

Verifica del comportamento di sincronizzazione della tabella MAC ARP & Nexus serie 9000 con trunk L2 non vPC

Sommario

[Introduzione](#)

[Premesse](#)

[Requisiti](#)

[Componenti usati](#)

[Topologia](#)

[Panoramica](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive il comportamento ARP e MAC Table che può verificarsi tra dispositivi Nexus 9000 che condividono un trunk non vPC Layer 2.

Premesse

Questo comportamento si verifica solo quando le SVI non utilizzano indirizzi MAC definiti dall'utente e la funzione vPC peer-gateway è configurata nel dominio vPC. Inoltre, può essere visualizzato solo quando la tabella ARP rimane popolata, mentre la tabella degli indirizzi MAC non ha una voce MAC per un dato host.

Il comportamento descritto in questo documento è una limitazione ASIC degli switch Nexus di prima generazione e non influisce sugli switch Nexus 9300 Cloud Scale (EX/FX/GX/C) e versioni successive. È stato documentato come parte dell'ID bug Cisco [CSCuh94866](#).

Requisiti

Conoscenze generali di Virtual Port Channel (vPC), funzionalità peer gateway di NXOS Virtual Port Channel e sistema operativo Nexus (NXOS).

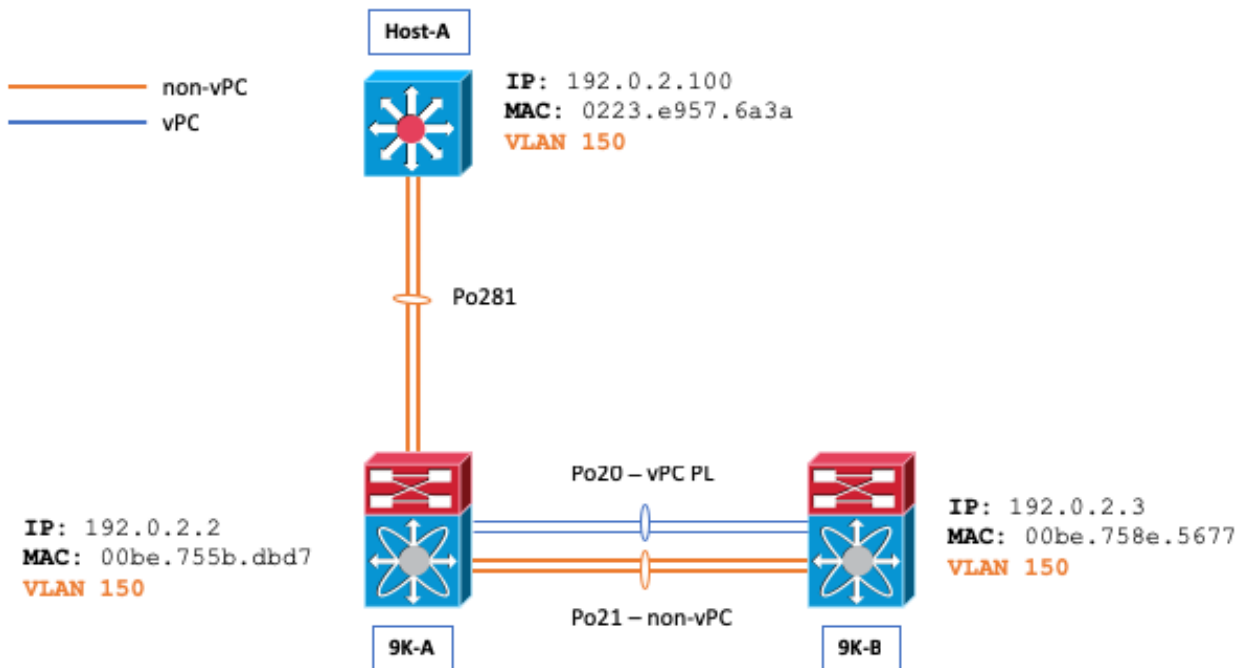
Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

- Nexus 3000s/Nexus 9000s (solo prima generazione)
- Funzionalità Virtual Port Channel (vPC)

- Funzione vPC Peer-Gateway
- Trunk non vPC Layer 2 (L2)
- SVI non vPC
- NX-OS 7.0(3)I7(5)

Topologia



Panoramica

Si consideri uno scenario in cui le tabelle ARP e MAC Address sono vuote tra l'host A e l'host N9K-B e in cui il ping viene avviato dall'host A all'host 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
```

Il ping tra l'host A e l'host A invia una richiesta ARP per 9K-B. La richiesta ARP parte dal Po21 sulla N9K-A (inondata sulla VLAN) e anche sul Po20 (tunneling tramite Cisco Fabric Services [CFS]). Di conseguenza, la tabella degli indirizzi MAC in 9K-B viene popolata correttamente e una voce ARP viene inserita nella tabella ARP di N9K-B che punta a Po21 (il trunk L2 non-vPC) per l'indirizzo MAC dell'host A di 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-channel121 <<<< Expected port-
channel
```

Il problema può essere rilevato quando l'indirizzo MAC per l'host A viene rimosso dalla tabella degli indirizzi MAC di N9K-B. L'indirizzo MAC può essere rimosso per diversi motivi, ad esempio la durata dell'indirizzo MAC, le notifiche TCN (Topology Change Notifications) del protocollo Spanning Tree Protocol (STP), l'esecuzione del comando `clear mac address-table dynamic` tramite l'interfaccia della riga di comando e così via.

```
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
```

Si noti che i ping hanno ancora esito positivo. Tuttavia, la voce ARP ora punta a Po20 (vPC PL) anziché a Po21, che non è il canale previsto a livello di porta perché VLAN 150 è una 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. |

È possibile usare il comando **show ip arp internal event-history** su entrambi gli switch Nexus 9000 per dimostrare che i pacchetti vengono tunneling tramite 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
```

Inoltre, è possibile usare la serie di comandi **debug ip arp** di **debug** sulla versione 9K-B per descrivere in dettaglio questo comportamento:

```
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 risposta ARP entra in 9K-A dall'host-A e viene quindi tunneling a 9K-B. Notare che 9K-A punta la risposta ARP al control plane, poiché il miglioramento del dominio vPC **peer-gateway** è stato abilitato. In questo modo, 9K-A instrada il pacchetto per conto di N9K-B, anche se questa è una 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
```

È possibile utilizzare la funzione di acquisizione dei pacchetti del control plane dell'etanalizzatore del sistema NX-OS per dimostrare che il control plane di 9K-B non vede mai questa risposta ARP in modo nativo.

```
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>
```

Attenzione: a seconda della sequenza di eventi e circostanze, si potrebbe verificare una perdita di pacchetti da N9K-B a 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
```

Questo comportamento si verifica quando gli indirizzi MAC SVI definiti dall'utente non sono configurati su SVI non vPC, anche se non vengono utilizzati per il routing delle adiacenze su vPC. Questo comportamento si applica solo agli switch Nexus 9000 di prima generazione.

Per risolvere questo problema, modificare l'indirizzo MAC delle SVI interessate.

```
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: a causa di una limitazione hardware, è possibile configurare solo 16 indirizzi MAC definiti dall'utente per dispositivo alla volta. Questa condizione è documentata nella [guida alla configurazione delle interfacce Cisco Nexus serie 9000 NX-OS](#).

Una volta applicata la soluzione alternativa, è possibile utilizzare la funzione di acquisizione pacchetti del control plane di Eanalyzer di NX-OS per mostrare come 9K-A non esegua mai punzonature della risposta ARP sul relativo control plane.

```
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
```

Informazioni correlate

Per ulteriori informazioni sui trunk non vPC di layer 2, sulle adiacenze di routing e sui requisiti MAC definiti dall'utente SVI, consultare il [documento Creazione di topologie per il routing su canale della porta virtuale](#).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).