Configuración de VLAN privada y UCS con VMware DVS o Cisco Nexus 1000v

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados Antecedentes** Configurar Diagrama de la red UCS con DVS de VMware DVS de VMware Switch ascendente N5k Cambio de comportamiento con UCS versión 3.1(3) Switch ascendente 4900 Verificación Troubleshoot Configuración con Nexus 1000v con puerto promiscuo en N5k ascendente Configuración de UCS Configuración de N1k Configuración con Nexus 1000v con puerto promiscuo en el perfil de puerto de enlace ascendente N1K Configuración de UCS Configuración de dispositivos ascendentes Configuración de N1K

Introducción

Este documento describe el soporte de VLAN privada (PVLAN) para Cisco Unified Computing System (UCS) en la versión 2.2(2c) y posteriores.

Precaución: Hay un cambio en el comportamiento que comienza con la versión 3.1(3a) del firmware de UCS, como se describe en la sección **Cambio de comportamiento con la versión 3.1(3) y posteriores de UCS**.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- UCS
- Switch virtual distribuido (DVS) Cisco Nexus 1000V (N1K) o VMware
- VMware
- Switching de capa 2 (L2)

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Una VLAN privada es una VLAN configurada para el aislamiento de L2 de otros puertos dentro de la misma VLAN privada. Los puertos que pertenecen a una PVLAN están asociados con un conjunto común de VLAN de soporte, que se utilizan para crear la estructura PVLAN.

Hay tres tipos de puertos PVLAN:

- Un puerto promiscuo se comunica con todos los demás puertos PVLAN y es el puerto utilizado para comunicarse con los dispositivos fuera de la PVLAN.
- Un puerto aislado tiene separación L2 completa (que incluye broadcasts) de otros puertos dentro de la misma PVLAN, con la excepción del puerto promiscuo.
- Un puerto de comunidad puede comunicarse con otros puertos en la misma PVLAN así como con el puerto promiscuo. Los puertos comunitarios se aíslan en L2 de los puertos de otras comunidades o de los puertos PVLAN aislados. Las transmisiones sólo se propagan a otros puertos de la comunidad y al puerto promiscuo.

Consulte <u>RFC 5517</u>, <u>VLAN privadas de Cisco Systems</u>: <u>Seguridad escalable en un entorno de</u> <u>varios clientes</u> para comprender la teoría, el funcionamiento y los conceptos de las PVLAN.

Configurar

Diagrama de la red

Con Nexus 1000v o DVS de VMware



Nota: Este ejemplo utiliza VLAN 1750 como la principal, 1785 como aislada y 1786 como VLAN de comunidad.

UCS con DVS de VMware

1. Para crear la VLAN principal, haga clic en el botón de radio **Primary** como el Tipo de uso compartido, e ingrese un **ID de VLAN** de 1750 como se muestra en la imagen.

Name: 1750 VLAN ID: 1750 Native VLAN: No Fabric ID: Dual Network Type: Lan If Type: Vitual Locale: External Transport Type: Ether Owner: Local If Type: If Type: Ether Multicast Policy Name: <not set=""> If Type: If Type: Ether Multicast Policy Instance: org-root/mc-policy-default If Type: Isolated Community Secondary VLANs Isolated Community Isolated Isolated Isolated Name ID Type Transport Native VLAN Sharing Multicast Policy Isolated 1785 1785 Lan Ether No Isolated Isolated 1786 1786 Lan Ether No Community Isolated</not>				
Native VLAN: No Fabric ID: Dual Network Type: Lan If Type: Virtual Locale: External Transport Type: Ether Owner: Local Transport Type: Ether Multicast Policy Name: <not set=""> Create Multicast Pol Multicast Policy Name: org=root/mc-policy-default Create Multicast Pol Sharing Type: None Print Create Secondary Secondary VLNs Secondary VLNs Transport Native VLAN Sharing Multicast Pol Name ID Type Transport Native VLAN Sharing Multicast Pol 1785 Lan Ether No Community Isolated Isolated Isolated</not>	٦			
Network Type: Lan If Type: Virtual Local: External Transport Type: Ether Owner: Local If Type: If Type: <td></td>				
Locale: External Owner: Local Multicast Policy Name: <not set=""> Multicast Policy Name: <not set=""> Multicast Policy Name: <not set=""> Multicast Policy Instance: org-root/mc-policy-default Sharing Type: None None Primary Isolated Community Secondary VLANs Secondary VLANs Y Print Name ID Type Transport Name ID Type Transport Name ID Type Transport Naitive VLAN Sharing Multicast Policy 1785 Ian Ether No Community</not></not></not>				
Owner: Local Multicast Policy Name: <not set=""> Multicast Policy Name: One or primary or Isolated or Community Secondary VLANs Filter Filter Frint Name ID Type Transport Native VLAN Sharing Multicast Policy Multicast Policy Multicast Policy ID Type Transport Native VLAN Sharing Multicast Policy Multicast Policy ID Type Transport Native No Isolated Isolate</not>				
Multicast Policy Name: <i>org + oot set> Multicast Policy Instance: org + oot/mc-policy-default Sharing Type: None ● Primary ● Isolated ● Community Secondary VANs Secondary VANs Secondary VENs Filter Print Name ID Type Transport Name ID Type Transport Native VLAN Sharing Multicast Policy 1785 Lan Ether No I786 Lan Ether No Community</i>	Owner: Local			
Multicast Policy Instance: org-root/mc-policy-default Sharing Type: Isolated Community Secondary VLANs Secondary VLANs Filter Print Name ID Type Transport Native VLAN Sharing Multicast Pol 1785 1785 Lan Ether No Isolated Image: Community 1786 1786 Lan Ether No Community Image: Community	су			
Sharing Type: None Primary Isolated Community Secondary VLANS Filter Print Name ID Type Transport Native VLAN Sharing Multicast Po 1785 1785 Lan Ether No Isolated 1786 Lan Ether No Community				
Secondary VLANs Secondary VLANs Secondary VLANs Image: Secondary VLANs Secondary VLANs Name ID Type Transport Native VLAN Sharing Multicast Point Name ID Type Transport Native VLAN Sharing Multicast Point 1785 1785 Lan Ether No Isolated Isolated 1786 1786 Lan Ether No Community Isolated				
Secondary VLANs Filter Export Print Name ID Type Transport Native VLAN Sharing Multicast Port 1785 1785 Lan Ether No Isolated 1000000000000000000000000000000000000				
A Filter Export Print Name ID Type Transport Native VLAN Sharing Multicast Po 1785 1785 Lan Ether No Isolated 1786 1786 Lan Ether No Community				
NameIDTypeTransportNativeVLAN SharingMulticast Pol17851785LanEtherNoIsolated17861786LanEtherNoCommunity				
1785LanEtherNoIsolated17861786LanEtherNoCommunity	i 🖶			
1786 Lan Ether No Community				
	\mathbf{r}			
<				

2. Cree las VLAN **Aisladas** y **comunitarias** en consecuencia como se muestra en las imágenes. Ninguno de estos debe ser una VLAN nativa.

Properties	
Name: 1785	VLAN ID: 1785
Native VLAN: No	Fabric ID: Dual
Network Type: Lan	If Type: Virtual
Locale: External	Transport Type: Ether
Owner: Local	
Sharing Type: O None O Primary	● Isolated ○ Community Primary VLAN: VLAN 1750 (1750) ▼
- ··· _	
Primary VLAN Properties	
Name: 1750	VLAN ID: 1750
realized as a set	
Native VLAN: No	Fabric ID: Dual
Native VLAN: No Network Type: Lan	Fabric ID: Dual If Type: Virtual
Native VLAN: No Network Type: Lan Locale: External	Fabric ID: Dual If Type: Virtual Transport Type: Ether
Native VLAN: No Network Type: Lan Locale: External Owner: Local	Fabric ID: Dual If Type: Virtual Transport Type: Ether
Native VLAN: No Network Type: Lan Locale: External Owner: Local Multicast Policy Name: <not set=""></not>	Fabric ID: Dual If Type: Virtual Transport Type: Ether
Native VLAN: No Network Type: Lan Locale: External Owner: Local Multicast Policy Name: <not set=""></not>	Fabric ID: Dual If Type: Virtual Transport Type: Ether

Properties						
Name: 1786			VLAN ID:	1786		
Native VLAN: No			Fabric ID:	Dual		
Network Type: Lan			If Type:	Virtual		
Locale: External			Transport Type:	Ether		
Owner: Local						
Sharing Type: O None	○ Primary ○ Isolated	Community	Primary VLAN:	VI AN 175	0 (1750)	-
Changer, per	0	<u> </u>			0 (1700)	
Primary VLAN Propertie						
Name:	1750	VLAN ID:	1750			
Native VLAN:	No	Fabric ID:	Dual			
Network Type:	Lan	If Type:	Virtual			
Locale:	External	Transport Type:	Ether			
Owner:	Local					
Multicast Policy Name:	<not set=""></not>	+ Create Mult	icast Policy			
Multicast Policy Name:	<not set=""></not>	🕂 Create Mult	icast Policy			
Multicast Policy Name: Multicast Policy Instance:	<not set=""></not>	🛨 Create Mult	icast Policy			

3. La tarjeta de interfaz de red virtual (vNIC) en el perfil de servicio lleva VLAN regulares y PVLAN, como se ve en la imagen.

General VLANs Statistics Faults Events			
🔍 Filter 👄 Export 🔂 Print			
VLAN	VLAN ID	Oper VLAN	Native VLAN
1750	1750	fabric/lan/net-1750	O
1785	1785	fabric/lan/net-1785	0
1786	1786	fabric/lan/net-1786	۲
default	1	fabric/lan/net-default	\bigcirc
qam-121	121	fabric/lan/net-qam-121	0
qam-221	221	fabric/lan/net-qam-221	0

4. El canal de puerto de enlace ascendente en UCS transporta VLAN regulares así como PVLAN:

interface port-channel1 description U: Uplink switchport mode trunk pinning border switchport trunk allowed vlan 1,121,221,321,1750,1785-1786 speed 10000 F240-01-09-UCS4-A(nxos)#F240-01-09-UCS4-A(nxos)# show vlan private-vlan Primary Secondary Type Ports -----__ _____ 1785 1786 1750 isolated 1750 community

DVS de VMware

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

VmwareDVS 🚯



vlan 1750 private-vlan primary private-vlan association 1785-1786

vlan 1785 private-vlan isolated

vlan 1786 private-vlan community

interface Vlan1750

ip address 10.10.175.252/24 private-vlan mapping 1785-1786

no shutdown

interface port-channel114

Description To UCS switchport mode trunk switchport trunk allowed vlan 1,121,154,169,221,269,321,369,1750,1785-1786 spanning-tree port type edge spanning-tree bpduguard enable spanning-tree bpdufilter enable vpc 114 <=== if there is a 5k pair in vPC configuration only then add this line to both N5k

Cambio de comportamiento con UCS versión 3.1(3)

Antes de la versión 3.1(3) de UCS, podría tener una VM en una VLAN comunitaria para comunicarse con una VM en la VLAN principal en VMware DVS donde reside la VM de VLAN principal dentro de UCS. Este comportamiento era incorrecto, ya que la VM principal siempre debe estar en sentido ascendente o fuera de UCS. Este comportamiento se documenta a través del ID de defecto <u>CSCvh87378</u>.

A partir de la versión 2.2(2) de UCS en adelante, debido a un defecto en el código, la VLAN de la comunidad pudo comunicarse con la VLAN principal que estaba presente detrás de la FI. Pero Aislado nunca pudo comunicarse con el primario detrás de la FI. Tanto las VM (aisladas como las comunitarias) todavía pueden comunicarse con el primario fuera de la FI.

A partir de 3.1(3), este defecto permite a la comunidad comunicarse con el primario detrás de la FI, se rectificó y, por lo tanto, las VM comunitarias no podrán comunicarse con una VM en la VLAN principal que reside dentro de UCS.

Para resolver esta situación, la VM principal tendría que moverse (hacia el norte) fuera de UCS. Si no es una opción, la VM principal tendría que moverse a otra VLAN que sea una VLAN normal y no una VLAN privada.

Por ejemplo, antes del firmware 3.1(3), una VM en la VLAN 1786 de la comunidad podría comunicarse con una VM en la VLAN 1750 principal que reside dentro de UCS; sin embargo, esta comunicación se interrumpiría en el firmware 3.1(3) y posterior, como se muestra en la imagen.

<u>CSCvh87378</u> se ha abordado en 3.2(3l) y 4.0.4e y superiores para que podamos tener la Vlan principal detrás de UCS. Sin embargo, tenga en cuenta que la vlan aislada dentro de UCS no podrá comunicarse con la vlan principal dentro de UCS. Solo la vlan de comunidad y la vlan principal pueden comunicarse entre sí cuando ambos están detrás de UCS.



Switch ascendente 4900

Nota: En este ejemplo, 4900 es la interfaz L3 a la red externa. Si su topología para L3 es diferente, haga los cambios correspondientes

En el switch 4900, tome estos pasos y configure el puerto promiscuo. La PVLAN termina en el puerto promiscuo.

- 1. Active la función PVLAN si es necesario.
- 2. Cree y asocie las VLAN tal como se hace en Nexus 5K.
- 3. Cree el puerto promiscuo en el puerto de salida del switch 4900. A partir de este punto, los paquetes de VLAN 1785 y 1786 se ven en VLAN 1750 en este caso.

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

En el router ascendente, cree una subinterfaz sólo para la VLAN 1750. En este nivel, los requisitos dependen de la configuración de red que utilice:

interface GigabitEthernet0/1.1

encapsulation dot1Q 1750

IP address10.10.175.254/24

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Este procedimiento describe cómo probar la configuración para VMware DVS con el uso de PVLAN.

1. Ejecute pings a otros sistemas configurados en el grupo de puertos, así como al router u otro dispositivo en el puerto promiscuo. Los ping al dispositivo que pasa por el puerto promiscuo deben funcionar, mientras que aquellos a otros dispositivos en la VLAN aislada deben fallar como se muestra en las imágenes.

🥵 win_1750_vmw_isolated on 🛑 121.12	
File View VM	
🗒 Server Manager	
File Action View Help	
Server Manager (WIN-OHHIS16UTC Server Manager (WIN-OHHIS16UT04)	
Roles Roles Administrator: Command Prompt Autoconfiguration Enabled : Yes	
Diagnost C:\Users\Administrator> Configur C:\Users\Administrator> C:\Users\Administrator>ping 10.10.175.252	
Pinging 10.10.175.252 with 32 bytes of data: Reply from 10.10.175.252: bytes=32 time=1ms TTL=25 Reply from 10.10.175.252: bytes=32 time<1ms TTL=25 Reply from 10.10.175.252: bytes=32 time<1ms TTL=25 Reply from 10.10.175.252: bytes=32 time<1ms TTL=25	5 5 5 5 5
Ping statistics for 10.10.175.252: Packets: Sent = 4, Received = 4, Lost = 0 (0% Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = 1ms, Average = Oms	loss),
C:\Users\Administrator>ping 10.10.175.132	
Pinging 10.10.175.132 with 32 bytes of data: Reply from 10.10.175.131: Destination host unreach Reply from 10.10.175.131: Destination host unreach Reply from 10.10.175.131: Destination host unreach Reply from 10.10.175.131: Destination host unreach	able. able. able. able.
Ping statistics for 10.10.175.132: Packets: Sent = 4, Received = 4, Lost = 0 (0%	loss),
C:\Users\Administrator> C:\Users\Administrator>ipconfig /all	
Windows IP Configuration	
	T04
Primary Dns Suffix	104
Ethernet adapter Local Area Connection 4:	
Connection-specific DNS Suffix .: Description	rnet Adapter #3 57-7F 1 <preferred) Ø 2</preferred)

Verifique las tablas de direcciones MAC para ver dónde se está aprendiendo su MAC. En todos los switches, el MAC debe estar en la VLAN aislada excepto en el switch con el puerto promiscuo.

En el switch promiscuo, el MAC debe estar en la VLAN principal.

2. UCS como se muestra en la imagen.

P 191.75 - PuTTY	
F240-01-09-UCS4-A(nxos)#	A
F240-01-09-UCS4-A(nxos)#	
F240-01-09-UCS4-A(nxos) #	
F240-01-09-UCS4-A(nxos)#	
F240-01-09-UCS4-A(nxos)#	
F240-01-09-UCS4-A(nxos)#	
F240-01-09-UCS4-A(nxos)#	
F240-01-09-UCS4-A(nxos)# show mac address-table vlan 1785	
Legend:	
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay N	IAC
age - seconds since last seen, + - primary entry using VPC Peer-Link	
VLAN MAC Address Type age Secure NIFI Ports/SWID.SS.	LD.LID
* 1785 0050.568e.577f dynamic 0 F F Veth2486	
F240-01-09-UCS4-A(nxos)#	
F240-01-09-UCS4-A(nxos)# show mac address-table vlan 1786	
Legend:	
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC, (R) - Routed MAC, O - Overlay MAC	4AC
age - seconds since last seen,+ - primary entry using vPC Peer-Lin)	c
VLAN MAC Address Type age Secure NTFY Ports/SWID.SS	ID.LID
++++++++	
* 1786 0050.568e.73c2 dynamic 0 F F Veth2486	
* 1786 0050.568e.76d7 dynamic 0 F F Veth2486	
F240-01-09-0CS4-A(nxos) #	

3. Verifique en el flujo ascendente n5k el mismo MAC, la salida similar a la anterior debe estar presente en n5k y como se muestra en la imagen.

```
f241-01-08-5596-a# show mac address-table | inc 577f
* 1785
          0050.568e.577f
                            dynamic
                                      170
                                                 F
                                                      F
                                                         Po114
f241-01-08-5596-a#
f241-01-08-5596-a# show mac address-table | inc 73c2
* 1786
          0050.568e.73c2
                            dynamic
                                      10
                                                 F
                                                      F
                                                         Po114
f241-01-08-5596-a# show mac address-table | inc 76d7
* 1786
          0050.568e.76d7 dynamic
                                      30
                                                 F
                                                      F
                                                         Po114
f241-01-08-5596-a#
```

Configuración con Nexus 1000v con puerto promiscuo en N5k ascendente

Configuración de UCS

La configuración de UCS (que incluye la configuración vNIC de perfil de servicio) permanece igual que en el ejemplo con VMware DVS.

Configuración de N1k

vlan 1750 private-vlan primary private-vlan association 1785-1786 vlan 1785 private-vlan isolated vlan 1786 private-vlan community same uplink port-profile is being used for regular vlans & pvlans. In this example vlan 121 & 221 are regular vlans but you can change them accordingly port-profile type ethernet pvlan-uplink-no-prom switchport mode trunk mtu 9000 switchport trunk allowed vlan 121,221,1750,1785-1786 channel-group auto mode on mac-pinning system vlan 121 no shutdown state enabled vmware port-group port-profile type vethernet pvlan_1785 switchport mode private-vlan host switchport private-vlan host-association 1750 1785 switchport access vlan 1785 no shutdown state enabled vmware port-group

port-profile type vethernet pvlan_1786 switchport mode private-vlan host switchport access vlan 1786 switchport private-vlan host-association 1750 1786 no shutdown state enabled vmware portgroup

Este procedimiento describe cómo probar la configuración.

1. Ejecute pings a otros sistemas configurados en el grupo de puertos, así como al router u otro dispositivo en el puerto promiscuo. Los ping al dispositivo que pasa por el puerto promiscuo deben funcionar, mientras que aquellos a otros dispositivos en la VLAN aislada deben fallar, como se muestra en la sección anterior y en las imágenes.