Risoluzione dei problemi relativi all'inoltro esterno ACI

Sommario

Introduzione

In questo documento viene descritto come comprendere e risolvere i problemi relativi a un'uscita L3in ACI

Premesse

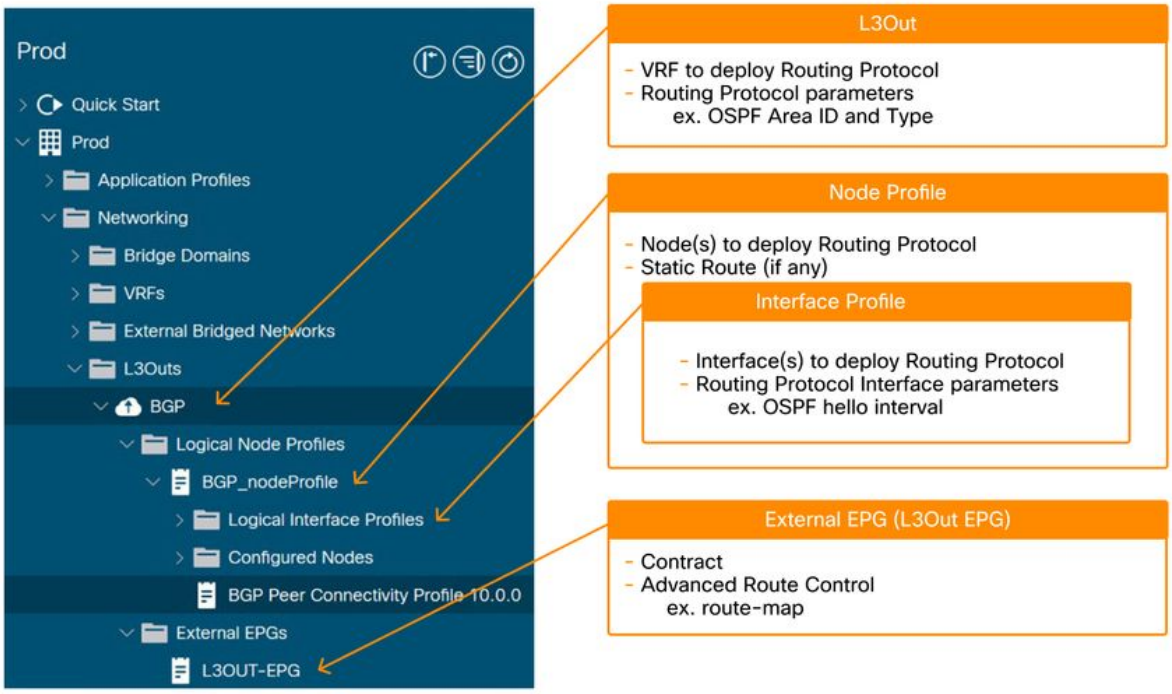
Il materiale di questo documento è stato estratto dal manuale Troubleshooting Cisco Application Centric Infrastructure, Second Edition specificatamente **External Forwarding - Overview (Inoltro esterno), External Forwarding (Inoltro esterno) - Adiacenze (Adiacenze), External Forwarding (Inoltro esterno) - Annuncio router (Inoltro esterno), External Forwarding (Inoltro esterno) - Contract (Contratto) e L3out (Inoltro esterno) - Share L3out (Condivisione** capitoli).

Panoramica

Componenti L3Out

Nella figura seguente vengono illustrati i principali elementi costitutivi necessari per configurare un L3 esterno (L3Out).

Componenti principali di un'uscita L3



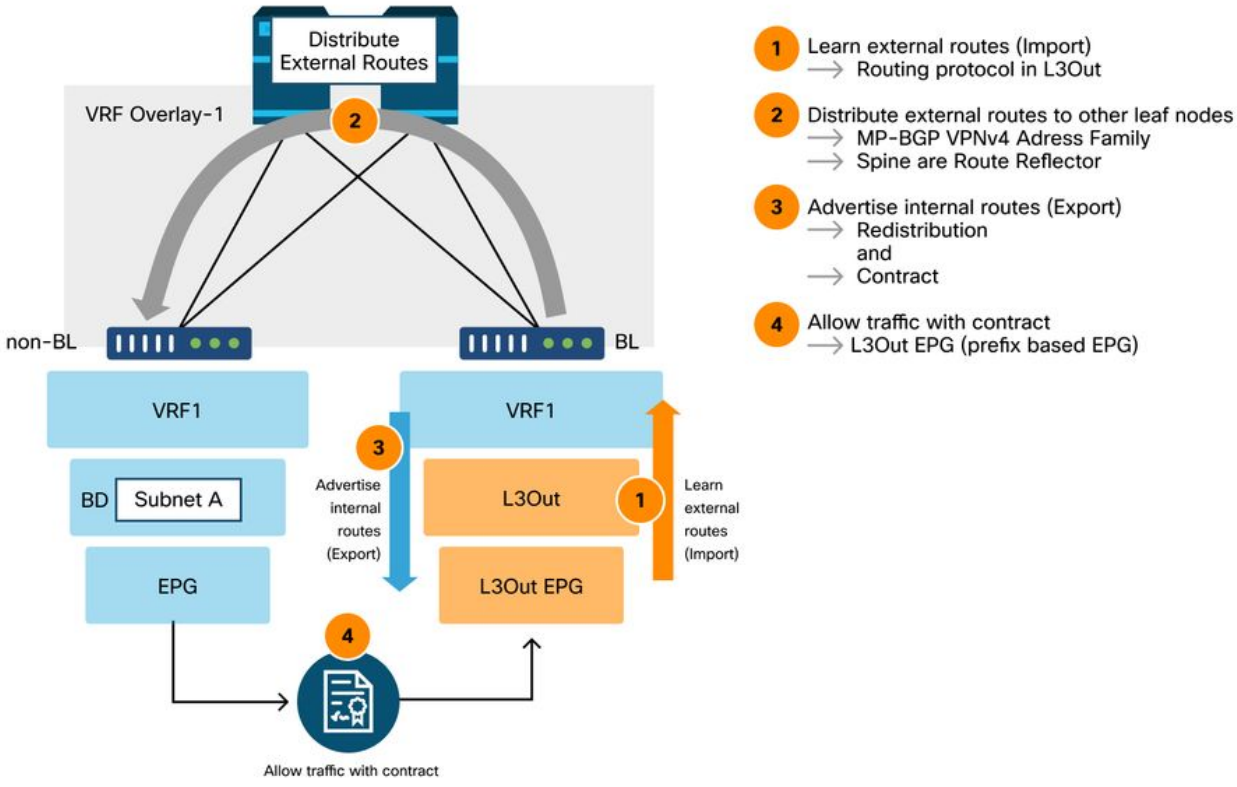
1. Radice di L3Out: Selezionare un protocollo di routing da distribuire (ad esempio OSPF, BGP).Selezionare un VRF per distribuire il protocollo di routing.Selezionare un dominio L3Out per definire le interfacce foglia e la VLAN disponibili per l'uscita L3D.

2. Profilo nodo: Selezionare gli switch foglia per distribuire il protocollo di routing. Questi sono generalmente noti come 'Border Leaf Switches' (BL).Configurare il RID (Router-ID) per il protocollo di routing su ciascuna foglia di bordo. A differenza di un router normale, ACI non assegna automaticamente l'ID del router in base a un indirizzo IP sullo switch.Configurare una route statica.
3. Profilo interfaccia: Configurare le interfacce foglia per eseguire il protocollo di routing. Tipo di interfaccia (SVI, porta instradata, sottointerfaccia), ID interfaccia e indirizzi IP, ecc.Selezionare un criterio per i parametri del protocollo di routing a livello di interfaccia, ad esempio l'intervallo hello.
4. EPG esterno (L3Out EPG): Un 'EPG esterno' è un requisito difficile per implementare tutte le policy legate all'L3Out, come indirizzi IP o SVI per stabilire i router adiacenti. I dettagli su come utilizzare gli EPG esterni verranno trattati più avanti.

Routing esterno

Il diagramma seguente mostra l'operazione di alto livello necessaria per il ciclo esterno.

Flusso di routing esterno di alto livello



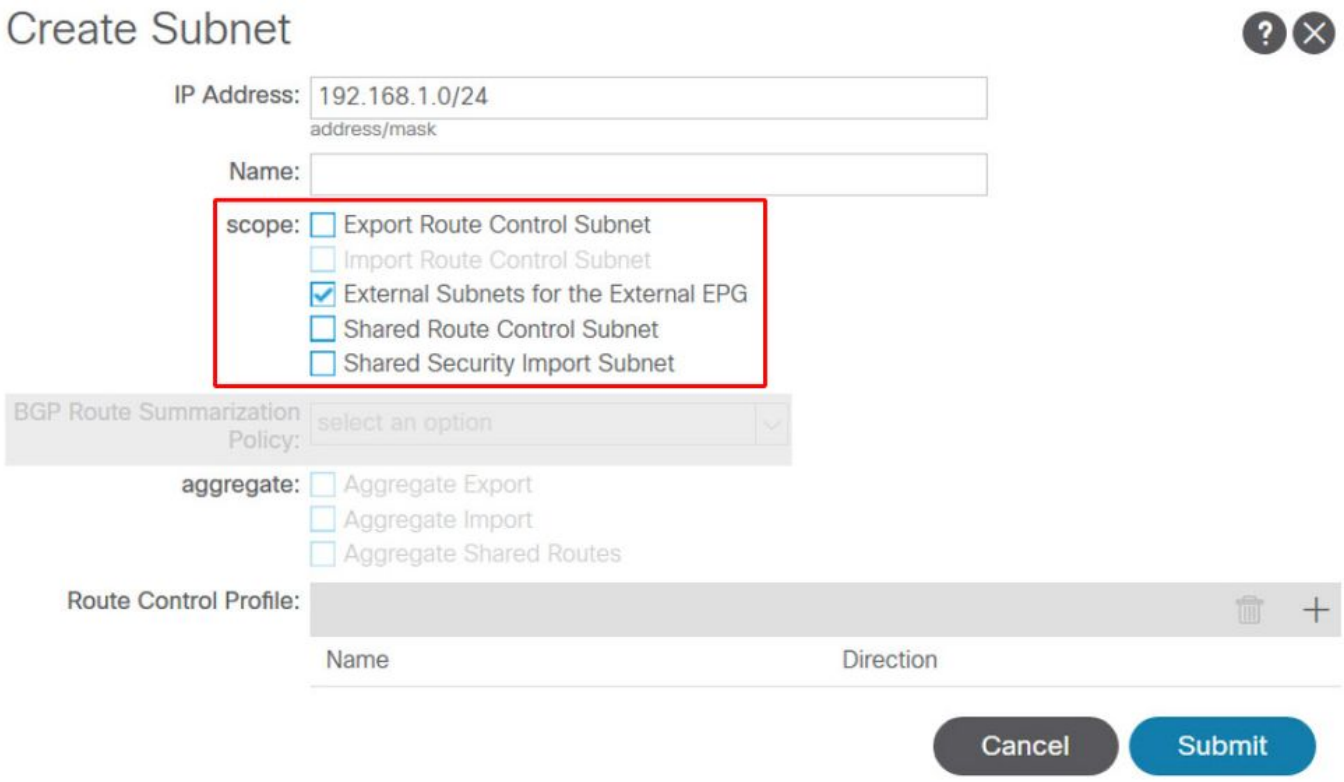
1. Le BL stabiliranno le adiacenze del protocollo di routing con i router esterni.
2. I prefissi di route vengono ricevuti da router esterni e vengono inseriti in MP-BGP come percorso della famiglia di indirizzi VPNv4. Almeno due nodi della spine devono essere configurati come riflettori di route BGP per riflettere le route esterne verso tutti i nodi foglia.
3. I prefissi interni (subnet BD) e/o i prefissi ricevuti da altri L3Out devono essere ridistribuiti esplicitamente nel protocollo di routing per essere annunciati al router esterno.
4. Applicazione della sicurezza: un'uscita L3contiene almeno un'uscita L3EPG. È necessario utilizzare o fornire un contratto nell'EPG L3Out (denominato anche l3extInstP dal nome della

classe) per consentire il traffico in entrata e in uscita da L3Out.

Opzioni di configurazione EPG L3Out

Nella sezione L3Out EPG, le subnet possono essere definite con una serie di opzioni 'Scope' e 'Aggregate', come illustrato di seguito:

Subnet L3Out definita che include la definizione 'scope'



Opzioni 'Ambito':

- **Esporta subnet di controllo route:** questo ambito consente di annunciare (esportare) una subnet da ACI all'esterno tramite L3Out. Benché questo sia principalmente per il routing di transito, potrebbe essere utilizzato anche per pubblicizzare una subnet BD come descritto nella sezione "Annuncio subnet ACI BD".
- **Importa subnet di controllo route:** questo ambito riguarda l'apprendimento (importazione) di una subnet esterna da L3Out. Per impostazione predefinita, questo ambito è disabilitato, quindi è disattivato e una foglia di confine apprende tutte le route da un protocollo di routing. È possibile abilitare questo ambito quando è necessario limitare le route esterne apprese tramite OSPF e BGP. Non è supportato per EIGRP. Per utilizzare questo ambito, è necessario prima abilitare 'Importa applicazione controllo route' su un determinato L3Out.
- **Subnet esterne per l'EPG (import-security):** questo ambito viene utilizzato per consentire i pacchetti con la subnet configurata da o verso l'L3Out con un contratto. Classifica un pacchetto nell'EPG L3Out configurato in base alla subnet in modo che sia possibile applicare un contratto sull'EPG L3Out al pacchetto. Questo ambito è una corrispondenza di prefisso più lunga anziché una corrispondenza esatta come altri ambiti per la tabella di routing. Se 10.0.0.0/16 è configurato con 'Subnet esterne per EPG esterno' in L3Out EPG A, tutti i pacchetti con IP in quella subnet, come 10.0.1.1, saranno classificati in L3Out EPG A per

usare un contratto su di esso. Ciò non significa che 'Subnet esterne per l'ambito EPG esterno' installi una route 10.0.0.0/16 in una tabella di routing. Verrà creata una tabella interna diversa per mappare una subnet a un EPG (pcTag) esclusivamente per un contratto. Non ha alcun effetto sul comportamento del protocollo di routing. L'ambito deve essere configurato su un L3Out che apprende la subnet.
- **Subnet di controllo route condivisa:** questo ambito prevede la perdita di una subnet esterna in un altro VRF. ACI utilizza MP-BGP e Route Target per la perdita di una route esterna da un VRF a un altro. Questo ambito crea un elenco di prefissi con la subnet, che viene utilizzata come filtro per esportare/importare route con destinazione route in MP-BGP. L'ambito deve essere configurato su un L3Out che apprende la subnet nel VRF originale.
- **Subnet di importazione della sicurezza condivisa:** questo ambito viene utilizzato per consentire i pacchetti con la subnet configurata quando i pacchetti vengono spostati tra VRF con L3Out. Una route in una tabella di routing è trapelata a un altro VRF con 'Subnet di controllo della route condivisa' come indicato in precedenza. Tuttavia, un altro VRF non ha ancora saputo a quale EPG deve appartenere la route trapelata. La 'Subnet importazione protezione condivisa' informa un altro VRF dell'EPG L3Out a cui appartiene la route perduta. Pertanto, questo ambito può essere utilizzato solo quando si utilizza anche "Subnet esterne per EPG esterno", altrimenti il VRF originale non sa a quale EPG L3Out appartiene la subnet. Questo ambito è anche la corrispondenza di prefisso più lunga.

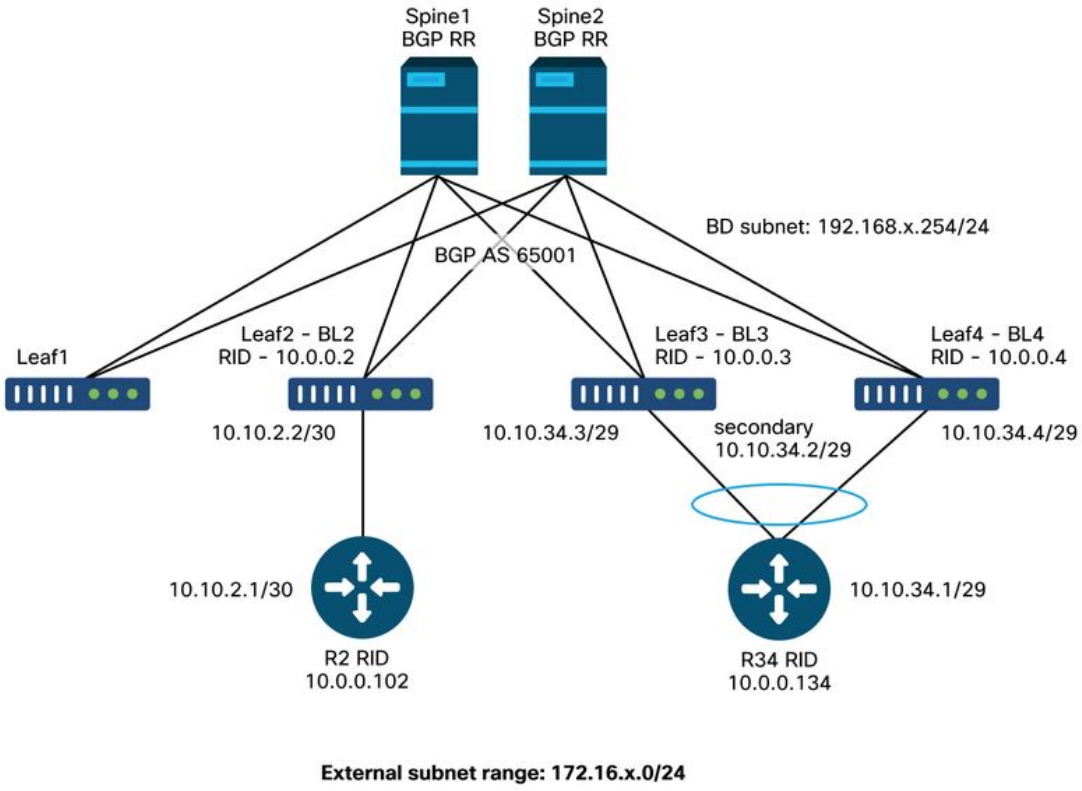
Opzioni 'Aggregate':

- **Esportazione aggregata:** questa opzione può essere utilizzata solo per 0.0.0.0/0 con 'Export Route Control Subnet'. Quando sia 'Export Route Control Subnet' che 'Aggregate Export' sono abilitati per 0.0.0.0/0; crea un prefix-list con '0.0.0.0/0 le 32' che corrisponde a qualsiasi subnet. Pertanto, questa opzione può essere utilizzata quando un'uscita L3D deve annunciare (esportare) qualsiasi route verso l'esterno. Quando è necessaria un'aggregazione più granulare, è possibile utilizzare la mappa/profilo della route con un elenco di prefissi esplicito.
- **Importazione aggregata:** questa opzione può essere utilizzata solo per 0.0.0.0/0 con 'Import Route Control Subnet'. Quando sia 'Importa subnet di controllo route' che 'Importazione aggregata' sono abilitate per 0.0.0.0/0, viene creato un elenco di prefissi con '0.0.0.0/0 le 32' che corrisponde a qualsiasi subnet. Pertanto, questa opzione può essere utilizzata quando un'uscita L3 deve apprendere (importare) qualsiasi route dall'esterno. Tuttavia, è possibile ottenere lo stesso risultato disabilitando 'Importa applicazione controllo route', che è l'impostazione predefinita. Quando è necessaria un'aggregazione più granulare, è possibile utilizzare la mappa/profilo della route con un elenco di prefissi esplicito.
- **Route condivise aggregate:** questa opzione può essere utilizzata per qualsiasi subnet con 'Subnet di controllo route condivise'. Quando sia 'Shared Route Control Subnet' che 'Aggregate Shared Routes' sono abilitate per 10.0.0.0/8, ad esempio, crea un prefisso-elenco con '10.0.0.0/8 le 32' che corrisponde a 10.0.0.0/8, 10.1.0.0/16 e così via.

Topologia L3Out utilizzata in questa sezione

In questa sezione verrà utilizzata la topologia seguente:

Topologia L3Out



Adiacenti

Questa sezione spiega come risolvere i problemi e verificare le adiacenze del protocollo di routing sulle interfacce L3Out.

Di seguito sono riportati alcuni parametri per verificare che siano applicabili a tutti i protocolli di routing esterno ACI:

- **ID router:** in ACI, ogni L3Out deve utilizzare lo stesso ID router nello stesso VRF sulla stessa foglia, anche se i protocolli di routing sono diversi. Inoltre, solo uno degli L3Out sulla stessa foglia può creare un loopback con l'ID del router, che in genere è BGP.
- **MTU:** sebbene il requisito minimo dell'MTU sia solo per l'adiacenza OSPF, si consiglia di far corrispondere l'MTU di tutti i protocolli di routing per essere certi che i pacchetti jumbo utilizzati per lo scambio o gli aggiornamenti delle route possano essere trasmessi senza frammentazione, in quanto la maggior parte dei frame del control plane vengono inviati con il bit DF impostato (non frammentare), che causa il rifiuto del frame se le sue dimensioni superano la MTU massima dell'interfaccia.
- **MP-BGP Router Reflector:** se non si specifica questa opzione, il processo BGP non verrà avviato sui nodi foglia. Sebbene non sia necessario per OSPF o EIGRP solo per stabilire un router adiacente, è comunque necessario che i BL distribuiscano le route esterne ad altri nodi foglia.
- **Errori:** verificare sempre gli errori durante e dopo il completamento della configurazione.

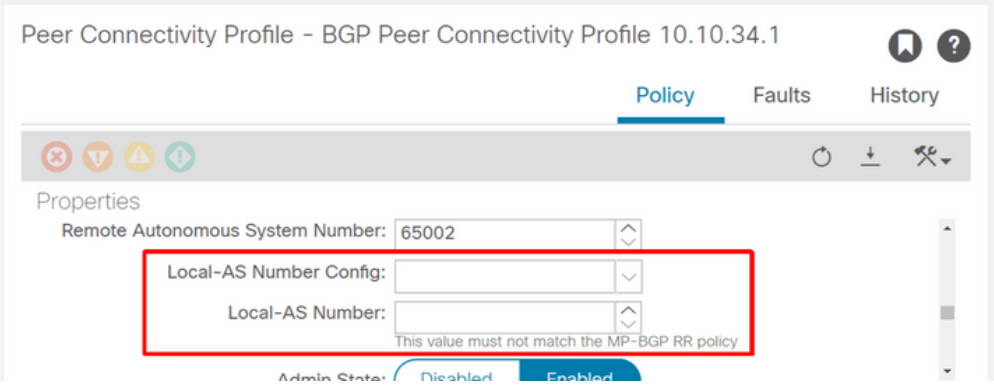
BGP

Questa sezione utilizza un esempio di peer eBGP tra il loopback su BL3, BL4 e R34 dalla topologia nella sezione Panoramica. Il BGP AS su R34 è 65002.

Verificare i seguenti criteri quando si stabilisce un'adiacenza BGP.

- Numero AS BGP locale (lato ACI BL).

Profilo connettività peer - Local-AS

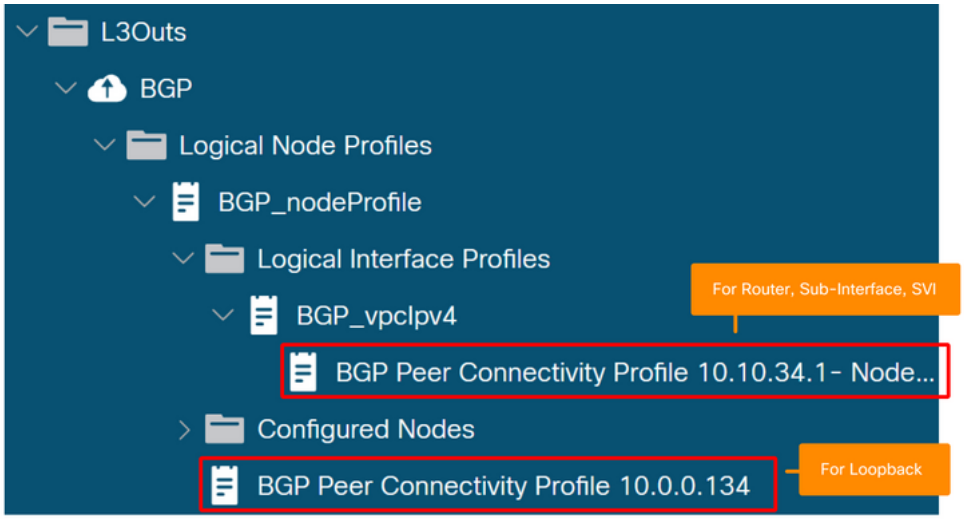


Il numero BGP AS di un utente L3Out sarà automaticamente uguale al numero BGP AS dell'infra-MP-BGP configurato nella policy BGP Route Reflector. La configurazione 'Local AS' nel profilo di connettività peer BGP non è richiesta a meno che non si abbia bisogno di nascondere ACI BGP AS al mondo esterno. Ciò significa che i router esterni devono puntare al BGP AS configurato nel BGP Route Reflector.

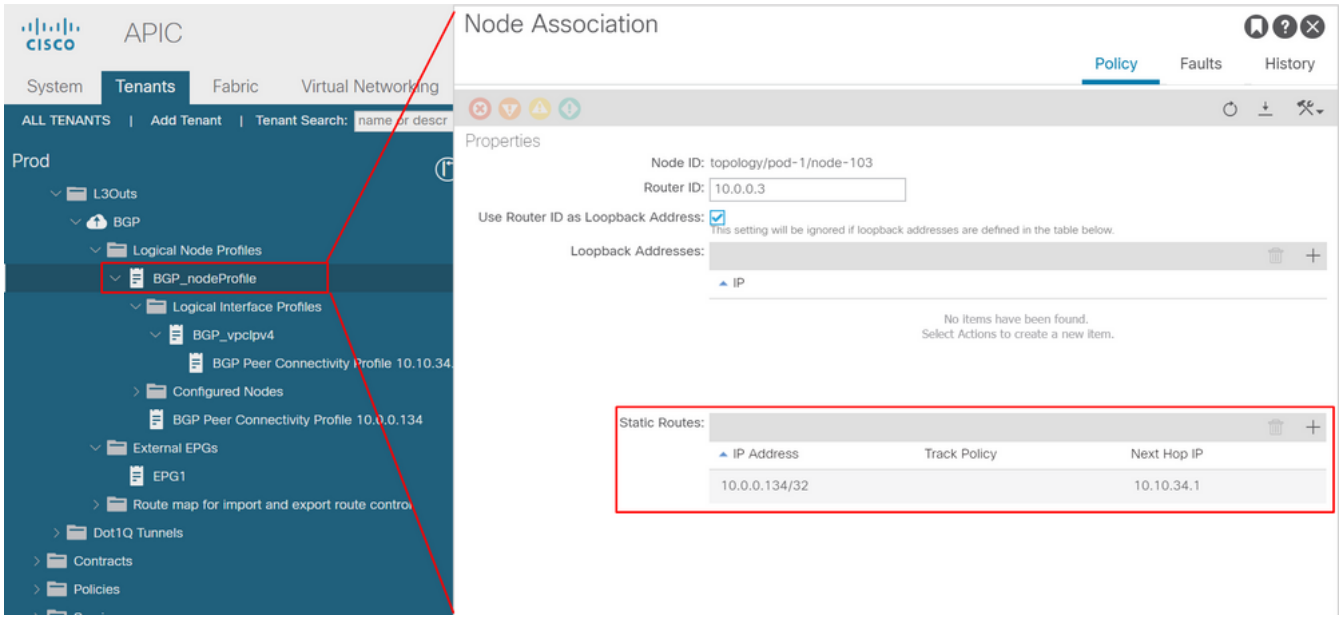
NOTA: lo scenario in cui è richiesta la configurazione di Local AS è lo stesso del comando standalone 'local-as' di NX-OS.

- Numero AS BGP remoto (lato esterno) **Profilo connettività peer - AS remoto**

Il numero BGP AS remoto è richiesto solo per eBGP quando il valore BGP AS del router adiacente è diverso da quello di ACI BGP AS.IP di origine per la sessione peer BGP.**L3Out — Profilo connettività peer BGP**



ACI supporta il sourcing di una sessione BGP dall'interfaccia di loopback su un tipico tipo di interfaccia ACI L3Out (routing, sottointerfaccia, SVI).Se una sessione BGP deve avere origine da un loopback, configurare il profilo BGP Peer Connectivity nel profilo del **nodo** logico.Se la sessione BGP deve avere origine da un'interfaccia/sottointerfaccia/SVI instradata, configurare il profilo BGP Peer Connectivity in Logical **Interface** Profile.Raggiungibilità IP peer BGP.**Profilo nodo logico - Associazione nodo**



Quando gli IP peer BGP sono loopback, verificare che il BL e il router esterno siano raggiungibili dall'indirizzo IP del peer. È possibile utilizzare route statiche o OSPF per ottenere la raggiungibilità agli IP peer.**Verifica CLI BGP (esempio eBGP con loopback)**Gli output CLI per i passi riportati di seguito sono raccolti dalla BL3 nella topologia dalla sezione Panoramica.**1. Verificare se la sessione BGP è stata stabilita**'State/PfxRcd' nell'output CLI seguente indica che la sessione BGP è stabilita.

```
f2-leaf3# show bgp ipv4 unicast summary vrf Prod:VRF1
BGP summary information for VRF Prod:VRF1, address family IPv4 Unicast
BGP router identifier 10.0.0.3, local AS number 65001

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
```

```
10.0.0.134      4 65002      10      10       10    0    0 00:06:39 0
```

Se in 'State/PfxRcd' è visualizzato Idle o Active, i pacchetti BGP non vengono ancora scambiati con il peer. In uno scenario di questo tipo, controllare quanto segue e passare al passaggio successivo.

- Accertarsi che il router esterno punti correttamente all'ACI BGP AS (local AS number 65001).
- Verificare che ACI BGP Peer Connectivity Profile stia specificando l'IP del router adiacente corretto da cui il router esterno sta inviando la sessione BGP (10.0.0.134).
- Verificare che il profilo ACI BGP Peer Connectivity stia specificando il router adiacente corretto AS del router esterno (numero di sistema autonomo remoto nella GUI visualizzato nella CLI come 65002).

2. Verificare i dettagli del router adiacente BGP (profilo connettività peer BGP)

Il comando seguente mostra i parametri chiave per la definizione dei router adiacenti BGP.

- IP router adiacente: 10.0.0.134 .
- BGP AS router adiacente: remoto AS 65002.
- IP di origine: Utilizzo di loopback3 come origine di aggiornamento.
- Multi-hop eBGP: Il peer BGP esterno potrebbe essere a una distanza massima di 2 hop.

```
f2-leaf3# show bgp ipv4 unicast neighbors vrf Prod:VRF1
BGP neighbor is 10.0.0.134,  remote AS 65002, ebgp link,  Peer index 1
 BGP version 4, remote router ID 10.0.0.134
 BGP state = Established, up for 00:11:18
 Using loopback3 as update source for this peer
 External BGP peer might be upto 2 hops away

...

  For address family: IPv4 Unicast
...
Inbound route-map configured is permit-all, handle obtained
Outbound route-map configured is exp-l3out-BGP-peer-3047424, handle obtained
Last End-of-RIB received 00:00:01 after session start
Local host: 10.0.0.3, Local port: 34873
 Foreign host: 10.0.0.134, Foreign port: 179
 fd = 64
```

Una volta stabilito correttamente il peer BGP, l'host locale e l'host esterno vengono visualizzati nella parte inferiore dell'output.

3. Verificare la raggiungibilità IP del peer BGP

```
f2-leaf3# show ip route vrf Prod:VRF1
10.0.0.3/32, ubest/mbest: 2/0, attached, direct
   *via 10.0.0.3, lo3, [0/0], 02:41:46, local, local
   *via 10.0.0.3, lo3, [0/0], 02:41:46, direct
10.0.0.134/32, ubest/mbest: 1/0
   *via 10.10.34.1, vlan27, [1/0], 02:41:46, static    <--- neighbor IP reachability via static
route
10.10.34.0/29, ubest/mbest: 2/0, attached, direct
   *via 10.10.34.3, vlan27, [0/0], 02:41:46, direct
   *via 10.10.34.2, vlan27, [0/0], 02:41:46, direct
```

```
10.10.34.2/32, ubest/mbest: 1/0, attached
   *via 10.10.34.2, vlan27, [0/0], 02:41:46, local, local
10.10.34.3/32, ubest/mbest: 1/0, attached
   *via 10.10.34.3, vlan27, [0/0], 02:41:46, local, local
```

Accertarsi che il ping sull'IP adiacente funzioni dall'IP di origine di ACI BGP.

```
f2-leaf3# iping 10.0.0.134 -V Prod:VRF1 -S 10.0.0.3
PING 10.0.0.134 (10.0.0.134) from 10.0.0.3: 56 data bytes
64 bytes from 10.0.0.134: icmp_seq=0 ttl=255 time=0.571 ms
64 bytes from 10.0.0.134: icmp_seq=1 ttl=255 time=0.662 ms
```

4. Controllare la stessa cosa sul router esterno

Di seguito è riportato un esempio di configurazione sul router esterno (NX-OS standalone).

```
router bgp 65002
 vrf f2-bgp
   router-id 10.0.0.134
   neighbor 10.0.0.3
     remote-as 65001
     update-source loopback134
     ebgp-multihop 2
     address-family ipv4 unicast
   neighbor 10.0.0.4
     remote-as 65001
     update-source loopback134
     ebgp-multihop 2
     address-family ipv4 unicast

interface loopback134
 vrf member f2-bgp
 ip address 10.0.0.134/32

interface Vlan2501
 no shutdown
 vrf member f2-bgp
 ip address 10.10.34.1/29

vrf context f2-bgp
 ip route 10.0.0.0/29 10.10.34.2
```

5. Fase aggiuntiva — tcpdump

Sui nodi foglia ACI, lo strumento tcpdump può sniffare l'interfaccia CPU 'kpm_inb' per verificare se i pacchetti del protocollo hanno raggiunto la CPU foglia. Usare la porta L4 179 (BGP) come filtro.

```
f2-leaf3# tcpdump -ni kpm_inb port 179
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on kpm_inb, link-type EN10MB (Ethernet), capture size 65535 bytes
20:36:58.292903 IP 10.0.0.134.179 > 10.0.0.3.34873: Flags [P.], seq 3775831990:3775832009, ack
807595300, win 3650, length 19: BGP, length: 19
20:36:58.292962 IP 10.0.0.3.34873 > 10.0.0.134.179: Flags [.], ack 19, win 6945, length 0
20:36:58.430418 IP 10.0.0.3.34873 > 10.0.0.134.179: Flags [P.], seq 1:20, ack 19, win 6945,
length 19: BGP, length: 19
20:36:58.430534 IP 10.0.0.134.179 > 10.0.0.3.34873: Flags [.], ack 20, win 3650, length 0
```

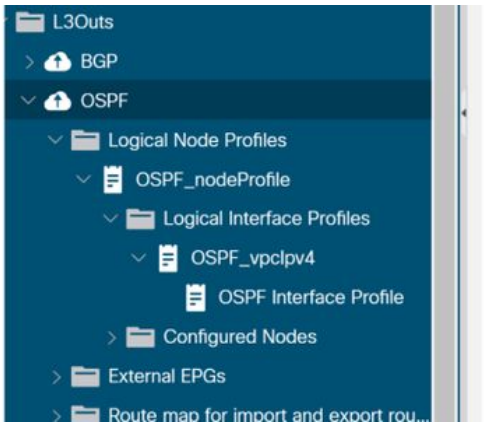
OSPF

In questa sezione viene utilizzato un esempio di relazioni OSPF tra BL3, BL4 e R34 dalla topologia nella sezione Panoramica con OSPF AreaID 1 (NSSA).

Di seguito sono riportati i criteri comuni per verificare la presenza di adiacenze OSPF.

- ID e tipo area OSPF

L3Out — Profilo interfaccia OSPF — ID e tipo di area



Come per qualsiasi dispositivo di routing, è necessario che ID e tipo dell'area OSPF corrispondano su entrambi i router adiacenti. Di seguito sono riportate alcune limitazioni specifiche ACI relative alle configurazioni di ID area OSPF:

- Un'uscita L3 può avere un solo ID area OSPF.
- Due L3Out possono utilizzare lo stesso ID area OSPF nello stesso VRF solo quando si trovano su due nodi foglia diversi.

Sebbene non sia necessario che l'ID OSPF sia la backbone 0, nel caso del routing di transito è necessario che si trovi tra due host OSPF L3 sulla stessa foglia; uno di essi deve utilizzare l'area OSPF 0 in quanto qualsiasi scambio di route tra le aree OSPF deve passare attraverso l'area OSPF 0.

- MTU

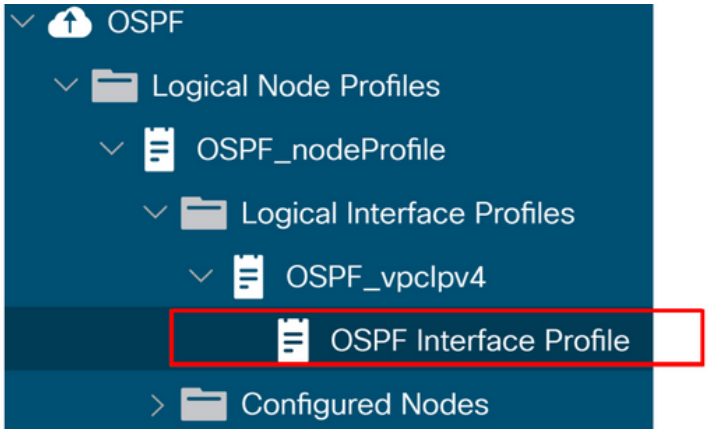
Profilo interfaccia logica - SVI

L'MTU predefinita su ACI è di 9000 byte, anziché di 1500 byte, valore generalmente utilizzato sui dispositivi di routing tradizionali. Verificare che l'MTU corrisponda alla periferica esterna. Quando l'istituzione del router adiacente OSPF non riesce a causa di MTU, rimane bloccato in

EXCHANGE/DROTHER.

- Subnet mask IP. OSPF richiede che l'IP adiacente utilizzi la stessa subnet mask.
- Profilo interfaccia OSPF.

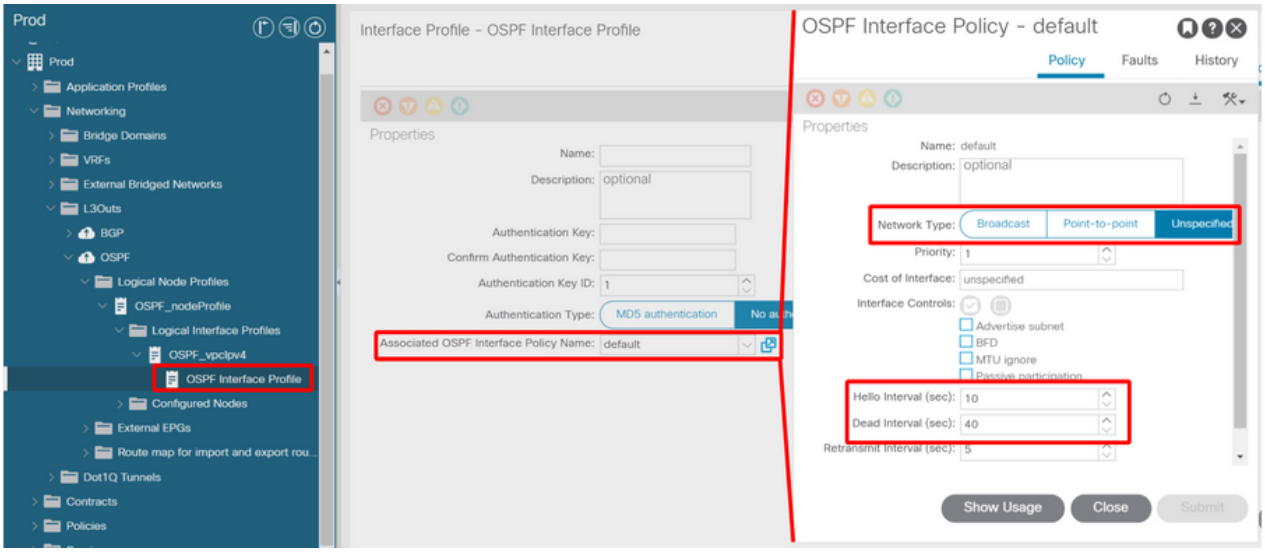
Profilo interfaccia OSPF



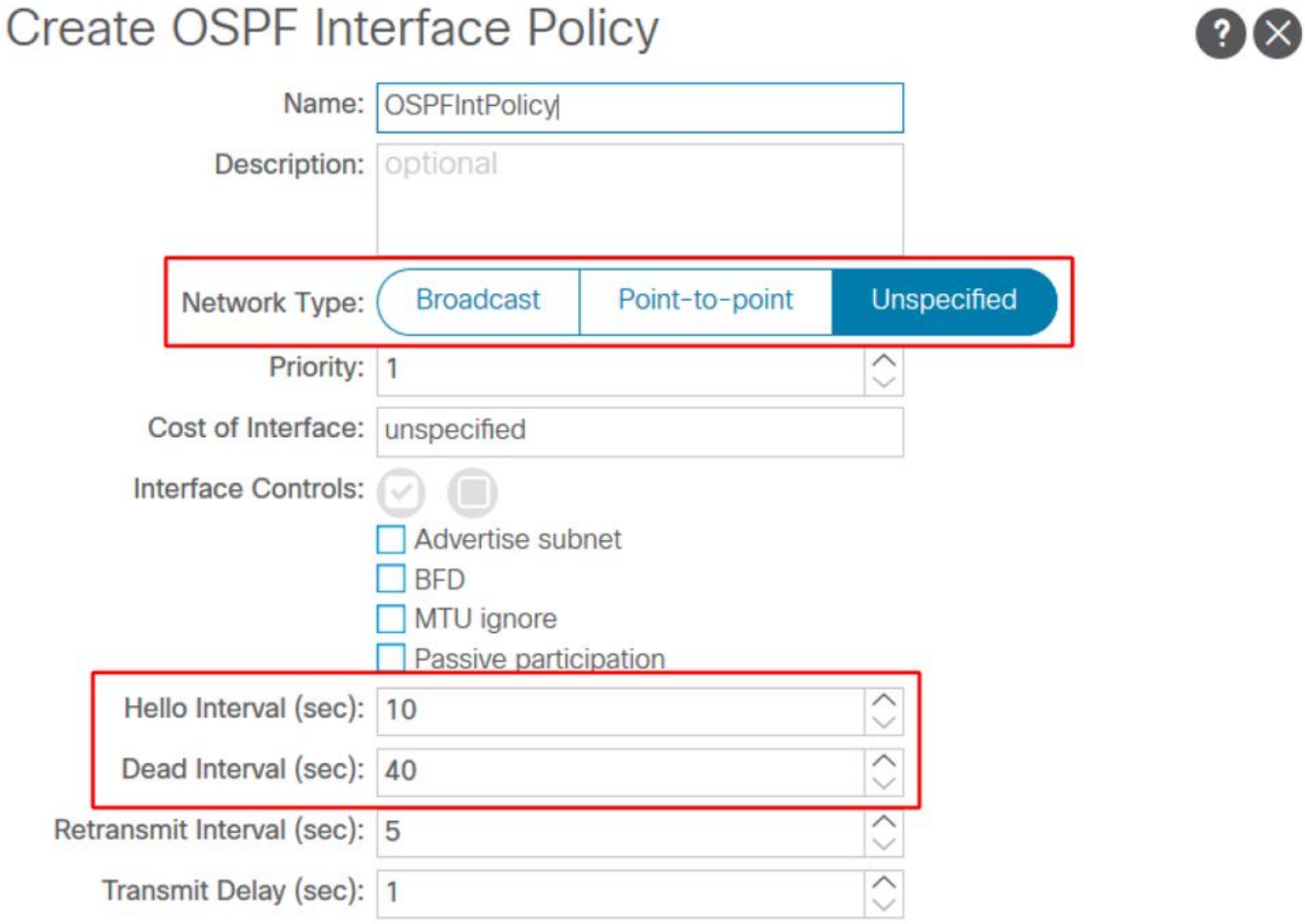
Equivale a 'ip router ospf <tag> area <id area>' in una configurazione NX-OS standalone per abilitare OSPF sull'interfaccia. In caso contrario, le interfacce foglia non verranno unite a OSPF.

- OSPF Hello / Dead Timer, tipo di rete

Profilo interfaccia OSPF: Hello/Dead timer e tipo di rete



Dettagli criteri interfaccia OSPF



OSPF richiede che i timer Hello e Dead corrispondano su ciascun dispositivo adiacente. Questi sono configurati nel profilo di interfaccia OSPF.

Verificare che il tipo di rete dell'interfaccia OSPF corrisponda al dispositivo esterno. Se la periferica esterna utilizza il tipo Point-to-Point, anche il lato ACI deve configurare esplicitamente Point-to-Point. Questi sono configurati anche nel profilo di interfaccia OSPF.

Verifica CLI OSPF

Gli output CLI nei seguenti passaggi vengono raccolti da BL3 nella sezione "Panoramica" della topologia.

1. Controllare lo stato dei router adiacenti OSPF

Se 'State' è impostato su 'FULL' nella CLI seguente, la risorsa adiacente OSPF verrà stabilita correttamente. In caso contrario, passare al passaggio successivo per controllare i parametri.

```
f2-leaf3# show ip ospf neighbors vrf Prod:VRF2
OSPF Process ID default VRF Prod:VRF2
Total number of neighbors: 2
Neighbor ID     Pri State            Up Time  Address         Interface
10.0.0.4          1 FULL/DR          00:47:30 10.10.34.4      Vlan28      <--- neighbor with BL4
10.0.0.134        1 FULL/DROTHER     00:00:21 10.10.34.1      Vlan28      <--- neighbor with R34
```

In ACI, quando si utilizza lo stesso ID VLAN con una SVI, i BL formeranno un vicinato OSPF tra loro sopra i router esterni. Infatti, ACI ha un dominio di flooding interno chiamato L3Out BD (o

External BD) per ciascun ID VLAN nelle SVI L3Out. Notare che l'ID VLAN 28 è una VLAN interna chiamata IP-VLAN (VLAN indipendente dalla piattaforma) anziché la VLAN effettiva (VLAN di incapsulamento dell'accesso) usata sul cavo. Usare il comando seguente per verificare l'accesso alla VLAN di crittografia ('vlan-2502').

```
f2-leaf3# show vlan id 28 extended
 VLAN Name                                Encap            Ports
 ---- ----------------------------------- ---------------- ------------------------
 28   Prod:VRF2:l3out-OSPF:vlan-2502      vxlan-14942176,  Eth1/13, Po1
                                          vlan-2502
```

Èpossibile ottenere lo stesso output anche tramite l'ID della VLAN di accesso.

```
f2-leaf3# show vlan encap-id 2502 extended
 VLAN Name                                Encap            Ports
 ---- ----------------------------------- ---------------- ------------------------
 28   Prod:VRF2:l3out-OSPF:vlan-2502      vxlan-14942176,  Eth1/13, Po1
                                          vlan-2502
```

2. Controllare l'area OSPF

Assicurarsi che l'ID e il tipo dell'area OSPF siano identici ai router adiacenti. Se il profilo dell'interfaccia OSPF è mancante, l'interfaccia non verrà aggiunta a OSPF e non verrà visualizzata nell'output CLI di OSPF.

```
f2-leaf3# show ip ospf interface brief vrf Prod:VRF2
OSPF Process ID default VRF Prod:VRF2
Total number of interface: 1
Interface               ID     Area            Cost   State    Neighbors Status
Vlan28                  94     0.0.0.1         4      BDR      2         up
f2-leaf3# show ip ospf vrf Prod:VRF2
Routing Process default with ID 10.0.0.3 VRF Prod:VRF2
...
  Area (0.0.0.1)
       Area has existed for 00:59:14
       Interfaces in this area: 1 Active interfaces: 1
       Passive interfaces: 0  Loopback interfaces: 0
       This area is a NSSA area
       Perform type-7/type-5 LSA translation
       SPF calculation has run 10 times
        Last SPF ran for 0.001175s
       Area ranges are
       Area-filter in 'exp-ctx-proto-3112960'
       Area-filter out 'permit-all'
       Number of LSAs: 4, checksum sum 0x0
```

3. Controllare i dettagli dell'interfaccia OSPF

Verificare che i parametri a livello di interfaccia soddisfino i requisiti per la definizione dei router adiacenti OSPF, ad esempio subnet IP, tipo di rete, timer Hello/Dead. Notare l'ID VLAN per specificare che la SVI è una PI-VLAN (vlan28)

```
f2-leaf3# show ip ospf interface vrf Prod:VRF2
Vlan28 is up, line protocol is up
```

```
   IP address 10.10.34.3/29, Process ID default VRF Prod:VRF2, area 0.0.0.1
   Enabled by interface configuration
   State BDR, Network type BROADCAST, cost 4
   Index 94, Transmit delay 1 sec, Router Priority 1
   Designated Router ID: 10.0.0.4, address: 10.10.34.4
   Backup Designated Router ID: 10.0.0.3, address: 10.10.34.3
   2 Neighbors, flooding to 2, adjacent with 2
   Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5
     Hello timer due in 0.000000
   No authentication
   Number of opaque link LSAs: 0, checksum sum 0

f2-leaf3# show interface vlan28
Vlan28 is up, line protocol is up, autostate disabled
  Hardware EtherSVI, address is  0022.bdf8.19ff
  Internet Address is 10.10.34.3/29
  MTU 9000 bytes, BW 10000000 Kbit, DLY 1 usec
```

4. Verificare la raggiungibilità IP al router adiacente

Sebbene i pacchetti OSPF Hello siano pacchetti multicast locali, i pacchetti OSPF DBD richiesti per il primo scambio OSPF LSDB sono unicast. Pertanto, è necessario verificare anche la raggiungibilità unicast per l'istituzione del vicinato OSPF.

```
f2-leaf3# iping 10.10.34.1 -V Prod:VRF2
PING 10.10.34.1 (10.10.34.1) from 10.10.34.3: 56 data bytes
64 bytes from 10.10.34.1: icmp_seq=0 ttl=255 time=0.66 ms
64 bytes from 10.10.34.1: icmp_seq=1 ttl=255 time=0.653 ms
```

5. Controllare lo stesso sul router esterno

Di seguito sono riportati alcuni esempi di configurazioni sul router esterno (NX-OS standalone)

```
router ospf 1
    vrf f2-ospf
    router-id 10.0.0.134
    area 0.0.0.1 nssa

interface Vlan2502
    no shutdown
    mtu 9000
    vrf member f2-ospf
    ip address 10.10.34.1/29
    ip router ospf 1 area 0.0.0.1
```

Verificare anche l'MTU sull'interfaccia fisica.

6. Fase aggiuntiva — tcpdump

Sui nodi foglia ACI, l'utente può eseguire tcpdump sull'interfaccia della CPU 'kpm_inb' per verificare se i pacchetti del protocollo hanno raggiunto la CPU foglia. Sebbene esistano più filtri per OSPF, IP Protocol Number è il filtro più completo.

- Numero protocollo IP: proto 89 (IPv4) o ip6 proto 0x59 (IPv6)
- Indirizzo IP del router adiacente: host <ip>

- Mcast IP locale collegamento OSPF: host 24.0.0.5 o host 24.0.0.6

```
f2-leaf3# tcpdump -ni kpm_inb proto 89
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on kpm_inb, link-type EN10MB (Ethernet), capture size 65535 bytes
22:28:38.231356 IP 10.10.34.4 > 224.0.0.5: OSPFv2, Hello, length 52
22:28:42.673810 IP 10.10.34.3 > 224.0.0.5: OSPFv2, Hello, length 52
22:28:44.767616 IP 10.10.34.1 > 224.0.0.5: OSPFv2, Hello, length 52
22:28:44.769092 IP 10.10.34.3 > 10.10.34.1: OSPFv2, Database Description, length 32
22:28:44.769803 IP 10.10.34.1 > 10.10.34.3: OSPFv2, Database Description, length 32
22:28:44.775376 IP 10.10.34.3 > 10.10.34.1: OSPFv2, Database Description, length 112
22:28:44.780959 IP 10.10.34.1 > 10.10.34.3: OSPFv2, LS-Request, length 36
22:28:44.781376 IP 10.10.34.3 > 10.10.34.1: OSPFv2, LS-Update, length 64
22:28:44.790931 IP 10.10.34.1 > 224.0.0.6: OSPFv2, LS-Update, length 64
```

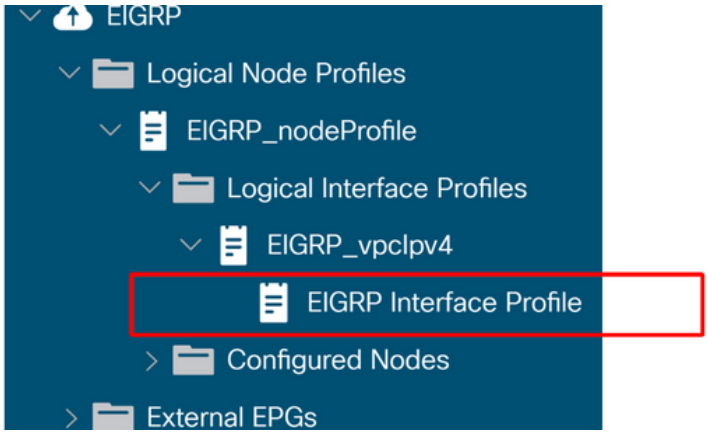
EIGRP

Questa sezione utilizza un esempio di vicinanza EIGRP tra BL3, BL4 e R34 dalla topologia nella sezione "Panoramica" con EIGRP AS 10.

I criteri comuni per la determinazione dell'adiacenza del protocollo EIGRP sono i seguenti.

- EIGRP AS: a un'uscita L3è assegnato un EIGRP AS. Deve corrispondere al dispositivo esterno.
- Profilo di interfaccia EIGRP.

Profilo di interfaccia EIGRP



Equivale alla configurazione 'ip router eigrp <as>' su un dispositivo NX-OS autonomo. Senza questo, le interfacce foglia non si uniranno all'EIGRP.

- MTU

Anche se non è necessario che ciò corrisponda per stabilire semplicemente il vicinato EIGRP, i pacchetti di scambio della topologia EIGRP possono diventare più grandi della MTU massima consentita sulle interfacce tra peer e, poiché questi pacchetti non possono essere frammentati, vengono scartati e di conseguenza il vicinato EIGRP si blocca.

Verifica CLI EIGRP

Gli output CLI nei seguenti passaggi vengono raccolti da BL3 nella topologia dalla sezione

"Overview".

1. Controllare lo stato dei nodi adiacenti EIGRP

```
f2-leaf3# show ip eigrp neighbors vrf Prod:VRF3
EIGRP neighbors for process 10 VRF Prod:VRF3
H   Address                 Interface       Hold  Uptime  SRTT   RTO  Q  Seq
                                           (sec)         (ms)       Cnt Num
0   10.10.34.4              vlan29           14   00:12:58  1    50    0   6    <--- neighbor
with BL4
1   10.10.34.1              vlan29           13   00:08:44  2    50    0   4    <--- neighbor
with R34
```

In ACI, i BL formeranno un vicinato EIGRP tra loro al di sopra dei router esterni quando usano lo stesso ID VLAN con SVI. Infatti, un ACI ha un dominio di flooding interno chiamato L3Out BD (o External BD) per ciascun ID VLAN nelle SVI L3Out.

Notare che l'ID VLAN 29 è una VLAN interna chiamata IP-VLAN (VLAN indipendente dalla piattaforma) anziché la VLAN effettiva (VLAN di incapsulamento dell'accesso) usata sul cavo. Utilizzare il comando seguente per verificare l'accesso alla rete VLAN (vlan-2503).

```
f2-leaf3# show vlan id 29 extended
 VLAN Name                                Encap            Ports
 ---- ----------------------------------- ---------------- ------------------------
 29   Prod:VRF3:l3out-EIGRP:vlan-2503  vxlan-15237052,  Eth1/13, Po1
                                        vlan-2503
```

Èpossibile ottenere lo stesso output anche tramite l'ID della VLAN di accesso.

```
f2-leaf3# show vlan encap-id 2503 extended
 VLAN Name                                Encap            Ports
 ---- ----------------------------------- ---------------- ------------------------
 29   Prod:VRF3:l3out-EIGRP:vlan-2503  vxlan-15237052,  Eth1/13, Po1
                                        vlan-2503
```

2. Controllare i dettagli dell'interfaccia EIGRP

Verificare che EIGRP sia in esecuzione sull'interfaccia prevista. In caso contrario, selezionare Profilo interfaccia logica e Profilo interfaccia EIGRP.

```
f2-leaf3# show ip eigrp interfaces vrf Prod:VRF3
EIGRP interfaces for process 10 VRF Prod:VRF3
                        Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
vlan29             2        0/0         1       0/0          50             0
  Hello interval is 5 sec
  Holdtime interval is 15 sec
  Next xmit serial: 0
  Un/reliable mcasts: 0/2     Un/reliable ucasts: 5/10
  Mcast exceptions: 0    CR packets: 0    ACKs suppressed: 2
  Retransmissions sent: 2    Out-of-sequence rcvd: 0
  Classic/wide metric peers: 2/0
```

```
f2-leaf3# show int vlan 29
Vlan29 is up, line protocol is up, autostate disabled
  Hardware EtherSVI, address is  0022.bdf8.19ff
  Internet Address is 10.10.34.3/29
  MTU 9000 bytes, BW 10000000 Kbit, DLY 1 usec
```

3. Verificare la stessa condizione sul router esterno

Di seguito è riportato l'esempio di configurazione sul router esterno (NX-OS standalone).

```
router eigrp 10
 vrf f2-eigrp

interface Vlan2503
 no shutdown
 vrf member f2-eigrp
 ip address 10.10.34.1/29
 ip router eigrp 10
```

4. Fase aggiuntiva — tcpdump

Sui nodi foglia ACI, l'utente può eseguire tcpdump sull'interfaccia della CPU 'kpm_inb' per verificare se i pacchetti del protocollo hanno raggiunto la CPU della foglia. Utilizzare il protocollo IP numero 88 (EIGRP) come filtro.

```
f2-leaf3# tcpdump -ni kpm_inb proto 88
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on kpm_inb, link-type EN10MB (Ethernet), capture size 65535 bytes
23:29:43.725676 IP 10.10.34.3 > 224.0.0.10: EIGRP Hello, length: 40
23:29:43.726271 IP 10.10.34.4 > 224.0.0.10: EIGRP Hello, length: 40
23:29:43.728178 IP 10.10.34.1 > 224.0.0.10: EIGRP Hello, length: 40
23:29:45.729114 IP 10.10.34.1 > 10.10.34.3: EIGRP Update, length: 20
23:29:48.316895 IP 10.10.34.3 > 224.0.0.10: EIGRP Hello, length: 40
```

Annuncio route

In questa sezione vengono illustrati la verifica e la risoluzione dei problemi relativi alla pubblicità dei percorsi in ACI. In particolare, vengono esaminati esempi che prevedono:

- Annuncio subnet domini bridge.
- Annuncio route di transito.
- Importare ed esportare il controllo dei cicli di lavorazione.

In questa sezione viene descritto come risolvere le perdite di route relative agli output L3 condivisi nelle sezioni successive.

Flusso di lavoro annuncio route dominio bridge

Prima di esaminare la risoluzione dei problemi più comuni, l'utente dovrebbe acquisire familiarità con le modalità di funzionamento dell'annuncio del dominio di Bridge.

La pubblicità BD, quando BD e L3Out si trovano nello stesso VRF, implica:

- Rapporto contrattuale tra L3Out e l'EPG interno.
- Associazione dell'uscita L3A al dominio di bridge.
- Selezionare 'Pubblicizza esternamente' nella subnet BD.

Inoltre, è anche possibile controllare la pubblicità del dominio di bridge utilizzando i profili di route di esportazione che impediscono la necessità di associare l'uscita L3Out. Tuttavia, è necessario selezionare l'opzione 'Pubblicizza esternamente'. Si tratta di un caso di utilizzo meno comune, pertanto non verrà discusso qui.

Il rapporto contrattuale tra l'L3Out e l'EPG è necessario per fare in modo che il percorso statico pervasivo di BD venga spinto al BL. L'effettivo annuncio route viene gestito tramite ridistribuzione della route statica nel protocollo esterno. Infine, le route map di ridistribuzione verranno installate solo all'interno delle L3Out associate a BD. In questo modo il percorso non viene pubblicizzato tra tutti gli L3Out.

In questo caso, la subnet BD è 192.168.1.0/24 e deve essere pubblicizzata tramite OSPF L3Out.

Prima di applicare il contratto tra L3Out e EPG interno

```
leaf103# show ip route 192.168.1.0/24 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF
Route not found
```

Notare che il percorso di BD non è ancora presente sul BL.

Dopo l'applicazione del contratto tra L3Out e EPG interno

A questo punto non è stata eseguita alcuna altra configurazione. L3Out non è ancora associato a BD e il flag 'Pubblicizza esternamente' non è impostato.

```
leaf103# show ip route 10.0.1.0/24 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF
192.168.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
   *via 10.0.120.34%overlay-1, [1/0], 00:00:08, static, tag 4294967294
        recursive next hop: 10.0.120.34/32%overlay-1
```

Si noti che la route della subnet BD (indicata dal flag di diffusione) è ora distribuita nella BL. Si noti, tuttavia, che la route è contrassegnata. Questo valore di tag è un valore implicito assegnato alle route di BD prima di essere configurato con 'Pubblicizza esternamente'. Tutti i protocolli esterni impediscono la ridistribuzione del tag.

Dopo aver selezionato 'Pubblicizza esternamente' nella subnet BD

L3Out non è ancora stato associato a BD. Tuttavia, il tag è stato cancellato.

```
leaf103# show ip route 192.168.1.0/24 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF
192.168.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive *via 10.0.120.34%overlay-1, [1/0],
00:00:06, static recursive next hop: 10.0.120.34/32%overlay-1
```

A questo punto la route non viene ancora annunciata esternamente perché non esistono route-map e prefix-list corrispondenti al prefisso per la ridistribuzione nel protocollo esterno. È possibile verificare questa condizione con i seguenti comandi:

```
leaf103# show ip ospf vrf Prod:Vrf1
Routing Process default with ID 10.0.0.3 VRF Prod:Vrf1
Stateful High Availability enabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
Table-map using route-map exp-ctx-2392068-deny-external-tag
Redistributing External Routes from
  static route-map exp-ctx-st-2392068
  direct route-map exp-ctx-st-2392068
  bgp route-map exp-ctx-proto-2392068
  eigrp route-map exp-ctx-proto-2392068
  coop route-map exp-ctx-st-2392068
```

La route di BD è programmata come route statica, quindi controllare la mappa della route di ridistribuzione statica eseguendo 'show route-map <nome route-map>' e quindi 'show ip prefix-list <nome>' in tutti gli elenchi di prefissi presenti nella route-map. Eseguire questa operazione nel passaggio successivo.

Dopo l'associazione del connettore L3Out al BD

Come accennato in precedenza, questo passaggio consente di ottenere l'elenco dei prefissi che corrisponde alla subnet BD installata nella mappa dei percorsi di ridistribuzione statica del protocollo esterno.

```
leaf103# show route-map exp-ctx-st-2392068
route-map exp-ctx-st-2392068, deny, sequence 1
 Match clauses:
   tag: 4294967294
 Set clauses:

...
route-map exp-ctx-st-2392068, permit, sequence 15803
 Match clauses:
   ip address prefix-lists: IPv4-st16390-2392068-exc-int-inferred-export-dst
   ipv6 address prefix-lists: IPv6-deny-all
 Set clauses:
   tag 0
```

Verificare l'elenco dei prefissi:

```
leaf103# show ip prefix-list IPv4-st16390-2392068-exc-int-inferred-export-dst
ip prefix-list IPv4-st16390-2392068-exc-int-inferred-export-dst: 1 entries
  seq 1 permit 192.168.1.1/24
```

Èin corso la corrispondenza della subnet BD per la ridistribuzione in OSPF.

A questo punto il flusso di lavoro di configurazione e verifica è completo per l'annuncio della subnet BD all'esterno di L3Out. Al di là di questo punto, la verifica sarebbe specifica per il protocollo. Ad esempio:

- Per EIGRP, verificare che la route sia installata nella tabella della topologia con 'show ip eigrp topology vrf <nome>'
- Per OSPF, verificare che la route sia installata nella tabella del database come LSA esterno con 'show ip ospf database vrf <nome>'
- Per BGP, verificare che la route sia nel RIB BGP con 'show bgp ipv4 unicast vrf <nome>'

Annuncio route BGP

Per BGP, tutte le route statiche sono implicitamente consentite per la ridistribuzione. La route-map corrispondente alla subnet BD viene applicata a livello di router adiacente BGP.

```
leaf103# show bgp ipv4 unicast neighbor 10.0.0.134 vrf Prod:Vrf1 | grep Outbound
 Outbound route-map configured is exp-l3out-BGP-peer-2392068, handle obtained
```

Nell'esempio precedente, 10.0.0.134 è il router BGP adiacente configurato all'interno di L3Out.

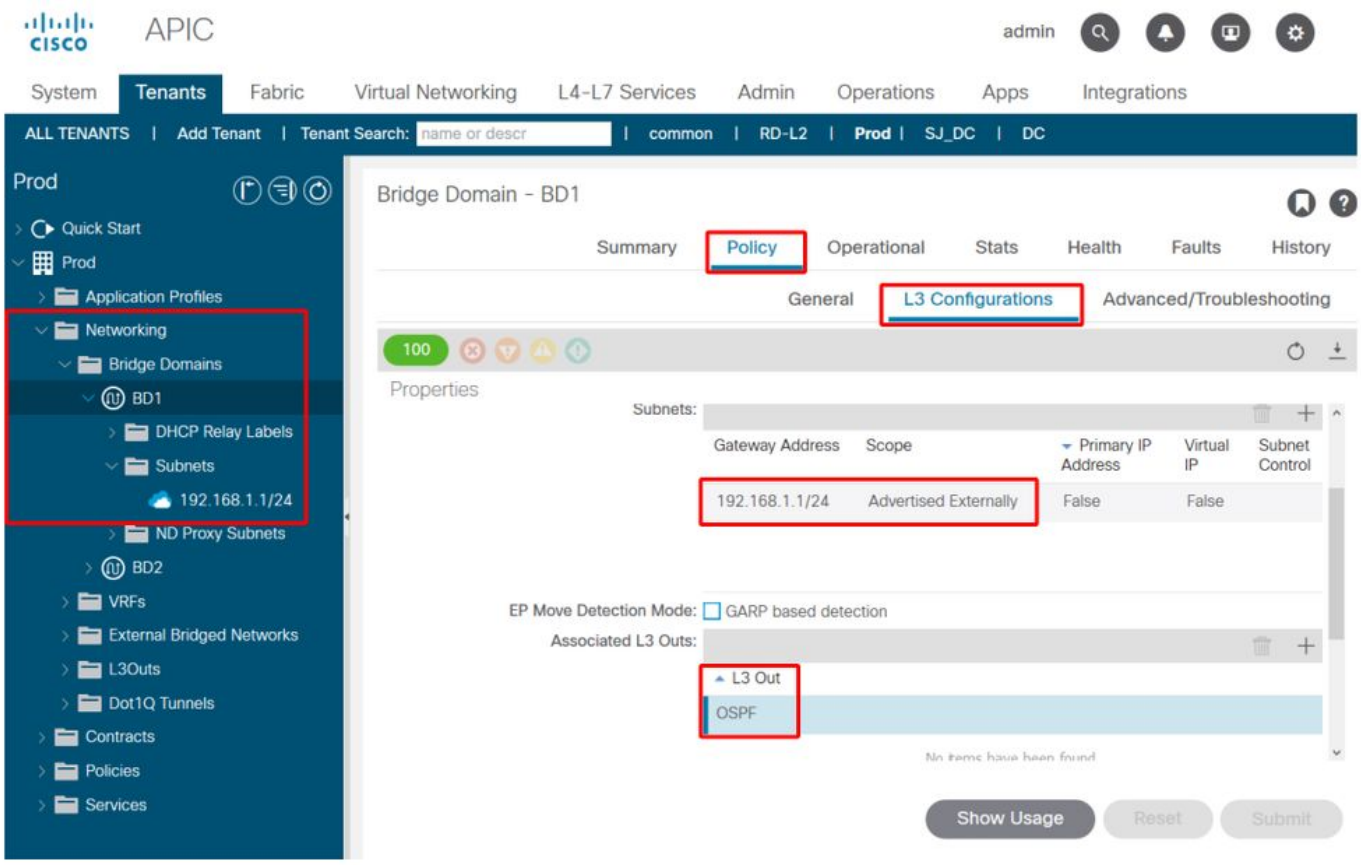
Annuncio route EIGRP

Analogamente a OSPF, viene utilizzata una route-map per controllare la ridistribuzione da Static a EIGRP. In questo modo solo le subnet associate all'output L3e impostate su 'Annuncia esternamente' devono essere ridistribuite. È possibile verificare questa condizione con questo comando:

```
leaf103# show ip eigrp vrf Prod:Vrf1
IP-EIGRP AS 100 ID 10.0.0.3 VRF Prod:Vrf1
 Process-tag: default
 Instance Number: 1
 Status: running
 Authentication mode: none
 Authentication key-chain: none
 Metric weights: K1=1 K2=0 K3=1 K4=0 K5=0
 metric version: 32bit
 IP proto: 88 Multicast group: 224.0.0.10
 Int distance: 90 Ext distance: 170
 Max paths: 8
 Active Interval: 3 minute(s)
 Number of EIGRP interfaces: 1 (0 loopbacks)
 Number of EIGRP passive interfaces: 0
 Number of EIGRP peers: 2
 Redistributing:
   static route-map exp-ctx-st-2392068
   ospf-default route-map exp-ctx-proto-2392068
   direct route-map exp-ctx-st-2392068
   coop route-map exp-ctx-st-2392068
   bgp-65001 route-map exp-ctx-proto-2392068
```

Di seguito è riportata la configurazione di funzionamento finale di BD.

Configurazione L3 dominio bridge



Scenario di risoluzione dei problemi relativi agli annunci delle route del dominio di bridge

In questo caso, il sintomo tipico è in genere rappresentato dal fatto che una subnet BD configurata non viene annunciata all'esterno di una rete L3Out. Seguire il flusso di lavoro precedente per individuare il componente interrotto.

Iniziare con la configurazione prima di ottenere un livello troppo basso verificando quanto segue:

- Esiste un contratto tra EPG e L3Out?
- L3Out è associato a BD?
- La subnet BD è impostata per la pubblicità esterna?
- L'adiacenza del protocollo esterno è attiva?

Possibile causa: BD non distribuito

Questo caso sarebbe applicabile in due diversi scenari, ad esempio:

- L'EPG interno utilizza l'integrazione VMM con l'opzione On Demand e nessun endpoint VM è stato collegato al gruppo di porte per l'EPG.
- L'EPG interno è stato creato ma non sono state configurate associazioni a percorsi statici oppure l'interfaccia su cui è configurato il percorso statico è inattiva.

In entrambi i casi, il BD non verrebbe implementato e, di conseguenza, il percorso statico BD non verrebbe indirizzato al BL. La soluzione consiste nel distribuire alcune risorse attive all'interno di un EPG collegato a questo BD in modo che la subnet venga distribuita.

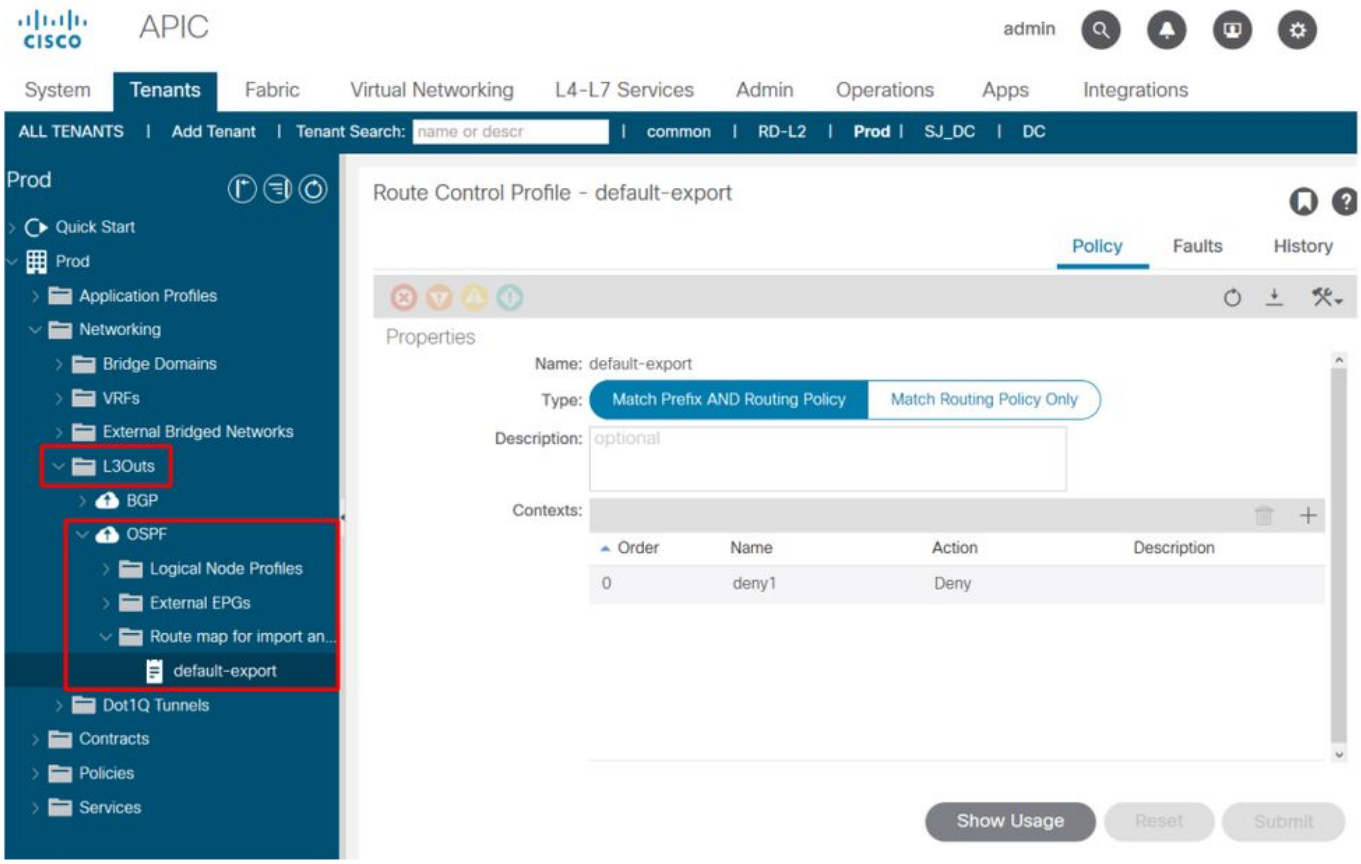
Possibile causa: OSPF L3Out è configurato come 'Stub' o 'NSSA' senza ridistribuzione

Quando OSPF viene utilizzato come protocollo L3Out, è necessario rispettare le regole OSPF di base. Le aree di stub non consentono le LSA ridistribuite ma possono invece annunciare una route predefinita. Le aree NSSA consentono percorsi ridistribuiti, ma è necessario selezionare 'Invia LSA ridistribuite nell'area NSSA' in L3Out. In alternativa, NSSA può anche annunciare una route predefinita disabilitando anche 'Origine riepilogo LSA'. Si tratta di uno scenario tipico in cui 'Invia LSA ridistribuite nell'area NSSA' verrebbe disabilitato.

Possibile causa: Profilo di route 'Default-Export' con un'azione 'Deny' configurata in L3Out

Quando i profili di route vengono configurati in un'istruzione L3Out con i nomi 'default-export' o 'default-import', vengono applicati implicitamente all'istruzione L3Out. Inoltre, se il profilo di route predefinito per l'esportazione è impostato su un'azione di negazione e configurato come 'Corrispondenza prefisso e criteri di routing', le subnet BD devono essere annunciate all'esterno di questo L3Out e vengono implicitamente negate:

Profilo route predefinito di negazione esportazione



Se è selezionata l'opzione 'Corrispondenza solo criteri di routing', le corrispondenze con prefissi nel profilo di route di esportazione predefinito non includeranno implicitamente le subnet BD.

Flusso di lavoro di importazione route esterna

In questa sezione viene descritto come ACI apprende le route esterne tramite un'uscita L3Out e le distribuisce ai nodi foglia interni. Esso copre anche i casi di transito e di perdita di itinerari nelle sezioni successive

Come nella sezione precedente, l'utente deve essere consapevole di ciò che accade a un livello superiore.

Per impostazione predefinita, tutte le route apprese tramite il protocollo esterno vengono ridistribuite nel processo BGP dell'infrastruttura interna. Ciò è vero indipendentemente dalle subnet configurate in EPG esterno e dai flag selezionati. Ci sono due esempi in cui questo non è vero.

- Se l'opzione 'Applicazione controllo route' nel criterio L3Out di livello superiore è impostata su 'Import'. In questo caso il modello di importazione route passerebbe da un modello di elenco di blocco (specificare solo gli elementi che non devono essere consentiti) a un modello di elenco permessi (tutto viene negato implicitamente se non diversamente configurato).
- Se il protocollo esterno è EIGRP o OSPF e un profilo di route Interleak utilizzato non corrisponde alle route esterne.

Affinché una route esterna venga distribuita a una foglia interna, è necessario che si verifichi quanto segue:

- Il percorso deve essere appreso sul BL dal router esterno. Per poter essere ridistribuita nel processo MP-BGP dell'infrastruttura, la route deve essere installata nella tabella di routing e non solo nel RIB del protocollo.
- Ènecessario consentire la ridistribuzione o l'annuncio della route nel processo BGP interno. Questa situazione deve verificarsi sempre, a meno che non si utilizzi l'imposizione del controllo della route di importazione o un profilo di route di interleak.
- Ènecessario configurare una policy BGP Route-Reflector da applicare a un gruppo di policy dei pod applicato al profilo del pod. Se non si applica questa impostazione, il processo BGP non verrà inizializzato sugli switch.

Se l'EPG/BD interno è nello stesso VRF dell'uscita L3D, i tre passaggi precedenti sono tutti necessari affinché l'EPG/BD interno utilizzi percorsi esterni.

Route installata nella tabella di routing BL

In questo caso, il percorso esterno da apprendere sui BL 103 e 104 è 172.16.20.1/32.

```
leaf103# show ip route 172.16.20.1 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

172.16.20.1/32, ubest/mbest: 1/0
    *via 10.10.34.3, vlan347, [110/20], 00:06:29, ospf-default, type-2
```

Èevidente che viene installato nella tabella di routing in modo da essere appreso tramite OSPF. Se non è stato visualizzato, controllare il protocollo individuale e verificare che le adiacenze siano attive. La route viene ridistribuita in BGP È possibile verificare la mappa della route di ridistribuzione dopo aver verificato che non vengano utilizzati né l'imposizione 'Import' né i profili della route di interleak esaminando la mappa della route utilizzata per il protocollo esterno alla ridistribuzione BGP. Vedere il comando seguente:

```
leaf103# show bgp process vrf Prod:Vrf1

Information regarding configured VRFs:
```

```
BGP Information for VRF Prod:Vrf1
VRF Type                        : System
VRF Id                          : 85
VRF state                       : UP
VRF configured                  : yes
VRF refcount                    : 1
VRF VNID                        : 2392068
Router-ID                       : 10.0.0.3
Configured Router-ID            : 10.0.0.3
Confed-ID                       : 0
Cluster-ID                      : 0.0.0.0
MSITE Cluster-ID                : 0.0.0.0
No. of configured peers         : 1
No. of pending config peers     : 0
No. of established peers        : 1
VRF RD                          : 101:2392068
VRF EVPN RD                     : 101:2392068
...
    Redistribution
        direct, route-map permit-all
        static, route-map imp-ctx-bgp-st-interleak-2392068
        ospf, route-map permit-all
        coop, route-map exp-ctx-st-2392068
        eigrp, route-map permit-all
```

In questo caso è evidente che la route map 'allow-all' viene utilizzata per la ridistribuzione da OSPF a BGP. Questa è l'impostazione predefinita. Da qui è possibile verificare la BL e controllare la route locale proveniente da BGP:

```
a-leaf101# show bgp ipv4 unicast 172.16.20.1/32 vrf Prod:Vrf1
BGP routing table information for VRF Prod:Vrf1, address family IPv4 Unicast
BGP routing table entry for 172.16.20.1/32, version 25 dest ptr 0xa6f25ad0
Paths: (2 available, best #2)
Flags: (0x80c0002 00000000) on xmit-list, is not in urib, exported
  vpn: version 16316, (0x100002) on xmit-list
Multipath: eBGP iBGP


  Advertised path-id 1, VPN AF advertised path-id 1
  Path type: redist 0x408 0x1 ref 0 adv path ref 2, path is valid, is best path
  AS-Path: NONE, path locally originated
    0.0.0.0 (metric 0) from 0.0.0.0 (10.0.0.3)
      Origin incomplete, MED 20, localpref 100, weight 32768
      Extcommunity:
          RT:65001:2392068
          VNID:2392068
          COST:pre-bestpath:162:110

  VRF advertise information:
  Path-id 1 not advertised to any peer

  VPN AF advertise information:
  Path-id 1 advertised to peers:
    10.0.64.64         10.0.72.66
  Path-id 2 not advertised to any peer
```

Nell'output sopra riportato, il valore 0.0.0.0/0 indica che l'origine è locale. L'elenco dei peer pubblicizzati sono i nodi della spine nella struttura che agiscono come Route-Reflector.

Verifica route su foglia interna

Il BL deve annunciarlo ai nodi della spine tramite la famiglia di indirizzi BGP VPNv4. I nodi della colonna vertebrale devono pubblicizzarla su tutti i nodi foglia con il VRF distribuito (vero per esempio senza perdita di percorso). Su uno dei nodi foglia eseguire 'show bgp vpnv4 unicast <route> vrf overlay-1' per verificare che sia in VPNv4

Utilizzare il comando seguente per verificare la route sulla foglia interna.

```
leaf101# show ip route 172.16.20.1 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

172.16.20.1/32, ubest/mbest: 2/0
    *via 10.0.72.64%overlay-1, [200/20], 00:21:24, bgp-65001, internal, tag 65001
         recursive next hop: 10.0.72.64/32%overlay-1
    *via 10.0.72.67%overlay-1, [200/20], 00:21:24, bgp-65001, internal, tag 65001
         recursive next hop: 10.0.72.67/32%overlay-1
```

Nell'output sopra riportato, il percorso viene appreso tramite BGP e gli hop successivi devono essere i TEP fisici (PTEP) dei BL.

```
leaf101# acidiag fnvread
      ID   Pod ID                 Name    Serial Number         IP Address    Role        State
LastUpdMsgId
-------------------------------------------------------------------------------------------
--------------
     103        1            a-leaf101      FDO20160TPS      10.0.72.67/32    leaf
active   0
     104        1            a-leaf103      FDO20160TQ0      10.0.72.64/32    leaf
active   0
```

Scenario di risoluzione dei problemi di route esterna

In questo scenario, la foglia interna (101) non riceve una o più route esterne.

Come sempre, prima di tutto controlla le basi. Assicurarsi che:

- Le adiacenze del protocollo di routing sono attive nei BL.
- Una policy BGP Route-Reflector viene applicata al Pod Policy-Group e al Pod Profile.

Se i criteri di cui sopra sono corretti, di seguito sono riportati alcuni esempi più avanzati della possibile causa del problema.

Possibile causa: VRF non implementato sulla foglia interna

In questo caso, il problema sarebbe che non ci sono EPG con risorse impiegate sulla foglia interna dove è prevista la rotta esterna. Ciò potrebbe essere causato da associazioni di percorso statico configurate solo su interfacce inattive o da EPG integrati in VMM in modalità su richiesta senza alcun allegato dinamico rilevato.

Poiché il VRF L3Out non è distribuito sulla foglia interna (verificare con 'show vrf' sulla foglia interna), la foglia interna non importerà la route BGP da VPNv4.

Per risolvere il problema, l'utente deve distribuire le risorse all'interno del VRF L3Out nella foglia interna.

Possibile causa: Importa applicazione route in uso

Come accennato in precedenza, quando l'imposizione del controllo delle route di importazione è abilitata, L3Out accetta solo route esterne esplicitamente consentite. In genere, la feature viene implementata come mappa tabella. Una mappa-tabella si trova tra la tabella di routing RIB del protocollo e la tabella di routing effettiva in modo che influisca solo su quanto presente nella tabella di routing.

Nell'output sottostante l'opzione Import Route-Control è abilitata, ma non sono presenti route consentite in modo esplicito. Notare che l'LSA si trova nel database OSPF ma non nella tabella di routing del BL:

```
leaf103# vsh -c "show ip ospf database external 172.16.20.1 vrf Prod:Vrf1"
        OSPF Router with ID (10.0.0.3) (Process ID default VRF Prod:Vrf1)

                Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
172.16.20.1     10.0.0.134      455         0x80000003 0xb9a0    0


leaf103# show ip route 172.16.20.1 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

Route not found
```

Di seguito è riportata la mappa tabella installata che causa questo comportamento:

```
leaf103# show ip ospf vrf Prod:Vrf1

 Routing Process default with ID 10.0.0.3 VRF Prod:Vrf1
 Stateful High Availability enabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Table-map using route-map exp-ctx-2392068-deny-external-tag
 Redistributing External Routes from..

leaf103# show route-map exp-ctx-2392068-deny-external-tag
route-map exp-ctx-2392068-deny-external-tag, deny, sequence 1
  Match clauses:
    tag: 4294967295
  Set clauses:
route-map exp-ctx-2392068-deny-external-tag, deny, sequence 19999
  Match clauses:
    ospf-area: 0.0.0.100
  Set clauses:
```

Qualsiasi attività di apprendimento nell'area 100, che è l'area configurata in questo L3Out, viene negata implicitamente da questa mappa di tabella in modo che non venga installata nella tabella di routing.

Per risolvere il problema, l'utente deve definire la subnet sull'EPG esterno con il flag 'Importa subnet di controllo route' o creare un profilo di route di importazione che corrisponda ai prefissi da installare.

- Si noti che l'imposizione dell'importazione non è supportata per EIGRP.
- Notare anche che per BGP, l'imposizione dell'importazione viene implementata come route-map in entrata applicata al router adiacente BGP. Per ulteriori informazioni su come verificare questa condizione, consultare la sottosezione "BGP Route Advertisement".

Possibile causa: è in uso un profilo Interleak

I profili di route Interleak sono utilizzati per gli output L3E EIGRP e OSPF e sono destinati a consentire il controllo di ciò che viene ridistribuito dall'IGP in BGP, nonché l'applicazione di policy come l'impostazione degli attributi BGP.

Senza un profilo di route con interleak, tutte le route vengono importate in modo implicito in BGP.

Senza un profilo di rotta con interleak:

```
leaf103# show bgp process vrf Prod:Vrf1

Information regarding configured VRFs:

BGP Information for VRF Prod:Vrf1
VRF Type                        : System
VRF Id                          : 85
VRF state                       : UP
VRF configured                  : yes
VRF refcount                    : 1
VRF VNID                        : 2392068
Router-ID                       : 10.0.0.3
Configured Router-ID            : 10.0.0.3
Confed-ID                       : 0
Cluster-ID                      : 0.0.0.0
MSITE Cluster-ID                : 0.0.0.0
No. of configured peers         : 1
No. of pending config peers     : 0
No. of established peers        : 1
VRF RD                          : 101:2392068
VRF EVPN RD                     : 101:2392068

...
    Peers      Active-peers    Routes     Paths      Networks   Aggregates
    1          1               7          11         0          0

    Redistribution
        direct, route-map permit-all
        static, route-map imp-ctx-bgp-st-interleak-2392068
        ospf, route-map permit-all
        coop, route-map exp-ctx-st-2392068
        eigrp, route-map permit-all
```

Con un profilo di rotta con interfoliazione:

```
a-leaf103# show bgp process vrf Prod:Vrf1

Information regarding configured VRFs:

BGP Information for VRF Prod:Vrf1
VRF Type                        : System
VRF Id                          : 85
VRF state                       : UP
VRF configured                  : yes
VRF refcount                    : 1
VRF VNID                        : 2392068
Router-ID                       : 10.0.0.3
Configured Router-ID            : 10.0.0.3
Confed-ID                       : 0
Cluster-ID                      : 0.0.0.0
MSITE Cluster-ID                : 0.0.0.0
No. of configured peers         : 1
No. of pending config peers     : 0
No. of established peers        : 1
VRF RD                          : 101:2392068
VRF EVPN RD                     : 101:2392068

...

    Redistribution
        direct, route-map permit-all
        static, route-map imp-ctx-bgp-st-interleak-2392068
        ospf, route-map imp-ctx-proto-interleak-2392068
        coop, route-map exp-ctx-st-2392068
        eigrp, route-map permit-all
```

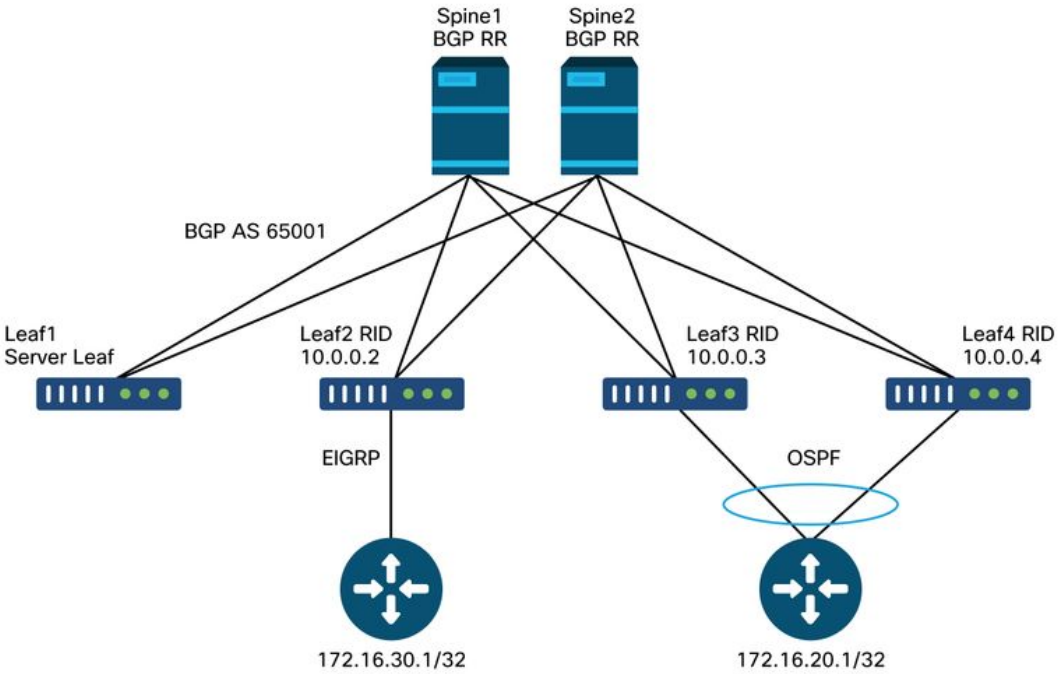
La route-map evidenziata in precedenza consente solo le corrispondenze esplicite nel profilo di interleak configurato. Se la route esterna non corrisponde, non verrà ridistribuita in BGP.

Flusso di lavoro annuncio route di transito

In questa sezione viene descritto come le route da un'uscita L3Out vengono annunciate in un'altra uscita L3Out. In questo scenario viene inoltre illustrato lo scenario in cui è necessario annunciare le route statiche configurate direttamente in un'uscita L3D. Non verranno presi in considerazione tutti i protocolli specifici, ma piuttosto le modalità di attuazione in ACI. In questo momento, non passerà al routing di transito tra VRF.

In questo scenario verrà utilizzata la topologia seguente:

Topologia di routing transit



Il flusso ad alto livello di come 172.16.20.1 verrebbe appreso da OSPF e quindi pubblicizzato in EIGRP, e le verifiche dell'intero processo e gli scenari di risoluzione dei problemi sono illustrati di seguito.

Per la route 172.16.20.1 da pubblicizzare nell'EIGRP, è necessario configurare uno dei seguenti elementi:

- La subnet da annunciare potrebbe essere definita sull'uscita EIGRP L3 con il flag 'Export Route-Control Subnet'. Come accennato nella sezione panoramica, questo flag viene utilizzato principalmente per il routing di transito e definisce le subnet da pubblicizzare al di fuori di tale L3Out.
- Configurare 0.0.0.0/0 e selezionare 'Esportazione aggregata' ed 'Esporta subnet di controllo route'. In questo modo viene creata una mappa dei percorsi per la ridistribuzione nel protocollo esterno che corrisponde a 0.0.0.0/0 e a tutti i prefissi più specifici (una corrispondenza effettiva qualsiasi). Si noti che quando si utilizza 0.0.0.0/0 con 'Aggregate Export', le route statiche non verranno associate per la ridistribuzione. In questo modo si evita di pubblicizzare inavvertitamente le route di BD che non devono essere pubblicizzate.
- Infine, è possibile creare un profilo di route di esportazione che corrisponda ai prefissi da annunciare. L'utilizzo di questo metodo può configurare l'opzione 'Aggregate' con prefissi diversi da 0.0.0.0/0.

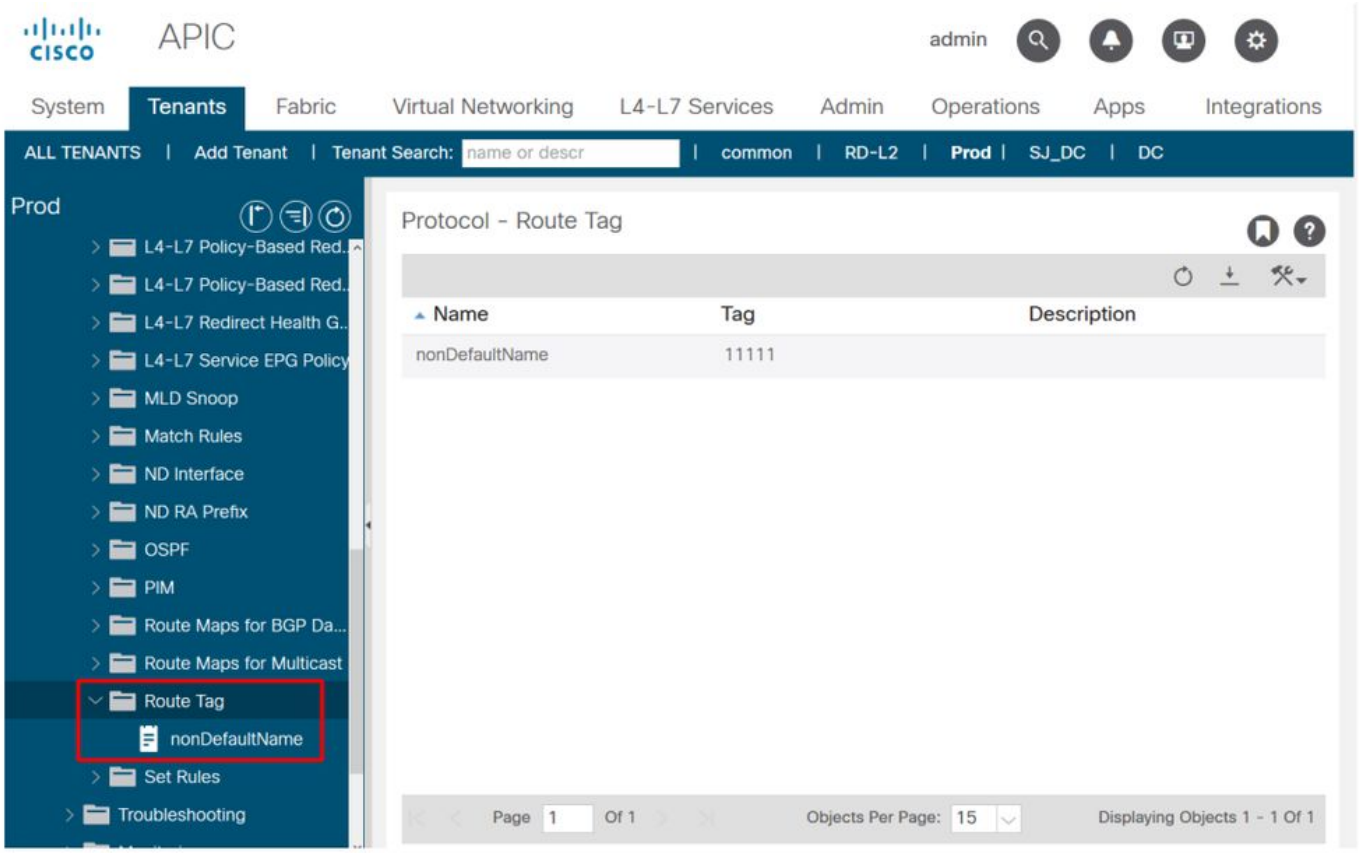
Le configurazioni precedenti determinerebbero l'annuncio del percorso di transito, ma è comunque necessario disporre di una policy di sicurezza per consentire il flusso del traffico del piano dati. Come per qualsiasi comunicazione da EPG a EPG, prima di autorizzare il traffico è necessario disporre di un contratto.

> Si noti che le subnet esterne duplicate con la subnet esterna per EPG esterno non possono essere configurate nello stesso VRF. Se configurate, le subnet devono essere più specifiche di 0.0.0.0. È importante configurare 'Subnet esterna per EPG esterno' solo per l'L3Out in cui viene ricevuta la route. Non configurarlo sull'uscita L3T che dovrebbe annunciare questa

route.

Èinoltre importante tenere presente che tutti i percorsi di transito sono contrassegnati con un tag VRF specifico. Per impostazione predefinita, questo tag è 4294967295. Il criterio di tag di route è configurato in 'Tenant > Rete > Protocolli > Tag di route:

Criteri tag route



Questo criterio di tag di route viene quindi applicato al VRF. Lo scopo di questo tag è essenzialmente quello di impedire cicli. Questo tag di route viene applicato quando il percorso di transito viene annunciato di nuovo da un'uscita L3D. Se tali route vengono quindi ricevute con lo stesso tag di route, la route viene eliminata.

Verificare che la route sia presente nella BL di ricezione tramite OSPF

Come per l'ultima sezione, verificare innanzitutto che la BL che deve ricevere inizialmente il percorso corretto.

```
leaf103# show ip route 172.16.20.1 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

172.16.20.1/32, ubest/mbest: 1/0
    *via 10.10.34.3, vlan347, [110/20], 01:25:30, ospf-default, type-2
```

Per il momento, si supponga che l'uscita pubblicitaria L3Out si trovi su una BL diversa (come nella topologia) (in scenari successivi si discuterà dove si trova sulla stessa BL).

Verificare che la route sia presente in BGP sull'host OSPF BL ricevente

Per poter annunciare la route OSPF al router EIGRP esterno, è necessario pubblicizzare la route in BGP sul BL OSPF ricevente.

```
leaf103# show bgp ipv4 unicast 172.16.20.1/32 vrf Prod:Vrf1
BGP routing table information for VRF Prod:Vrf1, address family IPv4 Unicast
BGP routing table entry for 172.16.20.1/32, version 30 dest ptr 0xa6f25ad0
Paths: (2 available, best #1)
Flags: (0x80c0002 00000000) on xmit-list, is not in urib, exported
  vpn: version 17206, (0x100002) on xmit-list
Multipath: eBGP iBGP

  Advertised path-id 1, VPN AF advertised path-id 1
  Path type: redist 0x408 0x1 ref 0 adv path ref 2, path is valid, is best path
  AS-Path: NONE, path locally originated
    0.0.0.0 (metric 0) from 0.0.0.0 (10.0.0.3)
      Origin incomplete, MED 20, localpref 100, weight 32768
      Extcommunity:
          RT:65001:2392068
          VNID:2392068
          COST:pre-bestpath:162:110

  VRF advertise information:

  Path-id 1 not advertised to any peer

  VPN AF advertise information:
  Path-id 1 advertised to peers:
    10.0.64.64         10.0.72.66
  Path-id 2 not advertised to any peer
```

La route è in BGP.

Verificare sulla BL EIGRP che deve annunciare il percorso che è installato

```
leaf102# show ip route 172.16.20.1 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

172.16.20.1/32, ubest/mbest: 2/0
    *via 10.0.72.67%overlay-1, [200/20], 00:56:46, bgp-65001, internal, tag 65001
         recursive next hop: 10.0.72.67/32%overlay-1
    *via 10.0.72.64%overlay-1, [200/20], 00:56:46, bgp-65001, internal, tag 65001
         recursive next hop: 10.0.72.64/32%overlay-1
```

Viene installata nella tabella di routing con gli hop successivi sovrapposti che puntano ai nodi foglia del bordo di origine.

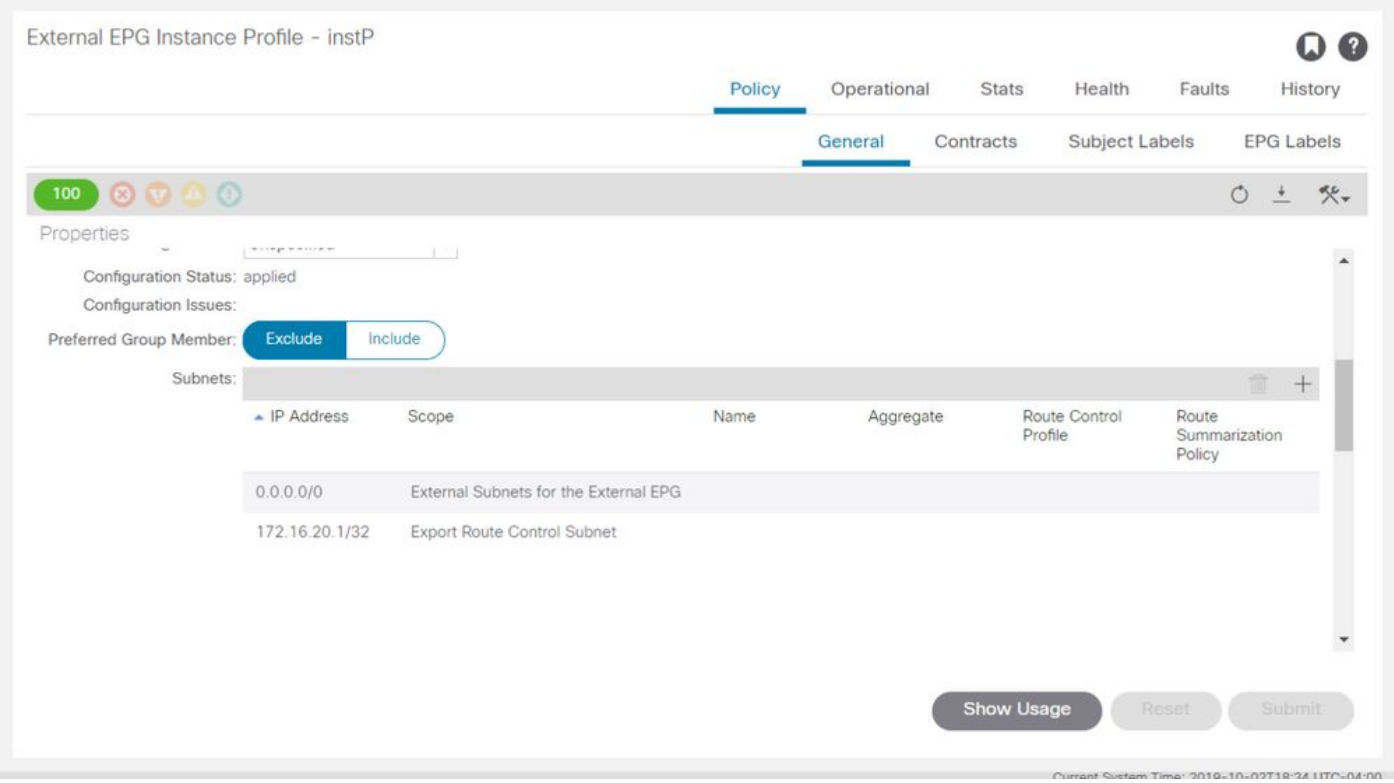
```
leaf102# acidiag fnvread

      ID   Pod ID                 Name    Serial Number         IP Address    Role        State
LastUpdMsgId
--------------------------------------------------------------------------------------------
```

```
--------------
     103        1            a-leaf101      FDO20160TPS      10.0.72.67/32    leaf
active   0
     104        1            a-leaf103      FDO20160TQ0      10.0.72.64/32    leaf
active   0
```

Verificare che la route sia annunciata nel BL

La route verrà annunciata da BL 102 in seguito all'impostazione del flag 'Esporta subnet di controllo della route' nella subnet configurata:

Esporta controllo route



Utilizzare il comando seguente per visualizzare la route-map creata come risultato del flag 'Esporta controllo route':

```
leaf102# show ip eigrp vrf Prod:Vrf1
IP-EIGRP AS 101 ID 10.0.0.2 VRF Prod:Vrf1
  Process-tag: default
  Instance Number: 1
  Status: running
  Authentication mode: none
  Authentication key-chain: none
  Metric weights: K1=1 K2=0 K3=1 K4=0 K5=0
  metric version: 32bit
  IP proto: 88 Multicast group: 224.0.0.10
  Int distance: 90 Ext distance: 170
  Max paths: 8
  Active Interval: 3 minute(s)
  Number of EIGRP interfaces: 1 (0 loopbacks)
  Number of EIGRP passive interfaces: 0
  Number of EIGRP peers: 1
  Redistributing:
    static route-map exp-ctx-st-2392068
```

```
    ospf-default route-map exp-ctx-proto-2392068
    direct route-map exp-ctx-st-2392068
    coop route-map exp-ctx-st-2392068
    bgp-65001 route-map exp-ctx-proto-2392068
```

Per cercare la 'ridistribuzione BGP > EIGRP', guardare la route-map. Tuttavia, la route-map deve essere la stessa indipendentemente dal fatto che il protocollo di origine sia OSPF, EIGRP o BGP. Le route statiche verranno controllate con una route-map diversa.

```
leaf102# show route-map exp-ctx-proto-2392068
route-map exp-ctx-proto-2392068, permit, sequence 15801
  Match clauses:
    ip address prefix-lists: IPv4-proto32771-2392068-exc-ext-inferred-export-dst
    ipv6 address prefix-lists: IPv6-deny-all
  Set clauses:
    tag 4294967295

a-leaf102# show ip prefix-list IPv4-proto32771-2392068-exc-ext-inferred-export-dst
ip prefix-list IPv4-proto32771-2392068-exc-ext-inferred-export-dst: 1 entries
   seq 1 permit 172.16.20.1/32
```

Nell'output precedente, il tag VRF viene impostato su questo prefisso per la prevenzione dei loop e la subnet configurata con 'Controllo route di esportazione' viene associata in modo esplicito.

Il routing di transito quando si ricevono e pubblicizzano le licenze BL è lo stesso

Come accennato in precedenza, quando i BL riceventi e pubblicitari sono diversi, la route deve essere pubblicizzata tramite il fabric utilizzando BGP. Quando le BL sono le stesse, la ridistribuzione o l'annuncio possono essere fatti direttamente tra i protocolli sulla foglia.

Di seguito vengono fornite brevi descrizioni di come viene implementata questa soluzione:

- **Routing in transito tra due host OSPF L3 sulla stessa foglia: l'**annuncio della route è controllato tramite un 'filtro di area' applicato al livello di processo OSPF. Un L3Out nell'Area 0 deve essere distribuito sulla foglia poiché le route vengono pubblicizzate tra le aree anziché tramite la ridistribuzione. Utilizzare 'show ip ospf vrf <nome>' per visualizzare l'elenco dei filtri. Visualizzare il contenuto del filtro utilizzando 'show route-map <nome filtro>'.
- **Routing in transito tra OSPF e EIGRP L3Out sulla stessa foglia: la** pubblicità delle route è controllata tramite route-map di ridistribuzione che possono essere visualizzate con 'show ip ospf' e 'show ip eigrp'. Si noti che se esistono più host OSPF L3T nello stesso BL, l'unico modo per ridistribuirli in uno solo di tali host OSPF L3T è se l'altro è uno stub o un NSSA con '**Invia LSA ridistribuite nell'area NSSA' disabilitato in modo** che non consenta alcuna LSA esterna.
- **Routing in transito tra OSPF o EIGRP e BGP sulla stessa foglia:** la pubblicità delle route nell'IGP è controllata tramite route-map di ridistribuzione. L'annuncio route in BGP è controllato tramite una route map in uscita applicata direttamente al router adiacente bgp a cui deve essere inviata la route. È possibile verificare questa condizione con 'show bgp ipv4 unicast neighbor <indirizzo router> vrf <nome> | grep in uscita".
- **Routing in transito tra due L3Out BGP sulla stessa foglia:** tutti gli annunci sono controllati tramite route-map applicate direttamente al vicino BGP a cui deve essere inviata la route. È possibile verificare questa condizione con 'show bgp ipv4 unicast neighbor <indirizzo router>

vrf <nome> | grep in uscita".

Scenari 1 per la risoluzione dei problemi relativi al routing transit: Route di transito non annunciata

In questo scenario di risoluzione dei problemi sono incluse route che devono essere apprese tramite un'istruzione L3Out e non tramite l'altra istruzione L3Out.

Come sempre, controllare le nozioni di base prima di esaminare qualsiasi elemento specifico di ACI.

- Le adiacenze di protocollo sono attive?
- Il percorso, che l'ACI dovrebbe pubblicizzare, è appreso da un protocollo esterno?
- Per BGP, il percorso viene eliminato a causa di alcuni attributi BGP? (percorso, ecc.).
- L'output L3 ricevente è presente nel database OSPF, nella tabella di topologia EIGRP o nella tabella BGP?
- Al gruppo di criteri POD viene applicata una policy BGP Route Reflector Policy applicata al profilo del pod?

Se tutte le verifiche di protocollo di base sono configurate correttamente, di seguito sono riportate altre cause comuni per un percorso di transito non annunciato.

Possibile causa: Nessuna area OSPF 0

Se la topologia interessata coinvolge due OSP L3Out sulla stessa foglia di bordo, è necessario che sia presente un'Area 0 per le route da un'area all'altra. Per ulteriori informazioni, vedere il punto precedente relativo al routing in transito tra due output OSPF L3 sulla stessa foglia.

Possibile causa: L'area OSPF è stub o NSSA

Ciò si verifica se l'uscita OSPF L3D è configurata con un'area Stub o NSSA non configurata per annunciare le LSA esterne. Con OSPF, le LSA esterne non vengono mai pubblicizzate nelle aree Stub. Vengono pubblicizzate nelle aree NSSA se si seleziona 'Invia LSA ridistribuite nell'area NSSA'.

Scenari n. 2 per la risoluzione dei problemi relativi al routing di transito: Route di transito non ricevuta

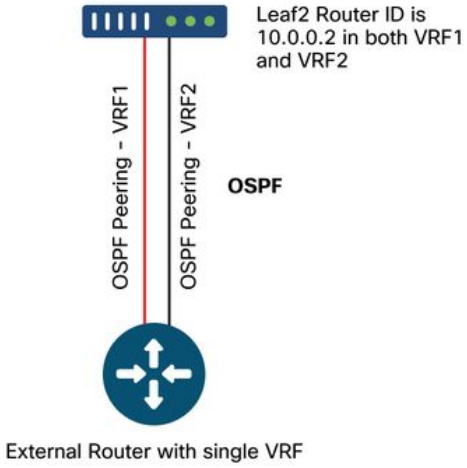
In questo scenario, il problema è che alcune route annunciate da un elemento L3Out ACI non vengono ricevute in un altro elemento L3Out. Questo scenario potrebbe essere applicabile se gli L3Out si trovano in due fabric separati e sono connessi da router esterni o se gli L3Out si trovano in VRF diverse e i percorsi vengono passati tra i VRF da un router esterno.

Possibile causa: BL è configurato con lo stesso ID router in più VRF

Dal punto di vista della configurazione, un ID router non può essere duplicato all'interno dello stesso VRF. Tuttavia, è in genere consigliabile utilizzare lo stesso ID router in VRF diverse, purché queste due VRF non siano collegate agli stessi domini del protocollo di routing.

Considerare la topologia seguente:

Router esterno con VRF singolo — Router di transito non ricevuto



Il problema in questo caso è che la foglia ACI rileva le LSA con il proprio Router-ID ricevuto, di conseguenza queste non vengono installate nel database OSPF.

Inoltre, se la stessa configurazione veniva rilevata su coppie VPC, le LSA venivano aggiunte ed eliminate continuamente su alcuni router. Ad esempio, il router vedrebbe le LSA provenienti dal proprio peer VPC con VRF e LSA provenienti dallo stesso nodo (con lo stesso Router-ID) e originate nell'altro VRF.

Per risolvere questo problema, l'utente deve verificare che un nodo abbia un ID router diverso e univoco all'interno di ogni VRF in cui ha un L3Out.

Possibile causa: instradamenti da un'uscita L3in un fabric ACI ricevuti su un altro fabric con lo stesso tag VRF

Il tag di route predefinito in ACI è sempre lo stesso, a meno che non venga modificato. Se le route vengono annunciate da un'uscita L3T di un fabric VRF o ACI a un'altra uscita L3T di un altro fabric VRF o ACI senza modificare i tag VRF predefiniti, le route verranno ignorate dai BL riceventi.

Per risolvere questo scenario, è sufficiente utilizzare una policy di assegnazione dei tag di route univoca per ogni VRF in ACI.

Scenari 3 per la risoluzione dei problemi relativi al routing di transito — Router annunciati in modo imprevisto

Questo scenario si verifica quando i percorsi di transito vengono pubblicizzati in un'uscita L3T in cui non sono destinati a essere pubblicizzati.

Possibile causa: utilizzo di 0.0.0.0/0 con 'Aggregate Export'

Quando una subnet esterna è configurata come 0.0.0.0/0 con 'Esporta subnet di controllo route' e 'Esporta aggregato', viene installata una corrispondenza per tutte le route-map di ridistribuzione. In questo caso, tutte le route sul BL apprese tramite OSPF, EIGRP o BGP vengono annunciate all'esterno dell'output L3T in cui è configurato.

Di seguito è riportata la route-map distribuita alla foglia come risultato dell'esportazione aggregata:

```
leaf102# show ip eigrp vrf Prod:Vrf1
IP-EIGRP AS 101 ID 10.0.0.2 VRF Prod:Vrf1
 Process-tag: default
 Instance Number: 1
 Status: running
 Authentication mode: none
 Authentication key-chain: none
 Metric weights: K1=1 K2=0 K3=1 K4=0 K5=0
 metric version: 32bit
 IP proto: 88 Multicast group: 224.0.0.10
 Int distance: 90 Ext distance: 170
 Max paths: 8
 Active Interval: 3 minute(s)
 Number of EIGRP interfaces: 1 (0 loopbacks)
 Number of EIGRP passive interfaces: 0
 Number of EIGRP peers: 1
 Redistributing:
   static route-map exp-ctx-st-2392068
   ospf-default route-map exp-ctx-proto-2392068
   direct route-map exp-ctx-st-2392068
   coop route-map exp-ctx-st-2392068
   bgp-65001 route-map exp-ctx-proto-2392068
 Tablemap: route-map exp-ctx-2392068-deny-external-tag , filter-configured
 Graceful-Restart: Enabled
 Stub-Routing: Disabled
 NSF converge time limit/expiries: 120/0
 NSF route-hold time limit/expiries: 240/0
 NSF signal time limit/expiries: 20/0
 Redistributed max-prefix: Disabled
 selfAdvRtTag: 4294967295
leaf102# show route-map exp-ctx-proto-2392068
route-map exp-ctx-proto-2392068, permit, sequence 19801
 Match clauses:
   ip address prefix-lists: IPv4-proto32771-2392068-agg-ext-inferred-export-dst
   ipv6 address prefix-lists: IPv6-deny-all
 Set clauses:
   tag 4294967295



leaf102# show ip prefix-list IPv4-proto32771-2392068-agg-ext-inferred-export-dst
    ip prefix-list IPv4-proto32771-2392068-agg-ext-inferred-export-dst: 1 entries
seq 1 permit 0.0.0.0/0 le 32
```

Questa è la prima causa dei loop di routing che coinvolgono un ambiente ACI.

Contratto e L3Out

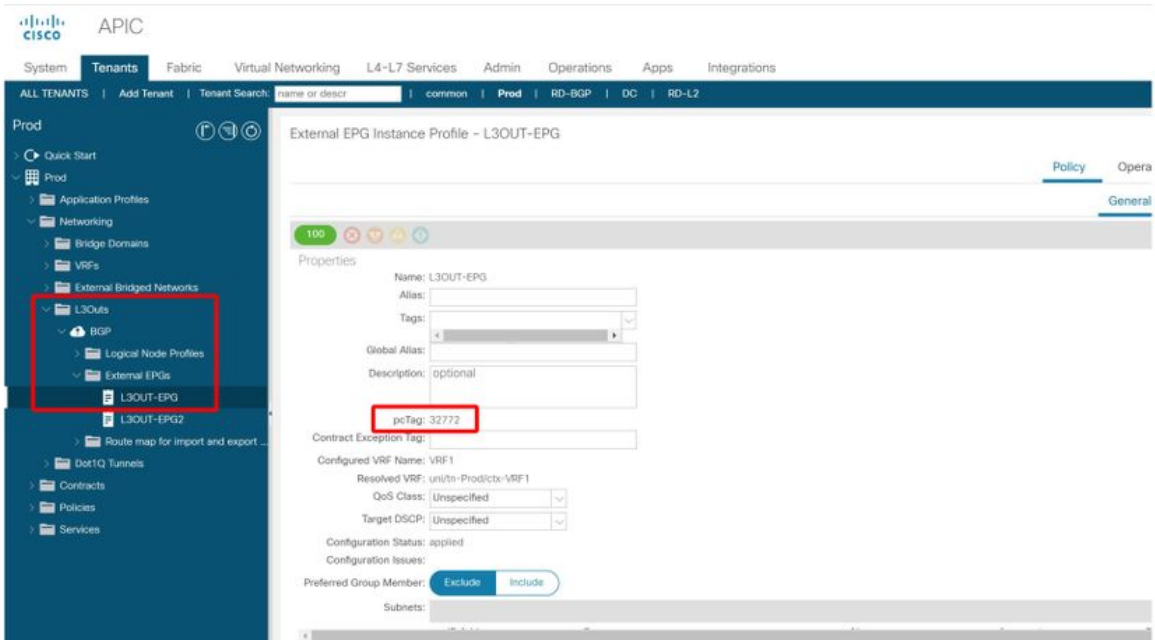
EPG basato sul prefisso su L3Out

In un EPG interno (non-L3Out), i contratti vengono applicati dopo aver derivato il pcTag dell'origine e il pcTag dell'EPG di destinazione. La VLAN/VXLAN di incapsulamento del pacchetto ricevuto sulla porta di download viene usata per guidare questo pcTag classificando il pacchetto nell'EPG. Ogni volta che si impara un indirizzo MAC o IP, questo viene appreso insieme al suo incapsulamento di accesso e al pcTag EPG associato. Per ulteriori informazioni su pcTag e sull'applicazione dei contratti, fare riferimento al capitolo "Security policies" (Policy di sicurezza).

L3Outs inoltre guida un pcTag utilizzando il suo L3Out EPG (External EPG) situato in 'Tenant > Networking > L3OUT > Networks > L3OUT-EPG'. Tuttavia, i router L3 non si basano sulle VLAN e sulle interfacce per classificare i pacchetti come tali. La classificazione è invece basata sul prefisso/subnet di origine in modo che corrisponda al prefisso più lungo. Pertanto, un EPG L3Out può essere definito **EPG basato su prefissi**. Dopo aver classificato un pacchetto in un L3Out basato su una subnet, il pacchetto segue un modello di applicazione dei criteri simile a quello di un normale EPG.

Il diagramma seguente illustra dove è possibile trovare il pcTag di un determinato EPG L3Out nell'interfaccia utente.

Posizione del pcTag per un L3Out



L'utente è responsabile della definizione della tabella EPG basata sul prefisso. A tale scopo, viene utilizzato l'ambito della subnet 'Subnet esterna per EPG esterno'. Ogni subnet impostata con tale ambito aggiungerà una voce in una tabella LPM (Longest Prefix Match) statica. Questa subnet punterà al valore pcTag che verrà utilizzato per qualsiasi indirizzo IP compreso in tale prefisso.

La tabella LPM delle subnet EPG basate sui prefissi può essere verificata sugli switch foglia utilizzando il seguente comando:

```
vsh -c 'show system internal policy-mgr prefix'
```

Osservazioni:

- L'ambito delle voci della tabella LPM è VRF VNID. La ricerca viene eseguita per vrf_vnid/src pcTag/dst pcTag.
- Ogni voce fa riferimento a un singolo pcTag. Di conseguenza, due EPG L3Out non possono utilizzare la stessa subnet con la stessa lunghezza di maschera all'interno dello stesso VRF.
- La subnet 0.0.0.0/0 utilizza sempre uno speciale pcTag 15. Pertanto, può essere duplicata, ma deve essere eseguita solo con una piena comprensione delle implicazioni relative all'applicazione delle policy.
- Questa tabella viene utilizzata in entrambe le direzioni. Da L3Out a Leaf Local Endpoint, il pcTag di origine viene derivato utilizzando questa tabella.Dall'endpoint locale foglia a L3Out, il

pcTag di destinazione viene derivato utilizzando questa tabella.

- Se il VRF dispone dell'impostazione di imposizione 'In entrata' per 'Direzione applicazione controllo criteri', la tabella dei prefissi LPM sarà presente nei BL L3Out e in tutti gli switch foglia del VRF con un contratto con L3Out.

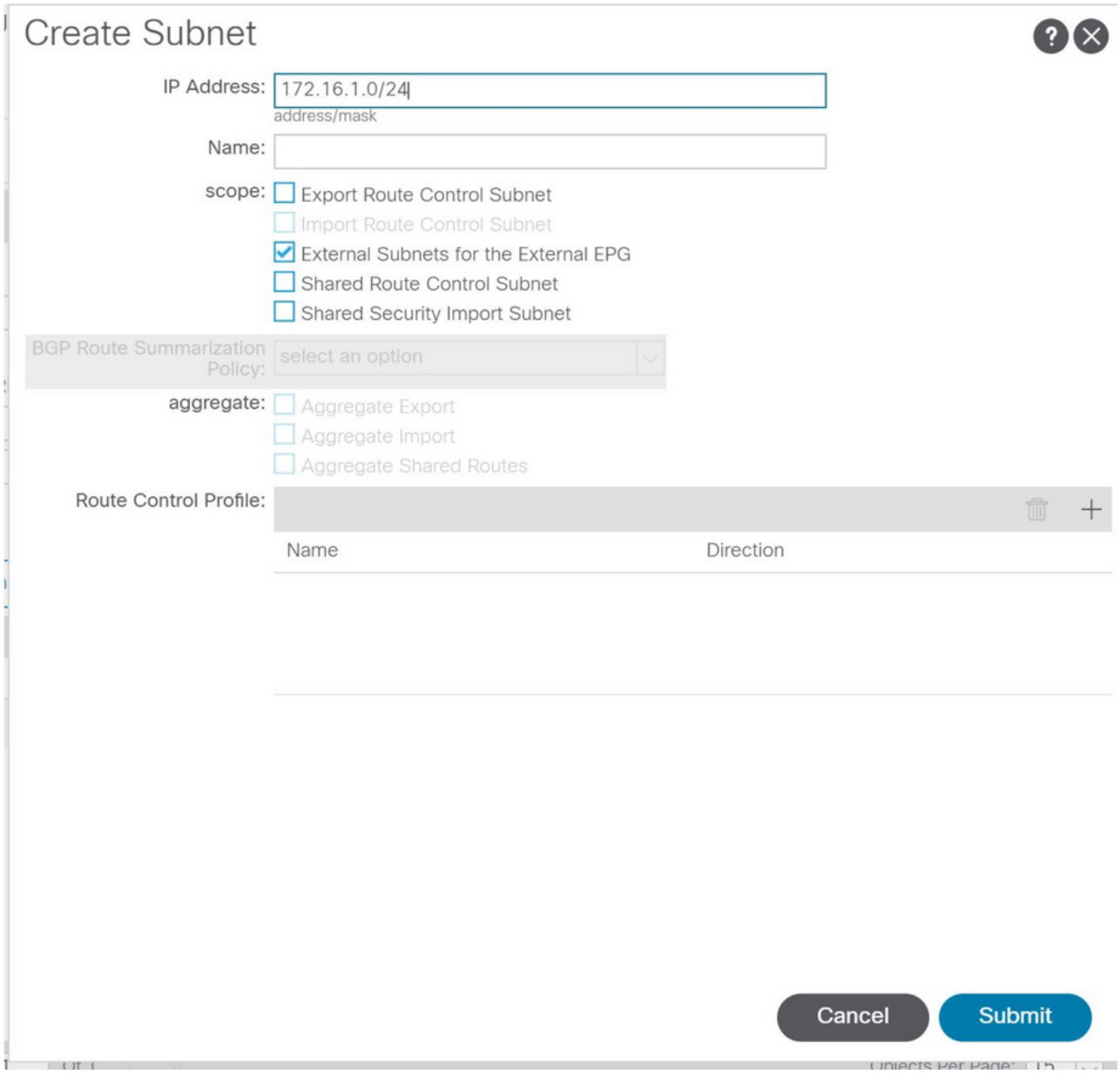
Esempio 1: Singolo L3Out con prefisso specifico

Scenario: Singola uscita BGP L3in vrf Prod:VRF1 con un'uscita L3EPG. Il prefisso 172.16.1.0/24 è stato ricevuto da un'origine esterna, quindi deve essere classificato nell'EPG L3Out.

```
bdsol-aci32-leaf3# show ip route 172.16.1.0  vrf Prod:VRF1
IP Route Table for VRF "Prod:VRF1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

172.16.1.0/24, ubest/mbest: 1/0
    *via 10.0.0.134%Prod:VRF1, [20/0], 00:56:14, bgp-132, external, tag 65002
         recursive next hop: 10.0.0.134/32%Prod:VRF1
```

Aggiungere innanzitutto la subnet alla tabella dei prefissi.

Subnet con ambito 'Subnet esterne per EPG esterno'



Verificare la programmazione dell'elenco di prefissi sugli switch foglia che hanno il VRF dell'uscita L3:

```
bdsol-aci32-leaf3# vsh -c ' show system internal  policy-mgr prefix ' |  egrep "Prod|==|Addr"
Vrf-Vni VRF-Id Table-Id Table-State  VRF-Name                     Addr
Class Shared Remote Complete
======= ======  ===========  =======  ============================
================================ ====== ====== ====== ========
2097154 35     0x23          Up     Prod:VRF1
0.0.0.0/0   15      True   True   False
2097154 35     0x23          Up     Prod:VRF1
172.16.1.0/24  32772   True   True   False
```

Il pcTag dell'EPG L3Out è 32772 nell'ambito vrf 2097154.

Esempio 2: Singola uscita L3D con più prefissi

Se si espande l'esempio precedente, in questo scenario L3Out riceve più prefissi. Quando l'immissione di ciascun prefisso è funzionalmente valida, un'opzione alternativa (a seconda del progetto previsto) consiste nell'accettare tutti i prefissi ricevuti sull'uscita L3D.

A tale scopo, è possibile utilizzare il prefisso '0.0.0.0/0'.

Subnet - 0.0.0.0/0

Policy | Faults | History

Properties

IP Address: 0.0.0.0/0
address/mask

Scope:
- [ ] Export Route Control Subnet
- [ ] Import Route Control Subnet
- [x] External Subnets for the External EPG
- [ ] Shared Route Control Subnet
- [ ] Shared Security Import Subnet

Aggregate:
- [ ] Aggregate Export
- [ ] Aggregate Import
- [ ] Aggregate Shared Routes

BGP Route Summarization Policy: select an option

Route Control Profile:

Name	Direction

No items have been found.
Select Actions to create a new item.

Il risultato è la seguente voce della tabella dei prefissi di policy-mgr:

```
bdsol-aci32-leaf3# vsh -c ' show system internal  policy-mgr prefix ' |  egrep "Prod|==|Addr"
Vrf-Vni VRF-Id Table-Id Table-State  VRF-Name                     Addr
Class Shared Remote Complete
======= ======  =========== =======  ============================
================================ ====== ====== ====== ========
2097154 35     0x23          Up     Prod:VRF1
0.0.0.0/0   15      True   True   False
2097154 35     0x23          Up     Prod:VRF1
172.16.1.0/24  32772   True   True   False
```

> Si noti che il valore di pcTag assegnato a 0.0.0.0/0 utilizza il valore 15 e non 32772. pcTag 15 è un pcTag di sistema riservato che viene utilizzato solo con il valore 0.0.0.0/0 che funge da carattere jolly per la corrispondenza di tutti i prefissi di un'uscita L3T.

Se il VRF dispone di un singolo L3Out con un singolo EPG L3Out che utilizza il prefisso 0.0.0.0/0, il prefisso della policy rimane univoco ed è l'approccio più semplice da utilizzare per intercettare tutti i dati.

Esempio 3a: Più EPG L3Out in un VRF

In questo scenario sono presenti più EPG L3Out nello stesso VRF.

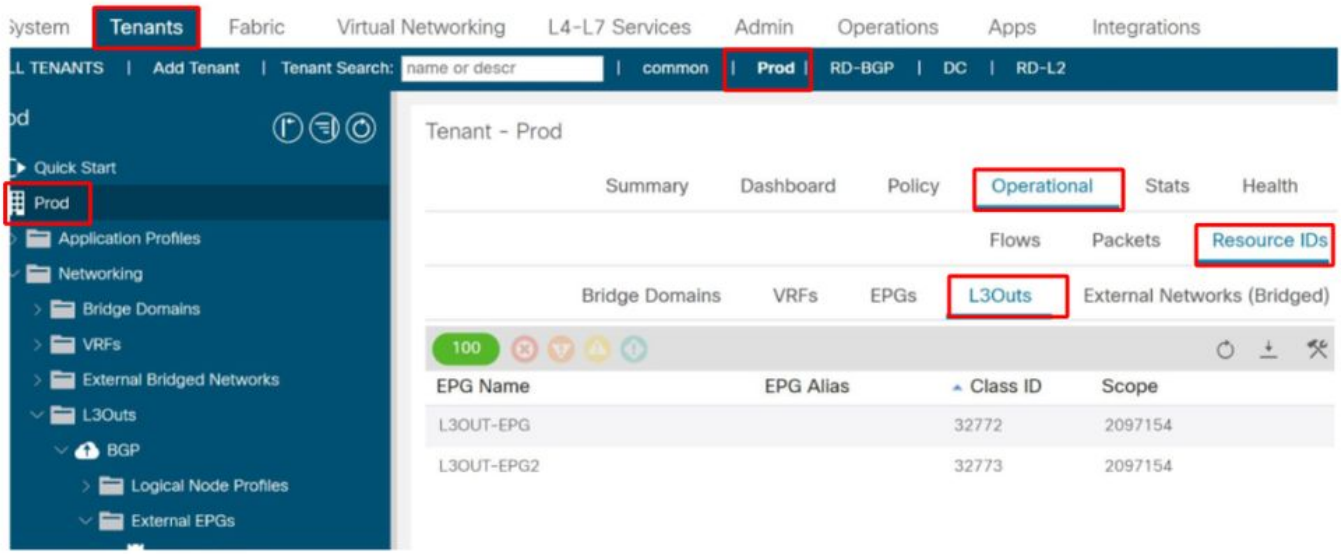
Nota: Dal punto di vista dell'EPG basato sul prefisso, le due configurazioni riportate di seguito daranno come risultato voci equivalenti della tabella dei prefissi di gestione delle policy LPM:

1. Due L3Out con un L3Out EPG ciascuno.
2. Un'uscita L3con due EPG L3Out

In entrambi gli scenari, il numero totale di EPG L3Out è 2. Ciò significa che a ciascuno di essi verrà assegnato un pcTag specifico e delle subnet associate.

Tutti i pcTag di un dato EPG L3Out possono essere visualizzati nella GUI all'indirizzo 'Tenant > Operational > Resource id > L3Outs'

Verifica del tag PC L3Out



In questo scenario, l'infrastruttura ACI riceve più prefissi dai router esterni e la definizione EPG L3Out è la seguente:

- 172.16.1.0/24 assegnato a L3OUT-EPG.
- 172.16.2.0/24 assegnato a L3OUT-EPG2.
- 172.16.0.0/16 assegnato a L3OUT-EPG (per intercettare il prefisso 172.16.3.0/24).

Per risolvere questo problema, la configurazione verrà definita come segue:

- L3OUT-EPG ha le subnet 172.16.1.0/24 e 172.16.0.0/16 entrambe con l'ambito 'Subnet esterna per EPG esterno'.
- L3OUT-EPG2 dispone della subnet 172.16.2.0/24 con ambito 'Subnet esterna per EPG esterno'.

Le voci della tabella dei prefissi risultanti saranno:

```
bdsol-aci32-leaf3# vsh -c 'show system internal  policy-mgr prefix' |  egrep "Prod|==|Addr"
Vrf-Vni VRF-Id Table-Id Table-State  VRF-Name                       Addr
Class Shared Remote Complete
======= ======  =========== =======  ============================
================================ ====== ====== ====== ========
2097154 35     0x23           Up     Prod:VRF1
0.0.0.0/0   15      True   True   False
2097154 35     0x23           Up     Prod:VRF1
172.16.1.0/24  32772   True    True    False
2097154 35     0x23           Up     Prod:VRF1
172.16.0.0/16  32772   True    True    False
2097154 35     0x23           Up     Prod:VRF1
172.16.2.0/24  32773   True    True    False
```

172.16.2.0/24 viene assegnato a pcTag 32773 (L3OUT-EPG2) e 172.16.0.0/16 a 32772 (L3OUT-EPG).

In questo scenario, la voce 172.16.1.0/24 è ridondante in quanto la supernet /16 è assegnata allo stesso EPG.

Più EPG L3Out sono utili quando l'obiettivo è applicare contratti diversi a gruppi di prefissi all'interno di un singolo EPG L3Out. Nell'esempio seguente viene illustrato come vengono in gioco i contratti con più EPG L3Out.

Esempio 3b: più EPG L3Out con contratti diversi

Questo scenario contiene le impostazioni seguenti:

- Contratto ICMP che consente solo l'uso di ICMP.
- Contratto HTTP che consente solo la porta di destinazione 80 TCP.
- EPG1 (pcTag 32770) fornisce il contratto HTTP utilizzato da L3OUT-EPG (pcTag 32772).
- EPG2 (pcTag 32771) fornisce il contratto ICMP utilizzato da L3OUT-EPG2 (pcTag 32773).

Verranno utilizzati gli stessi prefissi policymgr dell'esempio precedente:

- 172.16.1.0/24 in L3OUT-EPG deve consentire HTTP a EPG1
- 172.16.2.0/24 in L3OUT-EPG2 deve consentire ICMP a EPG2

prefisso policy-mgr e regole di zoning:

```
bdsol-aci32-leaf3# vsh -c ' show system internal  policy-mgr prefix ' |  egrep "Prod|==|Addr"
Vrf-Vni VRF-Id Table-Id Table-State  VRF-Name                   Addr
Class Shared Remote Complete
======= ======  =========== =======  ============================
================================ ====== ====== ====== ========
2097154 35     0x23          Up     Prod:VRF1
0.0.0.0/0   15      True   True   False
2097154 35     0x23          Up     Prod:VRF1
172.16.1.0/24  32772   True   True   False
2097154 35     0x23          Up     Prod:VRF1
172.16.0.0/16  32772   True   True   False
2097154 35     0x23          Up     Prod:VRF1
172.16.2.0/24  32773   True   True   False
```

```
bdsol-aci32-leaf3# show zoning-rule scope 2097154
+---------+--------+--------+----------+----------------+---------+---------+------+----------+-
---------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |  Action  |
Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------+----------+-
---------------------+
|   4326  |   0    |   0    | implicit |    uni-dir     | enabled | 2097154 |      | deny,log |
any_any_any(21)    |
|   4335  |   0    | 16387  | implicit |    uni-dir     | enabled | 2097154 |      |  permit  |
any_dest_any(16)   |
|   4334  |   0    |   0    | implarp  |    uni-dir     | enabled | 2097154 |      |  permit  |
any_any_filter(17)  |
|   4333  |   0    |   15   | implicit |    uni-dir     | enabled | 2097154 |      | deny,log |
any_vrf_any_deny(22) |
|   4332  |   0    | 16386  | implicit |    uni-dir     | enabled | 2097154 |      |  permit  |
any_dest_any(16)   |
|   4342  | 32771  | 32773  |    5     | uni-dir-ignore | enabled | 2097154 | ICMP |  permit  |
fully_qual(7)     |
|   4343  | 32773  | 32771  |    5     |     bi-dir     | enabled | 2097154 | ICMP |  permit  |
fully_qual(7)     |
|   4340  | 32770  | 32772  |    38    |    uni-dir     | enabled | 2097154 | HTTP |  permit  |
fully_qual(7)     |
|   4338  | 32772  | 32770  |    37    |    uni-dir     | enabled | 2097154 | HTTP |  permit  |
fully_qual(7)     |
+---------+--------+--------+----------+----------------+---------+---------+------+----------+-
---------------------+
```

Convalida del datapath tramite fTriage: flusso consentito dai criteri

Con un flusso ICMP tra 172.16.2.1 sulla rete esterna e 192.168.3.1 in EPG2, fTriage può essere utilizzato per intercettare e analizzare il flusso. In questo caso, avviare fTriage su entrambi gli switch foglia 103 e 104 in quanto il traffico può entrare in una delle due posizioni:

```
admin@apic1:~> ftriage route -ii LEAF:103,104 -sip 172.16.2.1 -dip 192.168.3.1
fTriage Status: {"dbgFtriage": {"attributes": {"operState": "InProgress", "pid": "14454",
"apicId": "1", "id": "0"}}}
Starting ftriage
Log file name for the current run is: ftlog_2019-10-02-22-30-41-871.txt
2019-10-02 22:30:41,874 INFO     /controller/bin/ftriage route -ii LEAF:103,104 -sip 172.16.2.1
-dip 192.168.3.1
2019-10-02 22:31:28,868 INFO     ftriage:     main:1165 Invoking ftriage with default password
and default username: apic#fallback\\admin
2019-10-02 22:32:15,076 INFO     ftriage:     main:839  L3 packet Seen on bdsol-aci32-leaf3
Ingress: Eth1/12 (Po1) Egress: Eth1/12 (Po1) Vnid: 11365
2019-10-02 22:32:15,295 INFO     ftriage:     main:242  ingress encap string vlan-2551
2019-10-02 22:32:17,839 INFO     ftriage:     main:271  Building ingress BD(s), Ctx
2019-10-02 22:32:20,583 INFO     ftriage:     main:294  Ingress BD(s) Prod:VRF1:l3out-BGP:vlan-
2551
2019-10-02 22:32:20,584 INFO     ftriage:     main:301  Ingress Ctx: Prod:VRF1
2019-10-02 22:32:20,693 INFO     ftriage:   pktrec:490  bdsol-aci32-leaf3: Collecting transient
losses snapshot for LC module: 1
2019-10-02 22:32:38,933 INFO     ftriage:     nxos:1404 bdsol-aci32-leaf3: nxos matching rule
id:4343 scope:34 filter:5
2019-10-02 22:32:39,931 INFO     ftriage:     main:522  Computed egress encap string vlan-2502
2019-10-02 22:32:39,933 INFO     ftriage:     main:313  Building egress BD(s), Ctx
2019-10-02 22:32:41,796 INFO     ftriage:     main:331  Egress Ctx Prod:VRF1
2019-10-02 22:32:41,796 INFO     ftriage:     main:332  Egress BD(s): Prod:BD2
2019-10-02 22:32:48,636 INFO     ftriage:     main:933  SIP 172.16.2.1 DIP 192.168.3.1
2019-10-02 22:32:48,637 INFO     ftriage:  unicast:973  bdsol-aci32-leaf3: <- is ingress node
2019-10-02 22:32:51,257 INFO     ftriage:  unicast:1202 bdsol-aci32-leaf3: Dst EP is local
2019-10-02 22:32:54,129 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: EP if(Po1) same as
egr if(Po1)
2019-10-02 22:32:55,348 INFO     ftriage:     misc:657  bdsol-aci32-leaf3:
DMAC(00:22:BD:F8:19:FF) same as RMAC(00:22:BD:F8:19:FF)
2019-10-02 22:32:55,349 INFO     ftriage:     misc:659  bdsol-aci32-leaf3: L3 packet getting
routed/bounced in SUG
2019-10-02 22:32:55,596 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: Dst IP is present in
SUG L3 tbl
2019-10-02 22:32:55,896 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: RW seg_id:11365 in
SUG same as EP segid:11365
2019-10-02 22:33:02,150 INFO     ftriage:     main:961  Packet is Exiting fabric with peer-
device: bdsol-aci32-n3k-3 and peer-port: Ethernet1/16
```

fTriage conferma la corrispondenza della regola di zoning alla regola ICMP da L3OUT_EPG2 a EPG:

```
2019-10-02 22:32:38,933 INFO     ftriage:     nxos:1404 bdsol-aci32-leaf3: nxos matching rule
id:4343 scope:34 filter:5
```

Convalida di datapath tramite fTriage: flusso non consentito dai criteri

Poiché il traffico ICMP ha origine da 172.16.1.1 (L3OUT-EPG) fino a 192.168.3.1 (EPG2), si prevede un calo delle policy.

```
admin@apic1:~> ftriage route -ii LEAF:103,104 -sip 172.16.1.1 -dip 192.168.3.1
fTriage Status: {"dbgFtriage": {"attributes": {"operState": "InProgress", "pid": "15139",
"apicId": "1", "id": "0"}}}
Starting ftriage
Log file name for the current run is: ftlog_2019-10-02-22-39-15-050.txt
2019-10-02 22:39:15,056 INFO     /controller/bin/ftriage route -ii LEAF:103,104 -sip 172.16.1.1
-dip 192.168.3.1
2019-10-02 22:40:03,523 INFO     ftriage:     main:1165 Invoking ftriage with default password
and default username: apic#fallback\\admin
2019-10-02 22:40:43,338 ERROR    ftriage:  unicast:234  bdsol-aci32-leaf3: L3 packet getting fwd
dropped, checking drop reason
2019-10-02 22:40:43,339 ERROR    ftriage:  unicast:234  bdsol-aci32-leaf3: L3 packet getting fwd
dropped, checking drop reason
SECURITY_GROUP_DENY              condition setcast:236  bdsol-aci32-leaf3: Drop reason -
SECURITY_GROUP_DENY              condition set
2019-10-02 22:40:43,340 INFO     ftriage:  unicast:252  bdsol-aci32-leaf3: policy drop flow
sclass:32772 dclass:32771 sg_label:34 proto:1
2019-10-02 22:40:43,340 INFO     ftriage:     main:681  : Ftriage Completed with hunch: None
fTriage Status: {"dbgFtriage": {"attributes": {"operState": "Idle", "pid": "0", "apicId": "0",
"id": "0"}}}
```

fTriage conferma che il pacchetto viene scartato con il motivo SECURITY_GROUP_DENY (perdita di criteri) e che il pcTag di origine derivato è 32772 e il pcTag di destinazione è 32771. Confrontando questo con le regole di suddivisione in zone, non ci sono chiaramente voci tra quelle EPG.

```
bdsol-aci32-leaf3# show zoning-rule  scope 2097154 src-epg 32772 dst-epg 32771
+---------+--------+--------+----------+-----+--------+-------+------+--------+----------+
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name | Action | Priority |
+---------+--------+--------+----------+-----+--------+-------+------+--------+----------+
+---------+--------+--------+----------+-----+--------+-------+------+--------+----------+
```

Esempio 4: più output L3 con prefissi multipli

Lo scenario è impostato in modo simile all'esempio 3 (definizioni EPG L3Out e L3Out), ma la rete definita in entrambi gli EPG L3Out è 0.0.0.0/0.

La configurazione del contratto è la seguente:

- Contratto ICMP1 che consente l'uso di ICMP.
- Contratto ICMP2 che consente l'uso di ICMP.
- EPG1 (pcTag 32770) fornisce un contratto ICMP1 utilizzato da L3OUT-EPG (pcTag 32772).
- EPG2 (pcTag 32771) fornisce un contratto ICMP2 utilizzato da L3OUT-EPG2 (pcTag 32773).

Questa configurazione può risultare ideale nel caso in cui la rete esterna annunci molti prefissi, ma sono presenti almeno due blocchi di prefissi che seguono modelli di flusso consentiti diversi. In questo esempio, un prefisso deve consentire solo ICMP1 e l'altro solo ICMP2.

Nonostante si utilizzi '0.0.0.0/0' due volte nello stesso VRF, nella tabella dei prefissi policy-mgr viene programmato un solo prefisso:

```
bdsol-aci32-leaf3# vsh -c ' show system internal  policy-mgr prefix ' |  egrep "Prod|==|Addr"
Vrf-Vni VRF-Id Table-Id Table-State  VRF-Name                  Addr
Class Shared Remote Complete
======= ======  ========== =======  ===========================
```

```
================================ ====== ====== ====== ========
2097154 35     0x23          Up     Prod:VRF1
```

Due flussi riesaminati di seguito. In base alla configurazione del contratto precedente, è previsto quanto segue:

1. da 172.16.2.1 (L3OUT-EPG2) a 192.168.3.1 (EPG2) **devono** essere consentiti da ICMP2
2. Da 172.16.2.1 (L3OUT-EPG2) a 192.168.1.1 (EPG1) **non devono** essere consentiti in quanto non esiste alcun contratto tra EPG1 e L3OUT-EPG2

Convalida di datapath tramite fTriage: flusso consentito dai criteri

Eseguire Triage con un flusso ICMP da 172.16.2.1 (L3OUT-EPG2) a 192.168.3.1 (EPG2 — pcTag 32771).

```
Starting ftriage
Log file name for the current run is: ftlog_2019-10-02-23-11-14-298.txt
2019-10-02 23:11:14,302 INFO     /controller/bin/ftriage route -ii LEAF:103,104 -sip 172.16.2.1
-dip 192.168.3.1
2019-10-02 23:12:00,887 INFO     ftriage:     main:1165 Invoking ftriage with default password
and default username: apic#fallback\\admin
2019-10-02 23:12:44,565 INFO     ftriage:     main:839  L3 packet Seen on bdsol-aci32-leaf3
Ingress: Eth1/12 (Po1) Egress: Eth1/12 (Po1) Vnid: 11365
2019-10-02 23:12:44,782 INFO     ftriage:     main:242  ingress encap string vlan-2551
2019-10-02 23:12:47,260 INFO     ftriage:     main:271  Building ingress BD(s), Ctx
2019-10-02 23:12:50,041 INFO     ftriage:     main:294  Ingress BD(s) Prod:VRF1:l3out-BGP:vlan-
2551
2019-10-02 23:12:50,042 INFO     ftriage:     main:301  Ingress Ctx: Prod:VRF1
2019-10-02 23:12:50,151 INFO     ftriage:   pktrec:490  bdsol-aci32-leaf3: Collecting transient
losses snapshot for LC module: 1
2019-10-02 23:13:08,595 INFO     ftriage:     nxos:1404 bdsol-aci32-leaf3: nxos matching rule
id:4336 scope:34 filter:5
2019-10-02 23:13:09,608 INFO     ftriage:     main:522  Computed egress encap string vlan-2502
2019-10-02 23:13:09,609 INFO     ftriage:     main:313  Building egress BD(s), Ctx
2019-10-02 23:13:11,449 INFO     ftriage:     main:331  Egress Ctx Prod:VRF1
2019-10-02 23:13:11,449 INFO     ftriage:     main:332  Egress BD(s): Prod:BD2
2019-10-02 23:13:18,383 INFO     ftriage:     main:933  SIP 172.16.2.1 DIP 192.168.3.1
2019-10-02 23:13:18,384 INFO     ftriage:  unicast:973  bdsol-aci32-leaf3: <- is ingress node
2019-10-02 23:13:21,078 INFO     ftriage:  unicast:1202 bdsol-aci32-leaf3: Dst EP is local
2019-10-02 23:13:23,926 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: EP if(Po1) same as
egr if(Po1)
2019-10-02 23:13:25,216 INFO     ftriage:     misc:657  bdsol-aci32-leaf3:
DMAC(00:22:BD:F8:19:FF) same as RMAC(00:22:BD:F8:19:FF)
2019-10-02 23:13:25,217 INFO     ftriage:     misc:659  bdsol-aci32-leaf3: L3 packet getting
routed/bounced in SUG
2019-10-02 23:13:25,465 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: Dst IP is present in
SUG L3 tbl
2019-10-02 23:13:25,757 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: RW seg_id:11365 in
SUG same as EP segid:11365
2019-10-02 23:13:32,235 INFO     ftriage:     main:961  Packet is Exiting fabric with peer-
device: bdsol-aci32-n3k-3 and peer-port: Ethernet1/16
```

Questo flusso è consentito (come previsto) dalla regola di suddivisione in zone 4336.

Convalida di datapath tramite fTriage: flusso non consentito dai criteri

Eseguire Ftriage con un flusso ICMP da 172.16.2.1 (L3OUT-EPG2) a 192.168.1.1 (EPG1 — pcTag 32770):

```
admin@apic1:~> ftriage route -ii LEAF:103,104 -sip 172.16.2.1 -dip 192.168.1.1
fTriage Status: {"dbgFtriage": {"attributes": {"operState": "InProgress", "pid": "31500",
"apicId": "1", "id": "0"}}}
Starting ftriage
Log file name for the current run is: ftlog_2019-10-02-23-53-03-478.txt
2019-10-02 23:53:03,482 INFO     /controller/bin/ftriage route -ii LEAF:103,104 -sip 172.16.2.1
-dip 192.168.1.1
2019-10-02 23:53:50,014 INFO     ftriage:     main:1165 Invoking ftriage with default password
and default username: apic#fallback\\admin
2019-10-02 23:54:39,199 INFO     ftriage:     main:839  L3 packet Seen on bdsol-aci32-leaf3
Ingress: Eth1/12 (Po1) Egress: Eth1/12 (Po1) Vnid: 11364
2019-10-02 23:54:39,417 INFO     ftriage:     main:242  ingress encap string vlan-2551
2019-10-02 23:54:41,962 INFO     ftriage:     main:271  Building ingress BD(s), Ctx
2019-10-02 23:54:44,765 INFO     ftriage:     main:294  Ingress BD(s) Prod:VRF1:l3out-BGP:vlan-
2551
2019-10-02 23:54:44,766 INFO     ftriage:     main:301  Ingress Ctx: Prod:VRF1
2019-10-02 23:54:44,875 INFO     ftriage:   pktrec:490  bdsol-aci32-leaf3: Collecting transient
losses snapshot for LC module: 1
2019-10-02 23:55:02,905 INFO     ftriage:     nxos:1404 bdsol-aci32-leaf3: nxos matching rule
id:4341 scope:34 filter:5
2019-10-02 23:55:04,525 INFO     ftriage:     main:522  Computed egress encap string vlan-2501
2019-10-02 23:55:04,526 INFO     ftriage:     main:313  Building egress BD(s), Ctx
2019-10-02 23:55:06,390 INFO     ftriage:     main:331  Egress Ctx Prod:VRF1
2019-10-02 23:55:06,390 INFO     ftriage:     main:332  Egress BD(s): Prod:BD1
2019-10-02 23:55:13,571 INFO     ftriage:     main:933  SIP 172.16.2.1 DIP 192.168.1.1
2019-10-02 23:55:13,572 INFO     ftriage:  unicast:973  bdsol-aci32-leaf3: <- is ingress node
2019-10-02 23:55:16,159 INFO     ftriage:  unicast:1202 bdsol-aci32-leaf3: Dst EP is local
2019-10-02 23:55:18,949 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: EP if(Po1) same as
egr if(Po1)
2019-10-02 23:55:20,126 INFO     ftriage:     misc:657  bdsol-aci32-leaf3:
DMAC(00:22:BD:F8:19:FF) same as RMAC(00:22:BD:F8:19:FF)
2019-10-02 23:55:20,126 INFO     ftriage:     misc:659  bdsol-aci32-leaf3: L3 packet getting
routed/bounced in SUG
2019-10-02 23:55:20,395 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: Dst IP is present in
SUG L3 tbl
2019-10-02 23:55:20,687 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: RW seg_id:11364 in
SUG same as EP segid:11364
2019-10-02 23:55:26,982 INFO     ftriage:     main:961  Packet is Exiting fabric with peer-
device: bdsol-aci32-n3k-3 and peer-port: Ethernet1/16
```

Questo flusso è consentito (imprevisto) dalla regola di suddivisione in zone 4341. Le regole di zoning devono essere analizzate per capirne il motivo.

Convalida datapath: regole di zoning

Le regole di zonizzazione corrispondenti alle ultime due prove sono le seguenti:

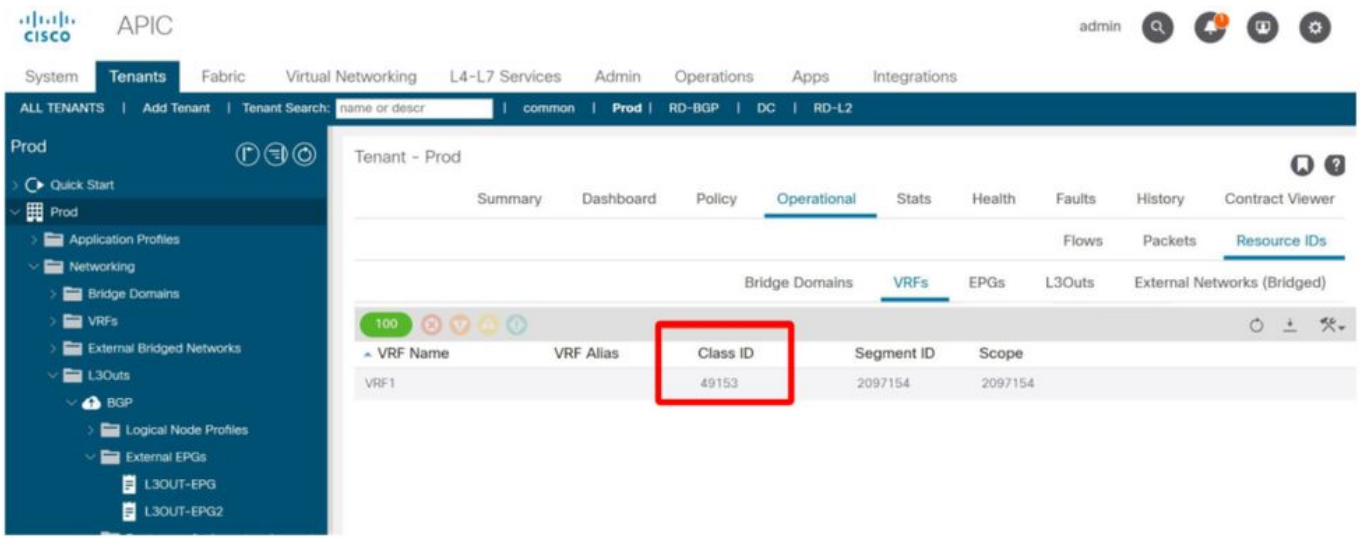
- Previsto — il flusso raggiunge la riga 4336 della regola di zoning (contratto ICMP2).
- Imprevisto: il flusso colpisce la riga 4341 della regola di zoning (contratto ICMP1).

```
+---------+--------+--------+----------+---------+---------+---------+-------+----------+-------
---------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |  Name |  Action  |
Priority       |
```

```
+---------+--------+--------+----------+---------+---------+---------+-------+----------+-------
---------------+
|   4326  |   0    |   0    | implicit | uni-dir | enabled | 2097154 |       | deny,log |
any_any_any(21)    |
|   4335  |   0    | 16387  | implicit | uni-dir | enabled | 2097154 |       |  permit  |
any_dest_any(16)   |
|   4334  |   0    |   0    | implarp  | uni-dir | enabled | 2097154 |       |  permit  |
any_any_filter(17)  |
|   4333  |   0    |   15   | implicit | uni-dir | enabled | 2097154 |       | deny,log |
any_vrf_any_deny(22) |
|   4332  |   0    | 16386  | implicit | uni-dir | enabled | 2097154 |       |  permit  |
any_dest_any(16)   |
|   4339  | 32770  |   15   |    5     | uni-dir | enabled | 2097154 | ICMP2 |  permit  |
fully_qual(7)      |
|   4341  | 49153  | 32770  |    5     | uni-dir | enabled | 2097154 | ICMP2 |  permit  |
fully_qual(7)      |
|   4337  | 32771  |   15   |    5     | uni-dir | enabled | 2097154 | ICMP1 |  permit  |
fully_qual(7)      |
|   4336  | 49153  | 32771  |    5     | uni-dir | enabled | 2097154 | ICMP1 |  permit  |
fully_qual(7)      |
+---------+--------+--------+----------+---------+---------+---------+-------+----------+-------
---------------+
```

Entrambi i flussi derivano il valore src pcTag di 49153. Si tratta del valore pcTag del VRF. È possibile verificare questa condizione nell'interfaccia utente:

Verifica del pcTag del VRF



Quanto segue si verifica quando il prefisso 0.0.0.0/0 è in uso con un'uscita L3:

- Il traffico da un EPG interno a un EPG L3Out con 0.0.0.0/0 produrrà un pcTag di destinazione di 15.
- Il traffico da un EPG L3Out con 0.0.0.0/0 a un EPG interno ACI deriva un pcTag di origine del VRF (49153).

Lo script contract_parser fornisce una vista olistica delle regole di zoning:

```
bdsol-aci32-leaf3# contract_parser.py --vrf Prod:VRF1
Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4]
[flags][contract:{str}] [hit=count]
```

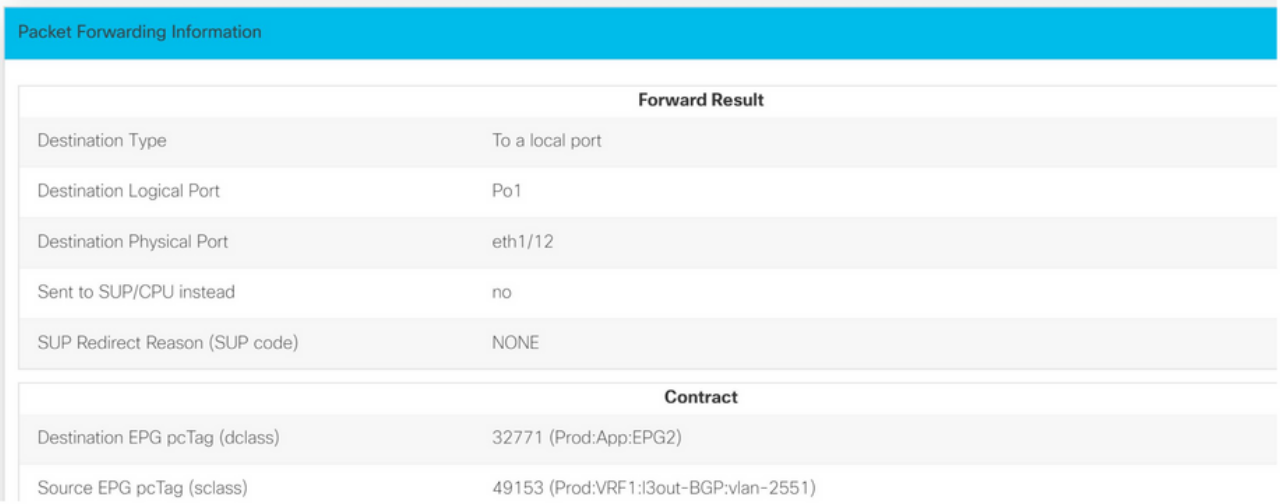
```
[7:4339] [vrf:Prod:VRF1] permit ip icmp tn-Prod/ap-App/epg-EPG1(32770) pfx-0.0.0.0/0(15)
[contract:uni/tn-Prod/brc-ICMP2] [hit=0]
[7:4337] [vrf:Prod:VRF1] permit ip icmp tn-Prod/ap-App/epg-EPG2(32771) pfx-0.0.0.0/0(15)
[contract:uni/tn-Prod/brc-ICMP] [hit=0]
[7:4341] [vrf:Prod:VRF1] permit ip icmp tn-Prod/vrf-VRF1(49153) tn-Prod/ap-App/epg-EPG1(32770)
[contract:uni/tn-Prod/brc-ICMP2] [hit=270]
[7:4336] [vrf:Prod:VRF1] permit ip icmp tn-Prod/vrf-VRF1(49153) tn-Prod/ap-App/epg-EPG2(32771)
[contract:uni/tn-Prod/brc-ICMP] [hit=0]
```

Conferma di pcTag utilizzato dal pacchetto tramite l'app ELAM Assistant

L'applicazione ELAM Assistant fornisce un altro metodo per confermare il pcTag di origine e di destinazione dei flussi di traffico in tempo reale.

La schermata seguente mostra il risultato ELAM per il traffico da pcTag 32771 a pcTag 49153.

Output dell'applicazione ELAM Assistant per src 3271 su dst 49153



Conclusioni

L'utilizzo di 0.0.0.0/0 deve essere attentamente monitorato all'interno di un VRF in quanto ogni L3Out che utilizza tale subnet erediterà i contratti applicati a ogni L3Out che lo utilizza. Ciò comporterà probabilmente flussi di autorizzazioni non pianificati.

L3Out condiviso

Panoramica

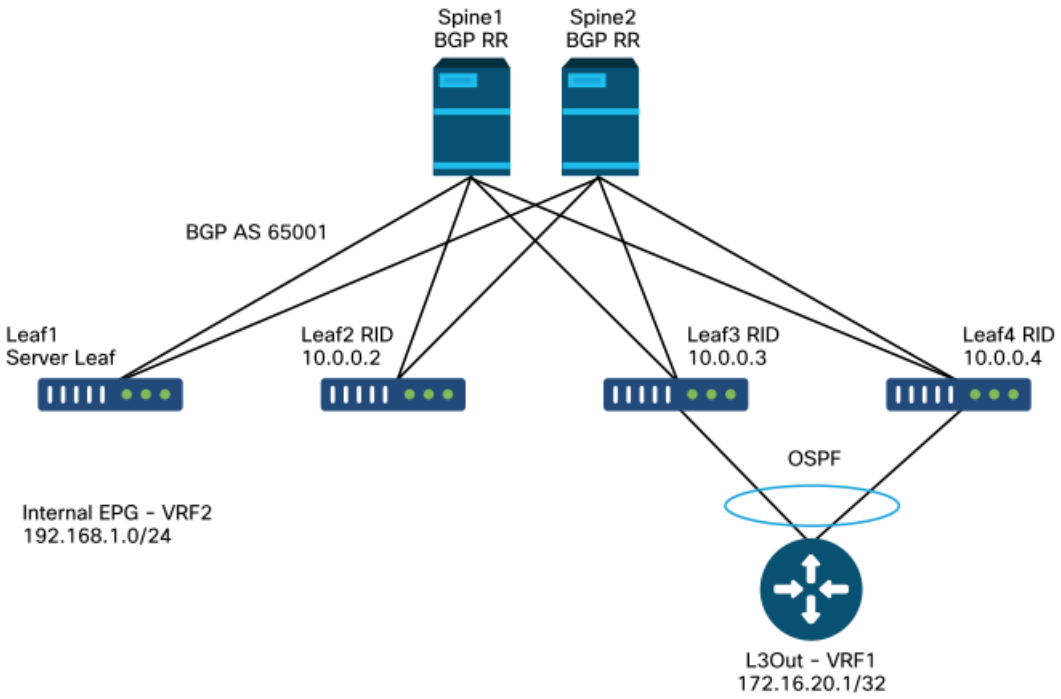
In questa sezione verrà descritto come risolvere i problemi relativi agli annunci route nelle configurazioni L3Out condivise. Il termine 'Shared L3Out' si riferisce allo scenario in cui un L3Out si trova in un VRF ma un EPG interno che ha un contratto con l'L3Out si trova in un altro VRF. Con Shared L3Outs, la route-leaking viene eseguita internamente al fabric ACI.

In questa sezione non verranno fornite informazioni dettagliate sulla risoluzione dei problemi relativi ai criteri di protezione. Per questo consultare il capitolo "Politiche di sicurezza" di questo libro. In questa sezione non verranno inoltre fornite informazioni dettagliate sulla classificazione del prefisso dei criteri esterni per motivi di sicurezza. Fare riferimento alla sezione "Contratto e

L3Out" del capitolo "inoltro esterno".

In questa sezione viene utilizzata la topologia seguente per gli esempi.

Topologia L3Out condivisa



Ad alto livello, affinché un'istruzione L3Out condivisa funzioni, è necessario che siano disponibili le seguenti configurazioni:

- Una subnet L3Out deve essere configurata con l'ambito 'Subnet di controllo route condivisa' per la perdita di route esterne nei VRF interni. È inoltre possibile selezionare l'opzione 'Aggregate Shared' per eseguire la perdita di tutte le route più specifiche della subnet configurata.
- Una subnet L3Out deve essere configurata con l'ambito 'Subnet importazione protezione condivisa' per programmare i criteri di protezione necessari per consentire la comunicazione tramite questo L3Out.
- La subnet BD interna deve essere impostata su 'Condivisa tra VRF' e su 'Pubblicizza esternamente' per programmare la subnet BD nel VRF esterno e pubblicizzarla.
- Ènecessario configurare un contratto con ambito 'tenant' o 'global' tra l'EPG interno e l'EPG esterno dell'L3Out condiviso.

Nella sezione successiva verranno forniti dettagli su come vengono pubblicizzate e apprese le route perse in ACI.

Flusso di lavoro L3Out condiviso — apprendimento di percorsi esterni

In questa sezione viene descritto il percorso di un percorso esterno appreso nel momento in cui

viene annunciato nel fabric.

Percorso esterno visto sul bordo

Questo comando visualizza la route esterna appresa da OSPF:

```
leaf103# show ip route 172.16.20.1/32 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

172.16.20.1/32, ubest/mbest: 1/0
    *via 10.10.34.3, vlan347, [110/20], 03:59:59, ospf-default, type-2
```

Successivamente, la route deve essere importata in BGP. Per impostazione predefinita, tutte le route esterne devono essere importate in BGP.

Verifiche BGP a bordo

La route deve essere inclusa nella famiglia di indirizzi BGP VPNv4 con una route-target da distribuire in tutta la struttura. La route-target è una community estesa BGP esportata dal VRF esterno e importata da qualsiasi VRF interno che deve ricevere il percorso.

Verificare quindi la route-target esportata dal VRF esterno sul BL.

```
leaf103# show bgp process vrf Prod:Vrf1

Information regarding configured VRFs:

BGP Information for VRF Prod:Vrf1
VRF Type                        : System
VRF Id                          : 85
VRF state                       : UP
VRF configured                  : yes
VRF refcount                    : 1
VRF VNID                        : 2392068
Router-ID                       : 10.0.0.3
Configured Router-ID            : 10.0.0.3
Confed-ID                       : 0
Cluster-ID                      : 0.0.0.0
MSITE Cluster-ID                : 0.0.0.0
No. of configured peers         : 1
No. of pending config peers     : 0
No. of established peers        : 0
VRF RD                          : 101:2392068
VRF EVPN RD                     : 101:2392068

...

    Wait for IGP convergence is not configured
    Export RT list:
        65001:2392068
    Import RT list:
        65001:2392068
```

```
    Label mode: per-prefix
```

L'output sopra riportato mostra che tutti i percorsi pubblicizzati dal VRF esterno in VPNv4 devono ricevere una route-target di 65001:2392068.

Quindi, verificare il percorso bgp:

```
leaf103# show bgp ipv4 unicast 172.16.20.1/32 vrf Prod:Vrf1
BGP routing table information for VRF Prod:Vrf1, address family IPv4 Unicast
BGP routing table entry for 172.16.20.1/32, version 30 dest ptr 0xa6f25ad0
Paths: (2 available, best #1)
Flags: (0x80c0002 00000000) on xmit-list, is not in urib, exported
  vpn: version 17206, (0x100002) on xmit-list
Multipath: eBGP iBGP

  Advertised path-id 1, VPN AF advertised path-id 1
  Path type: redist 0x408 0x1 ref 0 adv path ref 2, path is valid, is best path
  AS-Path: NONE, path locally originated
    0.0.0.0 (metric 0) from 0.0.0.0 (10.0.0.3)
      Origin incomplete, MED 20, localpref 100, weight 32768
      Extcommunity:
          RT:65001:2392068
          VNID:2392068
          COST:pre-bestpath:162:110

  VRF advertise information:
  Path-id 1 not advertised to any peer

  VPN AF advertise information:
  Path-id 1 advertised to peers:
    10.0.64.64         10.0.72.66
  Path-id 2 not advertised to any peer
```

L'output precedente mostra che il percorso ha la route-target corretta. Il percorso VPNv4 può essere verificato anche con il comando 'show bgp vpnv4 unicast 172.16.20.1 vrf overlay-1'.

Verifiche nella foglia del server

Affinché la foglia EPG interna possa installare il percorso pubblicizzato da BL, deve importare il percorso di destinazione (indicato sopra) nel VRF interno. È possibile controllare il processo BGP del VRF interno per verificare quanto segue:

```
leaf101# show bgp process vrf Prod:Vrf2

Information regarding configured VRFs:

BGP Information for VRF Prod:Vrf2
VRF Type                        : System
VRF Id                          : 54
VRF state                       : UP
VRF configured                  : yes
VRF refcount                    : 0
VRF VNID                        : 2916352
Router-ID                       : 192.168.1.1
Configured Router-ID            : 0.0.0.0
Confed-ID                       : 0
Cluster-ID                      : 0.0.0.0
```

```
MSITE Cluster-ID               : 0.0.0.0
No. of configured peers        : 0
No. of pending config peers    : 0
No. of established peers       : 0
VRF RD                         : 102:2916352
VRF EVPN RD                    : 102:2916352
...
    Wait for IGP convergence is not configured
    Import route-map 2916352-shared-svc-leak
    Export RT list:
        65001:2916352
    Import RT list:
        65001:2392068
        65001:2916352
```

L'output precedente mostra il VRF interno che importa il router-destinazione esportato dal VRF esterno. È inoltre presente un riferimento a 'Import Route-Map'. La route-map di importazione include i prefissi specifici definiti nell'output L3U condiviso con il flag 'Shared Route Control Subnet'.

Èpossibile controllare il contenuto della route-map per verificare che includa il prefisso esterno:

```
leaf101# show route-map 2916352-shared-svc-leak
route-map 2916352-shared-svc-leak, deny, sequence 1
 Match clauses:
   pervasive: 2
 Set clauses:
route-map 2916352-shared-svc-leak, permit, sequence 2
 Match clauses:
   extcommunity  (extcommunity-list filter): 2916352-shared-svc-leak
 Set clauses:
route-map 2916352-shared-svc-leak, permit, sequence 1000
 Match clauses:
   ip address prefix-lists: IPv4-2392068-16387-5511-2916352-shared-svc-leak
   ipv6 address prefix-lists: IPv6-deny-all
 Set clauses:
a-leaf101# show ip prefix-list IPv4-2392068-16387-5511-2916352-shared-svc-leak
ip prefix-list IPv4-2392068-16387-5511-2916352-shared-svc-leak: 1 entries
  seq 1 permit 172.16.20.1/32
```

L'output precedente mostra la route-map di importazione che include la subnet da importare.

Le verifiche finali includono il controllo che la route sia inclusa nella tabella BGP e che sia installata nella tabella di routing.

Tabella BGP su foglia server:

```
leaf101# show bgp ipv4 unicast 172.16.20.1/32 vrf Prod:Vrf2
BGP routing table information for VRF Prod:Vrf2, address family IPv4 Unicast
BGP routing table entry for 172.16.20.1/32, version 3 dest ptr 0xa763add0
Paths: (2 available, best #1)
Flags: (0x08001a 00000000) on xmit-list, is in urib, is best urib route, is in HW
  vpn: version 10987, (0x100002) on xmit-list
Multipath: eBGP iBGP

  Advertised path-id 1, VPN AF advertised path-id 1
  Path type: internal 0xc0000018 0x40 ref 56506 adv path ref 2, path is valid, is best path
             Imported from 10.0.72.64:5:172.16.20.1/32
```

```
  AS-Path: NONE, path sourced internal to AS
    10.0.72.64 (metric 3) from 10.0.64.64 (192.168.1.102)
      Origin incomplete, MED 20, localpref 100, weight 0
      Received label 0
      Received path-id 1
      Extcommunity:
          RT:65001:2392068
          VNID:2392068
          COST:pre-bestpath:162:110
      Originator: 10.0.72.64 Cluster list: 192.168.1.102
```

La route viene importata nella tabella BGP VRF interna e ha la destinazione prevista.

Èpossibile verificare le route installate:

```
leaf101# vsh -c "show ip route 172.16.20.1/32 detail vrf Prod:Vrf2"
IP Route Table for VRF "Prod:Vrf2"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF
172.16.20.1/32, ubest/mbest: 2/0
   *via 10.0.72.64%overlay-1, [200/20], 01:00:51, bgp-65001, internal, tag 65001 (mpls-vpn)
        MPLS[0]: Label=0 E=0 TTL=0 S=0 (VPN)
        client-specific data: 548
        recursive next hop: 10.0.72.64/32%overlay-1
        extended route information: BGP origin AS 65001 BGP peer AS 65001 rw-vnid: 0x248004
table-id: 0x36 rw-mac: 0
   *via 10.0.72.67%overlay-1, [200/20], 01:00:51, bgp-65001, internal, tag 65001 (mpls-vpn)
        MPLS[0]: Label=0 E=0 TTL=0 S=0 (VPN)
        client-specific data: 54a
        recursive next hop: 10.0.72.67/32%overlay-1
        extended route information: BGP origin AS 65001 BGP peer AS 65001 rw-vnid: 0x248004
table-id: 0x36 rw-mac: 0
```

Nell'output precedente viene utilizzato un comando 'vsh -c' specifico per ottenere l'output 'detail'. Il flag 'detail' include il VXLAN VNID di riscrittura. VXLAN VNID del VRF esterno. Quando la BL riceve il traffico della corsia dati con questo VNID, sa di prendere la decisione di inoltro nel VRF esterno.

Il valore rw-vnid è in formato esadecimale, pertanto la conversione in decimale restituirà il VRF VNID di 2392068. Cercare il VRF corrispondente utilizzando 'show system internal epm vrf all' | 2392068 grep". È possibile eseguire una ricerca globale in un file APIC utilizzando il comando 'moquery -c fvCtx -f 'fv.Ctx.seg="2392068"'.

Anche l'IP dell'hop successivo deve puntare ai PTEP BL e '%overlay-1' indica che la ricerca della route per l'hop successivo è nel VRF di overlay.

Flusso di lavoro L3Out condiviso: annuncio di route interne

Come nelle sezioni precedenti, la pubblicità delle subnet BD interne in un'uscita L3 condivisa viene gestita come segue:

- La subnet BD (VRF interna) viene installata sul BL (VRF esterna) come percorso statico. Questa distribuzione di route statica è il risultato della relazione contrattuale tra EPG interno e L3Out.

- La route statica viene ridistribuita nel protocollo esterno quando l'ambito 'Annunciato esternamente' è impostato nella subnet BD.

Verificare il percorso statico BD sul BL

```
leaf103# vsh -c "show ip route 192.168.1.0 detail vrf Prod:Vrf1"
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

192.168.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.120.34%overlay-1, [1/0], 00:55:27, static, tag 4294967292
         recursive next hop: 10.0.120.34/32%overlay-1
         vrf crossing information:  VNID:0x2c8000 ClassId:0 Flush#:0
```

Si noti che nell'output precedente il VNID del VRF interno è impostato per la riscrittura. L'hop successivo viene impostato anche sull'indirizzo proxy-v4-anycast.

Il percorso sopra indicato viene pubblicizzato esternamente tramite le stesse route-map illustrate nella sezione "Annuncio route".

Se una subnet BD è impostata su 'Pubblicizza esternamente', viene ridistribuita nel **protocollo esterno di ogni L3Out** con cui l'EPG interno ha una relazione contrattuale.

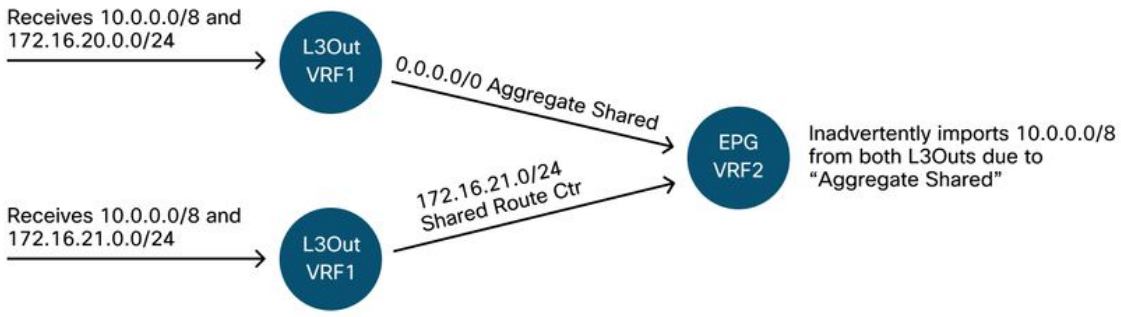
Scenario di risoluzione dei problemi L3Out condivisi — Perdita di route imprevista

In questo scenario sono presenti più L3Out nel VRF esterno e un EPG interno riceve un percorso da un L3Out in cui la rete **non è** definita con le opzioni di ambito 'condiviso'.

Utilizzo di 'Aggregate Shared'

Considerate la figura riportata di seguito.

Perdita di route imprevista



La mappa di importazione BGP con l'elenco dei prefissi programmato dai flag **'Shared Route Control Subnet'** viene applicata a livello VRF. Se un'uscita L3in VRF1 ha una subnet con 'Subnet di controllo della route condivisa', tutte le route ricevute su L3Out in VRF1 che corrispondono a

questa subnet di controllo della route condivisa verranno importate in VRF2.

La progettazione di cui sopra può generare flussi di traffico imprevisti. Se non ci sono contratti tra l'EPG interno e la pubblicità inaspettata L3Out EPG, allora ci saranno riduzioni del traffico.

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).