2.2(2C)之前的專用VLAN和Cisco UCS配置

目錄

簡介 必要條件 需求 採用元件 背景資訊 理論 UCS中的PVLAN實施 目標 設定 網路圖 vSwitch:上的PVLAN上游裝置上帶有混雜埠的隔離PVLAN UCS中的配置 配置上游裝置 疑難排解 N1K上的隔離PVLAN,上游裝置上的混雜埠 UCS中的配置 配置上游裝置 N1K的配置 疑難排解 N1K上的隔離PVLAN,N1K上行鏈路埠上的混雜埠 — 配置檔案 UCS中的配置 配置上游裝置 N1K的配置 疑難排解 N1K上的社群PVLAN,N1K上行鏈路埠上的混雜埠 — 配置檔案 疑難排解 VMware DVS上的隔離PVLAN和社群PVLAN混合埠 驗證 疑難排解

簡介

本檔案介紹思科整合運算系統(UCS)中的私人VLAN(PVLAN)支援,這是Cisco UCS Manager(UCSM)版本1.4中介紹的功能。 還詳細說明了在UCS環境中使用PVLAN時的功能、注意 事項和配置。

本文檔用於UCSM版本2.2(2C)及更早版本。在版本2.2(2C)之後的版本中,對UCSM進行了更改,支援ESXi DVS。對於PVLAN NIC,標籤的工作方式也發生了變化。

必要條件

需求

思科建議您瞭解以下主題:

- UCS
- Cisco Nexus 1000 V(N1K)
- VMware
- 第2層(L2)交換

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

背景資訊

理論

專用VLAN是配置為從同一個專用VLAN中的其他埠隔離第2層的VLAN。屬於PVLAN的連線埠與一 組常見的支援VLAN關聯,用於建立PVLAN架構。

PVLAN埠有三種型別:

- 混雜埠與所有其他PVLAN埠通訊,並且是用來與PVLAN外部裝置通訊的埠。
- 隔離連線埠與相同PVLAN中的其他連線埠完全分離L2(包括廣播),但混雜連線埠除外。
- community port可與同一PVLAN中的其他埠以及混雜埠通訊。在L2中,團體埠與其他團體中的 埠或隔離的PVLAN埠隔離。廣播只會傳播到團體中的其他連線埠和混雜連線埠。

請參閱<u>RFC 5517,Cisco Systems的私人VLAN:在多客戶端環境中實現可擴</u>展的安全性,以便瞭解 PVLAN的理論、操作和概念。

UCS中的PVLAN實施

UCS非常類似於Nexus 5000/2000架構,其中Nexus 5000與UCS 6100類似,Nexus 2000與UCS 2104交換矩陣擴展器類似。

UCS中PVLAN功能的許多限制是由Nexus 5000/2000實施中的限制引起的。

需要記住的重要一點是:

- UCS僅支援隔離埠。結合使用N1K後,您可以使用社群VLAN,但混雜埠也必須位於N1K上。
- •不支援混雜埠/中繼、社群埠/中繼或隔離中繼。
- 混雜埠需要位於UCS域之外,例如上游交換機/路由器或下游N1K。

目標

本文檔介紹適用於使用UCS的PVLAN的多種不同配置:

- 1. 上游裝置上帶有混雜埠的隔離PVLAN。
- 2. N1K上的隔離PVLAN,上游裝置上有混雜埠。
- 3. N1K上的隔離PVLAN, N1K上行鏈路埠配置檔案上的混雜埠
- 4. N1K上的社群PVLAN,N1K上行鏈路埠配置檔案上的混雜埠。
- 5. VMware分散式虛擬交換機(DVS)混雜埠上的隔離PVLAN。
- 6. VMware DVS上的社群PVLAN交換機混雜埠位於DVS上。

設定

網路圖

分散式交換機的所有示例的拓撲是:



沒有分散式交換機的所有示例的拓撲是:



vSwitch:上的PVLAN上游裝置上帶有混雜埠的隔離PVLAN

在此配置中,您將PVLAN流量通過UCS傳遞到上游的混合埠。由於不能在同一個vNIC上同時傳送 主和輔助VLAN,因此每個PVLAN的每個刀片需要一個vNIC,以便傳輸PVLAN流量。

UCS中的配置

以下過程介紹了如何建立主要和任何隔離VLAN。

附註:本示例使用266作為主用裝置,166作為隔離裝置;vlan ID由站點決定。

1. 要建立主VLAN,請按一下Primary作為共用型別,並輸入VLAN ID266:

Properties					
N	ame: 26	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. 要建立隔離VLAN,請按一下Isolated作為共用型別,輸入VLAN ID 166,然後選擇VLAN 266(266)作為主要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 Isolated 	Primary VLAN:	VLAN 266 (266)
Primary VLAN Propertie	:5		
Name: 3	266	VLAN ID: 2	266
Native VLAN: I	No	Fabric ID: I	Dual
Network Type: I	Lan	If Type: 1	Virtual
Locale: I	External	Transport Type: I	Ether
Multicast Policy Name:	<not set=""></not>	🛨 Create Multic	ast Policy
Multicast Policy Instance:	org-root/mc-policy-default	:	

3. 若要將VLAN新增到vNIC,請按一下VLAN 166的**選擇**覈取方塊,然後按一下關聯的**本地** VLAN單選按鈕。

/LANs	News		Ē
Select	Ivame		Ľ
	1233		
	1234		_
	124	©	
	126		
	166	•	
	266	©	
	777	©	
	Tbeaudre_177	©	
	Tbeaudre_277	©	
	Tbeaudre_377	0	
	Vlan 51	O	-

僅新增隔離VLAN,必須將其設定為主要,每個vNIC只能有一個。由於此處定義了本地 VLAN,因此請勿在VMware埠組上配置VLAN標籤。

配置上游裝置

以下過程介紹了如何配置Nexus 5K以將PVLAN傳遞到混雜埠所在的上游4900交換機。雖然並非在 所有環境中都必需此配置,但如果您必須將PVLAN通過另一台交換機,請使用此配置。

在Nexus 5K上,輸入以下命令,並檢查上行鏈路配置:

1. 開啟PVLAN功能:

Nexus5000-5(config)# feature private-vlan

2. 將VLAN新增為主用和隔離:

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. 將VLAN 266與隔離VLAN 166關聯:

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

4. 確保所有上行鏈路都已配置以中繼VLAN:

interface Ethernet1/1描述與4900的連線switchport mode trunk速度1000interface Ethernet1/3描述與FIB埠5的連線switchport mode trunk速度1000interface Ethernet1/4描述與 FIA埠5的連線switchport mode trunk速度1000

在4900交換機上,執行這些步驟,並設定混雜埠。PVLAN在混雜埠結束。

- 1. 如果需要,開啟PVLAN功能。
- 2. 按照在Nexus 5K上的步驟建立和關聯VLAN。
- 3. 在4900交換器的輸出連線埠上建立混雜連線埠。從此以後,來自VLAN 166的資料包會在 VLAN 266上看到。

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

- 在上游路由器上,只為VLAN 266建立子介面。在此級別,要求取決於您使用的網路配置:
 - 1. interface GigabitEthernet0/1.1
 - 2. encapsulation dot1Q 266
 - 3. IP address 209.165.200.225 255.255.255.224

疑難排解

此程式介紹如何測試配置。

1. 在每台交換器上設定交換器虛擬介面(SVI),允許您從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. 檢查MAC地址表,檢視您的MAC被獲取的位置。在所有交換機上,MAC應該位於隔離 VLAN中,但帶有混雜埠的交換機除外。在混雜交換器上,請注意MAC位於主要VLAN中。

在交換矩陣互聯上,在Veth1491上獲知MAC地址0050.56bd.7bef:

	_					_	-		~
d	³ 14.17.1	54.200 - PuTTY							×
F	340-31-	-9-1-B(nxos)# show ma	ac address-	table					-
L	egend:								
		* - primary entry, (G - Gateway	MAC,	(R) - Rout	ted	MAC, $O = Ove$	erlay MAC	
		age - seconds since	last seen,	+ - p	rimary entr	cy u	sing vPC Pe	er-Link	
	VLAN	MAC Address	Type	age	Secure	NTF	Y Ports		
2		+	++-		+	+	-+		
*	166	000c.29d2.495a	dynamic	80	F	F	Veth1491		
*	166	0025.b581.991e	static	ο	F	F	Veth1491		
ľ	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		
Ť	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		
Ť	177	0050.566b.01ad	dynamic	980	F	F	Veth1402		
*	177	0050.566c.d835	dynamic	10	F	F	Veth1472		
*	126	0025.b581.999e	static	ο	F	F	Veth1392		
*	124	0023.04c6.dbe2	dynamic	10	F	F	Veth1404		
*	124	0023.04c6.dbe3	static	ο	F	F	Veth1404		=
*	4044	0024.971f.6bc2	dynamic	ο	F	F	Eth2/1/9		
*	4044	0026.5108.0b2c	dynamic	0	F	F	Eth1/1/9		
Ť	4044	0026.5108.cac2	dynamic	0	F	F	Eth1/1/9		
Ŀ	-More								-
	and the second second second			and the second sec	the second se	-		and the second se	1

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

P F340-11-12-COMM.cisco.com - PuTTY	J
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, (K) - 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 E * 166 0050.56bd.6fd2 dynamic 100 F F Eth1/3 E * 166 0050.56bd.7bef dynamic 60 F F Eth1/4 F340.11.13-Nexus5000-5#	

在4900交換器上,MAC位址0050.56bd.7bef是在GigabitEthernet1/1上得知的:

🗗 F340-11	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 (311/1		
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 (311/1		
16	ffff.ffff.ffff	system (Gi1/1		
17	ffff.ffff.ffff	system (Gi1/1		
18	ffff.ffff.ffff	system (Gi1/1		
More-					Ŧ

在此配置中,此隔離VLAN中的系統無法相互通訊,但可以通過4900交換機上的混雜埠與其他系統 通訊。一個問題是如何配置下行裝置。在這種情況下,您使用VMware和兩個主機。

請記住,您必須為每個PVLAN使用一個vNIC。這些vNIC提供給VMware vSphere ESXi,然後您可 以建立埠組並讓來賓訪問這些埠組。

如果將兩個系統新增到同一交換機上的同一埠組,則它們可以彼此通訊,因為它們的通訊在 vSwitch上進行本地交換。在此系統中,有兩台刀鋒伺服器,每台伺服器有兩個主機。

在第一個系統上建立了兩個不同的埠組 — 一個稱為166,另一個稱為166A。每個介面都連線到單個 NIC,該NIC在UCS上的隔離VLAN中配置。目前每個連線埠群組只有一個訪客。在本例中,由於它 們在ESXi上是分開的,所以它們不能相互通訊。



在第二個系統上,只有一個埠組稱為166。此埠組中有兩個訪客。在此配置中,VM3和VM4可以相互通訊,即使您不希望發生這種情況。為了糾正此問題,您需要為隔離VLAN中的每個虛擬機器 (VM)配置單個NIC,然後建立連線到該vNIC的埠組。設定好後,只需將一位訪客加入連線埠群組。 裸機Windows安裝不存在此問題,因為您沒有這些基礎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上的隔離PVLAN,上游裝置上的混雜埠

在此配置中,您將PVLAN流量通過N1K,然後通過UCS傳遞到上游的混合埠。由於不能在同一個 vNIC上同時傳送主VLAN和輔助VLAN,因此每個PVLAN上行鏈路需要一個vNIC來傳輸PVLAN流量 。

UCS中的配置

以下過程介紹了如何建立主要和任何隔離VLAN。

附註:本示例使用266作為主用裝置,166作為隔離裝置;vlan ID由站點決定。

1. 要建立主VLAN,請按一下**Primary**作為共用型別:

VLAN ID: 266 Fabric ID: Dual If Type: Virtual Transport Type: Ether
Fabric ID: Dual If Type: Virtual Transport Type: Ether
If Type: Virtual Transport Type: Ether Treate Multicast Policy
ransport Type: Ether
+ Create Multicast Policy
ive VLAN Sharin 🛱
Isolated 🔺

2. 要建立隔離VLAN,請按一下Isolated作為共用型別:

Properties		
Name: 16	6	VLAN ID: 166
Native VLAN: No	1	Fabric ID: Dual
Network Type: La	n	If Type: Virtual
Locale: Ex	ternal	Transport Type: Ether
Sharing Type:) None 🕥 Primary 🧿 Isolated	Primary VLAN: VLAN 266 (266)
Primary VLAN Pro	operties	
	Name: 266	VLAN ID: 266
Native	VLAN: No	Fabric ID: Dual
Network	«Type: Lan	If Type: Virtual
I	Locale: External	Transport Type: Ether
Multicast Policy	Name: <pre> </pre> <pre> </pre>	🛨 Create Multicast Policy
Multicast Policy Ins	stance: org-root/mc-policy-defaul	lt

3. 要將VLAN新增到vNIC,請點選VLAN 166的選擇覈取方塊。VLAN 166沒有選擇本地VLAN。

LANs			
Select	Name	Native VLAN	
	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	

僅新增隔離VLAN,不得將其設定為本徵,並且每個vNIC只能有一個。由於未在此處定義本徵 VLAN,因此請標籤N1K上的本徵VLAN。標籤本地VLAN的選項在VMware DVS中不可用,因 此DVS不支援此選項。

配置上游裝置

以下步驟說明如何配置Nexus 5K,以便將PVLAN傳遞到混雜埠所在的上游4900交換機。雖然並非 在所有環境中都必需此配置,但如果您必須將PVLAN通過另一台交換機,請使用此配置。

在Nexus 5K上,輸入以下命令,並檢查上行鏈路配置:

1. 開啟PVLAN功能:

Nexus5000-5(config)# feature private-vlan

2. 將VLAN新增為主用和隔離:

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. 將VLAN 266與隔離VLAN 166關聯:

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

4. 確保所有上行鏈路都已配置以中繼VLAN:

interface Ethernet1/1描述與4900的連線switchport mode trunk速度1000interface Ethernet1/3描述與FIB埠5的連線switchport mode trunk速度1000interface Ethernet1/4描述與 FIA埠5的連線switchport mode trunk速度1000

在4900交換機上,執行這些步驟,並設定混雜埠。PVLAN在混雜埠結束。

- 1. 如果需要,開啟PVLAN功能。
- 2. 按照在Nexus 5K上的步驟建立和關聯VLAN。
- 3. 在4900交換器的輸出連線埠上建立混雜連線埠。從此以後,來自VLAN 166的資料包會在 VLAN 266上看到。

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

在上游路由器上,只為VLAN 266建立子介面。在此級別,要求取決於您使用的網路配置:

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

N1K的配置

以下過程介紹了如何將N1K配置為標準中繼,而不是PVLAN中繼。

- 1. 按照在Nexus 5K上的步驟建立和關聯VLAN。如需詳細資訊,請參閱上游裝置組態一節。
- 2. 為PVLAN流量建立上行埠配置檔案:

```
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. 為隔離VLAN建立埠組;為主要和隔離VLAN建立與主機關聯的PVLAN主機埠:

```
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,將正確的vNIC新增到PVLAN上行鏈路。這是您在UCS設定中的「配置」下將隔離VLAN新增到的vNIC。

B O	vmnic3		View Details	Select an uplink port gr
🖌 📷	vmnic4	pvlan	View Details	pvlan_uplink
iii (c)	vmnic5		View Details	Select an uplink port gr

5. 將VM新增到正確的埠組:

在Hardware(硬體)頁籤中,按一下**Network adapter 1**。為Network Connection:(網路連 線)下的Network(網路)標籤選擇**pvlan_guest(pvlan)**:

2 VM1 - Virtual Machine Properties	
Hardware Options Resources Profiles VServices	Virtual Machine Version: 8
Show All Devices Add Remove Connected	
Hardware Summary Connect at power on	
Memory 4096 MB	
CPUs 1 Gurrant adapter 5100	
Video card Video card Current adapter: E100	
WMCI device Restricted	
SCSI controller 0 LSI Logic SAS	
Hard disk 1 Virtual Disk	
CD/DVD drive 1 [datastore1] en_windo @ Automatic C Mani	ual
Network adapter 1 pvlan_guest (pvlan), Po DirectPath I/O	
Pioppy drive 1 Client Device Status: Not :	supported 📵
Network Connection	
Network label:	
pvlan_guest (pvlan)	-
Port: 32	
	Switch to advanced settings
Help	OK Cancel

疑難排解

此程式介紹如何測試配置。

1. 對埠組中配置的其他系統以及混雜埠上的路由器或其他裝置運行ping。通過混雜埠對裝置發出 的ping命令應該能正常工作,而向隔離VLAN中的其他裝置發出的這些ping命令應該會失敗。

an Administrator: C:\Windows\system32\cmd.exe _ 🗆 X 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 14.17.166.50: 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;這是因為您位於與PVLAN關聯的PVLAN主機埠中。由於VM的 學習方式,請確保不要在UCS系統上將PVLAN設定為本徵。另請注意,您會從連線埠通道得 知上游裝置,同時在主VLAN得知上游裝置。必須通過此方法學習這一點,因此您必須將主 VLAN作為PVLAN上行鏈路上的本地VLAN。

在此螢幕抓圖中,Veth3和Veth 4上的兩台裝置是VM。Po1上的裝置是經過混雜埠的上游路由 器。

pvlan# show mac address-table							
VLAN	MAC Address	Туре	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	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						
nszlenfi							

3. 在UCS系統上,您應該學習隔離VLAN中此通訊的所有MAC。您不應在此處看到上游:

F3 Le	40-31- gend:	9-1-B(nxos)# show	mac address	-table							
	-	* - primary entry, age - seconds sinc	G - Gatewa e last seen	y MAC, ,+ - pr	(R) - Rout imary entr	ed y u	MAC, sing	O - VPC	Overla Peer-L	y MAC ink	
	VLAN	MAC Address	Type -++	age 	Secure	NTF	Ү _+	Port	.s 		
*	166	000c.2996.9a1d	dynamic	10	F	F	Vetl	1491			
*	166	000c.29bc.589c	dynamic	270	F	F	Veth	n1491			
π	166	0025.b581.991e	static	0	F	F	Veth	1491			

4. 在Nexus 5K上,兩個VM位於隔離VLAN上,而上游裝置位於主VLAN上:

F340.1:	l.13-Nexus5000-5# sho	w mac addr	ess-tabl	le		
Legend	:					
	* - primary entry, (G - Gatewa	ay MAC,	(R) - Rout	ed 1	MAC, O - Overlay MAC
	age - seconds since	last seer	1,+ - pri	imary entr	y u:	sing vPC Peer-Link
VLA	MAC Address	Type	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. 在混合連線埠所在的4900交換器上,所有內容都位於主VLAN上:

Unicast vlan	Entries 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
Multica: vlan	st Entries mac address	type	ports	
1	0100.0ccc.ccce	svstem G	;i1/1	
1	1111.1111.1111	system G	;i1/1	
266	ffff.ffff.ffff	system G	i1/1,Gi1/2	

N1K上的隔離PVLAN,N1K上行鏈路埠上的混雜埠 — 配置檔案

在此配置中,將包含通向N1K的PVLAN流量,並且只有上游使用主VLAN。

UCS中的配置

以下過程介紹如何將主VLAN新增到vNIC。無需PVLAN配置,因為您只需要主要VLAN。

附註:本示例使用266作為主用裝置,166作為隔離裝置;vlan ID由站點決定。

1. 請注意,共用型別為無。

>> = LAN + () LAN Cloud + = VLANs + = VLAN 266 (266) General Ora Permissions VLAN Group Membership Exerts
General Org Permissions VLAN Group Membership Faults Events

2. 按一下VLAN 266的選擇覈取方塊以將主VLAN新增到vNIC。請勿將其設定為「本機」。

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	-			
🛨 Create	e VLAN		Garad			

配置上游裝置

以下過程介紹了如何配置上游裝置。在這種情況下,上游交換機只需要中繼埠,並且只需要中繼 VLAN 266,因為它是上游交換機看到的唯一VLAN。

在Nexus 5K上,輸入以下命令,並檢查上行鏈路配置:

1. 將VLAN新增為主要:

Nexus5000-5(config-vlan)# vlan 266

2. 確保所有上行鏈路都已配置以中繼VLAN:

interface Ethernet1/1描述與4900的連線switchport mode trunk速度1000interface Ethernet1/3描述與FIB埠5的連線switchport mode trunk速度1000interface Ethernet1/4描述與 FIA埠5的連線switchport mode trunk速度1000 在4900交換器上,執行以下步驟:

1. 在N1K上建立用作主鏈路的VLAN。

2. 將所有介面與4900交換機進行中繼連線,以便通過VLAN。 在上游路由器上,只為VLAN 266建立子介面。在此級別,要求取決於您使用的網路配置。

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

N1K的配置

以下過程介紹了如何配置N1K。

1. 建立並關聯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. 為PVLAN流量建立上行埠配置檔案,其中混雜埠已註明:

```
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. 為隔離VLAN建立埠組;為主要和隔離VLAN建立與主機關聯的PVLAN主機埠:

```
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,將正確的vNIC新增到PVLAN上行鏈路。這是您在UCS設定中的「配置」下將隔 離VLAN新增到的vNIC。

	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. 將VM新增到正確的埠組。

在Hardware(硬體)頁籤中,按一下**Network adapter 1**。為Network Connection下的 Network標籤選擇**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
Video card	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
Floppy drive 1	Client Device	Status: Not supported 1
		Network Connection
		Network label:
		nylan guest (nylan)
		Port: 32
		Switch to advanced settings
1		
Help		OK Cancel
		la l

疑難排解

此程式介紹如何測試配置。

1. 對埠組中配置的其他系統以及混雜埠上的路由器或其他裝置運行ping。通過混雜埠對裝置發出 的ping命令應該能正常工作,而向隔離VLAN中的其他裝置發出的這些ping命令應該會失敗。 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),
Approximate 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 14.17.166.50: Destination host unreachable.
Reply from 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; 這是因為您位於與PVLAN關聯的PVLAN主機埠中。另請注意 , 您會從連線埠通道得知上游裝置, 同時在主VLAN得知上游裝置。

在此螢幕抓圖中,Veth3和Veth 4上的兩台裝置是VM。Po1上的裝置是經過混雜埠的上游裝置。

pvlan(conf	fig-port-prof)# sho	ow mac ad	ldress-tabl	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)#				

在UCS系統上,您應該學習在N1K上使用的主VLAN中用於此通訊的所有MAC。您不應在此學習上游:

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都位於您選擇的主VLAN中:

F340.11. Legend:	.13-Nexus5000-5# shot	v mac addr	ess-tak	le			
VLAN	 primary entry, (age - seconds since MAC Address 	G - Gatewa last seen Type	ay MAC, 1,+ - pr age	(R) - Rout imary entr Secure 1	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	-+ Eth1/4 Eth1/4 Eth1/1	ш
F340.11	.13-Nexus5000-5# 📘						-

5. 在4900交換器上,所有內容均位於您選取的主VLAN上:

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上的社群PVLAN,N1K上行鏈路埠上的混雜埠 — 配置檔案

這是使用UCS的社群VLAN唯一支援的配置。

此配置與在<u>N1K上的隔離PVLAN中設定的配置相同,在N1K上行鏈路埠配置檔案部分設定了混雜</u>埠 。團體與隔離的唯一區別是PVLAN的配置。

要配置N1K,請像在Nexus 5K上那樣建立和關聯VLAN:

```
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
所有其他配置與N1K上的隔離PVLAN相同,N1K上行埠配置檔案上有混雜埠。
```

配置此配置後,您可以與連線到PVLAN使用的vEthernet埠配置檔案的所有VM通訊。

疑難排解

此程式介紹如何測試配置。

1. 對埠組中配置的其他系統以及混雜埠上的路由器或其他裝置運行ping。Ping經過混雜埠並到達 社群中的其他系統應該能正常工作。

٠

- 🗆 × 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 Reply from 14.17.166.61: bytes=32 time<1ms Reply from 14.17.166.61: bytes=32 time<1ms 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 = Oms, Maximum = 1ms, Average = Oms C:\Users\Administrator>ping 14.17.166.51 Pinging 14.17.166.51 with 32 bytes of data: Reply from 14.17.166.51: bytes=32 time<1ms TTL=128 Ping statistics for 14.17.166.51: Packets: Sent = 4, Received = 4, Lost = 0 (Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = Oms, Average = Oms Lost = 0 (0% loss), C:\Users\Administrator>

2. 所有其他故障排除與隔離PVLAN相同。

VMware DVS上的隔離PVLAN和社群PVLAN混合埠

由於DVS和UCS系統都存在配置問題,因此2.2(2c)版之前不支援帶有DVS和UCS的PVLAN。

驗證

目前沒有適用於這些配置的驗證程式。

疑難排解

前面部分提供的資訊可用於對配置進行故障排除。

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>客戶使用)支援某些show命令。使用輸出直譯器工具來檢視show命令輸 出的分析。