Überprüfung des Synchronisierungsverhaltens der Nexus Serie 9000 mit ARP- und MAC-Tabelle und L2-Nicht-vPC-Trunk

Inhalt

Einleitung

In diesem Dokument wird das Verhalten der ARP- und MAC-Tabelle beschrieben, das zwischen Nexus 9000-Geräten auftreten kann, die einen Layer-2-Trunk ohne vPC gemeinsam nutzen.

Hintergrundinformationen

Dieses Verhalten tritt nur auf, wenn SVIs keine benutzerdefinierten MAC-Adressen verwenden und die vPC-Peer-Gateway-Funktion in der vPC-Domäne konfiguriert ist. Außerdem wird sie möglicherweise nur angezeigt, wenn die ARP-Tabelle weiterhin ausgefüllt wird, während die MAC-Adresstabelle keinen MAC-Eintrag für einen bestimmten Host enthält.

Das in diesem Dokument beschriebene Verhalten stellt eine ASIC-Einschränkung für Nexus Switches der ersten Generation dar und hat keine Auswirkungen auf Cloud Scale-Switches (EX/FX/GX/C) der Nexus Serie 9300 und höher und wurde als Teil der Cisco Bug-ID CSCuh94866 dokumentiert.

Anforderungen

Allgemeinwissen über Virtual Port Channel (vPC), die Peer-Gateway-Funktion Virtual Port Channel von NXOS und das Nexus-Betriebssystem (NXOS)

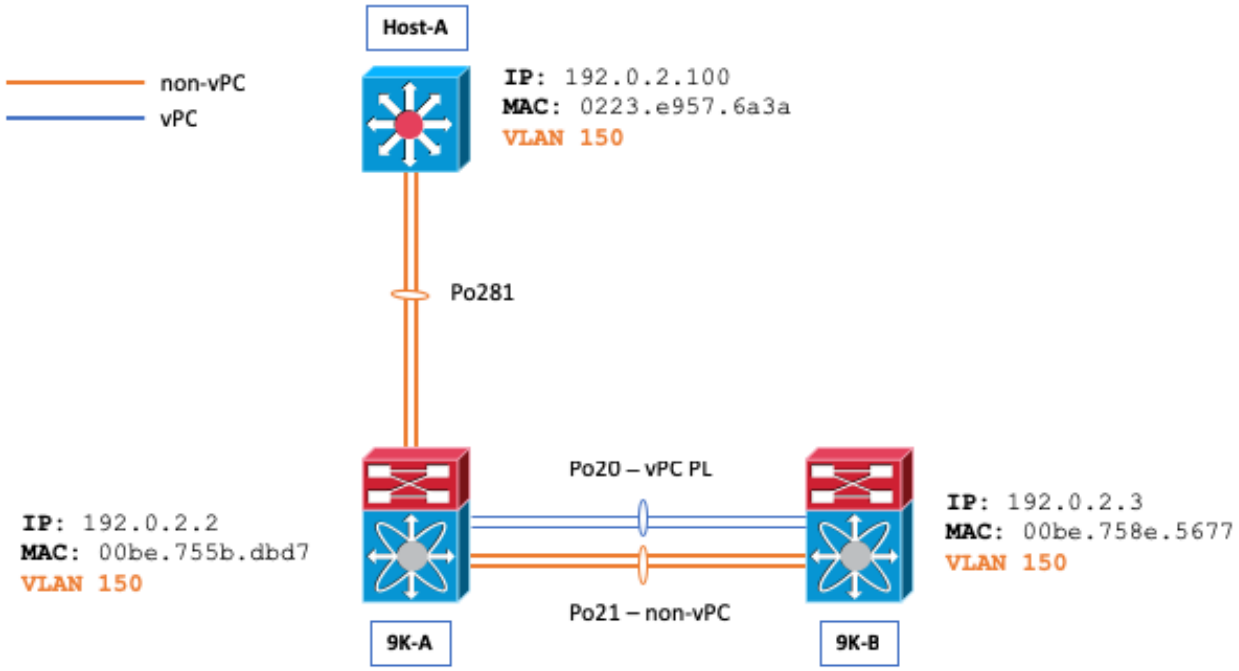
Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

- Nexus 3000s/Nexus 9000s (nur erste Generation)

- Virtual Port Channel-Funktion (vPC)
- vPC-Peer-Gateway-Funktion
- Nicht-vPC Layer 2 (L2)-Trunk
- Nicht-vPC-SVIs
- NX-OS 7.0(3)I7(5)

Topologie



Überblick

Nehmen wir ein Szenario, in dem die ARP- und MAC-Adresstabellen zwischen Host-A und N9K-B leer sind und ein Ping von Host-A zu N9K-B initiiert wird.

```
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
```

Der Ping von Host A veranlasst Host A, eine ARP-Anforderung für 9K-B zu senden. Die ARP-Anforderung geht am Po21 auf N9K-A (im VLAN geflutet) sowie am Po20 (über Cisco Fabric Services [CFS] getunnelt) aus. Dadurch wird die MAC-Adresstabelle auf 9K-B korrekt ausgefüllt, und ein ARP-Eintrag wird in die ARP-Tabelle von N9K-B eingefügt, der auf Po21 (den L2-Trunk ohne vPC) für die MAC-Adresse von Host-A von 0223.e957.6a3a verweist.

```
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
```

Das Problem tritt auf, wenn die MAC-Adresse für Host-A aus der MAC-Adresstabelle von N9K-B entfernt wird. Die MAC-Adresse kann aus verschiedenen Gründen entfernt werden, z. B. aufgrund von veralteten MAC-Adressen, STP-TCN (Topology Change Notifications), Ausführung des Befehls clear mac address-table dynamic über die Befehlszeilenschnittstelle usw.

```
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
```

Beachten Sie, dass die Pings weiterhin erfolgreich sind. Unser ARP-Eintrag verweist nun jedoch auf Po20 (vPC PL) anstelle von Po21, was nicht der erwartete Port-Channel ist, da VLAN 150 ein Nicht-VPC-VLAN ist:

```
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.
```

Mit dem Befehl **show ip arp internal event-history** auf beiden Nexus 9000-Switches können Sie nachweisen, dass Pakete über Cisco Fabric Services (CFS) getunnelt werden:

```
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
```

Sie können auch die **debug ip arp**-Reihe von Debug-Befehlen auf 9K-B verwenden, um dieses Verhalten zu beschreiben:

```
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
```

Die ARP-Antwort geht bei Host A in die 9K-A über und wird dann auf 9K-B getunnelt. Beachten Sie, dass die Funktion "9K-A" die ARP-Antwort an die Steuerungsebene sendet, wenn die vPC-Domänenerweiterung des **Peer-Gateways** aktiviert wurde. Dadurch wird 9K-A veranlasst, das Paket für N9K-B weiterzuleiten, obwohl es sich um ein Nicht-vPC-VLAN handelt.

```
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
```

Sie können die Paketerfassungsfunktion der Steuerungsebene von NX-OS Ethanalyzer verwenden, um zu zeigen, dass die Steuerungsebene von 9K-B diese ARP-Antwort niemals nativ sieht.

```
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>
```

> **Vorsicht**: Je nach Ereignissequenz und Umständen kann es zu Paketverlusten von N9K-B zu Host-A kommen.

```
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
```

Dieses Verhalten tritt auf, wenn benutzerdefinierte SVI-MAC-Adressen nicht auf Nicht-vPC-SVIs konfiguriert werden, auch wenn sie nicht für das Routing von Adjacencies über vPC verwendet werden. Dieses Verhalten gilt nur für Nexus 9000-Switches der ersten Generation.

Um dieses Verhalten zu umgehen, ändern Sie die MAC-Adresse der betroffenen SVIs.

```
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
```

> **Hinweis**: Aufgrund einer Hardwarebeschränkung können jeweils nur 16 benutzerdefinierte MAC-Adressen pro Gerät konfiguriert werden. Dies wird im Konfigurationshandbuch für Cisco Nexus-Schnittstellen der Serie 9000 NX-OS dokumentiert.

Nachdem die Problemumgehung angewendet wurde, können Sie die Paketerfassungsfunktion der Steuerungsebene von NX-OS Ethanalyzer verwenden, um zu zeigen, dass die Funktion "9K-A" die ARP-Antwort nie auf die Steuerungsebene durchschlägt.

```
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
```

Zugehörige Informationen

Weitere Informationen zu Layer-2-Trunks ohne vPC, Routing-Nachbarschaften und benutzerdefinierten SVI-MAC-Anforderungen finden Sie im Dokument Create Topology for Routing over Virtual Port Channel (Topologien für Routing über virtuellen Port-Channel erstellen).

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.