# 2.2(2C)之前的专用VLAN和Cisco UCS配置

### 目录

简介 先决条件 要求 使用的组件 背景信息 理论 UCS中的PVLAN实施 目标 配置 网络图 vSwitch上的PVLAN:上游设备上具有混杂端口的隔离PVLAN UCS中的配置 上游设备的配置 故障排除 N1K上的隔离PVLAN,上游设备上的混杂端口 UCS中的配置 上游设备的配置 配置N1K 故障排除 N1K上的隔离PVLAN,N1K上行链路端口配置文件上带有混杂端口 UCS中的配置 上游设备的配置 配置N1K 故障排除 N1K上的社区PVLAN,N1K上行链路端口配置文件上带有混杂端口 故障排除 VMware DVS混合端口上的隔离PVLAN和社区PVLAN 验证 故障排除

# 简介

本文档介绍思科统一计算系统(UCS)中的专用VLAN(PVLAN)支持,这是Cisco UCS Manager(UCSM)版本1.4中引入的一项功能。 它还详细说明了PVLAN在UCS环境中使用时的功能 、警告和配置。

本文档用于UCSM 2.2(2C)版和早期版本。在版本2.2(2C)以后的版本中,已对UCSM进行了更改 ,并支持ESXi DVS。标记对PVLAN网卡的工作方式也有所改变。

# 先决条件

要求

Cisco 建议您了解以下主题:

- UCS
- Cisco Nexus 1000 V(N1K)
- VMware
- 第2层(L2)交换

#### 使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

### 背景信息

#### 理论

专用VLAN是配置为与同一专用VLAN中的其他端口进行L2隔离的VLAN。属于PVLAN的端口与一组 通用的支持VLAN关联,这些VLAN用于创建PVLAN结构。

有三种类型的 PVLAN 端口:

- •混杂端口与所有其他PVLAN端口通信,是用于与PVLAN外部设备通信的端口。
- •隔离端口具有与同一PVLAN中的其他端口(包括广播)的完全L2分离(混杂端口除外)。
- **社区端口**可以与同一PVLAN中的其他端口以及混杂端口通信。在L2上,社区端口与其他社区或 隔离PVLAN端口的端口隔离。广播仅传播到团体中的其他端口和混杂端口。

请参<u>阅RFC 5517,Cisco Systems的专用VLAN:多客户端环境中的可扩展安</u>全性,以便了解 PVLAN的理论、操作和概念。

#### UCS中的PVLAN实施

UCS与Nexus 5000/2000架构非常相似,其中Nexus 5000与UCS 6100和Nexus 2000类似,与UCS 2104交换矩阵扩展器相似。

UCS中PVLAN功能的许多限制是由Nexus 5000/2000实施中的限制引起的。

需要记住的要点是:

- UCS仅支持隔离端口。使用N1K并入,您可以使用社区VLAN,但混杂端口也必须位于N1K上。
- •不支持混杂端口/中继、社区端口/中继或隔离中继。
- 混杂端口需要位于UCS域外,例如上游交换机/路由器或下游N1K。

本文档介绍适用于UCS的PVLAN的几种不同配置:

- 1. 上游设备上具有混杂端口的隔离PVLAN。
- 2. N1K上的隔离PVLAN,上游设备上的混杂端口。
- 3. N1K上的隔离PVLAN,N1K上行链路端口配置文件上的混杂端口
- 4. N1K上的社区PVLAN,N1K上行链路端口配置文件上的混杂端口。
- 5. VMware分布式虚拟交换机(DVS)混合端口上的隔离PVLAN。
- 6. VMware DVS交换机DVS上混合端口上的社区PVLAN。

## 配置

网络图

分布式交换机的所有示例的拓扑如下:



没有分布式交换机的所有示例的拓扑如下:



### vSwitch上的PVLAN:上游设备上具有混杂端口的隔离PVLAN

在此配置中,您将PVLAN流量通过UCS传递到上游的混杂端口。由于不能在同一个vNIC上同时发送主VLAN和辅助VLAN,因此每个PVLAN的每个刀片都需要一个vNIC,以传输PVLAN流量。

#### UCS中的配置

本过程介绍如何创建主VLAN和任何隔离VLAN。

注意:本示例使用266作为主要,166作为隔离;VLAN ID由站点确定。

1. 要创建主VLAN,请单击主作为共享类型,并输入VLAN ID 266:

Properties					
N	ame: <b>26</b>	6			VLAN ID: 266
Native V	LAN: No			F	abric ID: Dual
Network T	ype: La	n			If Type: Virtual
Lo	cale: Exi	ternal		Transpo	ort Type: Ether
Multicast Policy N	ame: <	not set>	-	🕂 Cre	ate Multicast Policy
Multicast Policy Insta	ince: <mark>or</mark> g	j-root/mc-po	licy-default		
Sharing T	ype: 🤇	) None 💿	Primary 🔘 Isola	ated	
	·· _				
Secondary VLANs					
🔍 Filter 📥 Export	능 Print	:			
Name ID		Туре	Transport	Native	VLAN Sharin 🖽
166 166		Lan	Ether	No	Isolated 🔺
•					

2. 要创建隔离VLAN,请单击**隔离**作为共享类型,输入**VLAN ID** 166,然后选择**VLAN** 266(266)作为主VLAN:

Properties			
Name: 166		VLAN ID:	166
Native VLAN: No		Fabric ID:	Dual
Network Type: Lan		If Type:	Virtual
Locale: External		Transport Type:	Ether
Sharing Type: 🔘 None	: 🔘 Primary 💿 Isolate	ed Primary VLAN:	VLAN 266 (266) 🛛 🔻
Primary VLAN Properti	es		
Name:	266	VLAN ID: 3	266
Native VLAN:	No	Fabric ID: I	Dual
Network Type:	Lan	If Type: <sup>y</sup>	Virtual
Locale:	External	Transport Type: I	Ether
Multicast Policy Name:	<not set=""></not>	🕂 🕂 Create Multic	ast Policy
Multicast Policy Instance:	org-root/mc-policy-defa	ult	

3. 要将VLAN添加到vNIC,请单击VLAN 166的选中复选框,然后单击关联的本征VLAN单选按钮

VLANs			
Select	Name	Native VLAN	₽
	default	©	
	1233	©	
	1234	0	
	124	©	
	126	©	=
<b>V</b>	166	۲	
	266	©	
	777	©	_
	Tbeaudre_177	©	
	Tbeaudre_277	©	
	Tbeaudre_377	©	
	Vlan_51	©	-

只添加隔离VLAN,必须将其设置为主VLAN,并且每个vNIC只能有一个。由于本征VLAN在此 处定义,因此请勿在VMware端口组上配置VLAN标记。

#### 上游设备的配置

0

这些步骤说明如何配置Nexus 5K,将PVLAN传递到混合端口所在的上游4900交换机。虽然并非所 有环境都需要此配置,但在必须通过另一台交换机传递PVLAN时,请使用此配置。

在Nexus 5K上,输入以下命令,并检查上行链路配置:

1. 打开PVLAN功能:

Nexus5000-5(config)# feature private-vlan

2. 将VLAN添加为主VLAN和隔离VLAN:

Nexus5000-5(config-vlan)# vlan 266 Nexus5000-5(config-vlan)# private-vlan primary

3. 将VLAN 266与隔离VLAN 166关联:

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

4. 确保配置所有上行链路以中继VLAN:

接口Ethernet1/1描述与4900的连接switchport mode trunkspeed 1000接口Ethernet1/3描述与 FIB端口5的连接switchport mode trunkspeed 1000接口Ethernet1/4描述与FIA端口5的连接 switchport mode trunkspeed 1000

在4900交换机上,执行以下步骤,并设置混杂端口。PVLAN在混杂端口结束。

- 1. 根据需要打开PVLAN功能。
- 2. 按照Nexus 5K上的操作创建并关联VLAN。
- 3. 在4900交换机的出口端口上创建混杂端口。从此开始,在本例中,VLAN 266上可以看到来自 VLAN 166的数据包。

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

- 在上游路由器上,仅为VLAN 266创建子接口。在此级别,要求取决于您使用的网络配置:
  - 1. interface GigabitEthernet0/1.1
  - 2. encapsulation dot1Q 266
  - 3. ip address 209.165.200.225 255.255.255.224

#### 故障排除

此步骤介绍如何测试配置。

1. 在每台交换机上配置交换机虚拟接口(SVI),这样您就可以从PVLAN ping SVI:

```
(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. 检查MAC地址表,以查看MAC的学习位置。在所有交换机上,MAC应位于隔离VLAN中,但 在具有混杂端口的交换机上除外。在混杂交换机上,请注意MAC位于主VLAN中。

在交换矩阵互联上,MAC地址0050.56bd.7bef在Veth1491上获知:

	1.000 D TTV							<b>X</b>
14.17.15	54.200 - PuTTY							~
40-31-	9-1-B(nxos)# show ma	ac address-	table					
gend:								
	* - primary entry, 0	6 - Gateway	7 MAC,	(R) - Rout	ted	MAC, O - Ov	erlay MAC	
	age - seconds since	last seen,	+ - p	rimary ent	ry u	sing vPC Pe	er-Link	
VLAN	MAC Address	Type	age	Secure	NTF	Y Ports		
	-++	++-		+	+	-+		
166	000c.29d2.495a	dynamic	80	F	F	Veth1491		
166	0025.b581.991e	static	ο	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								-
	14.17.19 40-31- gend: VLAN  166 166 266 266 177 177 177 177 177 177 177 177 177 1	14.17.154.200 - PuTTY 40-31-9-1-B(nxos) # show me gend: * - primary entry, 0 age - seconds since VLAN MAC Address 	<pre>14.17.154.200 - PuTTY 40-31-9-1-B(nxos) # show mac address- gend:</pre>	<pre>14.17.154.200 - PuTTY 40-31-9-1-B(nxos) # show mac address-table gend:</pre>	14.17.154.200 - PuTTY 40-31-9-1-B(nxos) # show mac address-table gend: * - primary entry, G - Gateway MAC, (R) - Row age - seconds since last seen, + - primary entry VLAN MAC Address Type age Secure 	14.17.154.200 - PuTTY 40-31-9-1-B(nxos) # show mac address-table gend: * - primary entry, G - Gateway MAC, (R) - Routed age - seconds since last seen,+ - primary entry u VLAN MAC Address Type age Secure NTF 	14.17.154.200 - PuTTY         40-31-9-1-B(nxos) # show mac address-table gend:         * - primary entry, G - Gateway NAC, (R) - Routed MAC, O - Ov age - seconds since last seen, + - primary entry using vPC Pe         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       0025.b581.991e       static       0       F       F       Veth1491         166       0025.b581.9a9d       static       0       F       F       Veth1491         166       0025.b581.9a9d       static       0       F       F       Veth1491         166       0025.b581.9a9d       static       0       F       F       Veth1475         166       0025.b581.9a9d       static       0       F       F       Veth1475         177       0025.b581.9a3f       dynamic       10       F       F       Veth1402         177       0025.b581.9a4d       dynamic       980       F       F       Veth1402         177       0050.566b.01ad       dynamic       10	<pre>14.17.154.200 - PuTTY 40-31-9-1-B(nxos) # show mac address-table gend:</pre>

在Nexus 5K上,MAC地址0050.56bd.7bef在Eth1/4上获取:

P F340-11-12-COMM.cisco.com - PuTTY	- <b>D</b> X
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: * - nrimary entry, G - Gateway M&C, (R) - Routed M&C, O - Overla	av MàC
age - seconds since last seen,+ - primary entry using vPC Peer-J	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 UUUC.29d2.495a dynamic 160 F F Eth1/4	
* 166 UUSU.S655d.61d2 dynamic 100 F F Eth1/3	E
F340.11.13-Nexus5000-5#	-

在4900交换机上,MAC地址0050.56bd.7bef在GigabitEthernet1/1上获知:

🗗 F340-1	1-05-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	
Multicas	st Entries				
vlan	mac address	type	ports		
	+	++-			
1	0100.0ccc.ccce	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	1111.1111.1111	system (	Gi1/1		
15	ffff.ffff.ffff	system (	Gi1/1		
16	ffff.ffff.ffff	system (	Gi1/1		
17	ffff.ffff.ffff	system (	Gi1/1		Ξ
18	1111.1111.1111	system (	Gi1/1		
More-					Ψ.

在此配置中,此隔离VLAN中的系统无法相互通信,但可以通过4900交换机上的混杂端口与其他系 统通信。一个问题是如何配置下行设备。在本例中,您使用的是VMware和两台主机。

请记住,每个PVLAN必须使用一个vNIC。这些vNIC显示给VMware vSphere ESXi,然后您可以创 建端口组并让访客访问这些端口组。

如果两个系统添加到同一交换机上的同一端口组,则它们可以相互通信,因为它们的通信在 vSwitch本地交换。在此系统中,有两个刀片,每个刀片有两台主机。

在第一个系统上,创建了两个不同的端口组 — 一个称为166,另一个称为166A。每个NIC都连接到 单个NIC,该NIC配置在UCS的隔离VLAN中。当前每个端口组只有一个访客。在这种情况下,由于 ESXi上的这些设备是分开的,因此它们无法相互通信。



在第二个系统上,只有一个端口组称为166。此端口组中有两个访客。在此配置中,VM3和VM4可以相互通信,即使您不希望发生这种情况。要更正此问题,您需要为隔离VLAN中的每个虚拟机 (VM)配置一个NIC,然后创建连接到该vNIC的端口组。配置完此配置后,只将一个访客放入端口组 。这不是裸机Windows安装的问题,因为您没有这些底层vSwitch。

Stan	dard Switch: vSwitch0	Remove	Properties
ç	Virtual Machine Port Group	Physical Adapters	tand by 🛛 🖓
P	VMkernel Port VMkernel Q vmk1 : 14.17.177.14   VLAN ID: 177		



### N1K上的隔离PVLAN,上游设备上的混杂端口

在此配置中,您将PVLAN流量先通过N1K,然后UCS传输到上游的混杂端口。由于不能在同一个 vNIC上同时发送主VLAN和辅助VLAN,因此每个PVLAN上行链路需要一个vNIC才能传输PVLAN流 量。

#### UCS中的配置

本过程介绍如何创建主VLAN和任何隔离VLAN。

注意:本示例使用266作为主要,166作为隔离;VLAN ID由站点确定。

1. 要创建主VLAN,请单击"主"作为"共享类型:

: 266			
		V.	LAN ID: 266
: No		Fa	bric ID: Dual
: Lan		1	f Type: Virtual
: External		Transpor	t Type: Ether
; <not set=""></not>	-	🕂 Crea	ate Multicast Policy
: org-root/mc-p	olicy-default		
; 🔘 None 🍥	Primary 🔘 Isola	ted	
Print			
Туре	Transport	Native	VLAN Sharin 🛱
Lan	Ether	No	Isolated 🔺
	: Lan : External : [ <not set=""> : org-root/mc-pr : None • Print Type Lan</not>	<pre># Lan # External # (not set&gt;</pre>	Image: Lan   Image: External   Image: I

2. 要创建隔离VLAN,请单击**隔离**作为共享类型:

Properties					
Name:	166		VLAN ID:	166	
Native VLAN:	No		Fabric ID:	Dual	
Network Type:	Lan		If Type:	Virtual	
Locale:	External		Transport Type:	Ether	
Sharing Type:	🔿 None 🕤 Primary	<ul> <li>Isolated</li> </ul>	Primary VLAN:	VLAN 266 (266)	•
-Primary VLAN	Properties				
	Name: 266		VLAN ID: 2	266	
Nal	tive VLAN: No		Fabric ID: I	Dual	
Netw	vork Type: Lan		If Type: <b>N</b>	Virtual	
	Locale: External		Transport Type: I	Ether	
Multicast Po	licy Name: <pre> <not set=""></not></pre>	-	🕂 Create Multic	ast Policy	
Multicast Policy	Instance: org-root/mc-	policy-default			

3. 要将VLAN添加到vNIC,请单击VLAN 166的**Select**复选框。VLAN 166没有选中Native VLAN。

LANs			
Select	Name	Native VLAN	f
	default	0	
	1233	0	
	1234	0	
	124	0	
	126	0	
	166	0	
	266	0	
	777	0	
	Tbeaudre_177	0	
	Tbeaudre_277	0	
	Tbeaudre_377	0	
	Vlan_51	0	

只添加隔离VLAN,不能将其设置为本征VLAN,并且每个vNIC只能有一个。由于本征VLAN未 在此处定义,因此请标记N1K上的本征VLAN。VMware DVS中不提供标记本征VLAN的选项 ,因此DVS不支持此选项。

#### 上游设备的配置

这些步骤说明如何配置Nexus 5K,以便将PVLAN传递到混杂端口所在的上游4900交换机。虽然并 非所有环境都需要此配置,但在必须通过另一台交换机传递PVLAN时,请使用此配置。

在Nexus 5K上,输入以下命令,并检查上行链路配置:

1. 打开PVLAN功能:

Nexus5000-5(config)# feature private-vlan

2. 将VLAN添加为主VLAN和隔离VLAN:

Nexus5000-5(config-vlan)# vlan 266 Nexus5000-5(config-vlan)# private-vlan primary

3. 将VLAN 266与隔离VLAN 166关联:

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

4. 确保配置所有上行链路以中继VLAN:

接口Ethernet1/1描述与4900的连接switchport mode trunkspeed 1000接口Ethernet1/3描述与 FIB端口5的连接switchport mode trunkspeed 1000接口Ethernet1/4描述与FIA端口5的连接 switchport mode trunkspeed 1000

在4900交换机上,执行以下步骤,并设置混杂端口。PVLAN在混杂端口结束。

- 1. 根据需要打开PVLAN功能。
- 2. 按照Nexus 5K上的操作创建并关联VLAN。
- 在4900交换机的出口端口上创建混杂端口。从此开始,在本例中,VLAN 266上可以看到来自 VLAN 166的数据包。

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

- 在上游路由器上,仅为VLAN 266创建子接口。在此级别,要求取决于您使用的网络配置:
  - 1. interface GigabitEthernet0/1.1
  - 2. encapsulation dot1Q 266
  - 3. ip address 209.165.200.225 255.255.255.224

#### 配置N1K

此程序描述如何将N1K配置为标准中继,而不是PVLAN中继。

- 1. 按照Nexus 5K上的操作创建并关联VLAN。有关详细信息,请参阅上游设备的配置部分。
- 2. 为PVLAN流量创建上行链路端口配置文件:

```
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. 为隔离VLAN创建端口组;为主VLAN和隔离VLAN创建具有主机关联的PVLAN主机端口:

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. 在vCenter中,将正确的vNIC添加到PVLAN上行链路。这是您在UCS设置中的配置下将隔离 VLAN添加到的vNIC。

<b>H</b> O	vmnic3		View Details	Select an uplink port gr
🗹 📖	vmnic4	pvlan	View Details	pvlan_uplink
<b>8</b> 8	vmnic5		View Details	Select an uplink port gr

5. 将VM添加到正确的端口组:

在"Hardware(硬件)"选项卡中,单**击"Network adapter 1(网络适配器1**)"。在"Network Connection:"下,为"Network"标签选择**pvlan\_guest(pvlan)。** 

🖉 VM1 - Virtual Machine Properties	1000		
Hardware Options Resources Profil	es VServices		Virtual Machine Version: 8
	Add Remove	Device Status	
Hardware  Memory  CPUs  Video card  VMCI device  SCSI controller 0  Hard disk 1  CD/DVD drive 1  Network adapter 1  Floppy drive 1	Summary 4096 MB 1 Video card Restricted LSI Logic SAS Virtual Disk [datastore1] en_windo pvlan_guest (pvlan), Po Client Device	Image: Connect at power on         Adapter Type         Current adapter:         MAC Address         [00:0c:29:bc:58:9c]         Image: Connection         OrectPath I/O         Status:         Network Connection         Network label:         [pvlan_guest (pvlan)         Port:       32	E1000 Manual Not supported  Switch to advanced settings
Help			OK Cancel

#### 故障排除

此步骤介绍如何测试配置。

1. 对端口组中配置的其他系统以及混杂端口上的路由器或其他设备执行ping操作。对经过混杂端 口的设备执行ping操作应该有效,而对隔离VLAN中的其他设备执行ping操作应该失败。

```
Administrator: 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.
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 = Oms, Maximum = 2ms, Average = Oms
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.
Ping statistics for 14.17.166.51:
Packets: Sent = 4, Received = 4, Lost = 0 <0% loss),
C:\Users\Administrator}_
```

2. 在N1K上,VM列在主VLAN上;这是因为您位于与PVLAN关联的PVLAN主机端口中。由于 VM的学习方式,请确保不要在UCS系统上将PVLAN设置为本征VLAN。另请注意,您从端口 通道学习上游设备,并且上游设备也在主VLAN上学习。必须通过此方法了解这一点,这就是 您将主VLAN作为PVLAN上行链路上的本征VLAN的原因。

在此屏幕截图中,Veth3和Veth 4上的两台设备是VM。Po1上的设备是经过混杂端口的上游路 由器。

pvlan# sho	ow mac address-tabl	le			
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	Vethi	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	Pol	3
Total MAC	Addresses: 17				
nulan#					

3. 在UCS系统上,您应该学习隔离VLAN中的所有MAC,以便进行此通信。您不应在此处看到上游:

F340-31- Legend:	-9-1-B(nxos)# show m	ac address-	-table					
VLAN	* - primary entry, age - seconds since MAC Address	G - Gateway last seen, Type	y MAC, + - pr age	(R) - Rout imary entr Secure	ed ) y u: NTF	MAC, ( sing v Y l	0 - Overlay vPC Peer-Li Ports	MAC nk
* 166 * 166 * 166	000c.2996.9a1d 000c.29bc.589c 0025.b581.991e	dynamic dynamic static	10 270 0	++ F F F	1 1 1	Veth: Veth: Veth:	1491 1491 1491 1491	

4. 在Nexus 5K上,两台虚拟机位于隔离VLAN中,而上游设备位于主VLAN中:

F340.11. Legend:	13-Nexus5000-5# sho	w mac addr	ess-table	2			
	* - primary entry, o age - seconds since	G - Gatewa last seem	ay MAC, (B 1,+ - prim	R) - Rout mary entr	ed l y u:	MAC, O - Overla sing vPC Peer-I	ay MAC .ink
VLAN	MAC Address	Туре	age	Secure	NTF	Y 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. 在混杂端口为4900交换机上,所有内容都位于主VLAN上:

Entries mac address	type	protocols	port
000c.2996.9a1d 000c.29bc.589c 0012.8032.86a9	dynamic dynamic dynamic	<pre>ip, ipx, assigned, other ip, ipx, assigned, other ip, ipx, assigned, other</pre>	GigabitEthernet1/1 GigabitEthernet1/1 GigabitEthernet1/2
st Entries			
mac address	type	ports	
	evetam		
ffff.ffff.ffff	system	Gi1/1	
ffff.ffff.ffff	system	Gi1/1,Gi1/2	
	Entries mac address 000c.2996.9a1d 000c.29bc.589c 0012.8032.86a9 st Entries mac address 0100.0ccc.ccce ffff.ffff.ffff	Entries mac address type 000c.2996.9a1d dynamic 000c.29bc.589c dynamic 0012.8032.86a9 dynamic st Entries mac address type 0100.0ccc.ccce system ffff.ffff.ffff system ffff.ffff.ffff system	Entries mac address type protocols 000c.2996.9a1d dynamic ip,ipx,assigned,other 000c.29bc.589c dynamic ip,ipx,assigned,other 0012.8032.86a9 dynamic ip,ipx,assigned,other st Entries mac address type ports 0100.0ccc.ccce system Gil/1 ffff.ffff.ffff system Gil/1 ffff.ffff.ffff system Gil/1,Gil/2

### N1K上的隔离PVLAN,N1K上行链路端口配置文件上带有混杂端口

在此配置中,您仅包含上游使用的主VLAN,从而包含到N1K的PVLAN流量。

#### UCS中的配置

此过程介绍如何将主VLAN添加到vNIC。无需PVLAN配置,因为您只需要主VLAN。

**注意:**本示例使用266作为主要,166作为隔离;VLAN ID由站点确定。

1. 请注意,共享类型为None。

>> 🗐 LAN + 🔿 LAN Cloud + 🗐 VLANs + 🗐 VLAN 266 (266)								
General Org Permissions YLAN Group Membershi	Faults Events							
Fault Summary       Image: Complexity of the second s	Properties Name: 266 Native VLAN: No Network Type: Lan Locale: External Multicast Policy Name: <not set=""> Multicast Policy Instance: org-root/me-policy-default Sharing Type: None Primary Isolate</not>	VLAN ID: 266 Fabric ID: Dual If Type: Virtual Transport Type: Ether Create Multicast Policy						

2. 单击VLAN 266的Select复选框,将主VLAN添加到vNIC。不要将其设置为本地。

Modify VLANs					
-VLANs -					
Select	Name	Native VLAN	E		
	default	©	A		
	1233				
	1234	0			
	124	©			
	126	0	E		
	166	©			
	266	<u> </u>			
	777	©			
	Tbeaudre_177	©			
	Tbeaudre_277	©			
	Tbeaudre_377	©			
	Vlan_51	Ô	-		

#### 上游设备的配置

这些步骤说明如何配置上游设备。在这种情况下,上游交换机只需要中继端口,而且只需中继 VLAN 266,因为它是上游交换机看到的唯一VLAN。

在Nexus 5K上,输入以下命令,并检查上行链路配置:

1. 将VLAN添加为主VLAN:

Nexus5000-5(config-vlan) # vlan 266

2. 确保配置所有上行链路以中继VLAN:

接口Ethernet1/1描述与4900的连接switchport mode trunkspeed 1000接口Ethernet1/3描述与 FIB端口5的连接switchport mode trunkspeed 1000接口Ethernet1/4描述与FIA端口5的连接 switchport mode trunkspeed 1000 在4900交换机上,执行以下步骤:

1. 在N1K上创建用作主VLAN。

2. 将所有接口中继到4900交换机和从4900交换机中继,以便VLAN通过。 在上游路由器上,仅为VLAN 266创建子接口。在此级别,要求取决于您使用的网络配置。

- 1. interface GigabitEthernet0/1.1
- 2. encapsulation dot1Q 266
- 3. ip address 209.165.200.225 255.255.255.224

#### 配置N1K

本步骤介绍如何配置N1K。

1. 创建并关联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. 为PVLAN流量创建上行链路端口配置文件,并注明混杂端口:

```
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. 为隔离VLAN创建端口组;为主VLAN和隔离VLAN创建具有主机关联的PVLAN主机端口:

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. 在vCenter中,将正确的vNIC添加到PVLAN上行链路。这是您在UCS设置中的配置下将隔离 VLAN添加到的vNIC。

<b>10</b>	vmnic3		View Details	Select an uplink port gr
🗹 💷	vmnic4	pvlan	View Details	pvlan_uplink
E.C.	vmnic5		View Details	Select an uplink port gr

5. 将VM添加到正确的端口组。

在"Hardware(硬件)"选项卡中,单**击"Network adapter 1(网络适配器1**)"。在"Network Connection"下,为"Network"标签选择**pvlan\_guest(pvlan)。** 

VM1 - Virtual Machine Properties	1000	
Hardware Options Resources Prof	iles vServices	Virtual Machine Version: 8
Show All Devices	Add Remove	Connected
Hardware	Summary	Connect at power on
Memory	4096 MB	Adapter Type
U CPUs	1 Video card	Current adapter: E1000
	Restricted	
SCSI controller 0	LSI Logic SAS	MAC Address
Hard disk 1	Virtual Disk	00:0c:29:bc:58:9c
CD/DVD drive 1	[datastore1] en_windo	C Automatic C Manual
Network adapter 1	pvlan_guest (pvlan), Po	DirectPath I/O
Hoppy drive 1	Client Device	Status: Not supported 1
		Network Connection
		Network label:
		pylan_guest (pylan)
		Port: 32
		Switch to advanced settings
Help		OK Cancel
		///

#### 故障排除

此步骤介绍如何测试配置。

1. 对端口组中配置的其他系统以及混杂端口上的路由器或其他设备执行ping操作。对经过混杂端 口的设备执行ping操作应该有效,而对隔离VLAN中的其他设备执行ping操作应该失败。 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 = Ø (0% loss),
Approxinate round trip times in milli-seconds:
Minimum = Øms, Maximum = Øms, Average = Øms
Control-C
C:\Users\Administrator>ping 14.17.166.51
Pinging 14.17.166.51 with 32 bytes of data:
Reply from 14.17.166.51 with 32 bytes of data:
Reply from 14.17.166.50: Destination host unreachable.
Ping statistics for 14.17.166.51:
Ping statisti

2. 在N1K上,VM列在主VLAN上;这是因为您位于与PVLAN关联的PVLAN主机端口中。另请注意,您从端口通道学习上游设备,并且上游设备也在主VLAN上学习。

在此屏幕截图中,Veth3和Veth 4上的两台设备是VM。Po1上的设备是经过混杂端口的上游设备。

pvlan(conf	fig-port-prof)# sho	ow mac ad	ldress-tab.	le	
VLAN	MAC Address	Type	lge	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(conf	fig-port-prof)# 📘				

3. 在UCS系统上,您应该在N1K上使用的主VLAN中学习所有MAC,以便进行此通信。您不应在 此处学习上游:

340-31-	-9-1-B(nxos)# show ma	ac address	-table				
egend:							
	* - primary entry, (	G - Gatewa	y MAC,	(R) - Route	ed M	IAC, $O = Over$	erlay 1
	age - seconds since	last seen	,+ - pr:	imary entry	y us	sing vPC Pe	er-Linł
VLAN	MAC Address	Type	age	Secure I	JTF Y	? 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	
	VLAN 266 266 177 177 126 124	340-31-9-1-B(nxos)# show mage         egend:         * - primary entry, (age - seconds since         VLAN       MAC Address         266       000c.2996.9a1d         266       000c.29bc.589c         177       0025.b581.9a3f         177       0025.b585.100a         126       000c.566b.01ad         126       0023.04c6.dbe2	340-31-9-1-B(nxos)# show mac address         egend:         * - primary entry, G - Gatewa         age - seconds since last seen         VLAN       MAC Address         Type        +-         266       000c.2996.9a1d         000c.29bc.589c       dynamic         177       0025.b581.9a3f       dynamic         177       0025.b585.100a       dynamic         177       0025.b581.993f       dynamic         126       0025.b581.999e       static         124       0023.04c6.dbe2       dynamic	340-31-9-1-B(nxos)# show mac address-table         egend:         * - primary entry, G - Gateway MAC,         age - seconds since last seen, + - pr         VLAN       MAC Address         Type       age         266       000c.2996.9a1d       dynamic         266       000c.29bc.589c       dynamic         177       0025.b581.9a3f       dynamic         177       0025.b585.100a       dynamic         126       0025.b581.999e       static         124       0023.04c6.dbe2       dynamic	340-31-9-1-B(nxos)# show mac address-table         egend:         * - primary entry, G - Gateway MAC, (R) - Route         age - seconds since last seen, + - primary entry         VLAN       MAC Address         Type       age         Secure N	340-31-9-1-B(nxos)# show mac address-table         egend:         * - primary entry, G - Gateway MAC, (R) - Routed M         age - seconds since last seen, + - primary entry us         VLAN       MAC Address         Type       age         Secure NTFY         266       000c.2996.9a1d         dynamic       100         F       F         266       000c.29bc.589c         dynamic       180         F       F         177       0025.b581.9a3f         177       0025.b585.100a         dynamic       350         F       F         126       0025.b581.999e         static       0         F       F	340-31-9-1-B(nxos)# show mac address-table         egend:         * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overage         age - seconds since last seen, + - primary entry using vPC Perevent         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       350       F       F       Veth1402         177       0025.b585.100a       dynamic       350       F       F       Veth1402         126       0025.b581.999e       static       0       F       F       Veth1402         124       0023.04c6.dbe2       dynamic       0       F       F       Veth1404

4. 在Nexus 5K上,所有MAC都位于您选择的主VLAN中:

F340.11. Legend:	.13-Nexus5000-5# shot	v mac addr	ess-tab	le			
VLAN	<pre>* - primary entry, ( age - seconds since MAC Address</pre>	G - Gatewa last seen Type	y MAC, ,+ - pr age	(R) - Rout imary entr Secure	ed y u NTF	MAC, O - Overlay MAC sing vPC Peer-Link Y Ports	
* 266 * 266 * 266	000c.2996.9a1d 000c.29bc.589c c84c.75f6.013f	dynamic dynamic dynamic dynamic	90 20 100	++ F F F	 F F F	-+ Eth1/4 Eth1/4 Eth1/1	ш
F340.11.	.13-Nexus5000-5# 🗧	-					-

5. 在4900交换机上,您选择的主VLAN上的所有内容均为:

Switch#s	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				
Multicas	st 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#								

### N1K上的社区PVLAN,N1K上行链路端口配置文件上带有混杂端口

这是使用UCS的社区VLAN唯一支持的配置。

此配置与在N1K上的隔离PVLAN中设置的配置相同,在<u>N1K上行链路端口配置文件部分中设置混杂</u> <u>端口。</u>社区和隔离之间的唯一区别是PVLAN的配置。

要配置N1K,请创建并关联VLAN,就像您在Nexus 5K上所做的那样:

```
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
所有其他配置与N1K上的隔离PVLAN相同,N1K上行链路端口配置文件上的混杂端口也相同。
```

配置后,您可以与连接到用于PVLAN的vEthernet端口配置文件的所有虚拟机通信。

#### 故障排除

此步骤介绍如何测试配置。

 1. 对端口组中配置的其他系统以及混杂端口上的路由器或其他设备执行ping操作。通过混杂端口 和到社区中其他系统的ping应该有效。

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 TIL=255
Reply from 14.17.166.61: bytes=32 time(1ms TIL=255
Reply from 14.17.166.61: bytes=32 time(1ms TIL=255
Reply from 14.17.166.61: bytes=32 time(1ms TIL=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: bytes=32 time(1ms TIL=128
Reply from 14.

2. 所有其他故障排除都与隔离的<u>PVLAN相同</u>。

### VMware DVS混合端口上的隔离PVLAN和社区PVLAN

由于DVS和UCS系统上的配置问题,在2.2(2c)版之前不支持带DVS和UCS的PVLAN。

### 验证

当前没有可用于这些配置的验证过程。

### 故障排除

前面部分提供了可用于排除配置故障的信息。

<u>命令输出解释程序工具(仅限注册用户)支持某些</u> **show 命令。**使用输出解释器工具来查看 show 命令输出的分析。