Vérification du comportement de synchronisation de la table MAC du & ARP de la gamme Nexus 9000 avec une agrégation L2 non vPC

Table des matières

Introduction

Ce document décrit le comportement des tables ARP et MAC qui peut se produire entre les périphériques Nexus 9000 qui partagent une agrégation de couche 2 non-vPC.

Informations générales

Ce comportement se produit uniquement lorsque les interfaces SVI n'utilisent pas d'adresses MAC définies par l'utilisateur et que la fonctionnalité de passerelle homologue vPC est configurée sous le domaine vPC. En outre, il peut uniquement être vu lorsque la table ARP reste remplie, alors que la table d'adresses MAC ne comporte pas d'entrée MAC pour un hôte donné.

Le comportement décrit dans ce document est une limitation ASIC des commutateurs Nexus de première génération et n'affecte pas les commutateurs Nexus 9300 Cloud Scale (EX/FX/GX/C) et ultérieurs et a été documenté dans le cadre de l'ID de bogue Cisco CSCuh94866.

Exigences

Connaissance générale de Virtual Port Channel (vPC), de la fonctionnalité de passerelle homologue NXOS Virtual Port Channel et du système d'exploitation Nexus (NXOS).

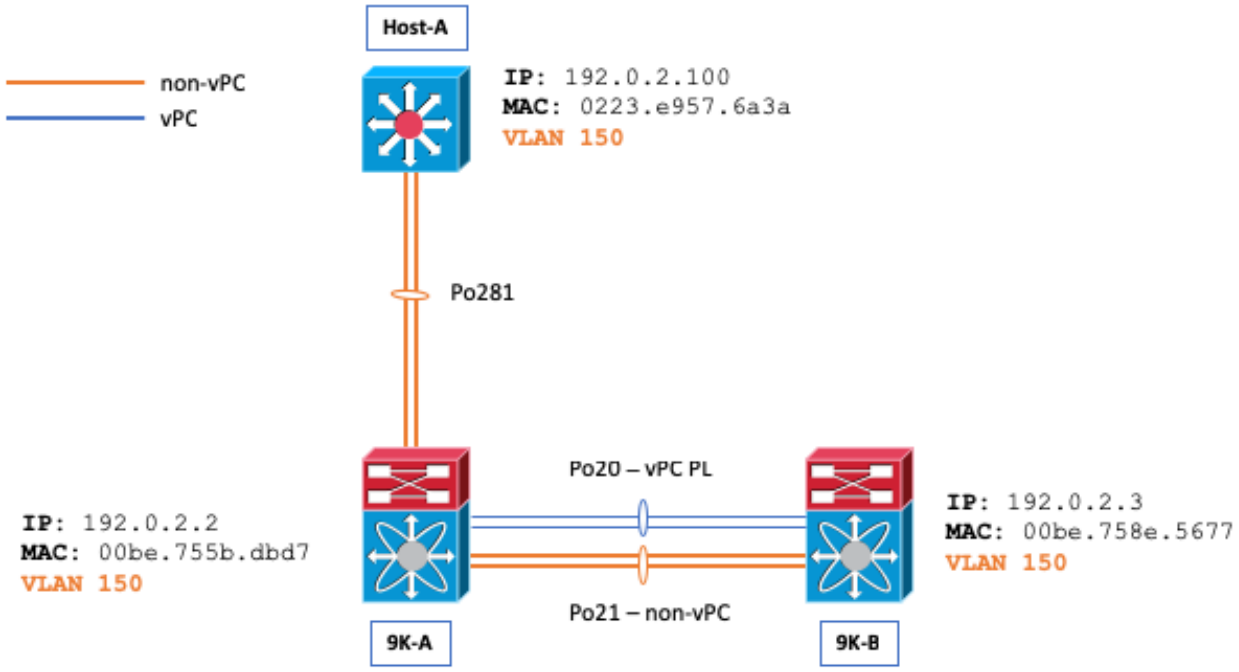
Composants utilisés

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

- Nexus 3000s/Nexus 9000s (première génération uniquement)
- Fonction Virtual Port Channel (vPC)
- Fonction de passerelle d'homologue vPC

- Liaison de couche 2 (L2) non vPC
- SVI non vPC
- NX-OS 7.0(3)I7(5)

Topologie



Aperçu

Imaginez un scénario dans lequel les tables d'adresses ARP et MAC sont vides entre l'hôte A et N9K-B, et une requête ping est lancée de l'hôte A vers 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
```

La requête ping de l'hôte A entraîne l'envoi d'une requête ARP pour 9K-B par l'hôte A. La requête ARP sort de Po21 sur N9K-A (inondée sur le VLAN), mais aussi sur Po20 (tunnelisé via Cisco Fabric Services [CFS]). Par conséquent, la table d'adresses MAC sur 9K-B est remplie correctement, et une entrée ARP est insérée dans la table ARP de N9K-B qui pointe vers Po21 (l'agrégation L2 non-vPC) pour l'adresse MAC de l'hôte A 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
```

Le problème se produit lorsque l'adresse MAC de l'hôte A est supprimée de la table d'adresses MAC de N9K-B. L'adresse MAC peut être supprimée pour diverses raisons, telles que le vieillissement de l'adresse MAC, les notifications de modification de topologie STP (Spanning Tree Protocol), l'exécution de la commande **clear mac address-table dynamic** via l'interface de ligne de commande, 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
```

Notez que les requêtes ping réussissent toujours ; cependant, notre entrée ARP pointe maintenant vers Po20 (la PL vPC) au lieu de Po21, qui n'est pas le port-channel attendu car VLAN 150 est un VLAN non-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.
```

Vous pouvez utiliser la commande **show ip arp internal event-history event** sur les deux commutateurs Nexus 9000 pour démontrer que les paquets sont tunnellisés via 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
```

Vous pouvez également utiliser la série de commandes **debug ip arp** de debug sur 9K-B pour détailler également ce comportement :

```
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 réponse ARP entre 9K-A de l'hôte A et est ensuite tunnellisée vers 9K-B. Notez que 9K-A envoie la réponse ARP au plan de contrôle, car l'amélioration du domaine vPC de la **passerelle homologue** a été activée. Cela amène 9K-A à acheminer le paquet pour le compte de N9K-B, même s'il s'agit d'un VLAN non-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
```

Vous pouvez utiliser la fonction de capture de paquets du plan de contrôle Ethanalyzer de NX-OS pour montrer que le plan de contrôle de 9K-B ne voit jamais cette réponse ARP de manière native.

```
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>
```

> **Attention** : selon la séquence d'événements et les circonstances, vous pourriez subir une perte de paquets de N9K-B vers l'hôte 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
```

Ce comportement se produit lorsque les adresses MAC définies par l'utilisateur de l'interface SVI ne sont pas configurées sur des interfaces SVI non-vPC, même lorsqu'elles ne sont pas utilisées pour le routage de contiguïtés sur vPC. Ce comportement s'applique uniquement aux commutateurs Nexus 9000 de première génération.

Pour contourner ce comportement, modifiez l'adresse MAC des interfaces SVI concernées.

```
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
```

> **Remarque** : en raison d'une limitation matérielle, vous ne pouvez configurer que 16 adresses MAC définies par l'utilisateur par périphérique à la fois. Ceci est documenté dans le Guide de configuration des interfaces NX-OS de la gamme Cisco Nexus 9000.

Une fois la solution de contournement appliquée, vous pouvez utiliser la fonction de capture de paquets du plan de contrôle Ethanalyzer de NX-OS pour montrer comment 9K-A ne transfère jamais la réponse ARP vers son plan de contrôle.

```
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
```

Informations connexes

Consultez le document Créer des topologies pour le routage sur le canal de port virtuel pour plus d'informations sur les agrégations non vPC de couche 2, les contiguïtés de routage et les exigences MAC définies par l'utilisateur SVI.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.