Resolución de problemas de reenvío externo ACI

Contenido

[Pérdida de ruta inesperada]

Introducción

Este documento describe los pasos para comprender y resolver problemas de una L3out en ACI

Antecedentes

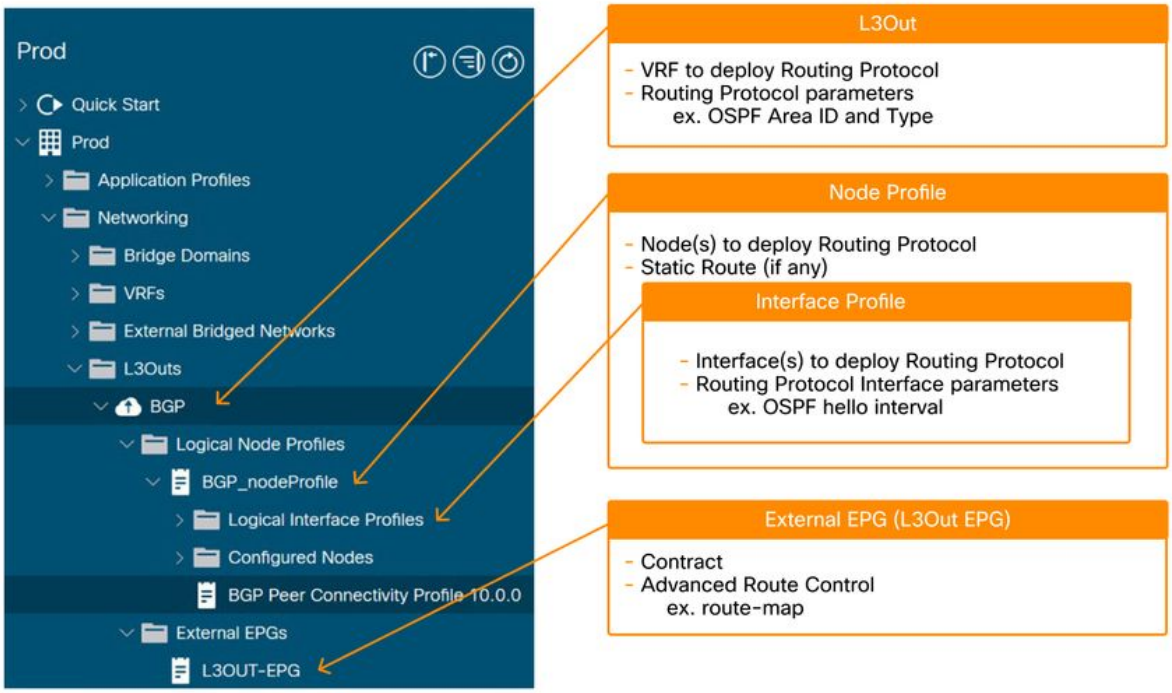
El material de este documento se extrajo del libro Troubleshooting Cisco Application Centric Infrastructure, Second Edition específicamente los capítulos **External Forwarding** - Overview, External Forwarding - Adjacencies, External Forwarding - Route advertisement, External Forwarding - Contract y L3out y **External Forwarding - Share L3out**.

Overview

Componentes L3Out

La siguiente imagen ilustra los principales bloques de creación necesarios para configurar una salida L3 externa (L3Out).

Componentes principales de una salida L3



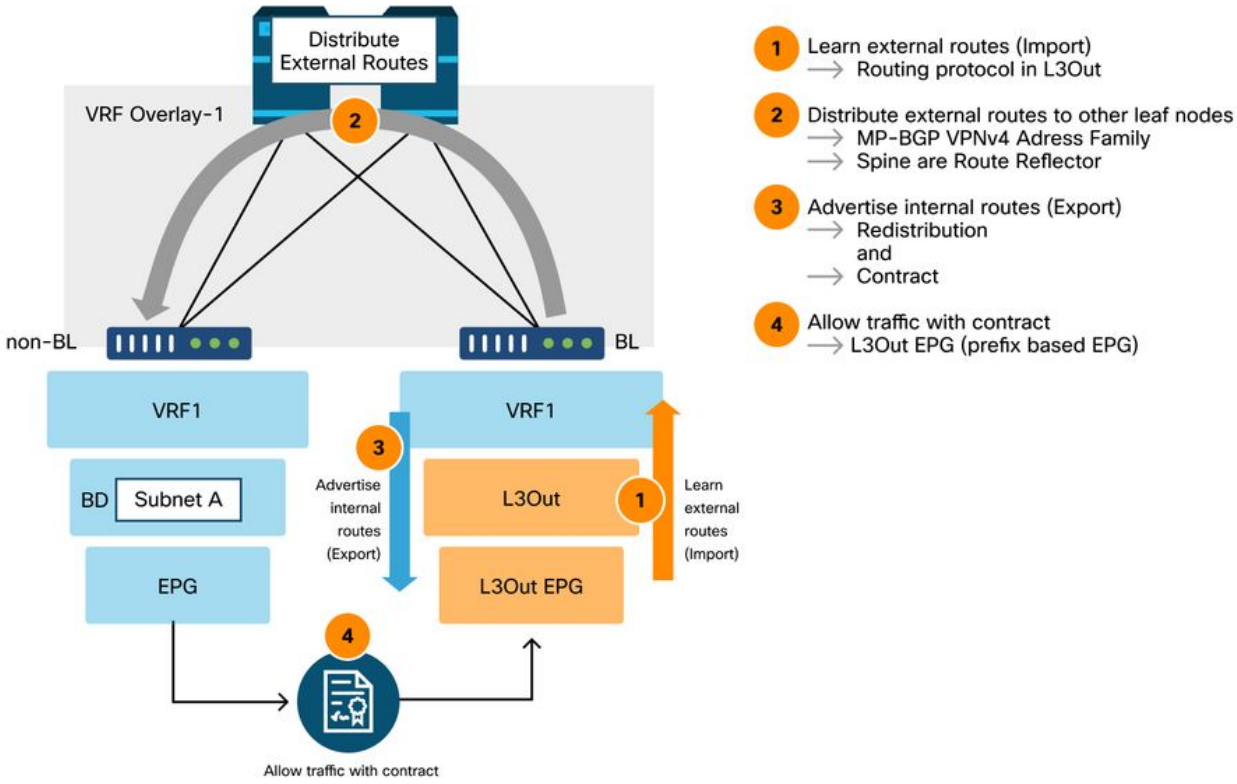
1. Raíz de L3Out: Seleccione un protocolo de routing para implementar (como OSPF o BGP).Seleccione un VRF para implementar el protocolo de routing.Seleccione un dominio L3Out para definir las interfaces de hoja disponibles y la VLAN para L3Out.
2. Perfil de nodo: Seleccione los switches de hoja para implementar el protocolo de routing. Estos se conocen normalmente como "switches de hoja de frontera" (BL).Configure el Router-ID (RID) para el protocolo de ruteo en cada hoja de borde. A diferencia de un router

normal, ACI no asigna automáticamente un ID de router basándose en una dirección IP del switch.Configure una ruta estática.
3. Perfil de interfaz: Configure las interfaces de hoja para ejecutar el protocolo de ruteo. es decir, tipo de interfaz (SVI, puerto enrutado, subinterfaz), ID de interfaz y direcciones IP, etc.Seleccione una política para los parámetros del protocolo de ruteo de nivel de interfaz (como el intervalo hello).
4. EPG externo (L3Out EPG): Un 'EPG externo' es un requisito obligatorio para implementar todas las políticas vinculadas a la salida L3, como direcciones IP o SVI para establecer vecinos. Más adelante se explicará cómo utilizar los EPG externos.

Routing externo

El siguiente diagrama muestra la operación de alto nivel involucrada para el ruteo externo.

Flujo de routing externo de alto nivel

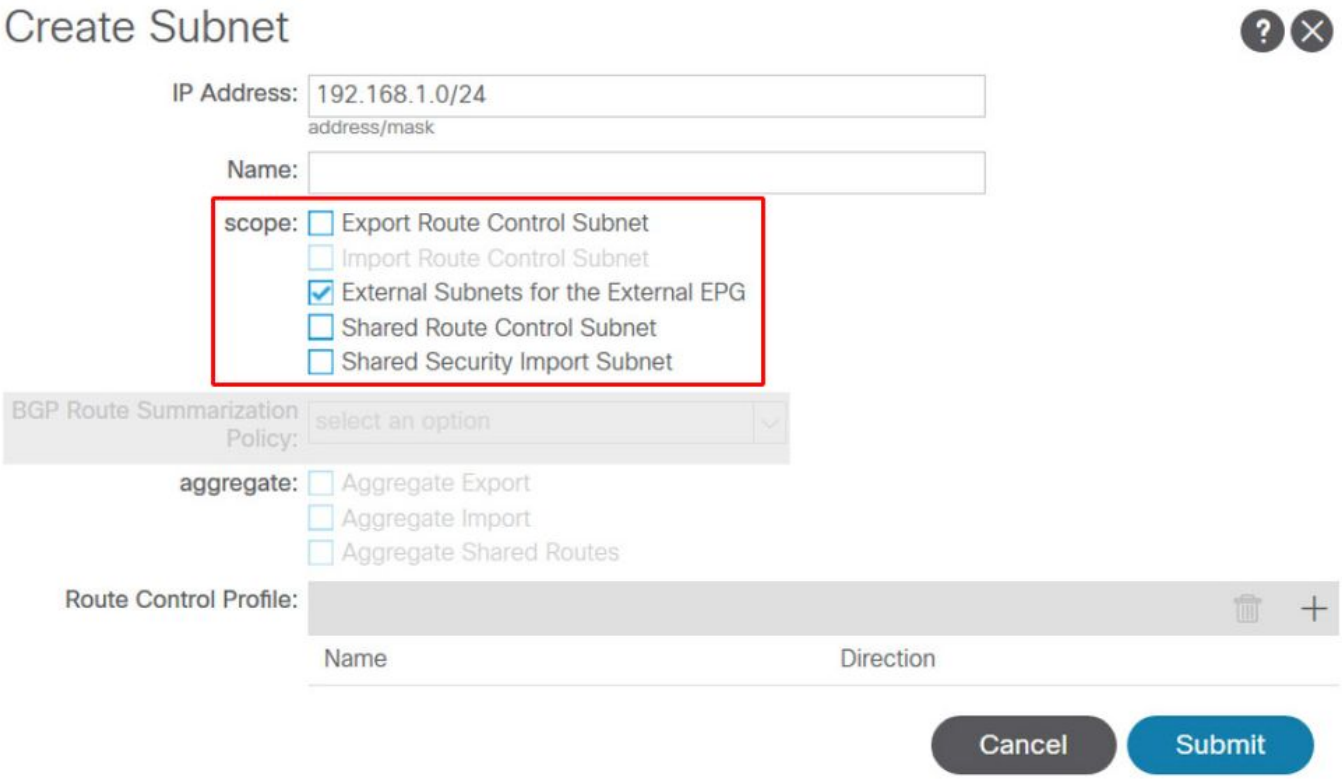


1. Las BL establecerán adyacencias de protocolo de ruteo con routers externos.
2. Los prefijos de ruta se reciben de los routers externos y se insertan en MP-BGP como la trayectoria de la familia de direcciones VPNv4. Como mínimo, se deben configurar dos nodos de columna como reflectores de ruta BGP para reflejar las rutas externas a todos los nodos de hoja.
3. Los prefijos internos (subredes BD) y/o los prefijos recibidos de otro L3Out deben ser explícitamente redistribuidos en el protocolo de ruteo para ser anunciados al router externo.
4. Aplicación de seguridad: un L3Out contiene al menos un EPG L3Out. Se debe consumir o proporcionar un contrato en el EPG L3Out (también denominado l3extInstP desde el nombre de clase) para permitir el tráfico entrante/saliente del L3Out.

Opciones de configuración de L3Out EPG

En la sección L3Out EPG, las subredes se pueden definir con una serie de opciones 'Scope' y 'Aggregate' como se ilustra a continuación:

Una subred L3Out que se está definiendo, incluida la definición de 'ámbito'



Opciones 'Scope':

- **Exportar subred de control de rutas:** este ámbito sirve para anunciar (exportar) una subred de ACI al exterior a través de L3Out. Aunque esto es principalmente para el ruteo de tránsito, también se podría utilizar para anunciar una subred de BD como se describe en la sección "Anuncio de subred de BD de ACI".
- **Importar subred de control de rutas:** Este ámbito trata sobre aprender (importar) una subred externa de L3Out. De forma predeterminada, este ámbito está deshabilitado, por lo que aparece atenuado y una hoja de borde (BL) detecta las rutas de un protocolo de routing. Este alcance se puede habilitar cuando necesita limitar las rutas externas aprendidas a través de OSPF y BGP. Esto no es compatible con EIGRP. Para utilizar este ámbito, 'Importar aplicación de control de ruta' debe estar habilitado primero en una salida L3 dada.
- **Subredes externas para el EPG externo (import-security):** Este alcance se utiliza para permitir paquetes con la subred configurada desde o hacia L3Out con un contrato. Clasifica un paquete en el EPG L3Out configurado basado en la subred para que se pueda aplicar al paquete un contrato en el EPG L3Out. Este ámbito es una coincidencia de prefijo más larga en lugar de una coincidencia exacta como otros ámbitos para la tabla de enrutamiento. Si 10.0.0.0/16 se configura con 'Subredes externas para el EPG externo' en L3Out EPG A, cualquier paquete con IP en esa subred, como 10.0.1.1, se clasificará en L3Out EPG A para utilizar un contrato en él. Esto no significa que el alcance 'Subredes externas para el EPG externo' instale una ruta 10.0.0.0/16 en una tabla de ruteo. Creará una tabla interna diferente

para asignar una subred a un EPG (pcTag) exclusivamente para un contrato. No tiene ningún efecto en los comportamientos del protocolo de ruteo. Este alcance debe configurarse en una L3Out que esté aprendiendo la subred.
- **Subred de control de ruta compartida:** este ámbito es filtrar una subred externa a otro VRF. ACI utiliza MP-BGP y Route Target para filtrar una ruta externa de un VRF a otro. Este ámbito crea una lista de prefijos con la subred, que se utiliza como filtro para exportar/importar rutas con destino de ruta en MP-BGP. Este alcance se debe configurar en un L3Out que esté aprendiendo la subred en el VRF original.
- **Subred de importación de seguridad compartida:** este ámbito se utiliza para permitir paquetes con la subred configurada cuando los paquetes se mueven a través de VRF con una salida L3. Una ruta en una tabla de ruteo se filtra a otro VRF con 'Subred de control de ruta compartida' como se mencionó anteriormente. Sin embargo, otro VRF aún no sabe a qué EPG debe pertenecer la ruta filtrada. La 'Subred de importación de seguridad compartida' informa a otro VRF del EPG L3Out al que pertenece la ruta filtrada. Por lo tanto, este alcance se puede utilizar solamente cuando también se utiliza 'Subredes Externas para el EPG Externo'; de lo contrario, el VRF original no sabe a cuál EPG L3Out pertenece la subred. Este ámbito es también la coincidencia de prefijo más larga.

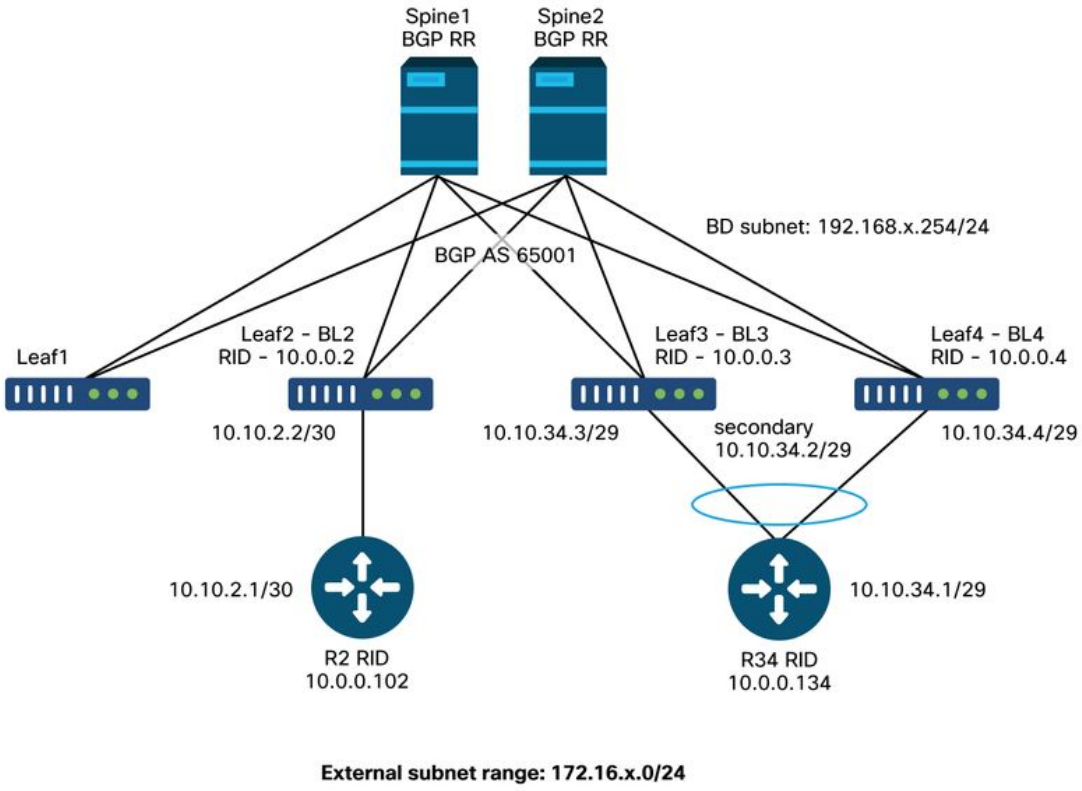
Opciones 'Aggregate':

- **Exportación Agregada:** Esta opción sólo se puede utilizar para 0.0.0.0/0 con 'Exportar subred de control de ruta'. Cuando 'Export Route Control Subnet' y 'Aggregate Export' están habilitados para 0.0.0.0/0; crea una lista de prefijos con '0.0.0.0/0 le 32' que coincide con cualquier subred. Por lo tanto, esta opción se puede utilizar cuando un L3Out necesita anunciar (exportar) cualquier ruta hacia el exterior. Cuando se requiere una agregación más granular, se puede utilizar Route Map/Profile con una lista de prefijos explícita.
- **Importación Agregada:** Esta opción sólo se puede utilizar para 0.0.0.0/0 con 'Importar Subred de Control de Ruta'. Cuando 'Import Route Control Subnet' y 'Aggregate Import' están habilitados para 0.0.0.0/0, crea una lista de prefijos con '0.0.0.0/0 le 32' que coincide con cualquier subred. Por lo tanto, esta opción se puede utilizar cuando un L3Out necesita aprender (importar) cualquier ruta desde el exterior. Sin embargo, lo mismo se puede lograr al inhabilitar 'Importar aplicación de control de ruta' que es el valor predeterminado. Cuando se requiere una agregación más granular, se puede utilizar Route Map/Profile con una lista de prefijos explícita.
- **Rutas compartidas agregadas:** Esta opción se puede utilizar para cualquier subred con 'Subred de control de rutas compartidas'. Cuando se habilitan 'Subred de control de ruta compartida' y 'Rutas compartidas agregadas' para 10.0.0.0/8 como ejemplo, se crea una lista de prefijos con '10.0.0.0/8 le 32' que coincide con 10.0.0.0/8, 10.1.0.0/16 y así sucesivamente.

Topología L3Out utilizada en esta sección

En esta sección se utilizará la siguiente topología:

Topología L3Out



Adyacencias

Esta sección explica cómo resolver problemas y verificar las adyacencias del protocolo de ruteo en las interfaces L3Out.

A continuación se muestran algunos parámetros para verificar que serán aplicables para todos los protocolos de ruteo externos de ACI:

- **ID de router:** En ACI, cada L3Out necesita utilizar el mismo ID de router en el mismo VRF en la misma hoja, incluso si los protocolos de routing son diferentes. Además, solamente una de esas L3Outs en la misma hoja puede crear un loopback con el ID del router, que es típicamente BGP.
- **MTU:** Aunque el requisito de hardware de MTU es solo para la adyacencia OSPF, se recomienda que coincida con la MTU para cualquier protocolo de ruteo para garantizar que cualquier paquete jumbo utilizado para el intercambio de rutas/actualizaciones se pueda transmitir sin fragmentación, ya que la mayoría de las tramas del plano de control se enviarán con el bit DF (no fragmentar) configurado, que descartará la trama si su tamaño excede la MTU máxima de la interfaz.
- **Reflector de Router MP-BGP:** Sin esto, el proceso BGP no se iniciará en los nodos de hoja. Aunque esto no es necesario para OSPF o EIGRP sólo para establecer un vecino, sigue siendo necesario para que las BL distribuyan rutas externas a otros nodos de hoja.
- **Fallos:** asegúrese siempre de comprobar los fallos durante y después de que se complete la configuración.

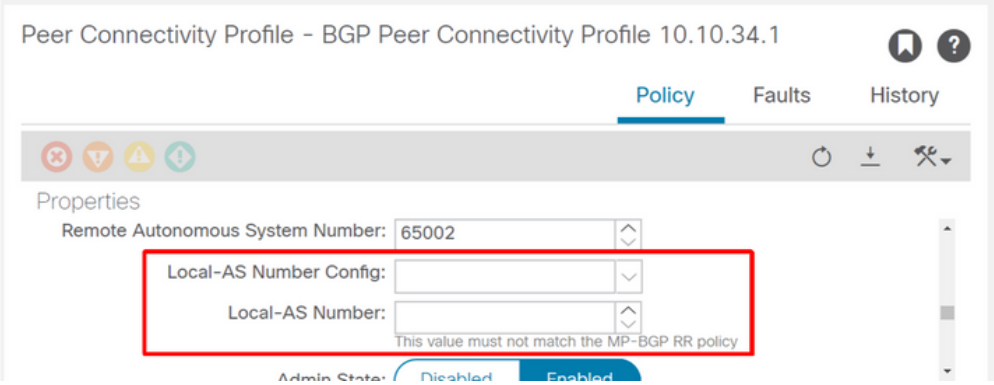
BGP

Esta sección utiliza un ejemplo de un peering eBGP entre el loopback en BL3, BL4 y R34 desde la topología en la sección de descripción general. El AS BGP en R34 es 65002.

Verifique los siguientes criterios al establecer una adyacencia BGP.

- Número AS de BGP local (lado BL de ACI).

Perfil de Conectividad de Peer: Local-AS

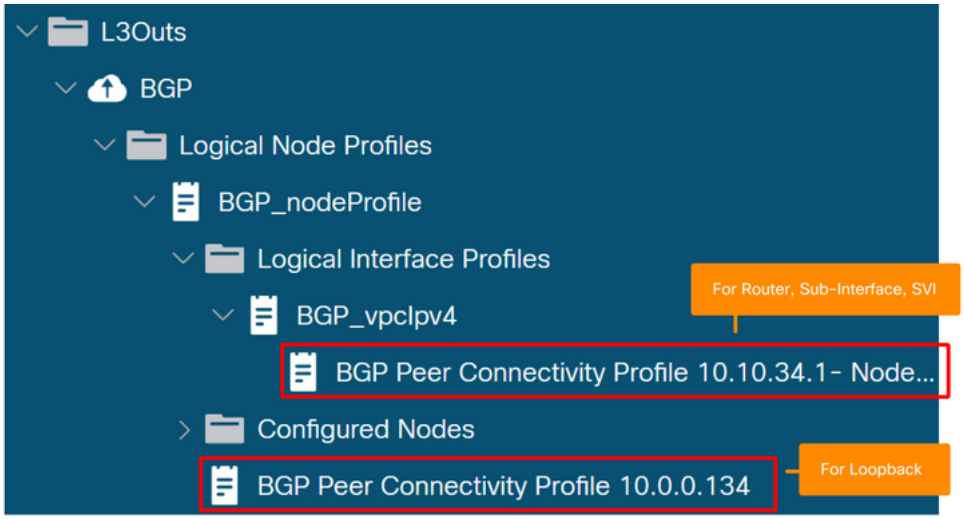


El número AS BGP de un usuario L3Out será automáticamente el mismo que el AS BGP para el infra-MP-BGP configurado en la política BGP Route Reflector. La configuración 'Local AS' en el perfil de conectividad de par BGP no es necesaria a menos que uno necesite disfrazar el AS BGP ACI al mundo exterior. Esto significa que los routers externos deben apuntar al AS BGP configurado en el reflector de ruta BGP.

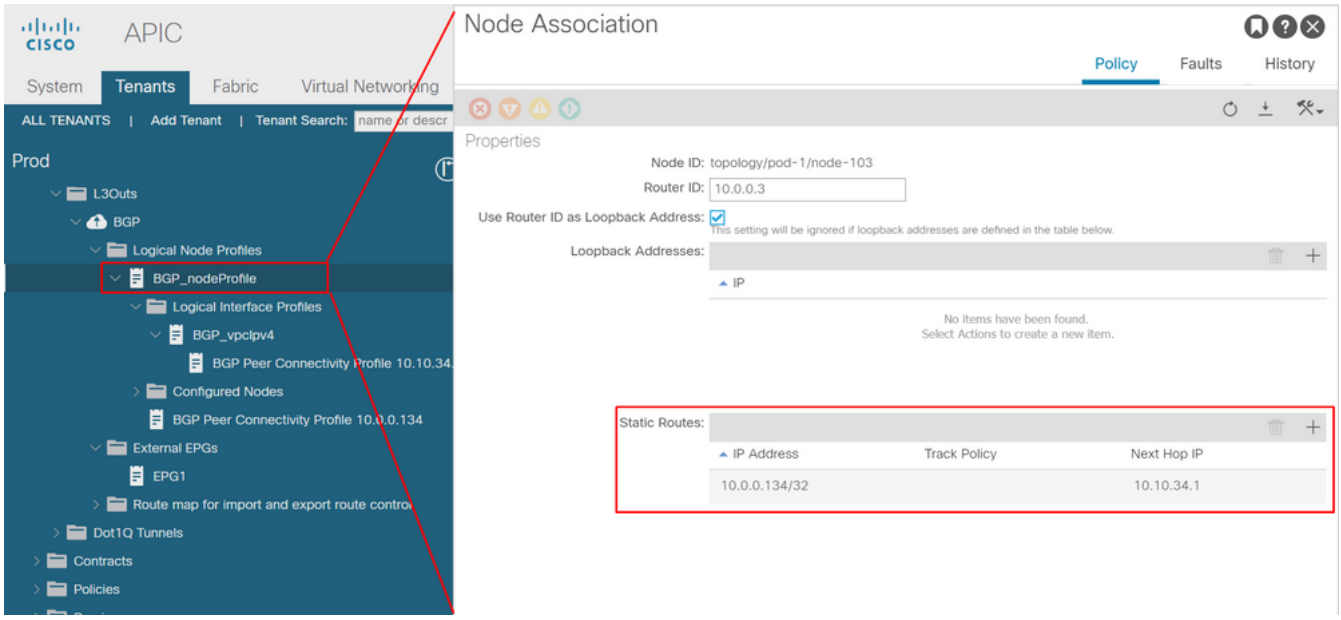
NOTA: El escenario donde se requiere la configuración de AS local es el mismo que el comando 'local-as' de NX-OS independiente.

- Número AS de BGP remoto (lado externo) **Perfil de conectividad de par: AS remoto**

El número de AS de BGP remoto sólo es necesario para eBGP donde el AS de BGP del vecino es diferente del AS de BGP de ACI.IP de origen para la sesión de peer BGP.**L3Out: Perfil de Conectividad de Peer BGP**



ACI admite el suministro de una sesión BGP desde la interfaz de bucle invertido sobre un tipo de interfaz L3Out de ACI típico (enrutada, subinterfaz, SVI).Cuando una sesión BGP debe originarse a partir de un loopback, configure el perfil de conectividad de par BGP bajo el perfil de **nodo** lógico.Cuando la sesión BGP deba originarse en una subinterfaz/SVI enrutada/subenrutada, configure el perfil de conectividad de par BGP bajo el perfil de **interfaz** lógica.Alcance de IP de peer BGP.**Perfil de nodo lógico: asociación de nodo**



Cuando los IPs de peer BGP son loopbacks, asegúrese de que el BL y el router externo tengan disponibilidad para la dirección IP del peer. Las rutas estáticas o OSPF se pueden utilizar para obtener accesibilidad a las IPs pares.**Verificación de BGP CLI (ejemplo de eBGP con loopback)**Los resultados de CLI para los siguientes pasos se recopilan de BL3 en la topología de la sección Descripción general.**1. Verifique si la sesión BGP está establecida**'State/PfxRcd' en la siguiente salida CLI significa que se ha establecido la sesión BGP.

```
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
```

Si 'State/PfxRcd' muestra Idle o Active, los paquetes BGP aún no se intercambian con el par. En este caso, compruebe lo siguiente y vaya al paso siguiente.

- Asegúrese de que el router externo esté apuntando al AS BGP de ACI correctamente (número AS local 65001).
- Asegúrese de que el perfil de conectividad de par BGP de ACI especifique la IP de vecino correcta desde la que el router externo está suministrando la sesión BGP (10.0.0.134).
- Asegúrese de que el perfil de conectividad de par BGP de ACI especifique el AS de vecino correcto del router externo (número de sistema autónomo remoto en la GUI que aparece en CLI como AS 65002).

2. Compruebe los detalles del vecino BGP (perfil de conectividad del par BGP)

El siguiente comando muestra los parámetros que son clave para el establecimiento de vecinos BGP.

- IP de vecino: 10.0.0.134.
- AS BGP vecino: remoto AS 65002.
- IP de origen: Uso de loopback3 como fuente de actualización.
- Multisalto eBGP: El par BGP externo puede estar hasta a 2 saltos de distancia.

```
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 vez que el peer BGP se ha establecido correctamente, los valores 'Host local' y 'Host externo' aparecen en la parte inferior de la salida.

3. Verifique el alcance IP para el par 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
```

Asegúrese de que el ping a la IP vecina funcione desde la IP de origen de 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. Verifique lo mismo en el router externo

A continuación se muestra un ejemplo de configuración del router externo (NX-OS independiente).

```
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. Paso adicional — tcpdump

En los nodos de hoja de ACI, la herramienta tcpdump puede rastrear la interfaz de CPU 'kpm_inb' para confirmar si los paquetes de protocolo llegaron a la CPU de hoja. Utilice el puerto L4 179 (BGP) como 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
```

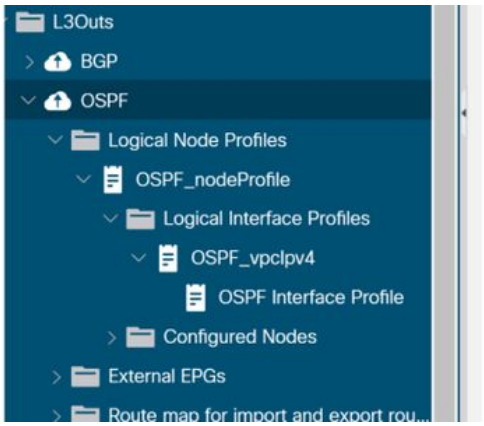
OSPF

Esta sección utiliza un ejemplo de vecinos OSPF entre BL3, BL4 y R34 desde la topología de la sección Overview con OSPF AreaID 1 (NSSA).

Los siguientes son los criterios comunes para verificar el establecimiento de adyacencia OSPF.

- ID y tipo de área OSPF

L3Out — Perfil de interfaz OSPF — ID y tipo de área



Al igual que cualquier dispositivo de ruteo, el ID de área OSPF y el tipo deben coincidir en ambos vecinos. Algunas limitaciones específicas de ACI en las configuraciones de ID de área OSPF incluyen:

- Un L3Out sólo puede tener un ID de área OSPF.
- Dos L3Outs pueden utilizar el mismo ID de área OSPF en el mismo VRF solamente cuando están en dos nodos de hoja diferentes.

Aunque el ID OSPF no necesita ser backbone 0, en el caso del ruteo de tránsito se requiere entre dos L3Outs OSPF en la misma hoja; uno de ellos debe utilizar el Área OSPF 0 porque cualquier intercambio de ruta entre las áreas OSPF debe realizarse a través del Área OSPF 0.

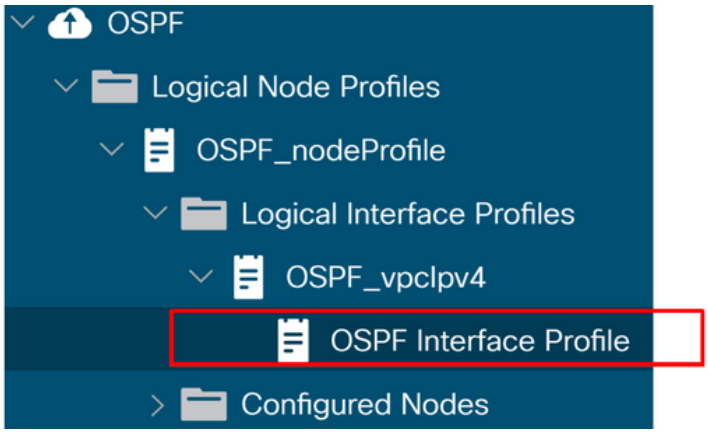
- MTU (unidad de transmisión básica)

Perfil de interfaz lógica: SVI

La MTU predeterminada en ACI es de 9000 bytes, en lugar de 1500 bytes, que es la que se utiliza habitualmente en los dispositivos de routing tradicionales. Asegúrese de que la MTU coincida con el dispositivo externo. Cuando el establecimiento de vecino OSPF falla debido a MTU, se atasca en EXCHANGE/DROTHER.

- Máscara de subred IP. OSPF requiere que la IP vecina utilice la misma máscara de subred.
- Perfil de interfaz OSPF.

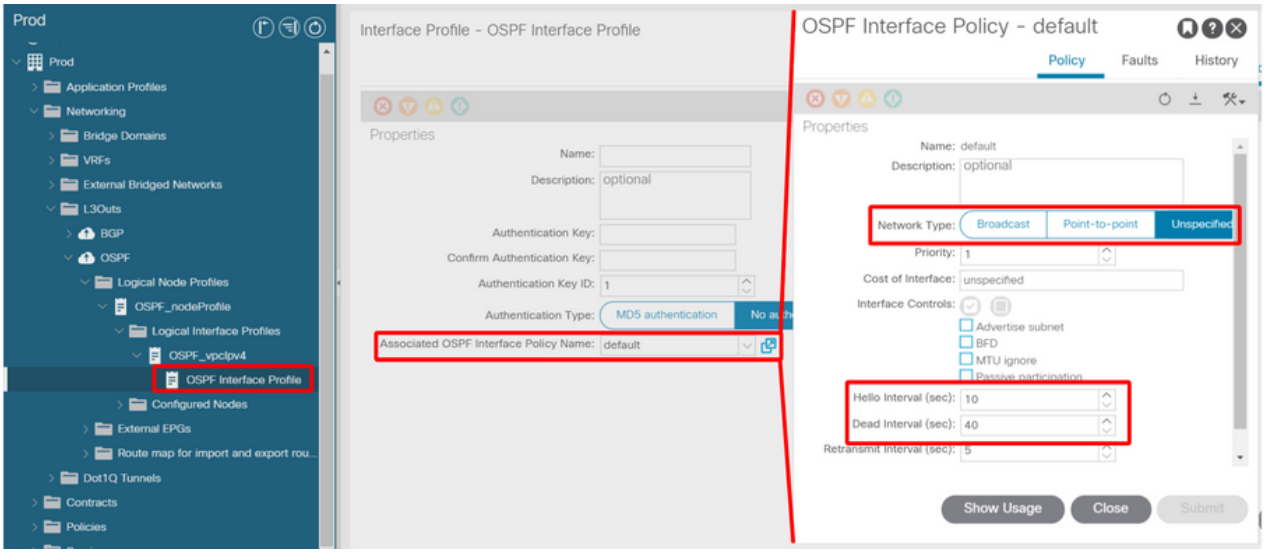
Perfil de interfaz OSPF



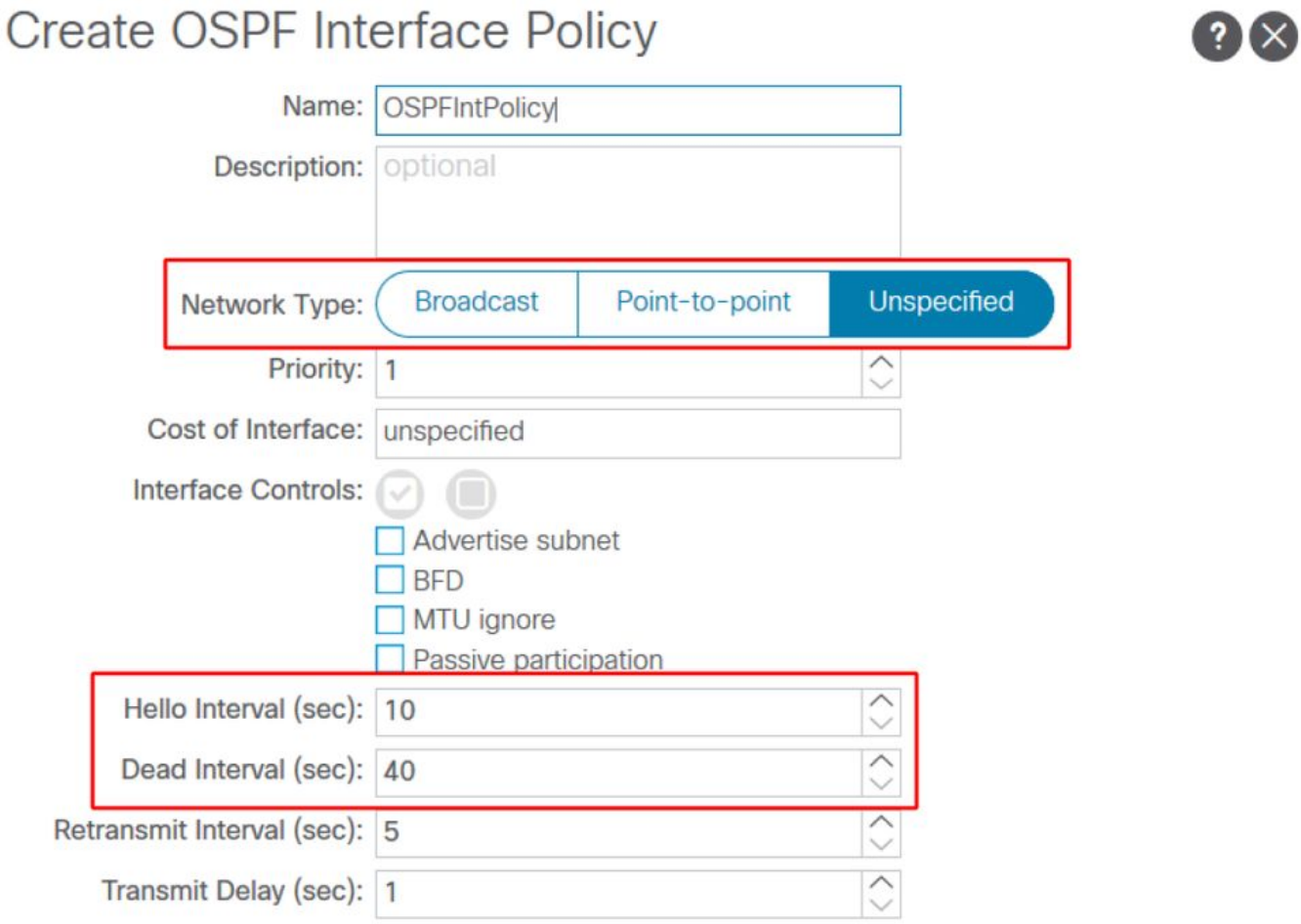
Esto equivale a 'ip router ospf <tag> area <area id>' en una configuración NX-OS independiente para habilitar OSPF en la interfaz. Sin esto, las interfaces de hoja no se unirán a OSPF.

- Hello OSPF / Temporizador inactivo, tipo de red

Perfil de interfaz OSPF: temporizador Hello / Dead y tipo de red



Detalles de la política de interfaz OSPF



OSPF requiere que los temporizadores Hello y Dead coincidan en cada dispositivo vecino. Estos se configuran en el perfil de interfaz OSPF.

Asegúrese de que el tipo de red de la interfaz OSPF coincida con el dispositivo externo. Cuando el dispositivo externo utiliza el tipo Punto a punto, el lado de ACI también debe configurar explícitamente Punto a punto. También se configuran en el perfil de interfaz OSPF.

Verificación de OSPF CLI

Los resultados de CLI de los siguientes pasos se recopilan de BL3 en la topología de la sección "Descripción general".

1. Verifique el estado del vecino OSPF

Si el 'Estado' es 'FULL' en la siguiente CLI, el vecino OSPF se establece correctamente. De lo contrario, vaya al paso siguiente para comprobar los parámetros.

```
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
```

En ACI, las BL formarán vecindades OSPF entre sí en la parte superior de los routers externos cuando usen el mismo ID de VLAN con una SVI. Esto se debe a que ACI tiene un dominio de

inundación interno denominado L3Out BD (o BD externo) para cada ID de VLAN en las SVI L3Out. Observe que el ID de VLAN 28 es una VLAN interna denominada PI-VLAN (VLAN independiente de la plataforma) en lugar de la VLAN real (VLAN de encapsulación de acceso) utilizada en el cable. Utilice el siguiente comando para verificar el acceso encap VLAN ('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
```

También se puede obtener la misma salida a través del ID de VLAN de encapsulamiento de acceso.

```
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. Verifique el área OSPF

Asegúrese de que el ID y el Tipo de área OSPF sean idénticos a los vecinos. Si falta el perfil de interfaz OSPF, la interfaz no se unirá a OSPF y no aparecerá en la salida de la CLI 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. Verifique los detalles de la interfaz OSPF

Asegúrese de que los parámetros de nivel de interfaz cumplan con los requisitos para el establecimiento de vecinos OSPF como subred IP, tipo de red y temporizador Hello/Dead. Tenga en cuenta el ID de VLAN para especificar que la SVI es 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. Verifique el alcance de IP al vecino

Aunque los paquetes Hello OSPF son paquetes Link Local Multicast, los paquetes DBD OSPF requeridos para el primer intercambio LSDB OSPF son unicast. Por lo tanto, también se debe verificar la disponibilidad de unidifusión para el establecimiento de vecindad 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. Verifique lo mismo en el router externo

A continuación se muestran ejemplos de configuraciones del router externo (NX-OS independiente)

```
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
```

Asegúrese de verificar la MTU también en la interfaz física.

6. Paso adicional — tcpdump

En los nodos de hoja de ACI, el usuario puede realizar tcpdump en la interfaz de CPU 'kpm_inb' para verificar si los paquetes de protocolo han alcanzado la CPU de hoja. Aunque hay varios filtros para OSPF, el número de protocolo IP es el filtro más completo.

- Número de protocolo IP: proto 89 (IPv4) o ip6 proto 0x59 (IPv6)

- Dirección IP del vecino: host <ip>
- IP de multidifusión local de enlace OSPF: host 224.0.0.5 o host 224.0.0.6

```
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
```

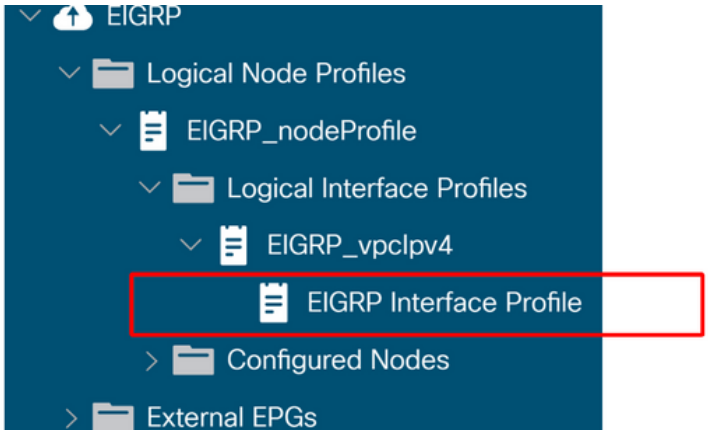
EIGRP

Esta sección utiliza un ejemplo de vecindad EIGRP entre BL3, BL4 y R34 desde la topología de la sección "Overview" con EIGRP AS 10.

Los siguientes son los criterios comunes para el establecimiento de adyacencia EIGRP.

- EIGRP AS: a L3Out se le asigna un AS EIGRP. Esto debe coincidir con el dispositivo externo.
- Perfil de interfaz EIGRP.

Perfil de interfaz EIGRP



Esto equivale a la configuración 'ip router eigrp <as>' en un dispositivo NX-OS independiente. Sin esto, las interfaces de hoja no se unirán a EIGRP.

- MTU (unidad de transmisión básica)

Aunque esto no tiene que coincidir simplemente para establecer la vecindad EIGRP, los paquetes de intercambio de topología EIGRP pueden llegar a ser más grandes que la MTU máxima permitida en las interfaces entre los pares, y dado que estos paquetes no pueden fragmentarse, se descartan y, como resultado, la vecindad EIGRP se inestable.

Verificación CLI EIGRP

Los resultados de CLI de los siguientes pasos se recopilan de BL3 en la topología de la sección

"Descripción general".

1. Verifique el estado de vecino 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
```

En ACI, las BL formarán una vecindad EIGRP entre sí en la parte superior de los routers externos cuando utilicen el mismo ID de VLAN con SVI. Esto se debe a que una ACI tiene un dominio de inundación interno denominado L3Out BD (o BD externo) para cada ID de VLAN en las SVI L3Out.

Tenga en cuenta que el ID de VLAN 29 es una VLAN interna denominada PI-VLAN (VLAN independiente de la plataforma) en lugar de la VLAN real (VLAN de encapsulación de acceso) utilizada en el cable. Utilice el siguiente comando para verificar el acceso encap 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
```

También se puede obtener la misma salida a través del ID de VLAN de encapsulamiento de acceso.

```
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. Compruebe los detalles de la interfaz EIGRP

Asegúrese de que EIGRP se esté ejecutando en la interfaz esperada. Si no es así, verifique Perfil de interfaz lógica y Perfil de interfaz 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. Verifique lo mismo en el router externo

A continuación se muestra un ejemplo de configuración del router externo (NX-OS independiente).

```
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. Paso adicional — tcpdump

En los nodos de hoja de ACI, el usuario puede realizar tcpdump en la interfaz de CPU 'kpm_inb' para confirmar si los paquetes de protocolo alcanzaron la CPU de la hoja. Utilice el protocolo IP número 88 (EIGRP) como 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
```

Anuncio de ruta

Esta sección se centra en la verificación y la resolución de problemas de anuncios de rutas en ACI. Específicamente, se examinan ejemplos que incluyen:

- Anuncio de subred de dominios de puente.
- Anuncio de ruta de tránsito.
- Control de ruta de importación y exportación.

Esta sección analiza la fuga de rutas en lo que respecta a L3Outs compartidas en secciones posteriores.

Bridge Domain Route Adversement Workflow

Antes de buscar una solución de problemas común, el usuario debe familiarizarse con cómo se supone que funciona el anuncio de dominio de puente.

El anuncio de BD, cuando BD y L3Out están en el mismo VRF, implica:

- Tener una relación contractual entre el L3Out y el EPG interno.
- Asociación de L3Out al dominio de puente.
- Seleccionando 'Advertise Externally' en la subred BD.

Además, también es posible controlar el anuncio de Bridge Domain mediante perfiles de ruta de exportación que evitan la necesidad de asociar el L3Out. Sin embargo, debe seguir seleccionado "Anunciar externamente". Este es un caso práctico menos común, por lo que no se tratará aquí.

La relación de contrato entre el L3Out y el EPG es necesaria para hacer que la ruta estática ubicua de BD sea empujada al BL. El anuncio de ruta real se maneja a través de la redistribución de la ruta estática en el protocolo externo. Por último, los route-maps de redistribución sólo se instalarán dentro de las L3Outs asociadas al BD. De esta manera, la ruta no se anuncia en todas las L3Outs.

En este caso, la subred de BD es 192.168.1.0/24 y se debe anunciar a través de OSPF L3Out.

Antes de aplicar el contrato entre el L3Out y el 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
```

Observe que la ruta BD aún no está presente en la BL.

Después de aplicar el contrato entre el L3Out y el EPG interno

En este momento no se ha realizado ninguna otra configuración. El L3Out aún no está asociado al BD y el indicador 'Advertise Externally' no está configurado.

```
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
```

Observe que la ruta de subred BD (indicada por el indicador ubicuo) ahora está implementada en la BL. Observe, sin embargo, que la ruta está etiquetada. Este valor de etiqueta es un valor implícito asignado a rutas BD antes de ser configurado con 'Advertise Externally'. Todos los protocolos externos impiden que esta etiqueta se redistribuya.

Después de seleccionar "Advertise Externally" (Anunciar externamente) en la subred BD

El L3Out aún no ha sido asociado al BD. Sin embargo, observe que la etiqueta se ha borrado.

```
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
```

En este momento, la ruta todavía no se está anunciando externamente porque no hay un route-map y una lista de prefijos que coincidan con este prefijo para su redistribución en el protocolo externo. Esto se puede verificar con los siguientes comandos:

```
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 ruta BD está programada como una ruta estática, así que verifique el route-map de redistribución estática ejecutando 'show route-map <route-map name>' y luego 'show ip prefix-list <name>' en cualquier lista de prefijos que esté presente en el route-map. Realice esto en el siguiente paso.

Después de asociar el L3Out al BD

Como se mencionó anteriormente, este paso da como resultado la lista de prefijos que coincide con la subred BD que se está instalando en el mapa de ruta de redistribución de protocolo estático a externo.

```
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
```

Verifique la lista de prefijos:

```
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
```

La subred BD se está haciendo coincidir para redistribuirla en OSPF.

En este punto, el flujo de trabajo de configuración y verificación está completo para el anuncio de la subred BD fuera de L3Out. Pasado este punto, la verificación sería específica del protocolo. Por ejemplo:

- Para EIGRP, verifique que la ruta se esté instalando en la tabla de topología con 'show ip eigrp topology vrf <name>'
- Para OSPF, verifique que la ruta se esté instalando en la tabla de base de datos como un LSA externo con 'show ip ospf database vrf <name>'
- Para BGP, verifique que la ruta esté en el RIB BGP con 'show bgp ipv4 unicast vrf <name>'

anuncio de ruta BGP

Para BGP, todas las rutas estáticas se permiten implícitamente para la redistribución. El route-map que coincide con la subred BD se aplica en el nivel de vecino 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
```

En el ejemplo anterior, 10.0.0.134 es el vecino BGP configurado dentro de L3Out.

anuncio de ruta EIGRP

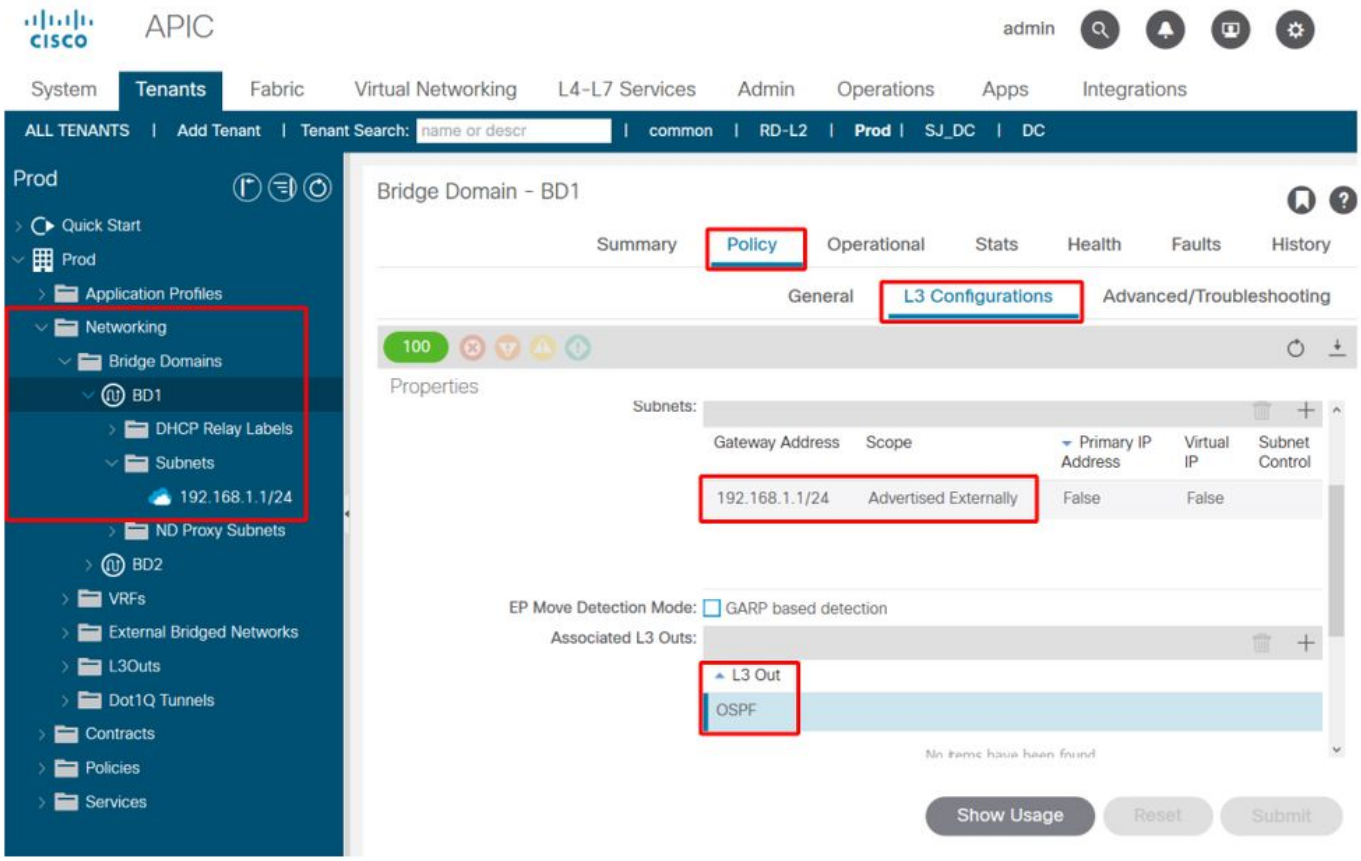
Al igual que OSPF, un route-map se utiliza para controlar la redistribución de Static a EIGRP. De esta manera, sólo las subredes asociadas a L3Out y configuradas como 'Advertise Externally' deben ser redistribuidas. Esto se puede verificar con este comando:

```
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
```

A continuación se muestra la configuración final de BD en funcionamiento.

Configuración de dominio de puente L3



Escenario de Troubleshooting de Bridge Domain Route Adversement

En este caso, el síntoma típico sería normalmente que una subred BD configurada no se está anunciando fuera de una salida L3. Siga el flujo de trabajo anterior para saber qué componente está dañado.

Comience con la configuración antes de obtener un nivel demasiado bajo comprobando lo siguiente:

- ¿Existe algún contrato entre el EPG y L3Out?
- ¿El L3Out está asociado al BD?
- ¿La subred BD está configurada para anunciarse externamente?
- ¿Está activa la adyacencia de protocolo externo?

Posible causa: BD no implementado

Este caso sería aplicable en un par de situaciones diferentes, como:

- El EPG interno usa la integración de VMM con la opción a demanda y no se han adjuntado terminales de VM al grupo de puertos para el EPG.
- Se ha creado el EPG interno pero no se han configurado enlaces de ruta estática o la interfaz en la que se ha configurado la ruta estática está inactiva.

En ambos casos, el BD no se implementaría y, como resultado, la ruta estática BD no se enviaría al BL. La solución aquí es implementar algunos recursos activos dentro de un EPG que está vinculado a este BD para que la subred se implemente.

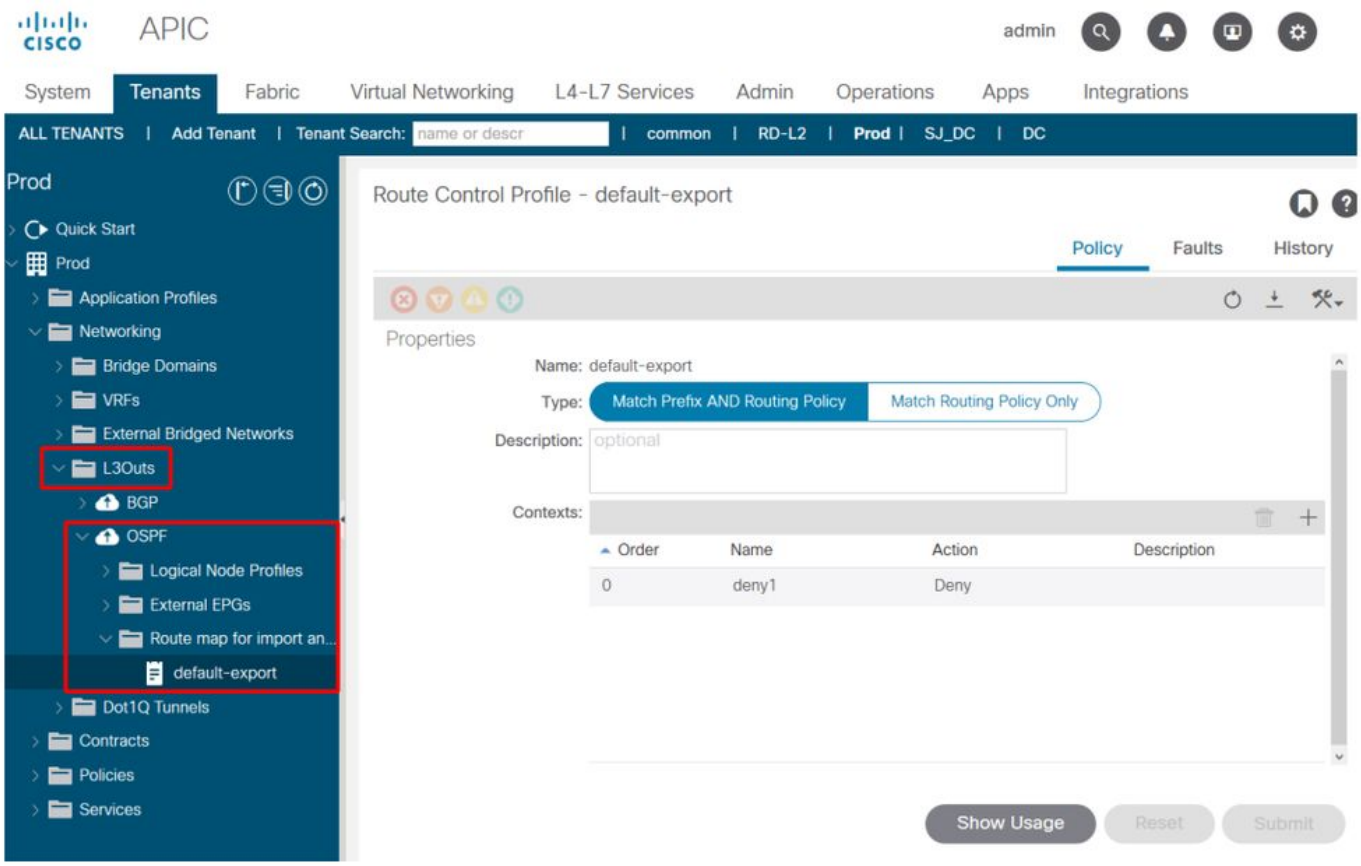
Posible causa: OSPF L3Out está configurado como 'Stub' o 'NSSA' sin redistribución

Cuando OSPF se utiliza como protocolo L3Out, se deben seguir las reglas OSPF básicas. Las áreas stub no permiten LSA redistribuidos pero pueden anunciar una ruta predeterminada en su lugar. Las áreas NSSA permiten rutas redistribuidas, pero 'Enviar LSA redistribuidos al área NSSA' debe estar seleccionado en L3Out. O NSSA también puede anunciar una ruta predeterminada desactivando 'Originate Summary LSA', que es un escenario típico donde 'Send Redistributed LSA's into NSSA Area' sería inhabilitado.

Posible causa: Perfil de ruta 'Default-Export' con una acción 'Deny' configurada en L3Out

Cuando los perfiles de ruta se configuran bajo una L3Out con los nombres de 'default-export' o 'default-import' se aplican implícitamente a la L3Out. Además, si default-export route-profile se establece en una acción de negación y se configura como 'Coincidir prefijo y política de ruteo', las subredes BD se deben anunciar fuera de este L3Out y se denegarán implícitamente:

Default-export Deny Route Profile



Las coincidencias de prefijo dentro del perfil de ruta de exportación predeterminado no incluirán implícitamente las subredes BD si se selecciona la opción 'Coincidir sólo con política de enrutamiento'.

Flujo de trabajo de importación de ruta externa

Esta sección trata sobre cómo ACI aprende las rutas externas a través de un L3Out y las distribuye a los nodos de hoja internos. También cubre casos prácticos de tránsito y fuga de rutas en secciones posteriores

Al igual que en la sección anterior, el usuario debe ser consciente de lo que ocurre en un nivel superior.

De forma predeterminada, todas las rutas aprendidas a través del protocolo externo se redistribuyen en el proceso BGP del fabric interno. Esto es así independientemente de las subredes configuradas en el EPG externo y de los indicadores seleccionados. Hay dos ejemplos en los que esto no es cierto.

- Si la opción 'Aplicación de control de ruta' en el nivel superior de la política L3Out está establecida en 'Importar'. En este caso, el modelo de importación de rutas pasaría de un modelo de lista de bloqueo (solo especifique lo que no se debe permitir) a un modelo de lista de permisos (todo se niega implícitamente a menos que se configure de otra manera).
- Si el protocolo externo es EIGRP o OSPF y se utiliza un perfil de ruta de interfiltración no coincide con las rutas externas.

Para que una ruta externa se distribuya en una hoja interna, debe ocurrir lo siguiente:

- La ruta se debe aprender en el BL desde el router externo. Para ser un candidato a redistribuir en el proceso de fabric MP-BGP, la ruta debe estar instalada en la tabla de ruteo en lugar de solamente en el protocolo RIB.
- Se debe permitir que la ruta se redistribuya o anuncie en el proceso BGP interno. Esto siempre debe suceder a menos que se utilice la aplicación de control de ruta de importación o un perfil de ruta Interleak.
- Se debe configurar y aplicar una política de reflector de ruta BGP a un grupo de políticas de grupo de dispositivos que se aplica al perfil de grupo de dispositivos. Si esto no se aplica, el proceso BGP no se inicializará en los switches.

Si el EPG/BD interno está en el mismo VRF que el L3Out, los tres pasos anteriores son todos los que se requieren para que el EPG/BD interno utilice rutas externas.

La ruta se instala en la tabla de routing BL

En este caso, la ruta externa que debe aprenderse en los BL 103 y 104 es 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
```

Es evidente que se instala en la tabla de ruteo tal como se aprende a través de OSPF. Si no se vio aquí, verifique el protocolo individual y asegúrese de que las adyacencias estén activas. La ruta se redistribuye en BGP El route-map de redistribución se puede verificar, después de verificar que no se utilizan ni los perfiles de ruta de 'Importar' ni los perfiles de ruta de Interleak, observando el route-map utilizado para el protocolo externo a la redistribución de BGP. Vea el

siguiente comando:

```
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
```

Aquí es evidente que el route-map 'permit-all' se utiliza para la redistribución OSPF a BGP. Este es el valor predeterminado. Desde aquí, se puede verificar BL y se verifica la ruta local que se origina en 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
```

En el resultado anterior, 0.0.0.0/0 indica que se originó localmente. La lista de peers a los que se anuncia son los nodos de columna del fabric que actúan como Route-Reflectors.

Verificar ruta en hoja interna

El BL debe anunciarlo a los nodos de columna a través de la familia de direcciones BGP VPNv4. Los nodos de columna deben anunciarlo a cualquier nodo de hoja con el VRF implementado (verdadero ejemplo de no fuga de ruta). En cualquiera de estos nodos de hoja, ejecute 'show bgp vpnv4 unicast <route> vrf overlay-1' para verificar que está en VPNv4

Utilice el siguiente comando para verificar la ruta en la hoja 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
```

En el resultado anterior, la ruta se aprende a través de BGP y los saltos siguientes deben ser los PASO físicos (PTEP) de los 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
```

escenario de Troubleshooting de Ruta Externa

En esta situación, la hoja interna (101) no recibe una ruta o rutas externas.

Como siempre, compruebe primero lo básico. Asegúrese de que:

- Las adyacencias del protocolo de ruteo están activas en las BL.
- Una política BGP Route-Reflector Policy se aplica al grupo de políticas de Pod y al perfil de Pod.

Si los criterios anteriores son correctos, a continuación se muestran algunos ejemplos más avanzados de lo que podría estar causando el problema.

Posible causa: VRF no implementado en la hoja interna

En este caso, el problema sería que no hay EPG con recursos implementados en la hoja interna donde se espera la ruta externa. Esto puede deberse a enlaces de ruta estática configurados únicamente en interfaces inactivas o a que solo hay EPG integrados de VMM en modo a demanda sin que se detecten archivos adjuntos dinámicos.

Debido a que el L3Out VRF no está implementado en la hoja interna (verifíquelo con 'show vrf' en la hoja interna), la hoja interna no importará la ruta BGP desde VPNv4.

Para resolver este problema, el usuario debe implementar recursos dentro del VRF L3Out en la hoja interna.

Posible causa: Se está utilizando la aplicación de ruta de importación

Como se mencionó anteriormente, cuando la aplicación del control de rutas de importación está habilitada, L3Out sólo acepta rutas externas que están permitidas explícitamente. Normalmente, la función se implementa como un mapa de tabla. Un mapa de tabla se ubica entre la RIB del protocolo y la tabla de ruteo real de modo que sólo afecta lo que está en la tabla de ruteo.

En el resultado que aparece debajo de Import Route-Control está habilitado, pero no hay rutas explícitamente permitidas. Observe que el LSA está en la base de datos OSPF pero no en la tabla de ruteo en el 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
```

Aquí está el mapa de tabla que ahora está instalado causando este comportamiento:

```
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:
```

Todo lo que se aprende en el área 100, que es el área configurada en este L3Out, es negado implícitamente por este mapa de tabla para que no se instale en la tabla de ruteo.

Para resolver este problema, el usuario debe definir la subred en el EPG externo con el indicador 'Importar subred de control de ruta' o crear un perfil de ruta de importación que coincida con los prefijos que se van a instalar.

- Tenga en cuenta que la aplicación de la importación no es compatible con EIGRP.
- Tenga en cuenta también que para BGP, la aplicación de la importación se implementa como un route-map entrante aplicado al vecino BGP. Consulte la subsección "BGP Route Advertisement" (Anuncio de ruta BGP) para obtener más información sobre cómo comprobarlo.

Posible causa: se está utilizando un perfil Interleak

Los perfiles de ruta Interleak se utilizan para EIGRP y L3Outs OSPF y están diseñados para permitir el control sobre lo que se redistribuye desde IGP en BGP, así como para permitir la aplicación de políticas como la configuración de atributos BGP.

Sin un Route-Profile interleak, todas las rutas se importan implícitamente a BGP.

Sin un perfil de ruta entrelazado:

```
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 perfil de ruta de entrelazado:

```
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
```

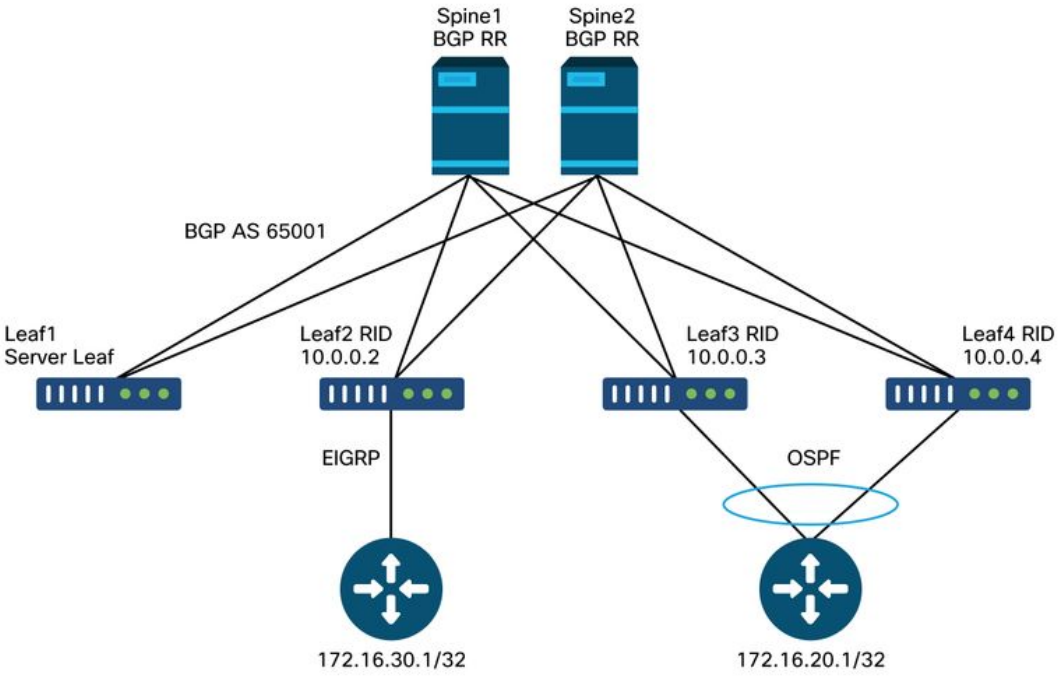
El mapa de ruta resaltado anteriormente sólo permitiría lo que se encuentra explícitamente coincidente en el perfil de interleak configurado. Si la ruta externa no coincide, no se redistribuirá en BGP.

Flujo de anuncio de ruta de tránsito

Esta sección trata sobre cómo las rutas de un L3Out se anuncian fuera de otro L3Out. Esto también cubriría el escenario donde las rutas estáticas que se configuran directamente en un L3Out necesitan ser anunciadas. No se abordará en cada consideración específica del protocolo, sino más bien en la forma en que se implementa en ACI. No entrará en el ruteo de tránsito entre VRF en este momento.

Este escenario utilizará la siguiente topología:

Topología de ruteo de tránsito



El flujo de alto nivel de cómo se aprendería 172.16.20.1 de OSPF y luego se anunciaría en EIGRP, y las verificaciones de todo el proceso y los escenarios de troubleshooting, se analizan a continuación.

Para que la ruta 172.16.20.1 se anuncie en EIGRP, se debe configurar una de las siguientes opciones:

- La subred que se anunciará podría definirse en el EIGRP L3Out con el indicador 'Exportar subred de control de rutas'. Como se mencionó en la sección de descripción general, este indicador se utiliza principalmente para el ruteo de tránsito y define las subredes que se deben anunciar fuera de ese L3Out.
- Configure 0.0.0.0/0 y seleccione 'Aggregate Export' y 'Export Route Control Subnet'. Esto crea un route-map para la redistribución en el protocolo externo que coincide con 0.0.0.0/0 y todos los prefijos que son más específicos (que es una coincidencia efectiva con cualquiera). Tenga en cuenta que cuando se utiliza 0.0.0.0/0 con 'Aggregate Export', las rutas estáticas no se buscarán para la redistribución. Esto es para prevenir la publicidad inadvertida de rutas BD que no deberían ser anunciadas.
- Por último, es posible crear un perfil de ruta de exportación que coincida con los prefijos que se anunciarán. Utilizando este método podría configurar la opción 'Aggregate' con prefijos además de 0.0.0.0/0.

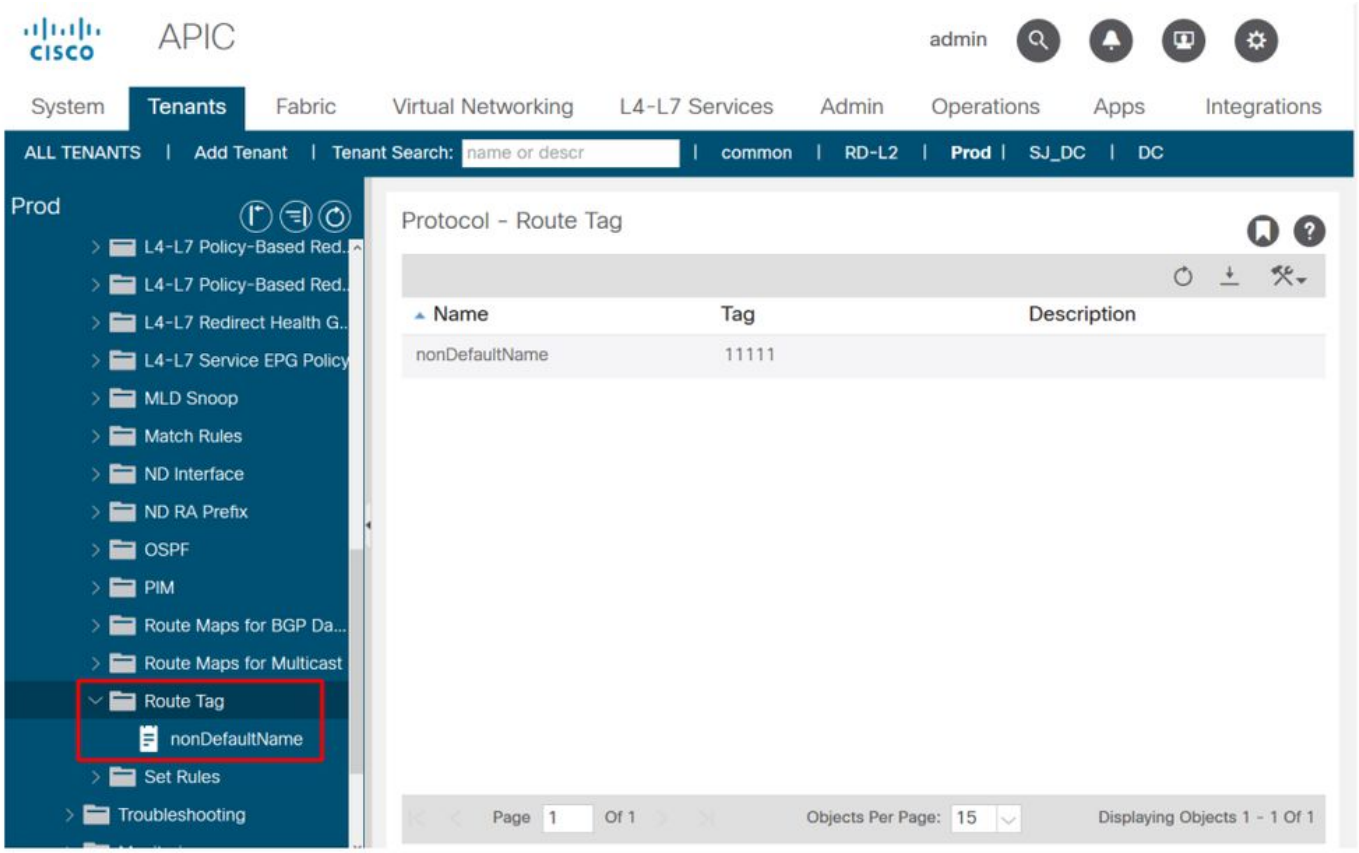
Las configuraciones anteriores darían como resultado que se anunciara la ruta de tránsito, pero aún así necesita tener una política de seguridad implementada para permitir que fluya el tráfico del plano de datos. Al igual que con cualquier comunicación de EPG a EPG, debe existir un contrato antes de permitir el tráfico.

> Tenga en cuenta que las subredes externas duplicadas con la 'Subred externa para EPG externo' no se pueden configurar en el mismo VRF. Cuando se configura, las subredes deben ser más específicas que 0.0.0.0. Es importante configurar 'Subred externa para EPG externo' solamente para la L3Out donde se recibe la ruta. No configure esto en el L3Out que

debería anunciar esta ruta.

También es importante comprender que todas las rutas de tránsito están etiquetadas con una etiqueta VRF específica. De forma predeterminada, esta etiqueta es 4294967295. La política de etiquetas de ruta se configura en 'Arrendatario > Redes > Protocolos > Etiqueta de ruta:

Política de etiquetas de ruta



Esta política de etiqueta de ruta se aplica al VRF. El propósito de esta etiqueta es esencialmente prevenir loops. Esta etiqueta de ruta se aplica cuando la ruta de tránsito se anuncia de vuelta de una L3Out. Si estas rutas se reciben con la misma etiqueta de ruta, la ruta se descarta.

Verifique que la ruta esté presente en el BL de recepción a través de OSPF

Al igual que en la última sección, primero verifique que la BL que debe recibir inicialmente la ruta correcta.

```
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
```

Por ahora, supongamos que el anuncio L3Out está en un BL diferente (como en la topología) (escenarios posteriores discutirán dónde está en el mismo BL).

Verifique que la ruta esté presente en BGP en el OSPF BL de recepción

Para que la ruta OSPF se anuncie al router EIGRP externo, la ruta debe anunciarse en BGP en el OSPF de recepción.

```
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 ruta está en BGP.

Verifique en el BL EIGRP que debe anunciar la ruta que está instalada

```
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
```

Se instala en la tabla de ruteo con saltos siguientes superpuestos que apuntan a los nodos de hoja de borde de origen.

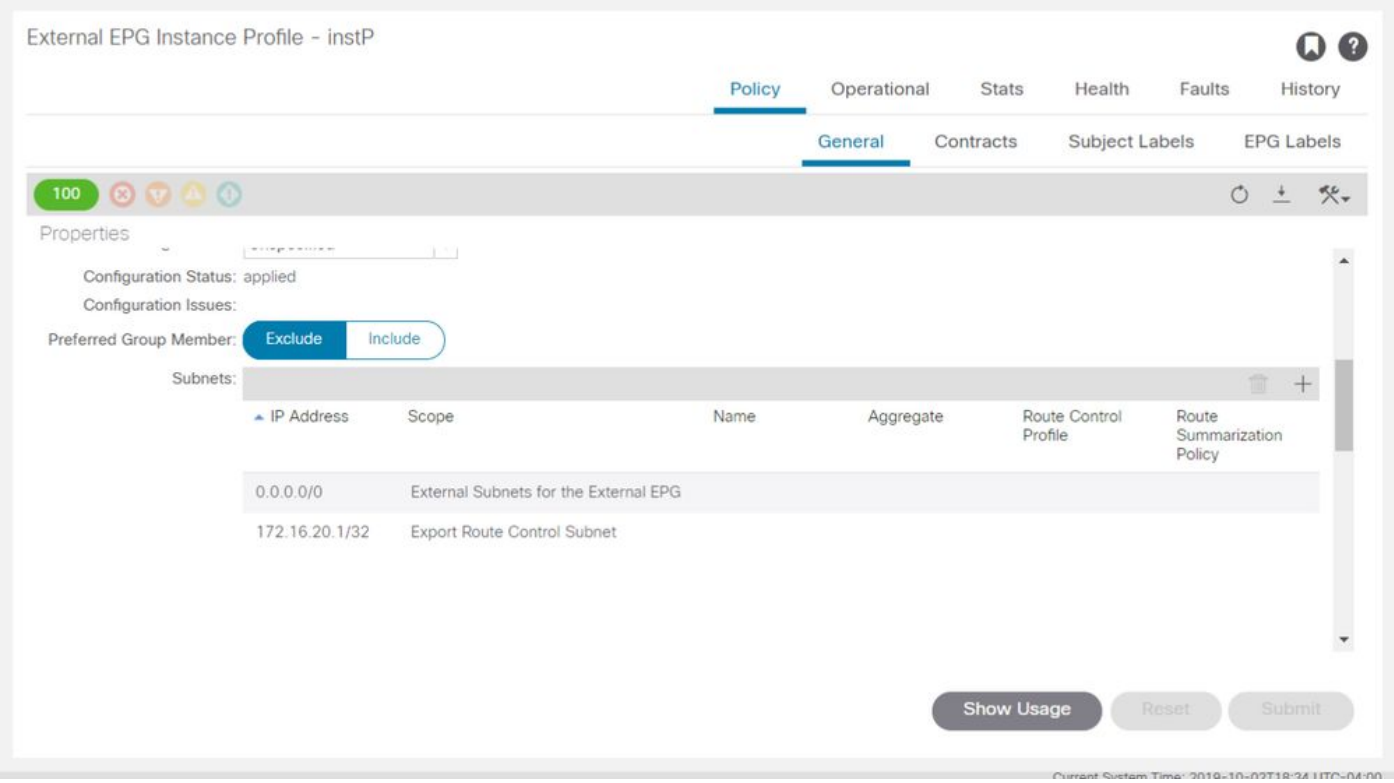
```
leaf102# acidiag fnvread

      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
```

Verifique que la ruta esté anunciada en la BL

La ruta será anunciada por BL 102 como resultado de la configuración del indicador 'Exportar subred de control de ruta' en la subred configurada:

Exportar control de ruta



Utilice el siguiente comando para ver el route-map que se crea como resultado de este indicador 'Exportar control de ruta':

```
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
```

Para buscar la 'redistribución BGP > EIGRP', mire el route-map. Sin embargo, el route-map debe ser el mismo independientemente de si el protocolo de origen es OSPF, EIGRP o BGP. Las rutas estáticas se controlarán con un route-map diferente.

```
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
```

En el resultado anterior, la etiqueta VRF se configura en este prefijo para la prevención de loops y la subred configurada con 'Control de ruta de exportación' coincide explícitamente.

El ruteo de tránsito al recibir y anunciar BL es el mismo

Como se mencionó anteriormente, cuando los BL de recepción y de publicidad son diferentes, la ruta debe anunciarse a través del fabric mediante BGP. Cuando las BL son iguales, la redistribución o publicidad se puede hacer directamente entre los protocolos en la hoja.

A continuación, se describen brevemente cómo se implementa:

- **Ruteo de tránsito entre dos L3Outs OSPF en la misma hoja:** El anuncio de ruta se controla a través de un 'filtro de área' aplicado al nivel de proceso OSPF. Se debe implementar una salida L3 en el Área 0 en la hoja, ya que las rutas se anuncian entre áreas en lugar de a través de la redistribución. Utilice 'show ip ospf vrf <name>' para ver la lista de filtros. Muestre el contenido del filtro mediante 'show route-map <filter name>'.
- **Ruteo de tránsito entre L3Outs OSPF y EIGRP en la misma hoja: el** anuncio de ruta se controla a través de mapas de ruta de redistribución que se pueden ver con 'show ip ospf' y 'show ip eigrp'. Tenga en cuenta que si existen múltiples L3Outs OSPF en la misma BL, la única manera de redistribuir en solo una de esas L3Outs OSPF es si la otra es un Stub o NSSA con **'Send redistributed LSAs into NSSA area' inhabilitado para** que no permita ningún LSA externo.
- **Ruteo de tránsito entre OSPF o EIGRP y BGP en la misma hoja:** El anuncio de ruta en el IGP se controla a través de mapas de ruta de redistribución. El anuncio de la ruta en BGP se controla a través de un route-map saliente aplicado directamente al vecino bgp que debe hacer la ruta enviada. Esto se puede verificar con 'show bgp ipv4 unicast neighbor <neighbor address> vrf <name> | grep Outbound'.
- **Ruteo de tránsito entre dos l3Outs BGP en la misma hoja:** Todo el anuncio se controla a través de mapas de ruta aplicados directamente al vecino BGP al que se debe enviar la ruta. Esto se puede verificar con 'show bgp ipv4 unicast neighbor <neighbor address> vrf <name> |

grep Outbound'.

Escenarios de Troubleshooting de Ruteo de Tránsito #1: Ruta de tránsito no anunciada

Este escenario de troubleshooting implica que las rutas que se deben aprender a través de un L3Out no se envían al otro L3Out.

Como siempre, compruebe los aspectos básicos antes de examinar cualquier aspecto específico de la ACI.

- ¿Están activas las adyacencias de protocolo?
- En primer lugar, ¿la ruta, que debería ser la publicidad de la ACI, se ha aprendido de un protocolo externo?
- Para BGP, ¿se está descartando la trayectoria debido a algún atributo BGP? (as-path, etc.).
- ¿La L3Out receptora la tiene en la base de datos OSPF, en la tabla de topología EIGRP o en la tabla BGP?
- ¿Se aplica una política de reflector de ruta BGP al grupo de políticas Pod que se aplica al perfil Pod?

Si todas las verificaciones básicas del protocolo están configuradas correctamente, a continuación se muestran algunas otras causas comunes para una ruta de tránsito que no se está anunciando.

Posible causa: Sin área OSPF 0

Si la topología afectada implica dos L3Outs OSP en la misma hoja de borde, debe haber un Área 0 para que las rutas se anuncien de un área a otra. Consulte la viñeta anterior "Routing de tránsito entre dos L3Outs OSPF en la misma hoja" para obtener más detalles.

Posible causa: El área OSPF es stub o NSSA

Esto se vería si OSPF L3Out está configurado con un área Stub o NSSA que no está configurada para anunciar LSA externos. Con OSPF, los LSA externos nunca se anuncian en áreas Stub. Se anuncian en áreas NSSA si se selecciona 'Enviar LSA redistribuidos en área NSSA'.

Escenarios de Troubleshooting de Ruteo de Tránsito #2: Ruta de tránsito no recibida

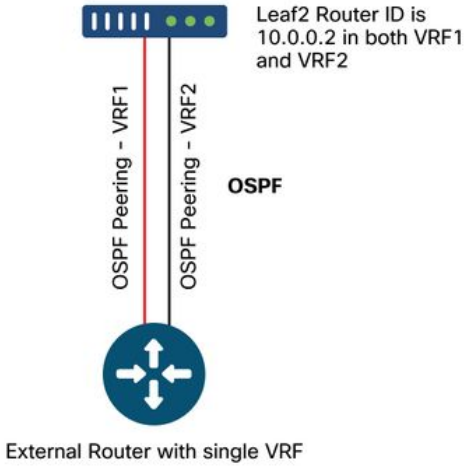
En esta situación, el problema es que algunas rutas anunciadas por un L3Out de ACI no se reciben de vuelta en otro L3Out. Este escenario podría ser aplicable si las L3Outs están en dos fabrics separados y están conectadas por routers externos o si las L3Outs están en VRFs diferentes y las rutas están siendo pasadas entre los VRFs por un router externo.

Posible causa: BL está configurado con el mismo ID de router en varios VRF

Desde una perspectiva de configuración, un ID de router no se puede duplicar dentro del mismo VRF. Sin embargo, generalmente es correcto utilizar el mismo router-id en diferentes VRFs, siempre y cuando los dos VRFs no estén conectados a los mismos dominios de protocolo de ruteo.

Tenga en cuenta la siguiente topología:

Router externo con un único VRF - Ruta de tránsito no recibida



El problema aquí sería que la hoja de ACI ve LSA con su propio Router-ID siendo recibido, dando como resultado que éstos no sean instalados en la base de datos OSPF.

Además, si se observara la misma configuración con los pares VPC, los LSA se agregarían y eliminarían continuamente en algunos routers. Por ejemplo, el router vería los LSA que vienen de su par VPC con VRF y los LSA que vienen del mismo nodo (con el mismo Router-ID) que se originaron en el otro VRF.

Para resolver este problema, el usuario debe asegurarse de que un nodo tenga un router-id diferente y único dentro de cada VRF en el que tenga un L3Out.

Posible causa: Rutas desde un L3Out en un fabric ACI recibido en otro fabric con la misma etiqueta VRF

La etiqueta de ruta predeterminada en ACI es siempre la misma a menos que se cambie. Si las rutas se anuncian de un L3Out en un entramado VRF o ACI a otro L3Out en otro entramado VRF o ACI sin cambiar las etiquetas VRF predeterminadas, las rutas serán descartadas por las BL receptoras.

La solución a este escenario es simplemente utilizar una política de Route-Tag única para cada VRF en ACI.

Escenarios de Troubleshooting de Ruteo de Tránsito #3 — Rutas de Tránsito anunciadas inesperadamente

Este escenario se vería cuando las rutas de tránsito se anuncian fuera de un L3Out donde no están destinadas a ser anunciadas.

Posible causa: uso de 0.0.0.0/0 con 'Exportación agregada'

Cuando una subred externa se configura como 0.0.0.0/0 con 'Export Route Control Subnet' y 'Aggregate Export' el resultado es que se instala una coincidencia con todo el route-map de redistribución. En este caso, todas las rutas en el BL que se aprendieron a través de OSPF, EIGRP o BGP se anuncian en el L3Out donde se configura.

A continuación se muestra el route-map que se implementa en la hoja como resultado de la

exportación agregada:

```
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
```

Esta es la causa número uno de los loops de ruteo que involucran un entorno ACI.

Contrato y L3Out

EPG basado en prefijo en L3Out

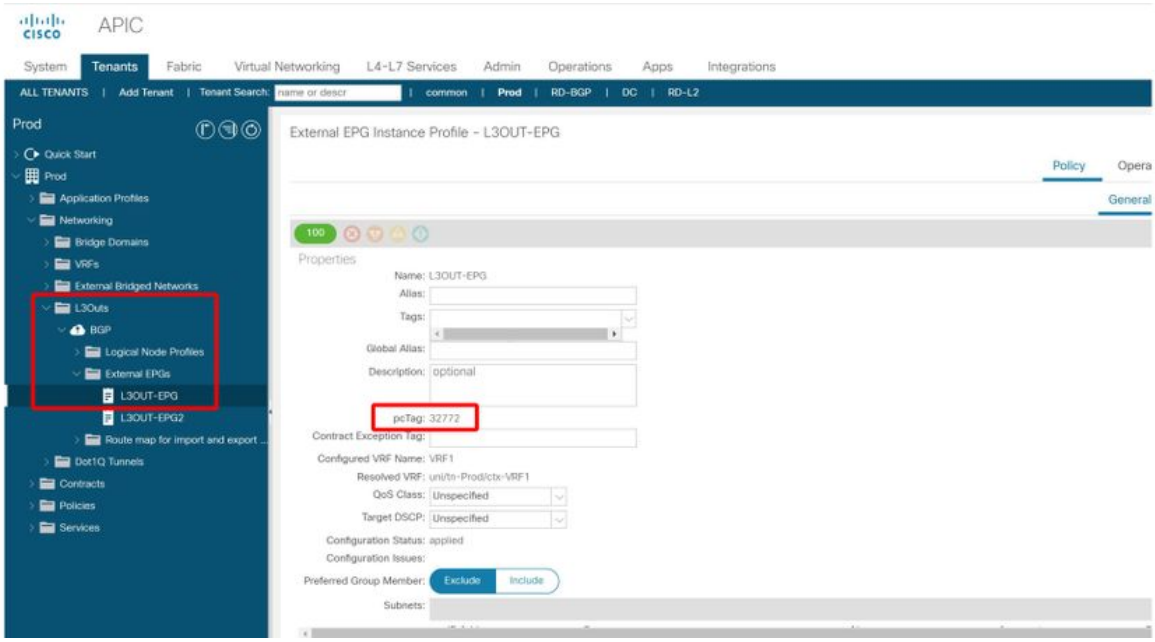
En un EPG interno (no L3Out), los contratos se aplican después de derivar la pcTag del origen y la pcTag del EPG de destino. La VLAN/VXLAN de encapsulación del paquete recibido en el puerto de enlace descendente se utiliza para dirigir esta pcTag clasificando el paquete en el EPG. Siempre que se aprende una dirección MAC o una dirección IP, se aprende junto con su encapsulación de acceso y la pcTag EPG asociada. Para obtener más información sobre pcTag y

la aplicación de contratos, consulte el capítulo "Políticas de seguridad".

L3Outs también impulsa una pcTag usando su L3Out EPG (EPG externo) ubicado bajo 'Arrendatario > Networking > L3OUT > Networks > L3OUT-EPG'. Sin embargo, las L3Outs no dependen de las VLAN e interfaces para clasificar los paquetes como tales. En su lugar, la clasificación se basa en el prefijo/subred de origen de la forma 'Coincidencia de prefijo más larga'. Por lo tanto, un EPG L3Out puede ser referido como un **EPG basado en prefijo**. Después de clasificar un paquete en un L3Out basado en una subred, sigue un patrón de aplicación de políticas similar al de un EPG normal.

El siguiente diagrama describe dónde se puede encontrar la pcTag de un EPG L3Out determinado dentro de la GUI.

Ubicación de pcTag para una salida L3



El usuario es responsable de definir la tabla EPG basada en prefijos. Esto se realiza mediante el ámbito de subred 'Subred externa para EPG externo'. Cada subred establecida con ese ámbito agregará una entrada en una tabla estática de coincidencia de prefijo más largo (LPM). Esta subred señalará al valor pcTag que se utilizará para cualquier dirección IP que se encuentre dentro de ese prefijo.

La tabla LPM de subredes EPG basadas en prefijo se puede verificar en los switches de hoja mediante el siguiente comando:

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

Comentarios:

- Las entradas de la tabla LPM se asignan a VRF VNID. La búsqueda se realiza por vrf_vnid/src pcTag/dst pcTag.
- Cada entrada apunta a una única pcTag. Como consecuencia, dos EPG L3Out no pueden utilizar la misma subred con la misma longitud de máscara dentro del mismo VRF.
- La subred 0.0.0.0/0 siempre utiliza una pcTag especial 15. Como tal, se puede duplicar, pero solo se debe hacer con un conocimiento completo de las implicaciones de aplicación de

políticas.

- Esta tabla se utiliza en ambas direcciones. De L3Out a Leaf Local Endpoint, el pcTag de origen se deriva utilizando esta tabla.Desde el punto final local de hoja hasta L3Out, el pcTag de destino se deriva mediante esta tabla.
- Si el VRF tiene la configuración de aplicación 'Ingress' para 'Policy Control Enforcement Direction', entonces la tabla de prefijos LPM estará presente en los L3Out BL así como en cualquier switch de hoja en el VRF que tenga un contrato con L3Out.

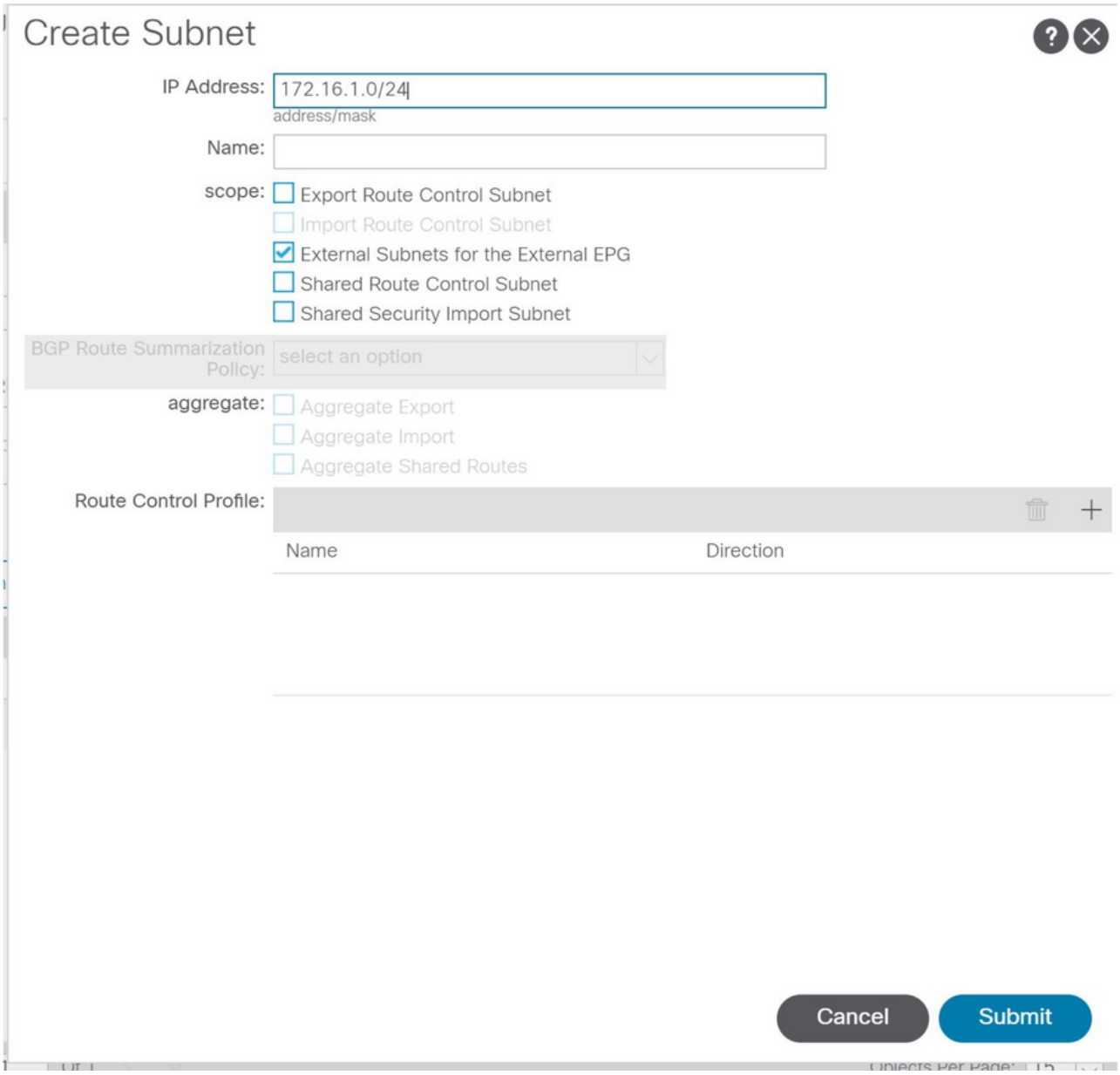
Ejemplo 1: L3Out única con prefijo específico

Situación: Un único BGP L3Out en vrf Prod:VRF1 con un EPG L3Out. El prefijo 172.16.1.0/24 está siendo recibido de una fuente externa, por lo que debe ser clasificado en el 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
```

Primero, agregue la subred a la tabla de prefijos.

Subred con alcance 'Subredes externas para el EPG externo'



Verifique la programación de la lista de prefijos en los switches de hoja que tienen el VRF del L3Out:

```
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
```

La pcTag del EPG L3Out es 32772 en el ámbito vrf 2097154.

Ejemplo 2: L3Out única con varios prefijos

Ampliando en el ejemplo anterior, en este escenario L3Out está recibiendo múltiples prefijos. Mientras que la introducción de cada prefijo es funcionalmente correcta, una opción alternativa (dependiendo del diseño previsto) es aceptar todos los prefijos recibidos en el L3Out.

Esto se puede lograr con el prefijo '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.

Esto da como resultado la siguiente entrada de tabla de prefijos de 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
```

> Tenga en cuenta que pcTag asignado a 0.0.0.0/0 utiliza el valor 15, no 32772. pcTag 15 es un sistema reservado pcTag que sólo se utiliza con 0.0.0.0/0 que actúa como comodín para coincidir con todos los prefijos de una salida L3.

Si el VRF tiene un único L3Out con un único L3Out EPG que utiliza el 0.0.0.0/0, el policy-prefix permanece único y es el enfoque más fácil de capturar todo.

Ejemplo 3a: Varios EPG L3Out en un VRF

En este escenario hay varios EPG L3Out en el mismo VRF.

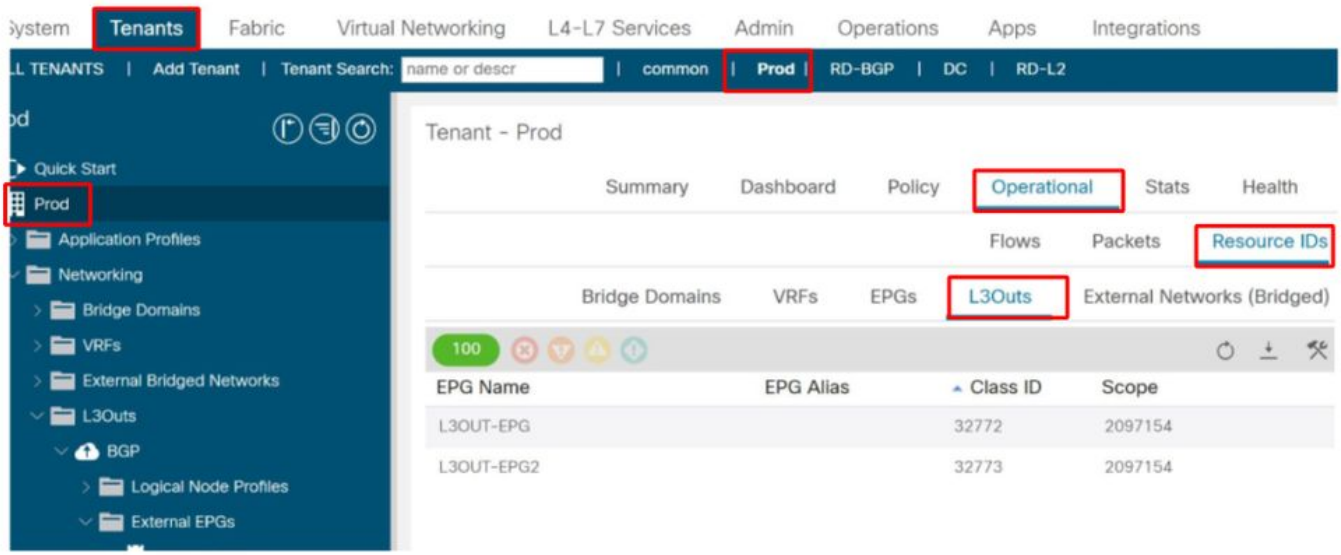
Nota: Desde una perspectiva EPG basada en prefijos, las dos configuraciones siguientes darán como resultado entradas de tabla de prefijos de LPM policy-mgr equivalentes:

1. Dos L3Outs con un EPG L3Out cada uno.
2. Una salida L3 con dos EPG L3Out

En ambos escenarios, el número total de EPG L3Out es 2. Esto significa que cada uno tendrá su propia pcTag y subredes asociadas.

Todas las etiquetas de pc de un EPG L3Out determinado se pueden ver en la GUI en 'Arrendatario > Operativo > Resource id > L3Outs'

Verificación de la pcTag L3Out



En esta situación, el fabric ACI recibe varios prefijos de los routers externos y la definición de EPG L3Out es la siguiente:

- 172.16.1.0/24 asignado a L3OUT-EPG.
- 172.16.2.0/24 asignado a L3OUT-EPG2.
- 172.16.0.0/16 asignado a L3OUT-EPG (para detectar el prefijo 172.16.3.0/24).

Para coincidir con esto, la configuración se definirá de la siguiente manera:

- L3OUT-EPG tiene la subred 172.16.1.0/24 y 172.16.0.0/16 ambas con el alcance 'Subred externa para el EPG externo'.
- L3OUT-EPG2 tiene la subred 172.16.2.0/24 con el alcance 'Subred externa para el EPG externo'.

Las entradas de la tabla de prefijos resultantes serán:

```
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 se asigna a pcTag 32773 (L3OUT-EPG2) y 172.16.0.0/16 se asigna a 32772 (L3OUT-EPG).

En este escenario, la entrada para 172.16.1.0/24 es redundante ya que la superred /16 está asignada al mismo EPG.

Múltiples EPG L3Out son útiles cuando el objetivo es aplicar diferentes contratos a grupos de prefijos dentro de un único L3Out. El siguiente ejemplo ilustra cómo los contratos entran en juego con varios EPG L3Out.

Ejemplo 3b: varios EPG L3Out con contratos diferentes

Este escenario contiene la siguiente configuración:

- Contrato ICMP que permite sólo ICMP.
- Contrato HTTP que sólo permite el puerto de destino TCP 80.
- EPG1 (pcTag 32770) proporciona el contrato HTTP consumido por L3OUT-EPG (pcTag 32772).
- EPG2 (pcTag 32771) proporciona el contrato ICMP consumido por L3OUT-EPG2 (pcTag 32773).

Se utilizarán los mismos prefijos policymgr del ejemplo anterior:

- 172.16.1.0/24 en L3OUT-EPG debería permitir HTTP a EPG1

- 172.16.2.0/24 en L3OUT-EPG2 debe permitir ICMP a EPG2

policy-mgr prefix y zoning-rules:

```
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)     |
+---------+--------+--------+----------+----------------+---------+---------+------+----------+-
---------------------+
```

Validación de ruta de datos mediante fTriage: flujo permitido por la política

Con un flujo ICMP entre 172.16.2.1 en la red externa y 192.168.3.1 en EPG2, fTriage se puede utilizar para capturar y analizar el flujo. En este caso, inicie fTriage en los switches de hoja 103 y 104, ya que el tráfico puede ingresar a cualquiera de ellos:

```
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 confirma el resultado de la regla de zonificación contra la regla ICMP de 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
```

Validación de ruta de datos mediante fTriage: flujo no permitido por la política

Con el tráfico ICMP originado desde 172.16.1.1 (L3OUT-EPG) hacia 192.168.3.1 (EPG2), se espera una caída de política.

```
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 confirma que el paquete se descarta con el motivo SECURITY_GROUP_DENY (caída de política) y que el pcTag de origen derivado es 32772 y el pcTag de destino es 32771. Si se compara con las reglas de zonificación, es evidente que no hay entradas entre esos 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 |
+---------+--------+--------+----------+-----+--------+-------+------+--------+----------+
+---------+--------+--------+----------+-----+--------+-------+------+--------+----------+
```

Ejemplo 4: múltiples L3Outs con prefijos múltiples

El escenario se configura de manera similar al ejemplo 3 (definiciones de EPG L3Out y L3Out), pero la red definida en ambos EPG L3Out es 0.0.0.0/0.

La configuración del contrato es la siguiente:

- Contrato ICMP1 que permite ICMP.
- Contrato ICMP2 que permite ICMP.
- EPG1 (pcTag 32770) proporciona el contrato ICMP1 que L3OUT-EPG consume (pcTag 32772).
- EPG2 (pcTag 32771) proporciona el contrato ICMP2 que L3OUT-EPG2 consume (pcTag 32773).

Esta configuración puede parecer ideal en el caso de que la red externa anuncie muchos prefijos, pero hay al menos dos fragmentos de prefijos que siguen diferentes patrones de flujo permitidos. En este ejemplo, un prefijo sólo debe permitir ICMP1 y el otro sólo ICMP2.

A pesar de usar '0.0.0.0/0' dos veces en el mismo VRF, sólo se programa un prefijo en la tabla de prefijos de 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
```

A continuación se examinan dos corrientes. Según la configuración del contrato anterior, se espera lo siguiente:

1. 172.16.2.1 (L3OUT-EPG2) a 192.168.3.1 (EPG2) **deben** ser permitidos por ICMP2
2. **No deben** permitirse los valores de 172.16.2.1 (L3OUT-EPG2) a 192.168.1.1 (EPG1), ya que no existe ningún contrato entre EPG1 y L3OUT-EPG2

Validación de ruta de datos mediante fTriage: flujo permitido por la política

Ejecute fTriage con un flujo ICMP de 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
```

Este flujo está permitido (como se esperaba) por la regla de zonificación 4336.

Validación de ruta de datos mediante fTriage: flujo no permitido por la política

Ejecute fTriage con un flujo ICMP de 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
```

Este flujo está permitido (inesperado) por la regla de zonificación 4341. Las reglas de zonificación ahora deben ser analizadas para entender por qué.

Validación de ruta de datos — zoning-rules

Las reglas de zonificación correspondientes a las últimas 2 pruebas son las siguientes:

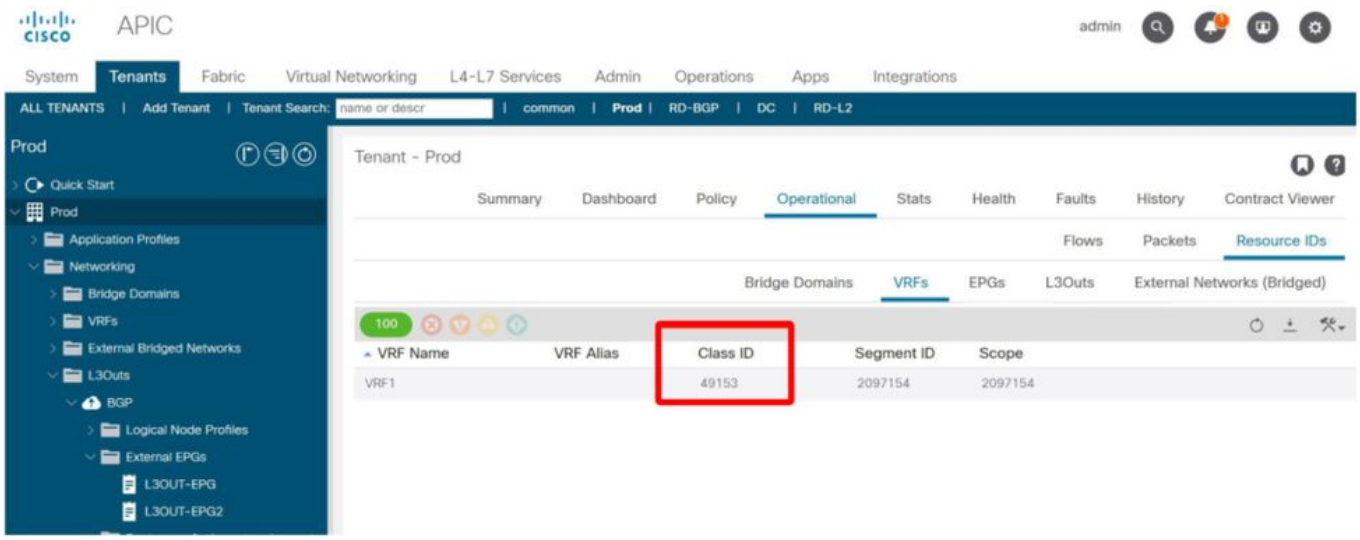
- Esperado: el flujo alcanza la línea de regla de zonificación 4336 (contrato ICMP2).
- Inesperado: el flujo alcanza la línea de regla de zonificación 4341 (contrato ICMP1).

```
+---------+--------+--------+----------+---------+---------+---------+-------+----------+-------
---------------+
| 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)     |
+---------+--------+--------+----------+---------+---------+---------+-------+----------+-------
--------------+
```

Ambos flujos derivan el valor src pcTag de 49153. Este es el valor pcTag del VRF. Esto se puede verificar en la interfaz de usuario:

Verificación de la pcTag del VRF



Lo siguiente sucede cuando el prefijo 0.0.0.0/0 está en uso con un L3Out:

- El tráfico de un EPG interno a un EPG L3Out con 0.0.0.0/0 derivará una pcTag de destino de 15.
- El tráfico de un EPG L3Out con 0.0.0.0/0 a un EPG interno de ACI derivará una pcTag de origen del VRF (49153).

La secuencia de comandos contract_parser ofrece una vista holística de las reglas de zonificación:

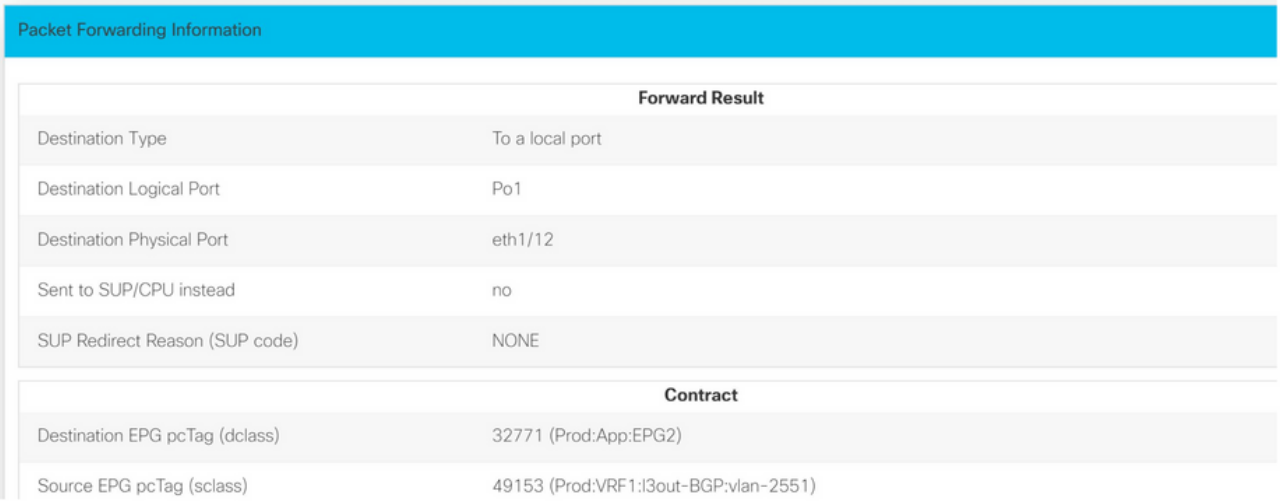
```
bdsol-aci32-leaf3# contract_parser.py --vrf Prod:VRF1
Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4]
[flags][contract:{str}] [hit=count]
[7:4339] [vrf:Prod:VRF1] permit ip icmp tn-Prod/ap-App/epg-EPG1(32770) pfx-0.0.0.0/0(15)
[contract:uni/tn-Prod/brc-ICMP2] [hit=0]
[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]
```

Confirmación de pcTag utilizado por el paquete mediante la aplicación ELAM Assistant

La aplicación ELAM Assistant ofrece otro método para confirmar el pcTag de origen y destino de los flujos de tráfico en vivo.

La captura de pantalla siguiente muestra el resultado de ELAM para el tráfico de pcTag 32771 a pcTag 49153.

Salida de la aplicación ELAM Assistant para src 32771 a dst 49153



Packet Forwarding Information

Forward Result	
Destination Type	To a local port
Destination Logical Port	Po1
Destination Physical Port	eth1/12
Sent to SUP/CPU instead	no
SUP Redirect Reason (SUP code)	NONE

Contract	
Destination EPG pcTag (dclass)	32771 (Prod:App:EPG2)
Source EPG pcTag (sclass)	49153 (Prod:VRF1:l3out-BGP:vlan-2551)

Conclusión

El uso de 0.0.0.0/0 debe ser seguido cuidadosamente dentro de un VRF ya que cada L3Out que utiliza esa subred heredará los contratos aplicados a cada otro L3Out que lo utiliza. Esto probablemente dará lugar a flujos de permisos no planificados.

L3Out compartida

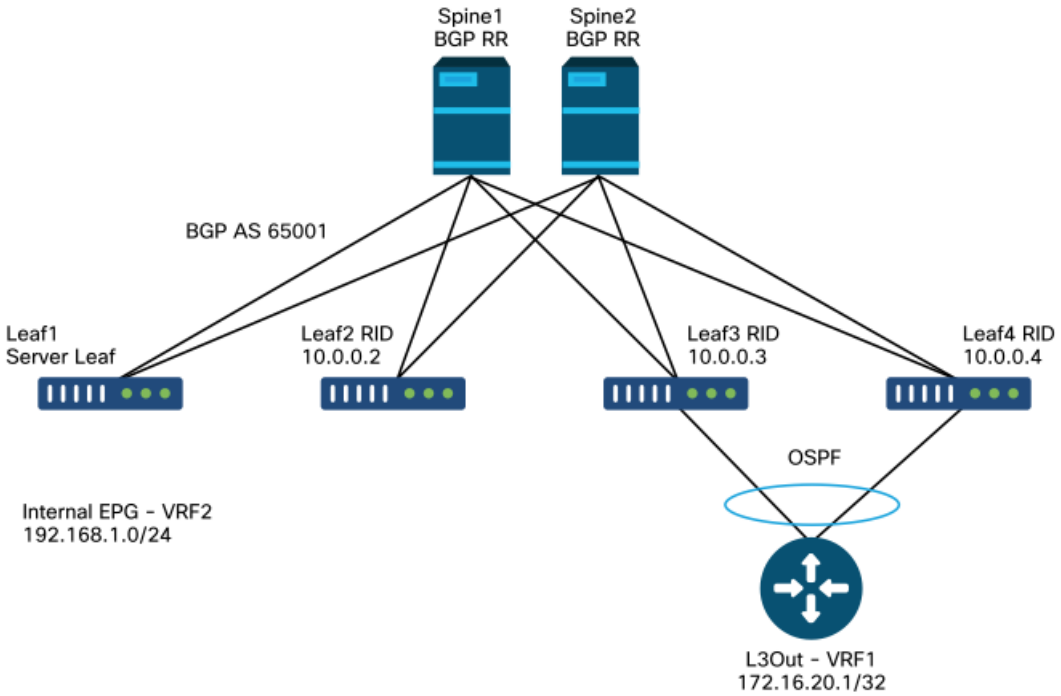
Overview

Esta sección discutirá cómo resolver problemas de anuncio de ruta en configuraciones L3Out compartidas. El término 'L3Out compartido' se refiere al escenario donde un L3Out está en un VRF pero un EPG interno que tiene un contrato con el L3Out está en otro VRF. Con las L3Outs compartidas, la fuga de rutas se realiza internamente al fabric de ACI.

Esta sección no profundizará en la resolución de problemas de políticas de seguridad. Para ello, consulte el capítulo "Políticas de seguridad" de este manual. Esta sección tampoco hablará en detalle sobre la clasificación de Prefijos de Política Externa por motivos de seguridad. Consulte la sección "Contrato y L3Out" en el capítulo "reenvío externo".

Esta sección utiliza la siguiente topología para nuestros ejemplos.

Topología L3Out compartida



En un nivel superior, deben existir las siguientes configuraciones para que una salida L3 compartida funcione:

- Una subred L3Out debe configurarse con el ámbito 'Subred de control de ruta compartida' para filtrar rutas externas en VRF internos. También se puede seleccionar la opción 'Compartido agregado' para filtrar todas las rutas que son más específicas que la subred configurada.
- Una subred L3Out debe configurarse con el ámbito 'Subred de importación de seguridad compartida' para programar las directivas de seguridad necesarias para permitir la comunicación a través de esta subred L3Out.
- La subred BD interna debe configurarse en 'Compartida entre VRFs' y 'Anunciar externamente' para programar la subred BD en el VRF externo y anunciarla.
- Se debe configurar un contrato de alcance 'tenant' o 'global' entre el EPG interno y el EPG externo del L3Out compartido.

En la siguiente sección se explicará en detalle cómo se anuncian y aprenden las rutas filtradas en ACI.

Flujo de trabajo de L3Out compartido: aprendizaje de rutas externas

En esta sección se describe la ruta de una ruta externa aprendida a medida que se anuncia en el fabric.

Ruta externa tal como se ve en la hoja de borde

Este comando mostrará la ruta externa aprendida de 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
```

A continuación, la ruta debe importarse en BGP. De forma predeterminada, todas las rutas externas deben importarse en BGP.

Verificaciones de BGP en la hoja de borde

La ruta debe estar en la familia de direcciones VPNv4 de BGP con un destino de ruta que se distribuirá por todo el fabric. El route-target es una comunidad BGP extendida exportada por el VRF externo e importada por cualquier VRF interno que necesite recibir la trayectoria.

Luego, verifique el route-target que está siendo exportado por el VRF externo en el 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
```

El resultado anterior muestra que cualquier trayectoria anunciada desde el VRF externo en VPNv4 debe recibir un route-target de 65001:2392068.

Luego, verifique la trayectoria 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
```

El resultado anterior muestra que la trayectoria tiene el route-target correcto. La trayectoria VPNv4 también se puede verificar mediante el comando 'show bgp vpnv4 unicast 172.16.20.1 vrf overlay-1'.

Verificaciones en la hoja del servidor

Para que la hoja de EPG interna instale la ruta anunciada por BL, debe importar el route-target (mencionado anteriormente) en el VRF interno. Se puede verificar el proceso BGP del VRF interno para validar esto:

```
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
```

El resultado anterior muestra el VRF interno que importa el route-target que es exportado por el VRF externo. Además, hay un 'Mapa de ruta de importación' al que se hace referencia. El route-map de importación incluye los prefijos específicos que se definen en el L3Out compartido con el indicador 'Subred de control de ruta compartida'.

El contenido del route-map se puede verificar para asegurarse de que incluye el prefijo externo:

```
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
```

El resultado anterior muestra el route-map de importación que incluye la subred que se va a importar.

Las verificaciones finales incluyen la comprobación de que la ruta está en la tabla BGP y que está instalada en la tabla de ruteo.

Tabla BGP en la hoja del servidor:

```
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 ruta se importa en la tabla interna de VRF BGP y tiene el route-target esperado.

Las rutas instaladas se pueden verificar:

```
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
```

El resultado anterior utiliza un comando específico 'vsh -c' para obtener el resultado 'detail'. El indicador 'detail' incluye el VNID de VXLAN de reescritura. Este es el VNID VXLAN del VRF externo. Cuando el BL recibe tráfico del plano de datos con este VNID, sabe que debe tomar la decisión de reenvío en el VRF externo.

El valor rw-vnid está en hexadecimal, por lo que al convertir a decimal se obtendrá el VRF VNID de 2392068. Busque el VRF correspondiente mediante 'show system internal epm vrf all | grep 2392068' en la hoja. Se puede realizar una búsqueda global en un APIC mediante el comando 'moquery -c fvCtx -f 'fv.Ctx.seg=="2392068"'".

La IP del siguiente salto también debe apuntar a los PTEPs BL y '%overlay-1' indica que la búsqueda de ruta para el siguiente salto está en el VRF de superposición.

Flujo de trabajo de L3Out compartido: anunciar rutas internas

Al igual que en las secciones anteriores, la publicación de subredes BD internas en una salida L3 compartida se gestiona de la siguiente manera:

- La subred BD (VRF interno) se instala en el BL (VRF externo) como ruta estática. Esta implementación de ruta estática es el resultado de la relación contractual entre el EPG interno y el L3Out.
- La ruta estática se redistribuye en el protocolo externo cuando el alcance 'Advertised Externally' se configura en la subred BD.

Verifique la ruta estática BD en el 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
```

Observe que en el resultado anterior el VNID del VRF interno está configurado para la reescritura. El salto siguiente también se establece en la dirección de difusión por proximidad proxy-v4.

La ruta anterior se anuncia externamente a través de los mismos mapas de ruta que se muestran en la sección "Anuncio de ruta".

Si una subred BD se establece en 'Advertise Externally', se redistribuye en **cada protocolo externo de L3Out** con el que el EPG interno tiene una relación de contrato.

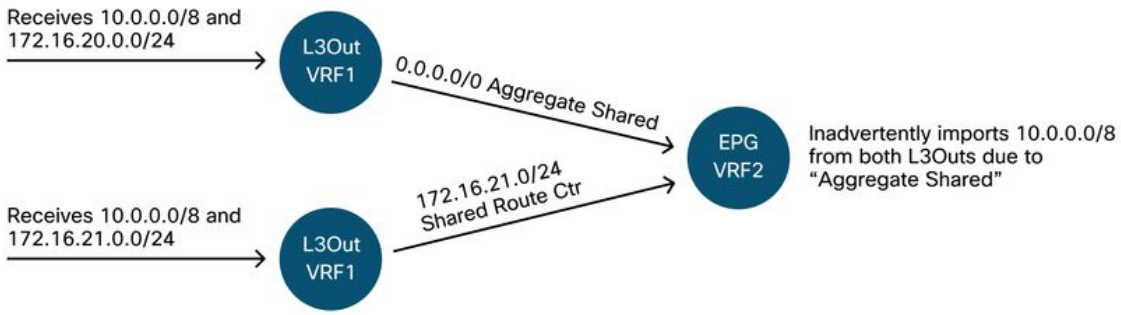
Escenario de solución de problemas de L3Out compartido: fuga de ruta inesperada

Este escenario tiene varias L3Outs en el VRF externo y un EPG interno está recibiendo una ruta de una L3Out donde la red **no está** definida con las opciones de alcance 'compartidas'.

Uso de 'Agregado compartido'

Tenga en cuenta la siguiente figura:

Pérdida de ruta inesperada



El mapa de importación BGP con la lista de prefijos programada desde los indicadores **'Subred de control de ruta compartida'** se aplica en el nivel VRF. Si un L3Out en VRF1 tiene una subred con 'Subred de control de ruta compartida', todas las rutas recibidas en L3Outs dentro de VRF1 que coincidan con esta subred de control de ruta compartida se importarán en VRF2.

El diseño anterior puede dar lugar a flujos de tráfico inesperados. Si no hay contratos entre el

EPG interno y el EPG L3Out de publicidad inesperada, habrá caídas de tráfico.

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

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

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