Verificar el comportamiento de sincronización de la tabla MAC de Nexus serie 9000 ARP & con línea troncal L2 sin vPC

Contenido

Introducción

Este documento describe el comportamiento de ARP y MAC Table que puede ocurrir entre los dispositivos Nexus 9000 que comparten un troncal de Capa 2 no vPC.

Antecedentes

Este comportamiento solo se produce cuando las SVI no utilizan direcciones MAC definidas por el usuario y la función de gateway de par vPC se configura en el dominio vPC. Además, sólo se puede ver cuando la tabla ARP permanece llena, mientras que la tabla de direcciones MAC no tiene una entrada MAC para un host determinado.

El comportamiento descrito en este documento es una limitación ASIC de los switches Nexus de primera generación y no afecta a los switches Nexus 9300 Cloud Scale (EX/FX/GX/C) y posteriores, y se ha documentado como parte de la identificación de error de Cisco CSCuh94866.

Requirements

Conocimiento general de Virtual Port Channel (vPC), la función de gateway por canal de puerto virtual de Nexus y el sistema operativo Nexus (NXOS).

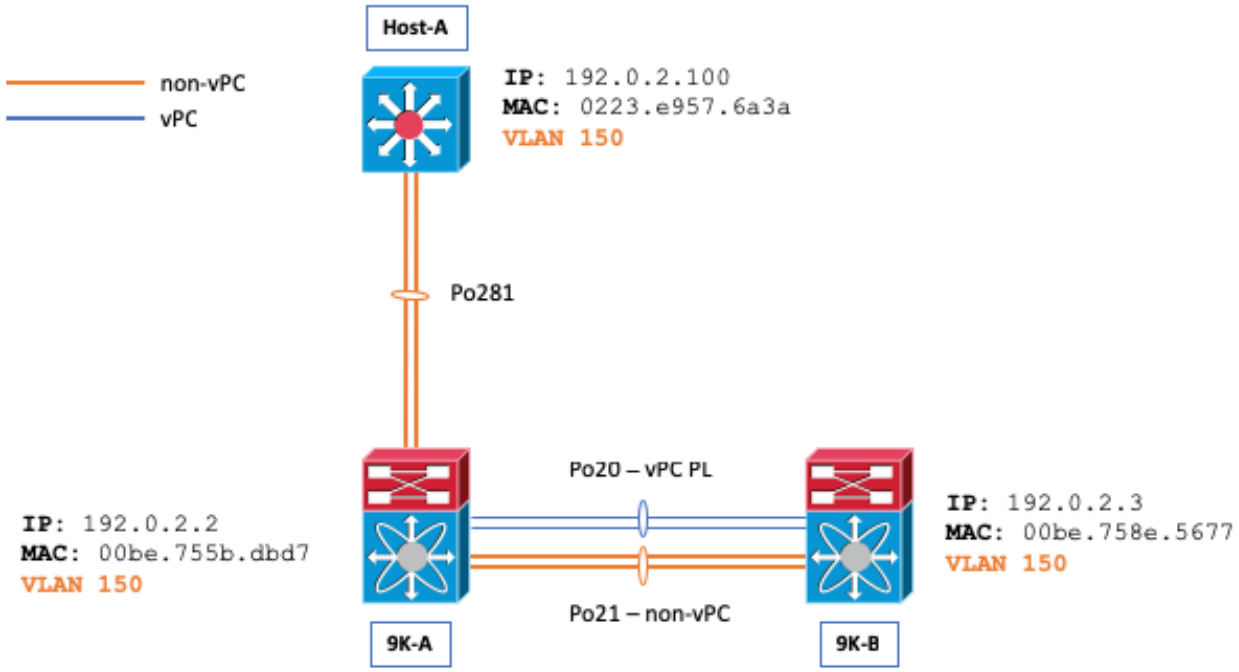
Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

- Nexus 3000s/Nexus 9000s (solo primera generación)
- Función Virtual Port Channel (vPC)

- Función de gateway de par vPC
- Troncal sin vPC de capa 2 (L2)
- SVI no vPC
- NX-OS 7.0(3)I7(5)

Topología



Overview

Considere un escenario donde las tablas ARP y MAC Address están vacías entre Host-A y N9K-B, y se inicia un ping desde Host-A a N9K-B.

```
Host-A# ping 192.0.2.3
PING 192.0.2.3 (192.0.2.3): 56 data bytes
36 bytes from 192.0.2.100: Destination Host Unreachable
Request 0 timed out
64 bytes from 192.0.2.3: icmp_seq=1 ttl=254 time=1.011 ms
64 bytes from 192.0.2.3: icmp_seq=2 ttl=254 time=0.763 ms
64 bytes from 192.0.2.3: icmp_seq=3 ttl=254 time=0.698 ms
64 bytes from 192.0.2.3: icmp_seq=4 ttl=254 time=0.711 ms

--- 192.0.2.3 ping statistics ---
5 packets transmitted, 4 packets received, 20.00% packet loss
round-trip min/avg/max = 0.698/0.795/1.011 ms
```

El ping del Host A hace que el Host A envíe una Solicitud ARP para 9K-B. La solicitud ARP sale del Po21 en N9K-A (inundado en la VLAN) mientras que también en Po20 (tunelado a través de Cisco Fabric Services [CFS]). Como resultado, la tabla de direcciones MAC en 9K-B se rellena correctamente, y se inserta una entrada ARP en la tabla ARP de N9K-B que apunta a Po21 (el trunk L2 no vPC) para la dirección MAC del Host-A de 0223.e957.6a3a.

```
N9K-B# show ip arp 192.0.2.100

Flags: * - Adjacencies learnt on non-active FHRP router
       + - Adjacencies synced via CFSoE
       # - Adjacencies Throttled for Glean
       CP - Added via L2RIB, Control plane Adjacencies
       PS - Added via L2RIB, Peer Sync
       RO - Re-Originated Peer Sync Entry
       D - Static Adjacencies attached to down interface

IP ARP Table
Total number of entries: 1
Address         Age       MAC Address     Interface       Flags
192.0.2.100   00:01:07  0223.e957.6a3a  Vlan150

N9K-B# show mac address-table address  | i i 6a3a
*  150     0223.e957.6a3a   dynamic  0         F      F    Po21

N9K-B# show ip arp detail | i 3a
192.0.2.100   00:03:22  0223.e957.6a3a  Vlan150          port-channel21   <<<< Expected port-
channel
```

El problema puede observarse cuando la dirección MAC para el Host-A se elimina de la tabla de direcciones MAC de N9K-B. La dirección MAC se puede eliminar por varios motivos, como la antigüedad de la dirección MAC, las notificaciones de cambio de topología (TCN) del protocolo de árbol de extensión (STP), la ejecución del comando clear mac address-table dynamic a través de la interfaz de línea de comandos, etc.

```
N9K-B# show ip arp 192.0.2.100

Flags: * - Adjacencies learnt on non-active FHRP router
       + - Adjacencies synced via CFSoE
       # - Adjacencies Throttled for Glean
       CP - Added via L2RIB, Control plane Adjacencies
       PS - Added via L2RIB, Peer Sync
       RO - Re-Originated Peer Sync Entry
       D - Static Adjacencies attached to down interface

IP ARP Table
Total number of entries: 1
Address         Age       MAC Address     Interface       Flags
192.0.2.100   00:00:29     0223.e957.6a3a  Vlan150              <<< ARP remains populated

N9K-B# show mac address-table address 0223.e957.6a3a
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan
   VLAN     MAC Address      Type      age     Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------




N9K-B# ping 192.0.2.100
PING 192.0.2.100 (192.0.2.100): 56 data bytes
64 bytes from 192.0.2.100: icmp_seq=0 ttl=253 time=1.112 ms
64 bytes from 192.0.2.100: icmp_seq=1 ttl=253 time=0.647 ms
64 bytes from 192.0.2.100: icmp_seq=2 ttl=253 time=0.659 ms
```

```
64 bytes from 192.0.2.100: icmp_seq=3 ttl=253 time=0.634 ms
64 bytes from 192.0.2.100: icmp_seq=4 ttl=253 time=0.644 ms

--- 192.0.2.100 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.634/0.739/1.112 ms
```

Observe que los pings aún son exitosos; sin embargo, nuestra entrada ARP ahora apunta a Po20 (vPC PL) en lugar de Po21, que no es el canal de puerto esperado ya que VLAN 150 es una VLAN que no es VPC:

```
N9K-B# show ip arp detail | i i 6a3a

Flags: * - Adjacencies learnt on non-active FHRP router
       + - Adjacencies synced via CFSoE
       # - Adjacencies Throttled for Glean
       CP - Added via L2RIB, Control plane Adjacencies
       PS - Added via L2RIB, Peer Sync
       RO - Re-Originated Peer Sync Entry

IP ARP Table for context default
Total number of entries: 2
Address         Age       MAC Address     Interface        Physical Interface  Flags
192.0.2.100   00:15:54   0223.e957.6a3a    Vlan150          port-channel20   <<< Not Po21 once
the issue is triggered.
```

Puede utilizar el comando **show ip arp internal event-history event** en ambos switches Nexus 9000 para demostrar que los paquetes se tunelizan a través de Cisco Fabric Services (CFS):

```
N9K-B# show ip arp internal event-history event | i i tunnel
    [116] [27772]: Tunnel Packets came with: vlan: 150, L2-SMAC :0223.e957.6a3a, L2-DMAC:
00be.758e.5677
    [116] [27772]: Received tunneled packet on iod: Vlan150, physical iod: port-channel20

N9K-A# show ip arp internal event-history event | i i tunnel
    [116] [28142]: Tunnel Packets sent with: vlan: 150, L2-SMAC :0223.e957.6a3a, L2-DMAC:
00be.758e.5677
    [116] [28142]: Tunnel it to peer destined to remote SVI's Gateway MAC. Peer Gateway Enabled
```

También puede utilizar la serie **debug ip arp** de comandos debug en 9K-B para detallar este comportamiento:

```
N9K-B# debug logfile TAC_ARP
N9K-B# debug ip arp packet
N9K-B# debug ip arp event
N9K-B# debug ip arp error

N9K-B# show debug logfile TAC_ARP | beg "15:31:23"
2018 Oct 11 15:31:23.954433 arp: arp_send_request_internal: Our own address 192.0.2.3 on
interface Vlan150,sender_pid =27661
2018 Oct 11 15:31:23.955221 arp: arp_process_receive_packet_msg: Received tunneled packet on
iod: Vlan150, physical iod: port-channel20
2018 Oct 11 15:31:23.955253 arp: arp_process_receive_packet_msg: Tunnel Packets came with: vlan:
150, L2-SMAC :0223.e957.6a3a, L2-DMAC: 00be.758e.5677
2018 Oct 11 15:31:23.955275 arp: (context 1) Receiving packet from Vlan150, logical interface
Vlan150 physical interface port-channel20, (prty 6) Hrd type 1 Prot type 800 Hrd len 6 Prot len
4 OP 2,  Pkt size 46
2018 Oct 11 15:31:23.955293 arp: Src 0223.e957.6a3a/192.0.2.100 Dst 00be.758e.5677/192.0.2.3
2018 Oct 11 15:31:23.955443 arp: arp_add_adj: arp_add_adj: Updating MAC on interface Vlan150,
phy-interface port-channel20, flags:0x1
2018 Oct 11 15:31:23.955478 arp: arp_adj_update_state_get_action_on_add: Different
```

```
MAC(0223.e957.6a3a) Successful action on add Previous State:0x10, Current State:0x10 Received
event:Data Plane Add, entry: 192.0.2.100, 0000.0000.0000, Vlan150, action to be taken
send_to_am:TRUE, arp_aging:TRUE
2018 Oct 11 15:31:23.955576 arp: arp_add_adj: Entry added for 192.0.2.100, 0223.e957.6a3a, state
2 on interface Vlan150, physical interface port-channel20, ismct 0. flags:0x10, Rearp (interval:
0, count: 0), TTL: 1500 seconds update_shm:TRUE
2018 Oct 11 15:31:23.955601 arp: arp_add_adj: Adj info: iod: 77, phy-iod: 91, ip: 192.0.2.100,
mac: 0223.e957.6a3a, type: 0, sync: FALSE, suppress-mode: ARP Suppression Disabled flags:0x10
```

La respuesta ARP ingresa 9K-A desde el Host-A y luego se tuneliza a 9K-B. Observe que 9K-A dirige la respuesta ARP al plano de control, ya que se ha habilitado la mejora del dominio **vPC de gateway de par**. Esto hace que 9K-A rutee el paquete en nombre de N9K-B, incluso si se trata de una VLAN que no es vPC.

```
N9K-A# ethanalyzer local interface inband display-filter arp limit-c 0

Capturing on inband
2018-10-11 15:32:47.378648 00:be:75:8e:56:77 -> ff:ff:ff:ff:ff:ff ARP Who has 192.0.2.100?  Tell
192.0.2.3 <<<<
2018-10-11 15:32:47.379262 02:23:e9:57:6a:3a -> 00:be:75:8e:56:77 ARP 192.0.2.100 is at
02:23:e9:57:6a:3a
```

Puede utilizar la función de captura de paquetes del plano de control de Ethanalyzer de NX-OS para mostrar que el plano de control de 9K-B nunca ve esta respuesta ARP de forma nativa.

```
N9K-B# ethanalyzer local interface inband display-filter arp limit-c 0

Capturing on inband
2018-10-11 15:33:30.053239 00:be:75:8e:56:77 -> ff:ff:ff:ff:ff:ff ARP Who has 192.0.2.100?  Tell
192.0.2.3
2018-10-11 15:34:16.817309 00:be:75:8e:56:77 -> ff:ff:ff:ff:ff:ff ARP Who has 192.0.2.100?  Tell
192.0.2.3
2018-10-11 15:34:42.222965 00:be:75:8e:56:77 -> ff:ff:ff:ff:ff:ff ARP Who has 192.0.2.44?  Tell
192.0.2.43
<snip>
```

> **Precaución**: Dependiendo de la secuencia de eventos y circunstancias, podría experimentar la pérdida de paquetes de N9K-B al Host-A

```
N9K-B# ping 192.0.2.100
PING 192.0.2.100 (192.0.2.100): 56 data bytes
36 bytes from 192.0.2.3: Destination Host Unreachable
Request 0 timed out
Request 1 timed out
Request 2 timed out
Request 3 timed out
Request 4 timed out

--- 192.0.2.100 ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss
```

Este comportamiento se produce cuando las direcciones MAC definidas por el usuario de SVI no se configuran en SVI que no son vPC, incluso cuando no se utilizan para enrutar adyacencias a través de vPC. Este comportamiento solo se aplica a los switches Nexus 9000 de primera generación.

Para evitar este comportamiento, cambie la dirección MAC de las SVI afectadas.

```
N9K-A(config)# interface Vlan150
N9K-A(config-if)# mac-address 0000.aaaa.0030
N9K-A(config-if)# end

N9K-B(config)# interface Vlan150
N9K-B(config-if)# mac-address 0000.bbbb.0030
N9K-B(config-if)# end
```

> **Nota**: debido a una limitación de hardware, solo puede tener 16 direcciones MAC definidas por el usuario configuradas por dispositivo a la vez. Esto se documenta en la Guía de Configuración de Interfaces NX-OS de Cisco Nexus serie 9000.

Después de aplicar la solución alternativa, puede utilizar la función de captura de paquetes del plano de control de Ethanalyzer de NX-OS para mostrar cómo 9K-A nunca dirige la respuesta ARP a su plano de control.

```
N9K-A# ethanalyzer local interface inband display-filter arp limit-c 0

Capturing on inband
2018-10-11 15:36:11.675108 00:00:bb:bb:00:30 -> ff:ff:ff:ff:ff:ff ARP Who has 192.0.2.100?  Tell
192.0.2.3
```

Información Relacionada

Consulte el documento Creación de Topologías para el Ruteo sobre el Canal de Puerto Virtual para obtener más información sobre los trunks no vPC de Capa 2, las adyacencias de ruteo y los requisitos de MAC definido por el usuario SVI.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).