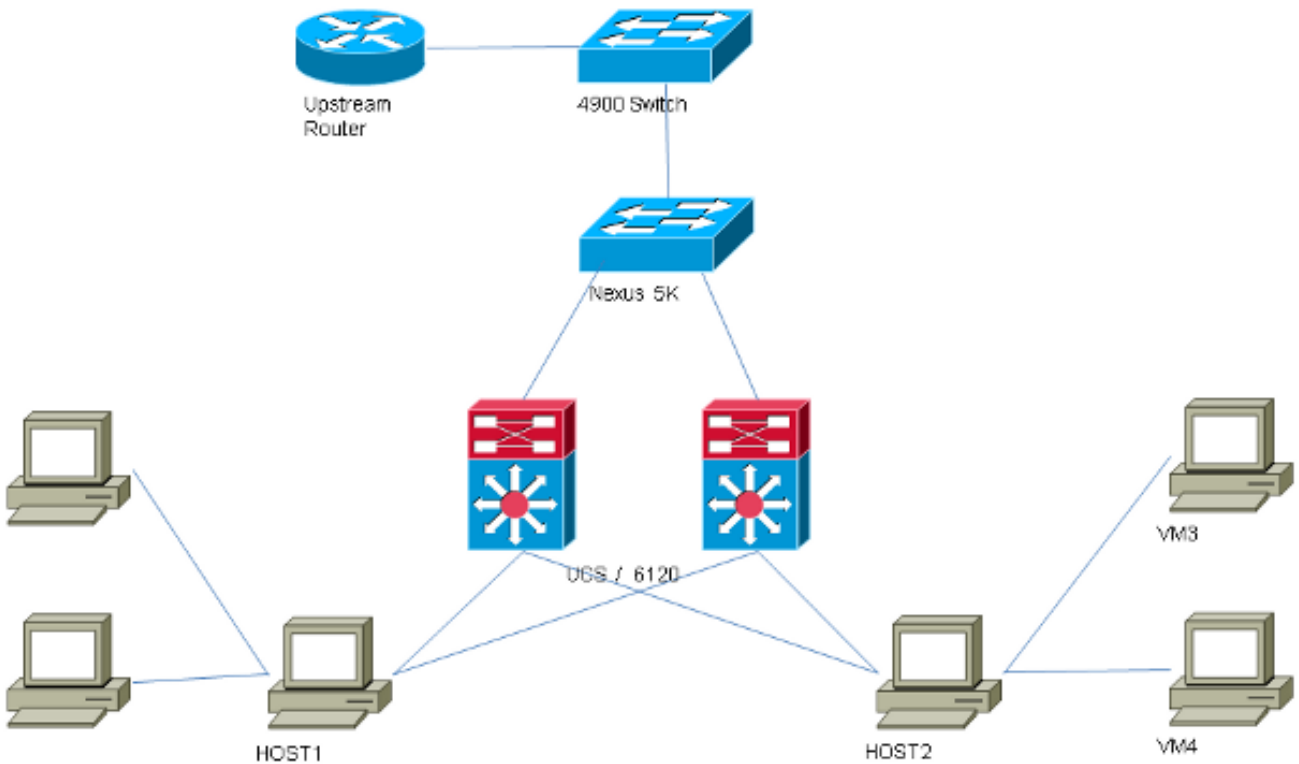
Configurazione

Diagrammi di rete

Di seguito è riportata la topologia di tutti gli esempi di switch distribuiti:



La topologia per tutti gli esempi senza switch distribuito è:



PVLAN su vSwitch: PVLAN isolata con porta promiscua su un dispositivo upstream

In questa configurazione, il traffico PVLAN viene trasmesso tramite UCS a una porta promiscua situata a monte. Poiché non è possibile inviare le VLAN primaria e secondaria sulla stessa vNIC, è

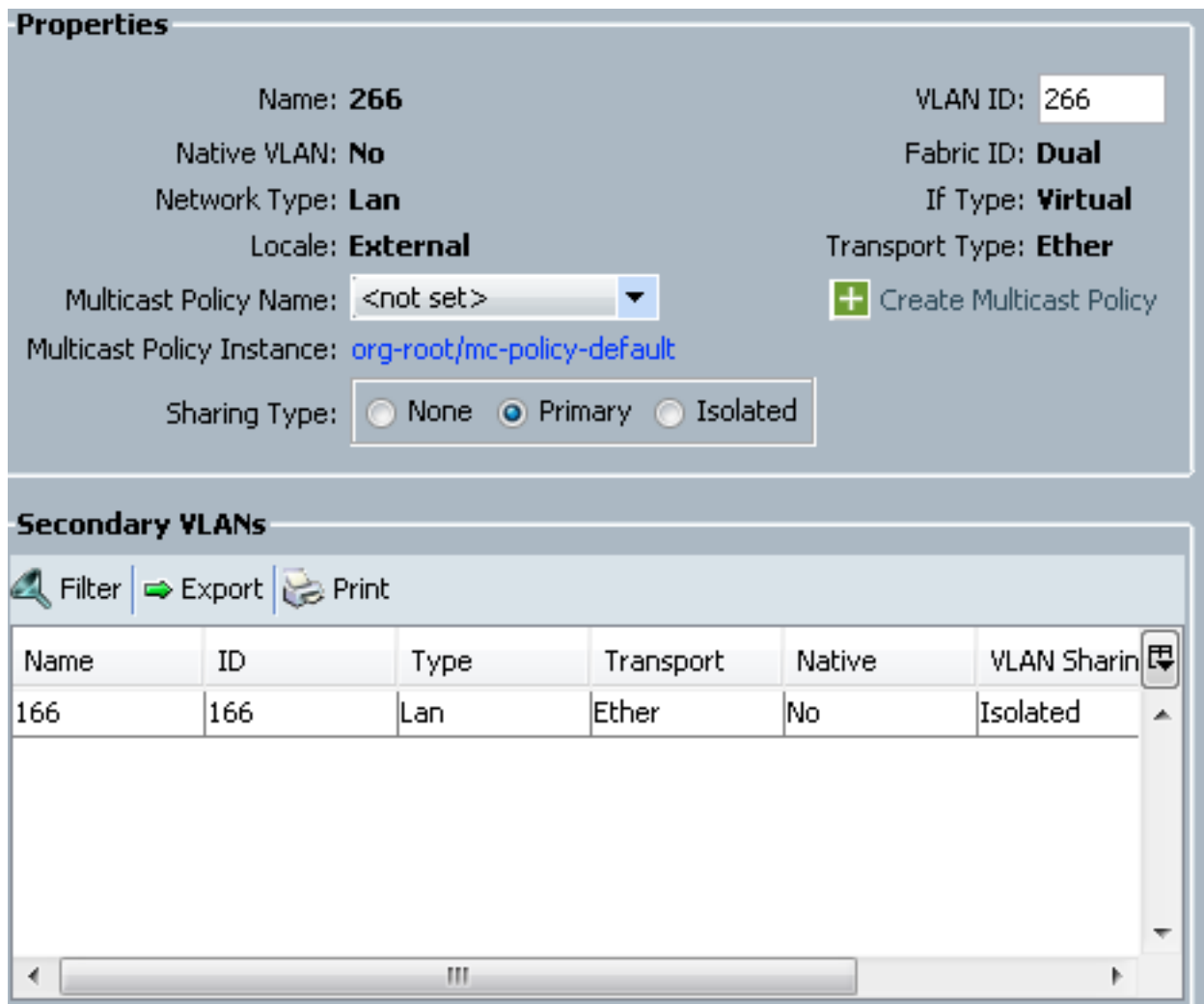
necessario un vNIC per ciascun blade per ciascuna PVLAN, per trasmettere il traffico PVLAN.

Configurazione in UCS

In questa procedura viene descritto come creare le VLAN primaria e quelle isolate.

Nota: In questo esempio si utilizza 266 come database primario e 166 come database isolato; gli ID VLAN saranno determinati dal sito.

1. Per creare la VLAN primaria, fare clic su **Primario** come tipo di condivisione, quindi immettere un **ID VLAN** di 266:



The screenshot displays the configuration interface for a VLAN in UCS. 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
- Buttons: + Create Multicast Policy

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

| Name | ID | Type | Transport | Native | VLAN Sharin |
|------|-----|------|-----------|--------|-------------|
| 166 | 166 | Lan | Ether | No | Isolated |

2. Per creare la VLAN isolata, fare clic su **Isolata** come tipo di condivisione, immettere un **ID VLAN** di 166 e scegliere **VLAN 266 (266)** come VLAN primaria:

Properties

Name: **166** VLAN ID:

Native VLAN: **No** Fabric ID: **Dual**

Network Type: **Lan** If Type: **Virtual**

Locale: **External** Transport Type: **Ether**

Sharing Type: None Primary Isolated Primary VLAN:

Primary VLAN Properties

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:

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

- Per aggiungere la VLAN alla scheda vNIC, selezionare la casella di controllo **Select** (Seleziona) per la VLAN 166 e fare clic sul pulsante di opzione **Native VLAN** associato.

Modify VLANs

| Select | Name | Native VLAN |
|-------------------------------------|--------------|----------------------------------|
| <input type="checkbox"/> | default | <input type="radio"/> |
| <input type="checkbox"/> | 1233 | <input type="radio"/> |
| <input type="checkbox"/> | 1234 | <input type="radio"/> |
| <input type="checkbox"/> | 124 | <input type="radio"/> |
| <input type="checkbox"/> | 126 | <input type="radio"/> |
| <input checked="" type="checkbox"/> | 166 | <input checked="" type="radio"/> |
| <input type="checkbox"/> | 266 | <input type="radio"/> |
| <input type="checkbox"/> | 777 | <input type="radio"/> |
| <input type="checkbox"/> | Tbeaudre_177 | <input type="radio"/> |
| <input type="checkbox"/> | Tbeaudre_277 | <input type="radio"/> |
| <input type="checkbox"/> | Tbeaudre_377 | <input type="radio"/> |
| <input type="checkbox"/> | vlan_51 | <input type="radio"/> |

Viene aggiunta solo la VLAN isolata, deve essere impostata come principale e può essercene solo una per ciascuna vNIC. Poiché la VLAN nativa è definita qui, non configurare il tagging VLAN sui gruppi di porte VMware.

Configurazione dei dispositivi upstream

Queste procedure descrivono come configurare un Nexus 5K in modo da passare la PVLAN a uno switch 4900 a monte con porta promiscua. Questa configurazione potrebbe non essere necessaria in tutti gli ambienti, ma deve essere utilizzata nel caso in cui si debba passare la PVLAN su un altro switch.

Sul Nexus 5K, immettere questi comandi e controllare la configurazione uplink:

1. Attivare la funzione PVLAN:

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

2. Aggiungere le VLAN come principali e isolate:

```
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. Associare la VLAN 266 alla VLAN 166 isolata:

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

4. Verificare che tutti gli uplink siano configurati per il trunk delle VLAN:

```
interfaccia Ethernet1/1 descrizione Connessione a 4900switchport mode trunk speed
1000interfaccia Ethernet1/3 descrizione Connessione alla porta FIB 5switchport mode
trunk speed 1000interfaccia Ethernet1/4 descrizione Connessione alla porta FIA 5switchport
mode trunk speed 1000
```

Sullo switch 4900, eseguire queste operazioni e configurare la porta promiscua. La PVLAN termina sulla porta promiscua.

1. Se necessario, attivare la funzione PVLAN.
2. Creare e associare le VLAN secondo le istruzioni del Nexus 5K.
3. Creare la porta promiscua sulla porta di uscita dello switch 4900. Da questo punto in poi, i pacchetti della VLAN 166 vengono visualizzati sulla VLAN 266 in questo caso.

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

Sul router upstream, creare una sottointerfaccia solo per la VLAN 266. A questo livello, i requisiti dipendono dalla configurazione di rete in uso:

1. interfaccia Gigabit Ethernet0/1.1

2. incapsulamento dot1Q 266
3. Indirizzo IP 209.165.200.225.255.255.224

Risoluzione dei problemi

In questa procedura viene descritto come eseguire il test della configurazione.

1. Configurare l'interfaccia virtuale dello switch (SVI) su ciascuno switch, in modo da poter eseguire il ping tra la SVI e la PVLAN:

```
(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. Controllare le tabelle degli indirizzi MAC per verificare dove viene appreso l'indirizzo MAC. Su tutti gli switch, l'indirizzo MAC deve essere nella VLAN isolata ad eccezione dello switch con la porta promiscua. Sullo switch promiscuo, notare che l'indirizzo MAC è nella VLAN primaria.

Sull'interfaccia fabric, l'indirizzo MAC 0050.56bd.7bef viene appreso su Veth1491:

```
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--
```

Sul Nexus 5K, l'indirizzo MAC 0050.56bd.7bef viene appreso su Eth1/4:


```

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#

```

Sullo switch 4900, l'indirizzo MAC 0050.56bd.7bef viene appreso su Gigabit Ethernet1/1:

```

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 questa configurazione, i sistemi di questa VLAN isolata non possono comunicare tra loro, ma possono comunicare con altri sistemi tramite la porta promiscua sullo switch 4900. Un problema è come configurare i dispositivi di downstream. In questo caso, si utilizza VMware e due host.

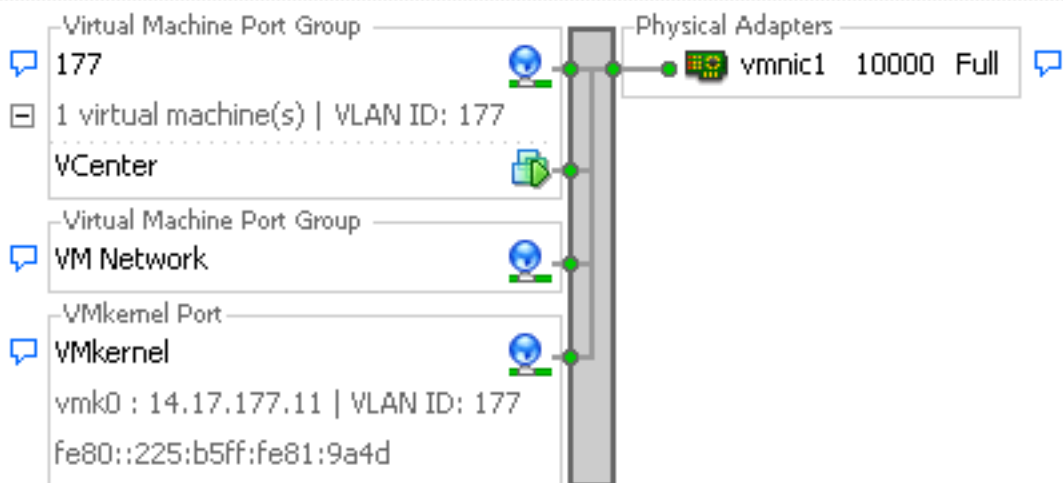
Tenere presente che è necessario utilizzare una vNIC per ciascuna PVLAN. Queste vNIC vengono presentate a VMware vSphere ESXi ed è quindi possibile creare gruppi di porte e assegnare guest a tali gruppi.

Se due sistemi vengono aggiunti allo stesso gruppo di porte sullo stesso switch, possono comunicare tra loro perché le loro comunicazioni vengono commutate localmente sullo switch vSwitch. In questo sistema, sono presenti due blade con due host ciascuno.

Sul primo sistema sono stati creati due diversi gruppi di porte, uno denominato 166 e l'altro denominato 166A. Ciascuna di esse è connessa a una singola NIC, configurata nella VLAN isolata sull'UCS. Attualmente esiste un solo guest per ogni gruppo di porte. In questo caso, poiché sono separati su ESXi, non possono comunicare tra loro.

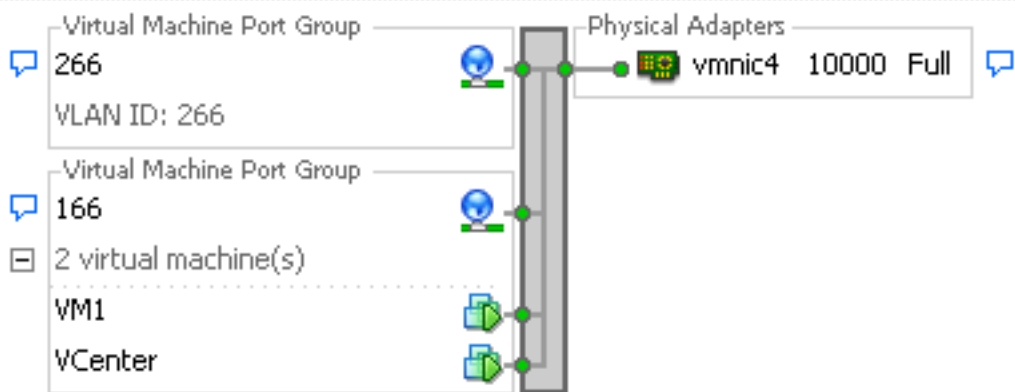
Standard Switch: vSwitch0

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



Standard Switch: vSwitch1

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



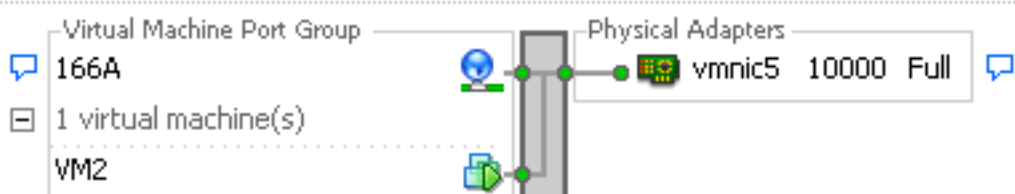
Standard Switch: vSwitch2

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



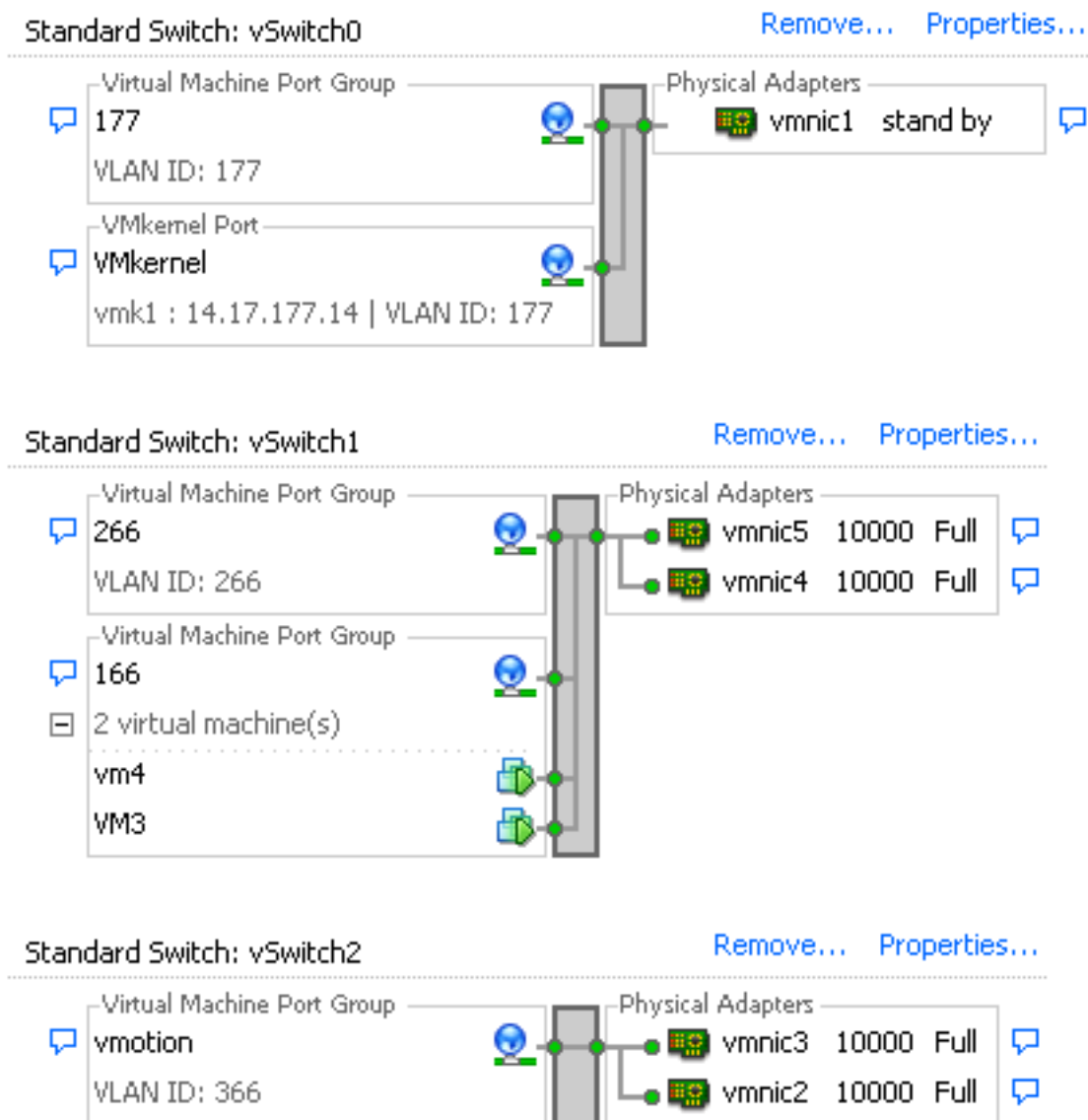
Standard Switch: vSwitch3

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



Sul secondo sistema, esiste un solo gruppo di porte chiamato 166. Ci sono due ospiti in questo gruppo di porte. In questa configurazione, VM3 e VM4 possono comunicare tra loro anche se non si desidera che ciò accada. Per risolvere questo problema, è necessario configurare una singola scheda NIC per ciascuna macchina virtuale (VM) presente nella VLAN isolata e quindi creare un gruppo di porte collegato alla vNIC. Una volta configurata questa opzione, inserire un solo guest

nel gruppo di porte. Questo non è un problema con l'installazione BMR di Windows in quanto non si dispone di questi vSwitch sottostanti.



PVLAN isolata su N1K con porta promiscua su un dispositivo upstream

In questa configurazione, il traffico PVLAN viene trasmesso attraverso un N1K e quindi l'UCS a una porta promiscua a monte. Poiché non è possibile inviare le VLAN primaria e secondaria sulla stessa vNIC, è necessaria una vNIC per ciascun uplink PVLAN per trasportare il traffico PVLAN.

Configurazione in UCS

In questa procedura viene descritto come creare le VLAN primaria e quelle isolate.

Nota: In questo esempio si utilizza 266 come database primario e 166 come database isolato; gli ID VLAN saranno determinati dal sito.

1. Per creare la VLAN primaria, fare clic su **Primario** come tipo di condivisione:

Properties

Name: **266** VLAN ID:
Native VLAN: **No** Fabric ID: **Dual**
Network Type: **Lan** If Type: **Virtual**
Locale: **External** Transport Type: **Ether**
Multicast Policy Name:
Multicast Policy Instance: [org-root/mc-policy-default](#)
Sharing Type: None Primary Isolated

Secondary VLANs

| |

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

2. Per creare la VLAN isolata, fare clic su **Isolata** come tipo di condivisione:

Properties

| | |
|--------------------------|---|
| Name: 166 | VLAN ID: <input type="text" value="166"/> |
| Native VLAN: No | Fabric ID: Dual |
| Network Type: Lan | If Type: Virtual |
| Locale: External | Transport Type: Ether |

Sharing Type: None Primary Isolated Primary VLAN:

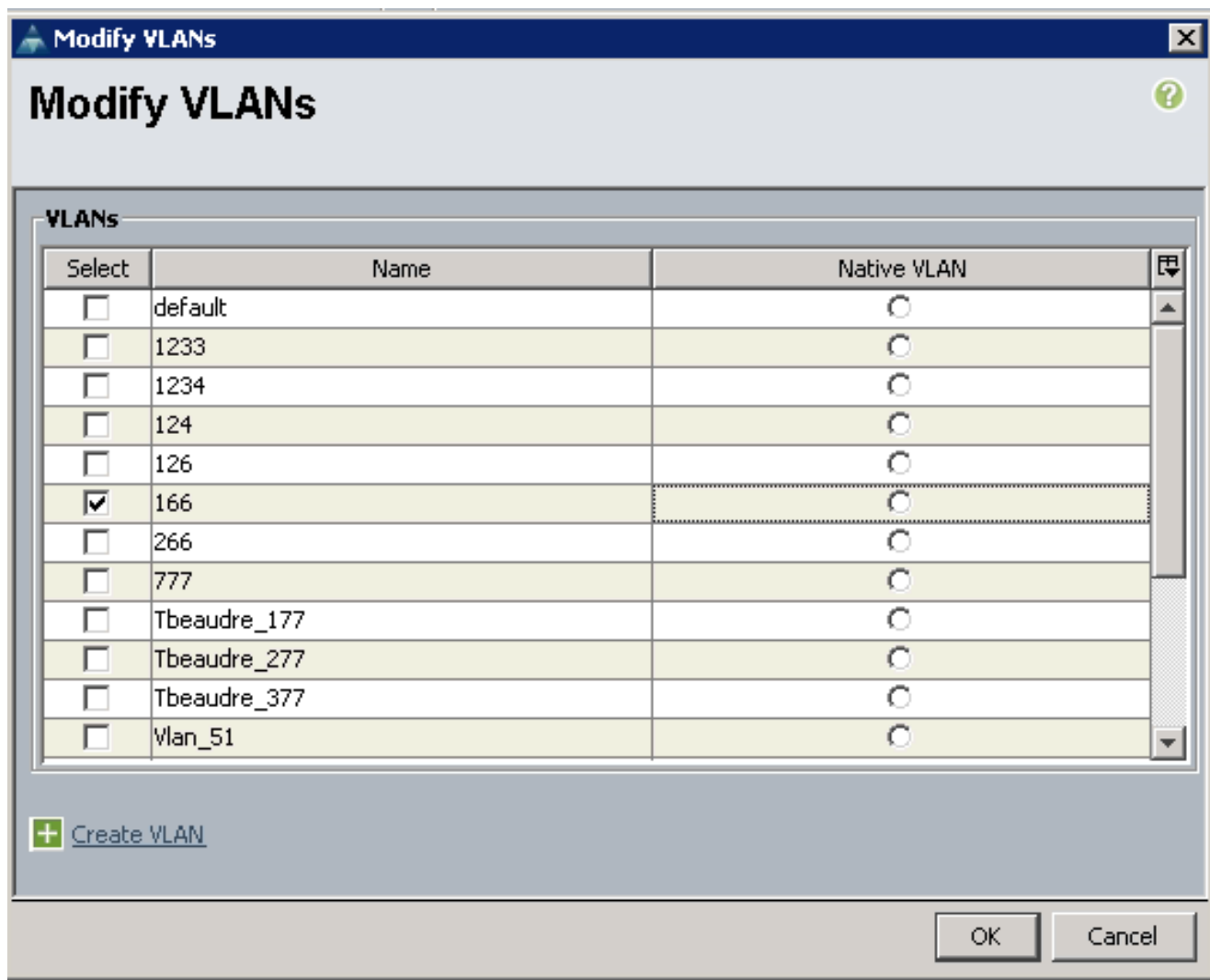
Primary VLAN Properties

| | |
|--------------------------|------------------------------|
| 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:

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

3. Per aggiungere la VLAN alla scheda vNIC, fare clic sulla casella di controllo **Select** (Seleziona) per la VLAN 166. Per la VLAN 166 non è selezionata la VLAN nativa.



Viene aggiunta solo la VLAN isolata, non deve essere impostata come nativa e può essercene solo una per ciascuna vNIC. Poiché la VLAN nativa non è definita qui, contrassegnare la VLAN nativa sull'N1K. L'opzione per contrassegnare una VLAN nativa non è disponibile nei DVS VMware, pertanto non è supportata nei DVS.

Configurazione dei dispositivi upstream

Queste procedure descrivono come configurare un Nexus 5K in modo da passare la PVLAN a uno switch 4900 a monte con porta promiscua. Questa configurazione potrebbe non essere necessaria in tutti gli ambienti, ma deve essere utilizzata nel caso in cui si debba passare la PVLAN su un altro switch.

Sul Nexus 5K, immettere questi comandi e controllare la configurazione uplink:

1. Attivare la funzione PVLAN:

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

2. Aggiungere le VLAN come principali e isolate:

```
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. Associare la VLAN 266 alla VLAN 166 isolata:

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

4. Verificare che tutti gli uplink siano configurati per il trunk delle VLAN:

```
interfaccia Ethernet1/1 descrizione Connessione a 4900 switchport mode trunk speed
1000
interfaccia Ethernet1/3 descrizione Connessione alla porta FIB 5 switchport mode
trunk speed 1000
interfaccia Ethernet1/4 descrizione Connessione alla porta FIA 5 switchport
mode trunk speed 1000
```

Sullo switch 4900, eseguire queste operazioni e configurare la porta promiscua. La PVLAN termina sulla porta promiscua.

1. Se necessario, attivare la funzione PVLAN.
2. Creare e associare le VLAN secondo le istruzioni del Nexus 5K.
3. Creare la porta promiscua sulla porta di uscita dello switch 4900. Da questo punto in poi, i pacchetti della VLAN 166 vengono visualizzati sulla VLAN 266 in questo caso.

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

Sul router upstream, creare una sottointerfaccia solo per la VLAN 266. A questo livello, i requisiti dipendono dalla configurazione di rete utilizzata:

1. interfaccia Gigabit Ethernet0/1.1
2. incapsulamento dot1Q 266
3. Indirizzo IP 209.165.200.225.255.255.255.224

Configurazione di N1K

In questa procedura viene descritto come configurare l'N1K come trunk standard, non come trunk PVLAN.

1. Creare e associare le VLAN secondo le istruzioni del Nexus 5K. Per ulteriori informazioni, consultare la sezione [Configurazione dei dispositivi upstream](#).
2. Creare un profilo di porta uplink per il traffico PVLAN:

```
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. Creare il gruppo di porte per la VLAN isolata; creare una porta host PVLAN con l'associazione host per le VLAN primaria e isolata:


```

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

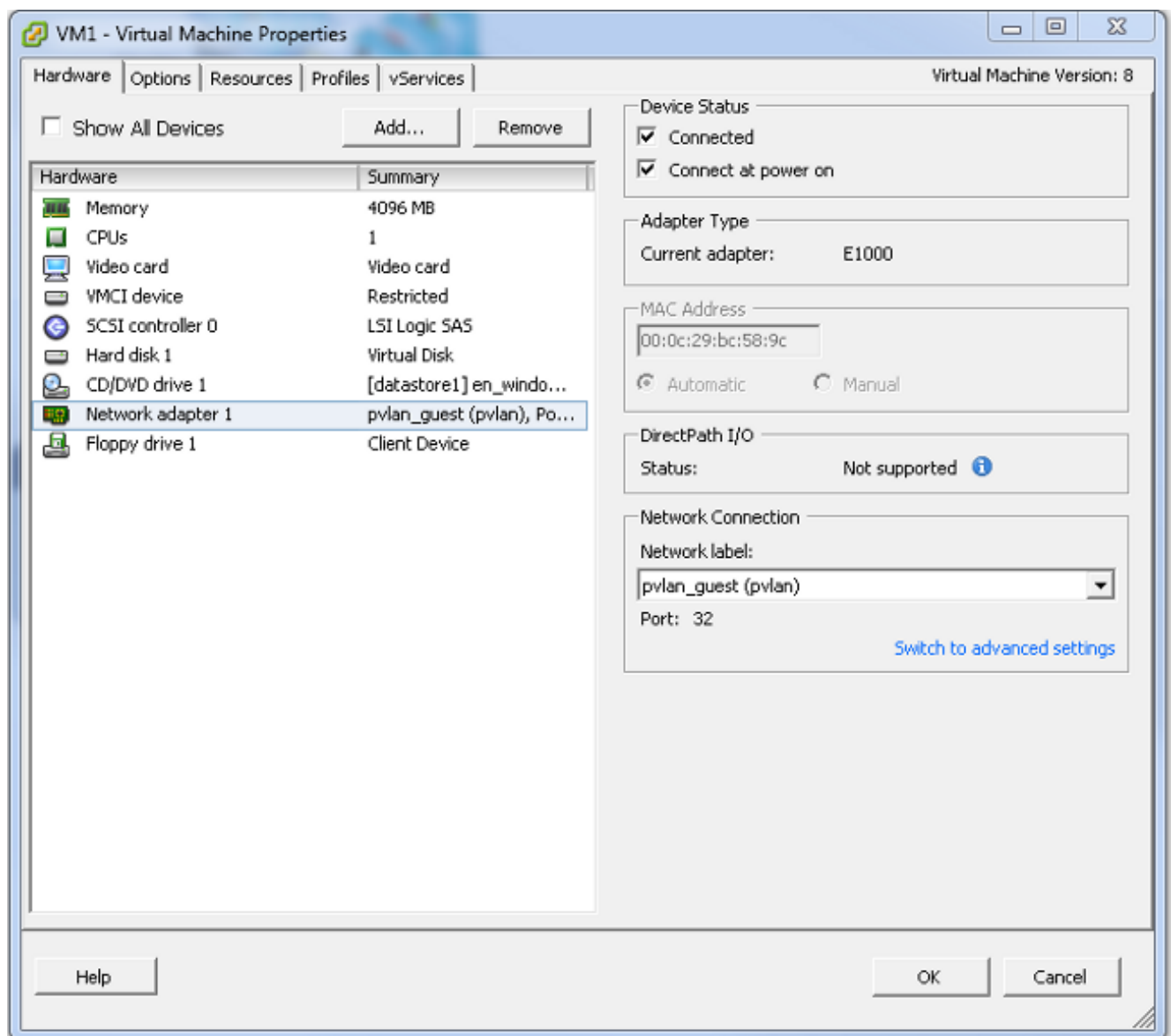
```

4. Nel vCenter, aggiungere la vNIC corretta all'uplink della PVLAN. La vNIC a cui è stata aggiunta la VLAN isolata nella configurazione nelle impostazioni UCS.

| | | | | | |
|-------------------------------------|--|--------|-------|---------------------------------|-----------------------------|
| <input type="checkbox"/> | | vmnic3 | -- | View Details... | Select an uplink port gr... |
| <input checked="" type="checkbox"/> | | vmnic4 | pvlan | View Details... | pvlan_uplink |
| <input type="checkbox"/> | | vmnic5 | -- | View Details... | Select an uplink port gr... |

5. Aggiungere la VM al gruppo di porte corretto:

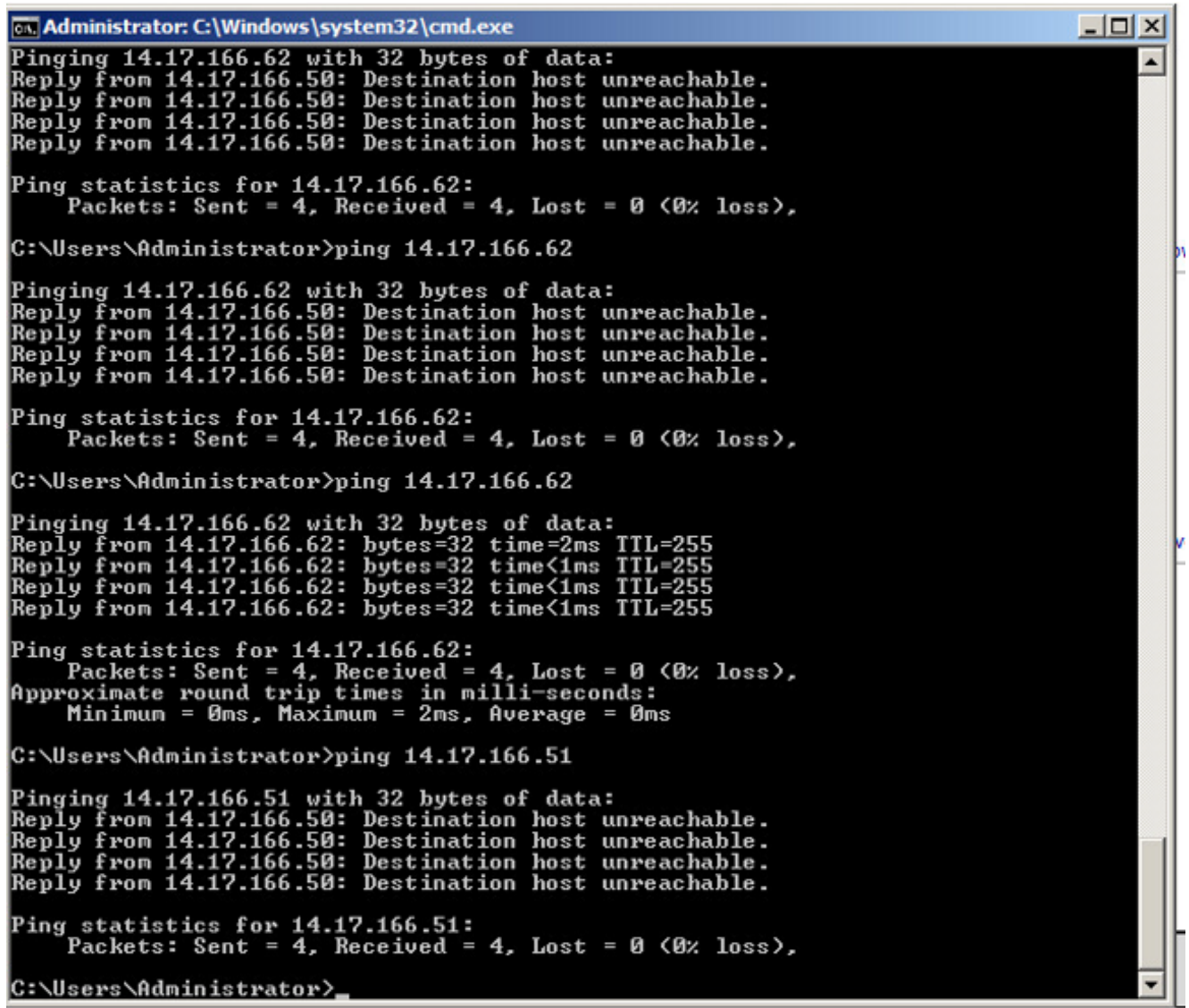
Nella scheda Hardware, fare clic su **Scheda di rete 1**. Scegliere **pvlan_guest (pvlan)** per l'etichetta Rete in Connessione di rete:



Risoluzione dei problemi

In questa procedura viene descritto come eseguire il test della configurazione.

1. Eseguire i ping su altri sistemi configurati nel gruppo di porte e sul router o su un altro dispositivo della porta promiscua. I ping verso il dispositivo oltre la porta promiscua dovrebbero funzionare, mentre quelli verso altri dispositivi nella VLAN isolata dovrebbero guastarsi.



```
C:\Windows\system32\cmd.exe
Pinging 14.17.166.62 with 32 bytes of data:
Reply from 14.17.166.50: Destination host unreachable.
Reply from 14.17.166.50: Destination host unreachable.
Reply from 14.17.166.50: Destination host unreachable.
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.
Reply from 14.17.166.50: Destination host unreachable.
Reply from 14.17.166.50: Destination host unreachable.
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.
Reply from 14.17.166.50: Destination host unreachable.
Reply from 14.17.166.50: Destination host unreachable.
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. Sulla N1K, le VM sono elencate sulla VLAN principale; questo si verifica perché le porte host PVLAN associate alla PVLAN sono attive. A causa di come vengono apprese le VM, verificare di non impostare la PVLAN come nativa sul sistema UCS. Notare anche che il dispositivo upstream viene ricavato dal canale della porta e che il dispositivo upstream viene acquisito anche sulla VLAN primaria. Per questo motivo, la VLAN primaria è la VLAN nativa sull'uplink PVLAN.

In questa schermata, i due dispositivi su Veth3 e Veth 4 sono le VM. Il dispositivo sul Po1 è il router upstream che è oltre la porta promiscua.

```

pvlan# 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    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. Sul sistema UCS, è necessario imparare tutti gli MAC, per questa comunicazione, nella VLAN isolata. La parte a monte non dovrebbe essere visualizzata:

```

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. Sul Nexus 5K, le due VM si trovano sulla VLAN isolata, mentre il dispositivo upstream si trova sulla VLAN primaria:

```

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. Sullo switch 4900, dove si trova la porta promiscua, tutto si trova sulla VLAN primaria:

| 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 |

PVLAN isolata su N1K con porta promiscua sul profilo della porta uplink N1K

In questa configurazione, il traffico PVLAN diretto alla VLAN N1K è contenuto e viene usata solo la VLAN principale a monte.

Configurazione in UCS

In questa procedura viene descritto come aggiungere la VLAN primaria alla vNIC. Non è necessaria la configurazione della PVLAN in quanto è sufficiente la VLAN principale.

Nota: In questo esempio si utilizza 266 come database primario e 166 come database isolato; gli ID VLAN saranno determinati dal sito.

1. Il tipo di condivisione è **Nessuno (None)**.

The screenshot shows the UCS configuration interface for VLAN 266. The breadcrumb navigation is: >> LAN > LAN Cloud > VLANs > VLAN 266 (266). The interface has tabs for General, Org Permissions, VLAN Group Membership, Faults, and Events. The 'General' tab is active.

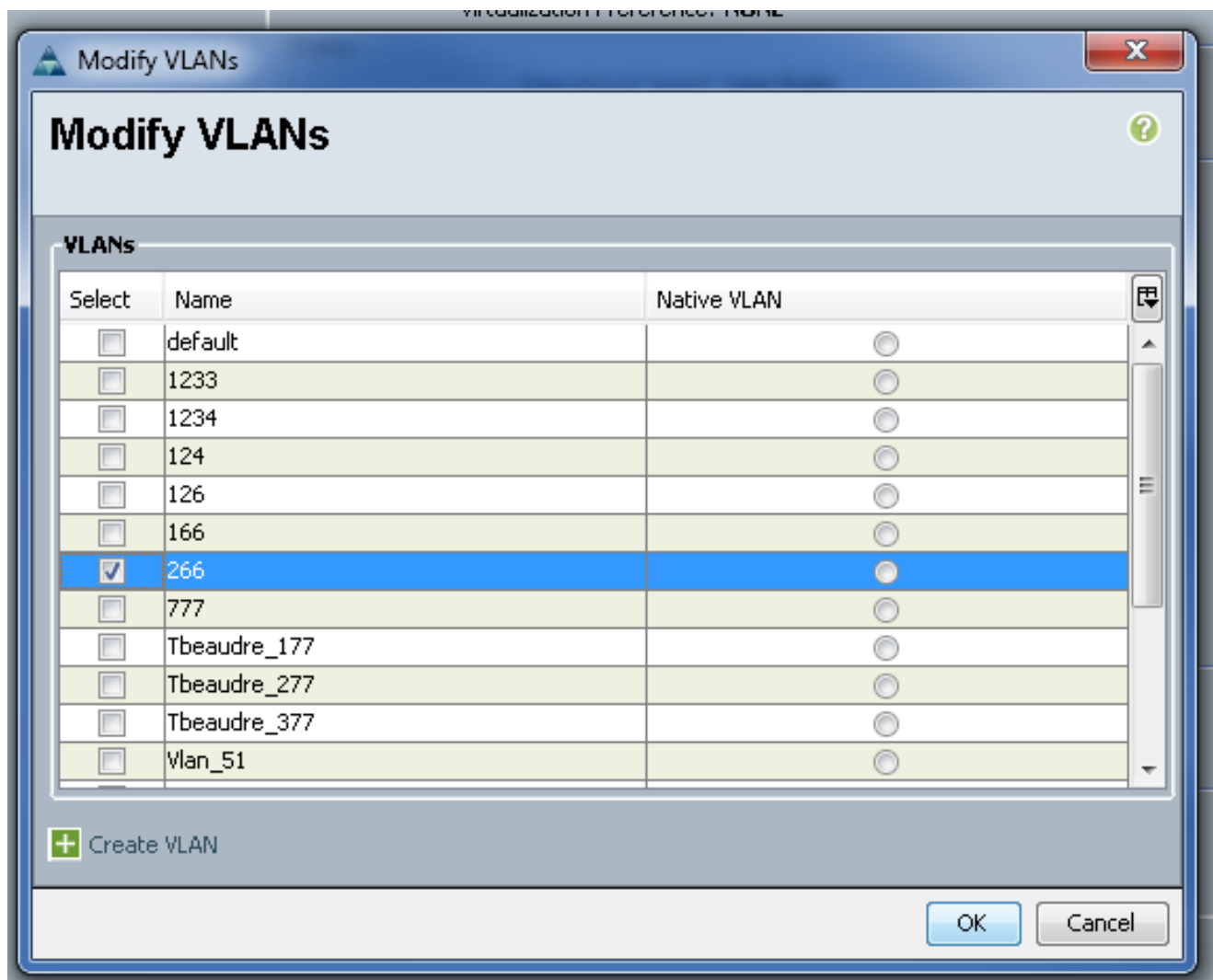
Fault Summary: Shows four status icons (Red X, Yellow Triangle, Yellow Triangle, Green Triangle) with a count of 0 for each.

Actions: Includes 'Modify VLAN Org Permissions' and 'Delete'.

Properties:

- 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: None Primary Isolated
- VLAN ID: 266
- Fabric ID: Dual
- If Type: Virtual
- Transport Type: Ether
- + Create Multicast Policy

2. Per aggiungere la VLAN primaria alla vNIC, selezionare la casella di controllo **Select** (Seleziona) per la VLAN 266. Non impostarlo come nativo.



Configurazione dei dispositivi upstream

Queste procedure descrivono come configurare i dispositivi upstream. In questo caso, gli switch a monte hanno bisogno solo di porte trunk e solo di una VLAN 266 perché è l'unica VLAN rilevata dagli switch a monte.

Sul Nexus 5K, immettere questi comandi e controllare la configurazione uplink:

1. Aggiungere la VLAN come principale:

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

2. Verificare che tutti gli uplink siano configurati per il trunk delle VLAN:

```
interfaccia Ethernet1/1descrizione Connessione a 4900switchport mode trunkspeed 1000interfaccia Ethernet1/3descrizione Connessione alla porta FIB 5switchport mode trunkspeed 1000interfaccia Ethernet1/4descrizione Connessione alla porta FIA 5switchport mode trunkspeed 1000
```

Sullo switch 4900, procedere come segue:

1. Creare le VLAN usate come primarie sulla scheda N1K.
2. Trunk di tutte le interfacce verso e dallo switch 4900 in modo che la VLAN venga passata.

Sul router upstream, creare una sottointerfaccia solo per la VLAN 266. A questo livello, i requisiti dipendono dalla configurazione di rete utilizzata.

1. interfaccia Gigabit Ethernet0/1.1
2. incapsulamento dot1Q 266
3. Indirizzo IP 209.165.200.225.255.255.255.224

Configurazione di N1K

In questa procedura viene descritto come configurare il modello N1K.

1. Creare e associare le VLAN:

```
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. Creare un profilo di porta uplink per il traffico PVLAN con la porta promiscua indicata di seguito:

```
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. Creare il gruppo di porte per la VLAN isolata; creare una porta host PVLAN con l'associazione host per le VLAN primaria e isolata:

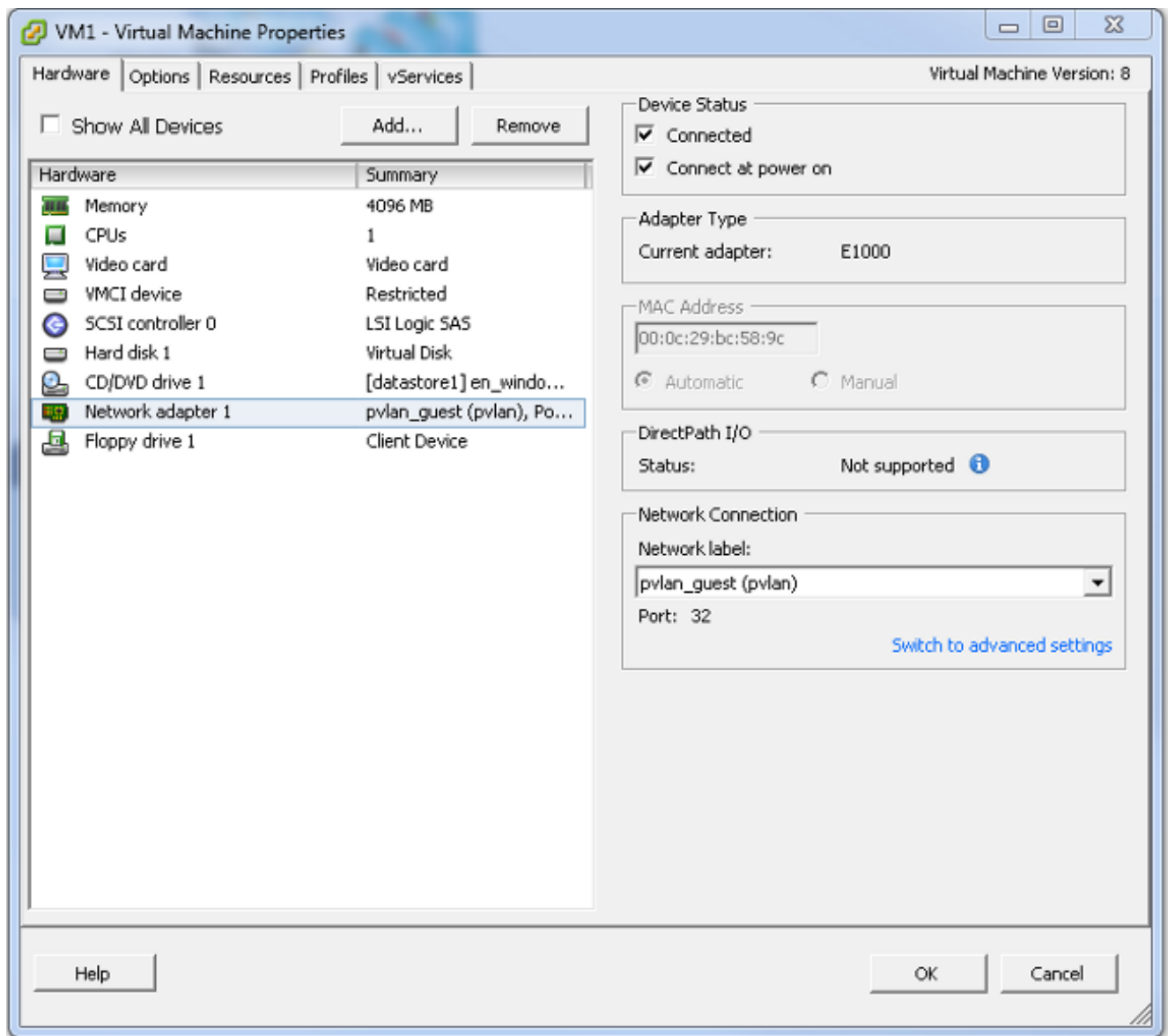
```
Switch(config)# port-profile type vethernet pvlan_guest
Switch(config-port-prof)# vmware port-group
Switch(config-port-prof)# switchport mode private-vlan host
Switch(config-port-prof)# switchport private-vlan host-association 266 166
Switch(config-port-prof)# no shut
Switch(config-port-prof)# state enabled
```

4. Nel vCenter, aggiungere la vNIC corretta all'uplink della PVLAN. La vNIC a cui è stata aggiunta la VLAN isolata nella configurazione nelle impostazioni UCS.

| | | | | |
|-------------------------------------|--|-------|---------------------------------|-----------------------------|
| <input type="checkbox"/> |  vmnic3 | -- | View Details... | Select an uplink port gr... |
| <input checked="" type="checkbox"/> |  vmnic4 | pvlan | View Details... | pvlan_uplink |
| <input type="checkbox"/> |  vmnic5 | -- | View Details... | Select an uplink port gr... |

5. Aggiungere la macchina virtuale al gruppo di porte corretto.

Nella scheda Hardware, fare clic su **Scheda di rete 1**. Scegliere **pvlan_guest (pvlan)** come etichetta di rete in Connessione di rete.



Risoluzione dei problemi

In questa procedura viene descritto come eseguire il test della configurazione.

1. Eseguire i ping su altri sistemi configurati nel gruppo di porte e sul router o su un altro dispositivo della porta promiscua. I ping verso il dispositivo oltre la porta promiscua dovrebbero funzionare, mentre quelli verso altri dispositivi nella VLAN isolata dovrebbero guastarsi.

```

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.
Reply from 14.17.166.50: Destination host unreachable.
Reply from 14.17.166.50: Destination host unreachable.
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. Sulla N1K, le VM sono elencate sulla VLAN principale; questo si verifica perché le porte host PVLAN associate alla PVLAN sono attive. Notare anche che il dispositivo upstream viene ricavato dal canale della porta e che il dispositivo upstream viene acquisito anche sulla VLAN primaria.

In questa schermata, i due dispositivi su Veth3 e Veth 4 sono le VM. Il dispositivo su Po1 è il dispositivo a monte che supera la porta promiscua.

```

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. Sul sistema UCS, si dovrebbero imparare tutti gli MAC, per questa comunicazione, nella VLAN primaria usata sulla N1K. Non dovresti imparare a monte qui:


```
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. Sul Nexus 5K, tutti gli MAC sono nella VLAN primaria selezionata:

```
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. Sullo switch 4900, tutto si trova sulla VLAN primaria selezionata:

```
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 su N1K con porta promiscua sul profilo della porta uplink N1K

Questa è l'unica configurazione supportata per le VLAN di comunità con UCS.

Questa configurazione è la stessa di quella configurata nella sezione [Isolated PVLAN on N1K with Promiscuous Port on the N1K Uplink Port-Profile](#). L'unica differenza tra community e isolato è la configurazione della PVLAN.

Per configurare il modello N1K, creare e associare le VLAN come per il modello Nexus 5K:

```
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
```

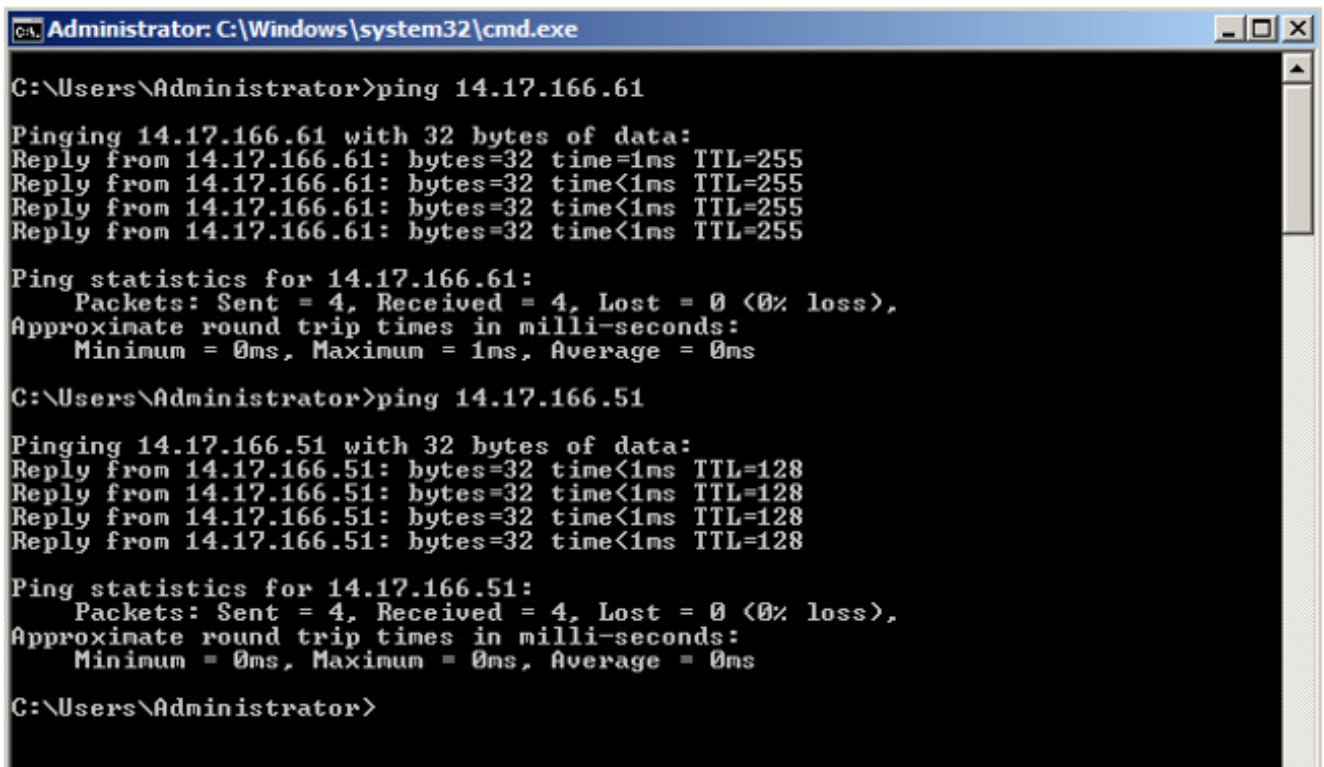
Tutte le altre configurazioni sono uguali alla PVLAN isolata su N1K con porta promiscua sul profilo di porta uplink N1K.

Una volta configurata questa opzione, è possibile comunicare con tutte le VM connesse al profilo di porta vEthernet utilizzato per la PVLAN.

Risoluzione dei problemi

In questa procedura viene descritto come eseguire il test della configurazione.

1. Eseguire i ping su altri sistemi configurati nel gruppo di porte e sul router o su un altro dispositivo della porta promiscua. I ping oltre il porto promiscuo e verso altri sistemi nella comunità dovrebbero funzionare.



```
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
Reply from 14.17.166.51: bytes=32 time<1ms TTL=128
Reply from 14.17.166.51: bytes=32 time<1ms TTL=128
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. Tutte le altre procedure per la risoluzione dei problemi sono uguali a quelle della [PVLAN isolata](#).

PVLAN isolata e PVLAN della community su porta promiscua VMware DVS su DVS

A causa dei problemi di configurazione sia sul DVS che sul sistema UCS, le PVLAN con DVS e UCS non sono supportate nelle versioni precedenti alla 2.2(2c).

Verifica

Attualmente non sono disponibili procedure di verifica per queste configurazioni.

Risoluzione dei problemi

Nelle sezioni precedenti sono disponibili informazioni utili per la risoluzione dei problemi relativi alle configurazioni.

Lo [strumento Output Interpreter \(solo utenti registrati\) supporta alcuni comandi show](#). Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show**.