Fehlerbehebung: ACI External Forwarding

Inhalt

Einleitung

In diesem Dokument werden die Schritte zum Verständnis und zur Fehlerbehebung für einen L3out in der ACI beschrieben

Hintergrundinformationen

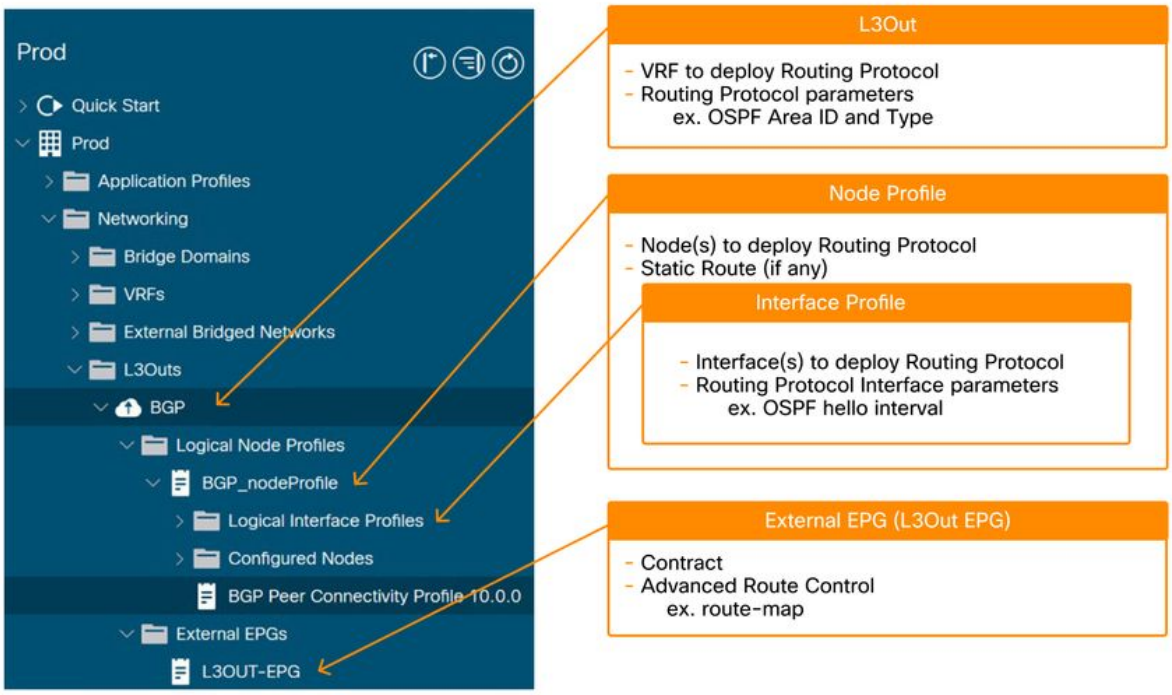
Das Material aus diesem Dokument wurde aus dem Buch Troubleshooting Cisco Application Centric Infrastructure, Second Edition (Fehlerbehebung) extrahiert, in dem es speziell um die **externe Weiterleitung (Übersicht, externe Weiterleitung - Nachbarschaften, externe Weiterleitung - Routenwerbung, externe Weiterleitung - Vertrag und L3out)** und **externe Weiterleitung - gemeinsame Nutzung von L3out-**Kapiteln geht.

Überblick

L3Out-Komponenten

Das folgende Bild zeigt die wichtigsten Bausteine, die für die Konfiguration eines L3-Outside (L3Out) erforderlich sind.

Hauptkomponenten eines L3Out



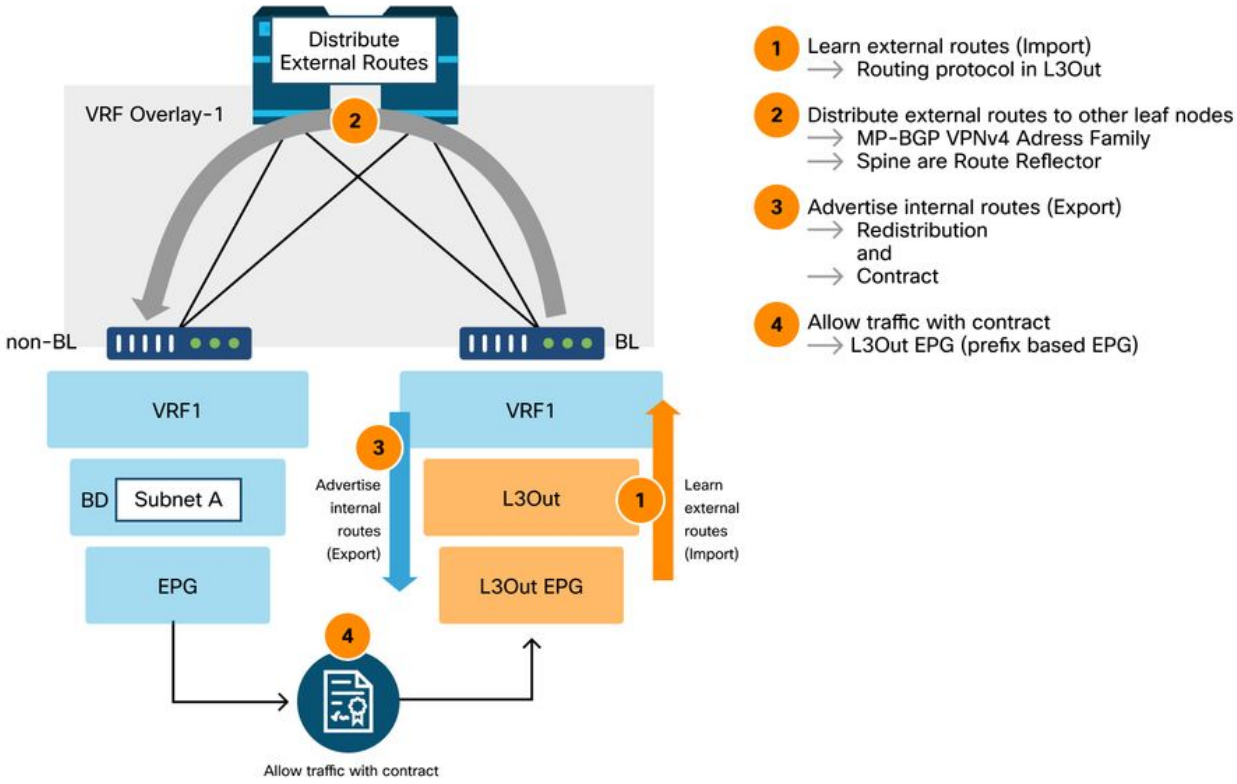
1. Root von L3Out: Wählen Sie ein bereitzustellendes Routing-Protokoll aus (z. B. OSPF, BGP).Wählen Sie eine VRF-Instanz aus, um das Routing-Protokoll bereitzustellen.Wählen Sie eine L3Out-Domäne aus, um die verfügbaren Leaf-Schnittstellen und das VLAN für das L3Out zu definieren.
2. Knotenprofil: Wählen Sie Leaf-Switches aus, um das Routing-Protokoll bereitzustellen. Diese werden üblicherweise als "Border Leaf Switches" (BL) bezeichnet.Konfigurieren Sie die Router-ID (RID) für das Routing-Protokoll auf jedem Grenz-Leaf. Anders als bei einem normalen Router weist die ACI die Router-ID nicht automatisch auf Basis der IP-Adresse des Switches zu.Konfigurieren Sie eine statische Route.

3. Schnittstellenprofil: Leaf-Schnittstellen zur Ausführung des Routing-Protokolls konfigurieren Schnittstellentyp (SVI, gerouteter Port, Subschnittstelle), Schnittstellen-ID und IP-Adressen usw.Wählen Sie eine Richtlinie für die Routing-Protokollparameter auf Schnittstellenebene aus (z. B. Hello-Intervall).
4. Externe EPG (L3Out-EPG): Eine "externe EPG" ist eine schwierige Anforderung, um alle mit dem L3Out verbundenen Richtlinien bereitzustellen, z. B. IP-Adressen oder SVIs, um Nachbarn zu bilden. Details zur Verwendung externer EPGs werden später erläutert.

Externes Routing

Das folgende Diagramm zeigt den übergeordneten Vorgang für externes Routing.

Externer Routing-Fluss auf hoher Ebene

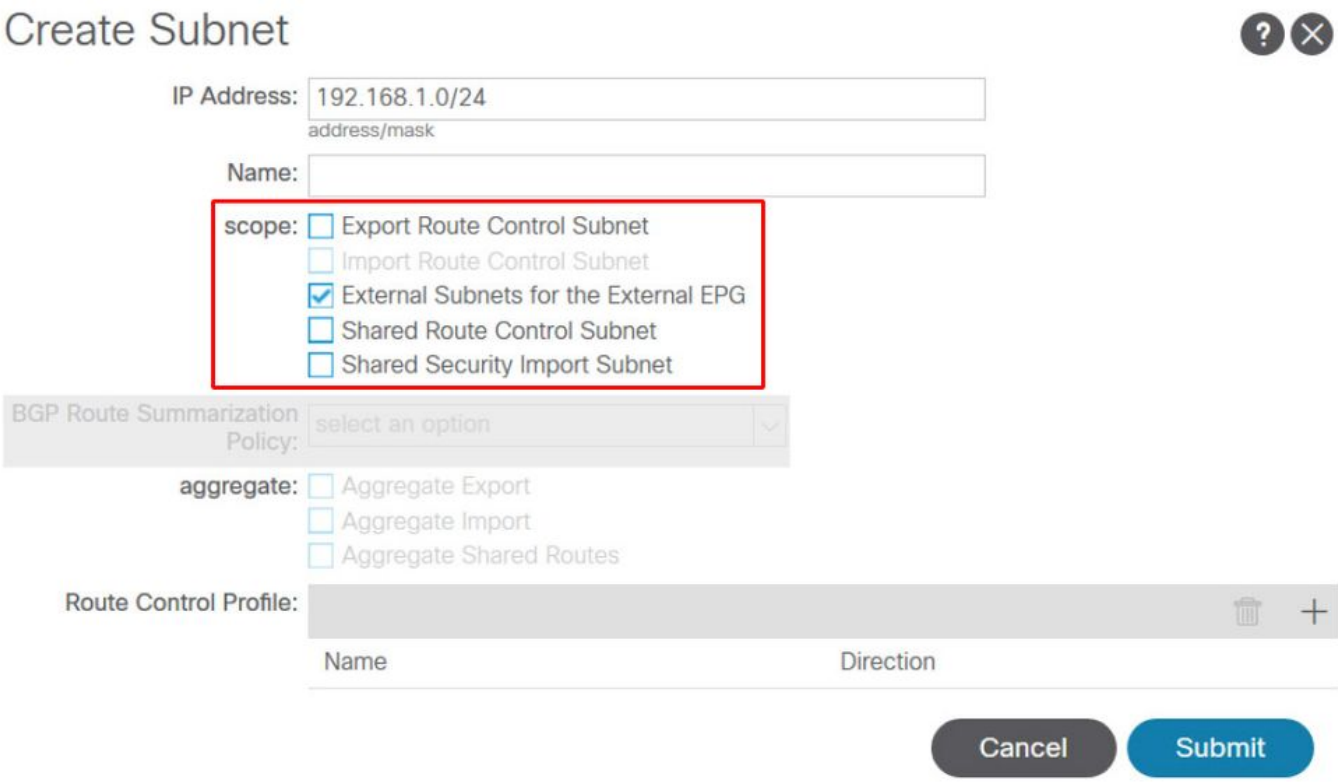


1. Die BLs stellen Routing-Protokoll-Nachbarschaften zu externen Routern her.
2. Routen-Präfixe werden von externen Routern empfangen und als Pfad zur VPNv4-Adressfamilie in das MP-BGP eingefügt. Mindestens zwei Spine-Knoten müssen als BGP-Routen-Reflektoren konfiguriert werden, um externe Routen zu allen Leaf-Knoten zu reflektieren.
3. Interne Präfixe (BD-Subnetze) und/oder Präfixe, die von anderen L3Out empfangen werden, müssen explizit im Routing-Protokoll neu verteilt werden, damit sie dem externen Router mitgeteilt werden.
4. Durchsetzung von Sicherheitsrichtlinien: Ein L3Out enthält mindestens eine L3Out-EPG. Ein Vertrag muss für die L3Out-EPG verwendet oder bereitgestellt werden (vom Klassennamen auch als l3extInstP bezeichnet), um den ein- und ausgehenden Datenverkehr aus dem L3Out zu ermöglichen.

L3Out EPG-Konfigurationsoptionen

Im Abschnitt zur L3Out-EPG können Subnetze mit einer Reihe von Optionen für "Umfang" und "Aggregation" definiert werden, wie unten gezeigt:

Ein L3Out-Subnetz, das definiert wird, einschließlich der Definition des Bereichs



Optionen für den Bereich:

- **Export Route Control Subnet (**Subnetz für die Exportroutensteuerung): In diesem Bereich wird ein Subnetz von der ACI über L3Out nach außen angekündigt (exportiert). Dies gilt zwar hauptsächlich für Transit-Routing, kann aber auch zum Ankündigen eines BD-Subnetzes verwendet werden, wie im Abschnitt "ACI BD-Subnetz-Ankündigung" beschrieben.
- **Import Route Control Subnet (Routensteuerungs-Subnetz importieren)**: In diesem Bereich wird ein externes Subnetz vom L3Out erlernt (importiert). Standardmäßig ist dieser Bereich deaktiviert, daher ist er ausgegraut, und ein Border Leaf (BL) lernt Routen von einem Routing-Protokoll. Dieser Bereich kann aktiviert werden, wenn externe Routen, die über OSPF und BGP empfangen werden, eingeschränkt werden müssen. Dies wird für EIGRP nicht unterstützt. Um diesen Bereich zu verwenden, muss 'Import Route Control Enforcement' (Durchsetzung der Routensteuerung importieren) zuerst für ein bestimmtes L3Out aktiviert werden.
- **Externe Subnetze für die externe EPG (import-security):** Dieser Bereich wird verwendet, um Pakete mit dem konfigurierten Subnetz von oder zu L3Out mit einem Vertrag zuzulassen. Es klassifiziert ein Paket anhand des Subnetzes in die konfigurierte L3Out-EPG, sodass ein Vertrag in der L3Out-EPG auf das Paket angewendet werden kann. Bei diesem Bereich handelt es sich um eine längste Präfixübereinstimmung, nicht um eine exakte Übereinstimmung wie bei anderen Bereichen für die Routing-Tabelle. Wenn 10.0.0.0/16 mit "Externen Subnetzen für die externe EPG" in L3Out-EPG A konfiguriert ist, werden alle

Pakete mit IP in diesem Subnetz, z. B. 10.0.1.1, in die L3Out-EPG A klassifiziert, um einen Vertrag darauf zu verwenden. Dies bedeutet nicht, dass "Externe Subnetze für die externe EPG" eine Route 10.0.0.0/16 in einer Routing-Tabelle installiert. Es wird eine andere interne Tabelle erstellt, in der ein Subnetz einer EPG (pcTag) zugeordnet wird, die nur einen Vertrag umfasst. Es hat keine Auswirkungen auf das Verhalten von Routing-Protokollen. Dieser Bereich muss für einen L3Out konfiguriert werden, der das Subnetz lernt.

- **Shared Route Control Subnet (Subnetz für gemeinsame Routenkontrolle)**: Dieser Bereich dient zum Weiterleiten eines externen Subnetzes an eine andere VRF-Instanz. Die ACI verwendet MP-BGP und Route Target, um eine externe Route von einer VRF-Instanz zu einer anderen zu leiten. Dieser Bereich erstellt eine Präfixliste mit dem Subnetz, die als Filter zum Exportieren/Importieren von Routen mit Routenziel im MP-BGP verwendet wird. Dieser Bereich muss für einen L3Out konfiguriert werden, der das Subnetz im ursprünglichen VRF lernt.
- **Shared Security Import Subnet (Gemeinsames Sicherheitsimport-Subnetz)**: Dieser Bereich wird verwendet, um Pakete mit dem konfigurierten Subnetz zuzulassen, wenn die Pakete über VRFs mit L3Out übertragen werden. Eine Route in einer Routing-Tabelle wird an eine andere VRF-Instanz mit "Shared Route Control Subnet" weitergeleitet, wie oben erwähnt. Einer anderen VRF-Instanz muss jedoch noch bekannt sein, zu welcher EPG die durchgesickerte Route gehören soll. Das "Shared Security Import Subnet" informiert eine andere VRF-Instanz der L3Out-EPG, zu der die geleakte Route gehört. Daher kann dieser Bereich nur verwendet werden, wenn auch "Externe Subnetze für die externe EPG" verwendet wird, da die ursprüngliche VRF-Instanz sonst nicht weiß, zu welcher L3Out-EPG das Subnetz gehört. Dieser Bereich ist auch die längste Präfixübereinstimmung.

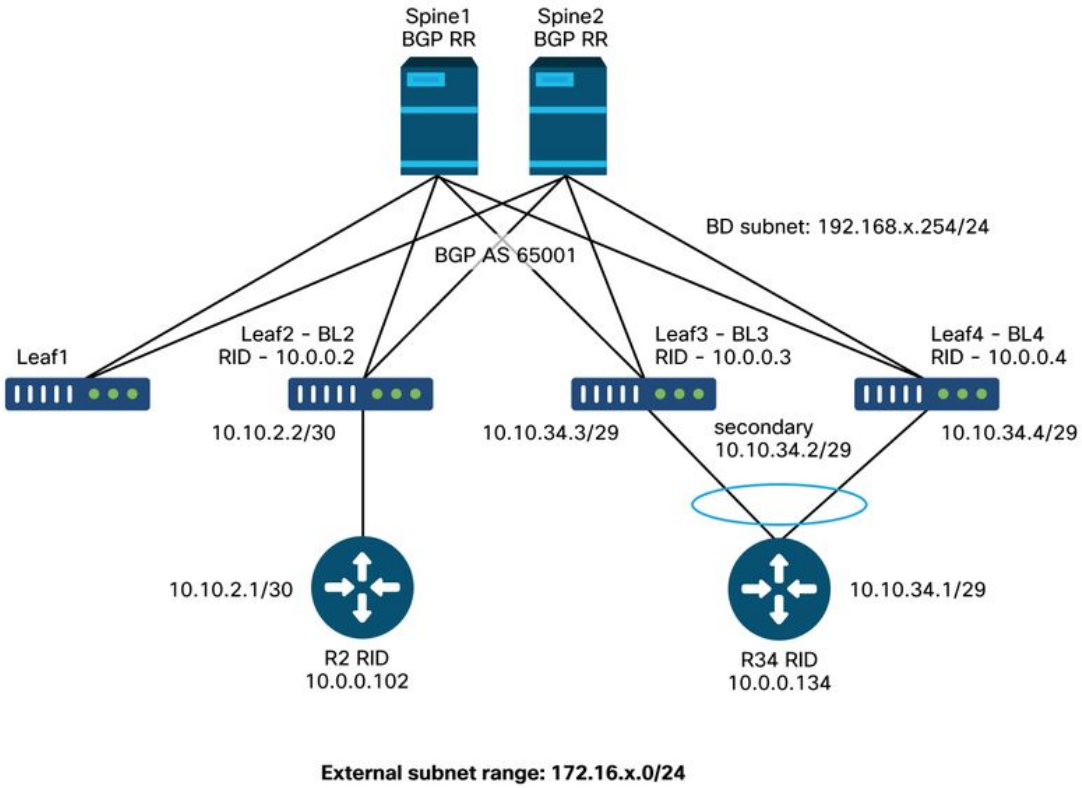
Aggregatoptionen:

- **Aggregatexport:** Diese Option kann nur für 0.0.0.0/0 mit "Export Route Control Subnet" verwendet werden. Wenn sowohl "Export Route Control Subnet" als auch "Aggregate Export" für 0.0.0.0/0 aktiviert sind; erstellt es eine Präfixliste mit '0.0.0.0/0 le 32', die mit allen Subnetzen übereinstimmt. Daher kann diese Option verwendet werden, wenn ein L3Out Routen nach außen ankündigen (exportieren) muss. Wenn eine detailliertere Aggregation erforderlich ist, kann Route Map/Profile mit einer expliziten Präfixliste verwendet werden.
- **Aggregatimport:** Diese Option kann nur für 0.0.0.0/0 mit "Import Route Control Subnet" verwendet werden. Wenn sowohl 'Import Route Control Subnet' als auch 'Aggregate Import' für 0.0.0.0/0 aktiviert sind, wird eine Präfixliste mit '0.0.0.0/0 le 32' erstellt, die mit allen Subnetzen übereinstimmt. Daher kann diese Option verwendet werden, wenn ein L3Out beliebige Routen von außen lernen (importieren) muss. Dasselbe kann jedoch erreicht werden, indem 'Import Route Control Enforcement' deaktiviert wird, was die Standardeinstellung ist. Wenn eine detailliertere Aggregation erforderlich ist, kann Route Map/Profile mit einer expliziten Präfixliste verwendet werden.
- **Gemeinsam genutzte Routen aggregieren:** Diese Option kann für alle Subnetze mit "Shared Route Control Subnet" verwendet werden. Wenn sowohl 'Shared Route Control Subnet' als auch 'Aggregate Shared Routes' für 10.0.0.0/8 aktiviert sind, wird eine Präfixliste mit '10.0.0.0/8 le 32' erstellt, die 10.0.0.0/8, 10.1.0.0/16 usw. entspricht.

In diesem Abschnitt verwendete L3Out-Topologie

In diesem Abschnitt wird die folgende Topologie verwendet:

L3Out-Topologie



Nachbarschaften

In diesem Abschnitt wird die Fehlerbehebung und Überprüfung der Routing-Protokoll-Nachbarschaften an L3Out-Schnittstellen erläutert.

Nachfolgend sind einige zu überprüfende Parameter aufgeführt, die für alle externen ACI-Routing-Protokolle gelten:

- **Router-ID:** In der ACI muss jedes L3Out dieselbe Router-ID in derselben VRF-Instanz auf demselben Leaf verwenden, selbst wenn sich die Routing-Protokolle unterscheiden. Außerdem kann nur einer dieser L3Outs auf demselben Leaf ein Loopback mit der Router-ID erstellen, bei der es sich in der Regel um BGP handelt.
- **MTU:** Obwohl die MTU nur für die OSPF-Adjacency dringend erforderlich ist, wird empfohlen, die MTU für alle Routing-Protokolle anzupassen, um sicherzustellen, dass alle für den Routenaustausch bzw. die Routenaktualisierungen verwendeten Jumbo-Pakete ohne Fragmentierung übertragen werden können, da die meisten Kontrollebenen-Frames mit festgelegtem DF-Bit gesendet werden (nicht fragmentieren). Dadurch wird der Frame verworfen, wenn seine Größe die maximale MTU der Schnittstelle überschreitet.
- **MP-BGP Router-Reflektor**: Andernfalls startet der BGP-Prozess nicht auf Leaf-Knoten. OSPF oder EIGRP müssen dies nicht nur zur Einrichtung eines Nachbarn, sondern auch für BLs zur Verteilung externer Routen an andere Leaf-Knoten durchführen.
- **Fehler:** Überprüfen Sie die Fehler immer während und nach der Konfiguration.

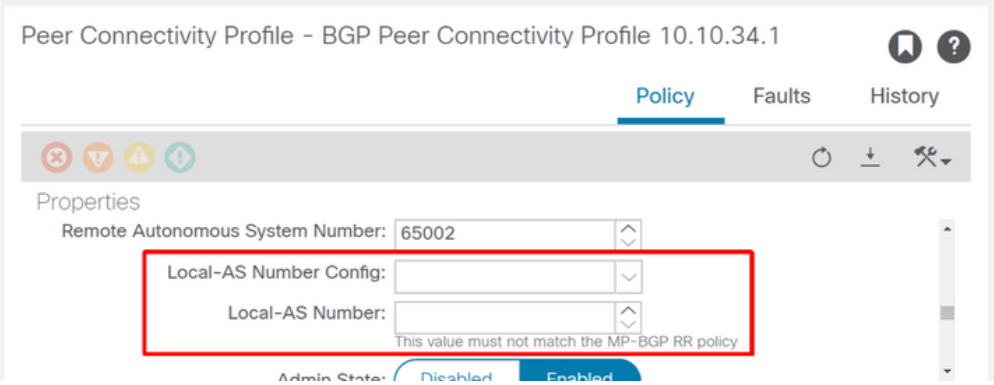
BGP

In diesem Abschnitt wird ein Beispiel für ein eBGP-Peering zwischen dem Loopback auf BL3, BL4 und R34 aus der Topologie im Abschnitt Overview verwendet. BGP AS auf R34 ist 65002.

Überprüfen Sie beim Einrichten einer BGP-Adjacency die folgenden Kriterien.

- Lokale BGP-AS-Nummer (ACI-BL-Seite)

Peer-Verbindungsprofil - Lokal-AS

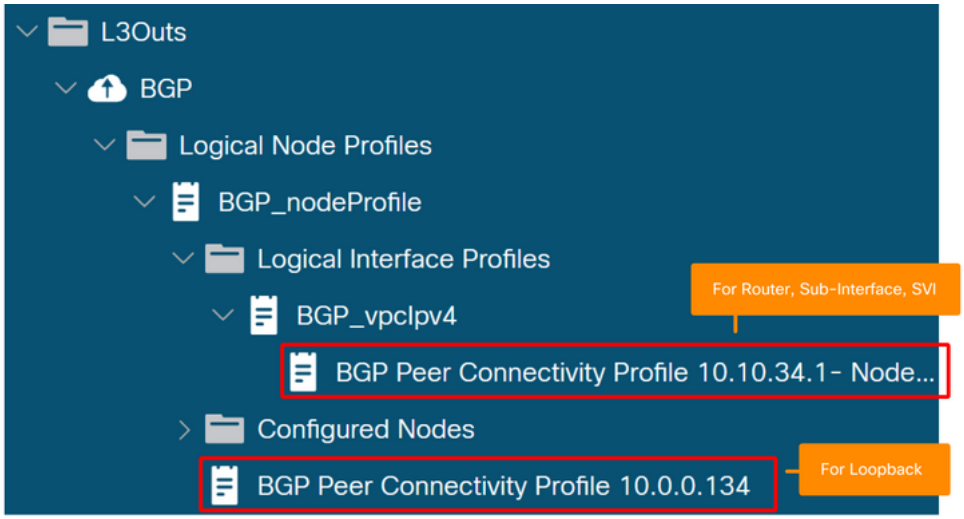


Die BGP-AS-Nummer eines Benutzer-L3Out entspricht automatisch der BGP-AS-Nummer für das infra-MP-BGP, das in der BGP-Routen-Reflektorrichtlinie konfiguriert wurde. Die Konfiguration des lokalen AS im BGP-Peer-Anschlussprofil ist nur erforderlich, wenn das ACI-BGP-AS nach außen getarnt werden muss. Das bedeutet, dass externe Router auf das im BGP-Routen-Reflektor konfigurierte BGP AS verweisen müssen.

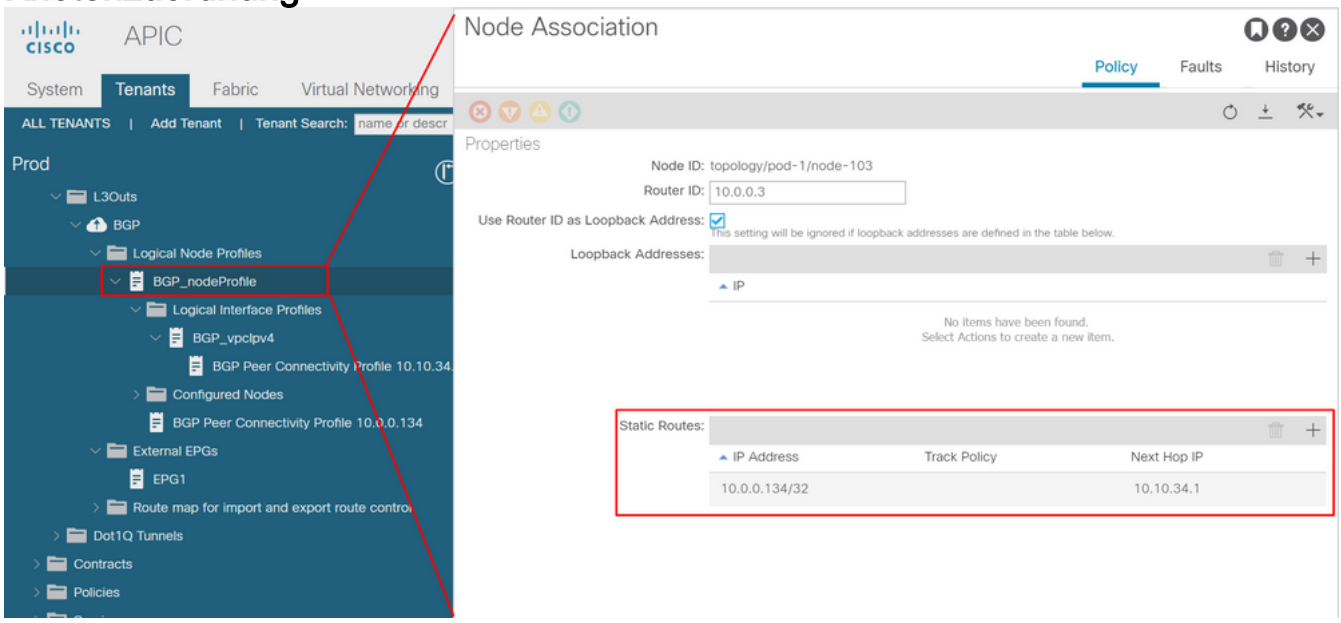
HINWEIS - Das Szenario, in dem eine lokale AS-Konfiguration erforderlich ist, entspricht dem eigenständigen NX-OS-Befehl "local-as".

- Remote-BGP-AS-Nummer (externe Seite) **Peer-Verbindungsprofil - Remote-AS**

Die Remote-BGP-AS-Nummer ist nur für eBGP erforderlich, bei dem sich das BGP-AS des Nachbarn vom ACI-BGP-AS unterscheidet.Quell-IP für BGP-Peer-Sitzung.**L3Out - BGP-Peer-Verbindungsprofil**



Die ACI unterstützt das Sourcing einer BGP-Sitzung über die Loopback-Schnittstelle und einen typischen ACI L3Out-Schnittstellentyp (geroutet, Subschnittstelle, SVI).Wenn eine BGP-Sitzung von einem Loopback ausgeht, konfigurieren Sie das BGP-Peer-Verbindungsprofil unter dem logischen **Knoten-**Profil.Wenn die BGP-Sitzung von einer gerouteten/untergeordneten Schnittstelle/SVI stammen muss, konfigurieren Sie das BGP-Peer-Verbindungsprofil unter dem logischen **Schnittstellenprofil**.IP-Verfügbarkeit des BGP-Peers.**Logisches Knotenprofil - Knotenzuordnung**



Wenn es sich bei den BGP-Peer-IPs um Loopbacks handelt, stellen Sie sicher, dass das BL und der externe Router mit der IP-Adresse des Peers erreichbar sind. Statische Routen oder OSPF können verwendet werden, um die Erreichbarkeit der Peer-IPs zu gewährleisten.**BGP-CLI-Verifizierung (eBGP mit Loopback-Beispiel)**Die CLI-Ausgaben für die folgenden Schritte werden in BL3 in der Topologie im Abschnitt Overview erfasst.**1. Überprüfen Sie, ob die BGP-Sitzung hergestellt wurde.**'State/PfxRcd' in der folgenden CLI-Ausgabe bedeutet, dass die BGP-Sitzung eingerichtet wird.

```
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
```

Wenn für "State/PfxRcd" die Einstellung Idle (Inaktiv) oder Active (Aktiv) angezeigt wird, werden BGP-Pakete noch nicht mit dem Peer ausgetauscht. Überprüfen Sie in einem solchen Szenario Folgendes, und fahren Sie mit dem nächsten Schritt fort.

- Stellen Sie sicher, dass der externe Router korrekt auf das ACI BGP AS verweist (lokale AS-Nummer 65001).
- Stellen Sie sicher, dass im ACI-BGP-Peer-Verbindungsprofil die richtige Nachbar-IP-Adresse angegeben ist, von der der externe Router die BGP-Sitzung bezieht (10.0.0.134).
- Stellen Sie sicher, dass im ACI-BGP-Peer-Konnektivitätsprofil der richtige Nachbar-AS des externen Routers angegeben ist (Remote Autonomous System Number in GUI, wird in CLI als AS 65002 angezeigt).

2. Überprüfen Sie die BGP-Nachbardaten (BGP-Peer-Konnektivitätsprofil)

Der folgende Befehl zeigt die Parameter, die für die Einrichtung des BGP-Nachbarn von entscheidender Bedeutung sind.

- IP des Nachbarn: 10.0.0.134.
- BGP-AS des Nachbarn: Remote AS 65002.
- Quell-IP: Loopback3 wird als Update-Adresse verwendet.
- eBGP-Multi-Hop: Der externe BGP-Peer kann bis zu 2 Hops entfernt sein.

```
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
```

Sobald der BGP-Peer richtig eingerichtet wurde, werden der 'Lokale Host' und der 'Ausländische Host' unten in der Ausgabe angezeigt.

3. Überprüfung der IP-Verfügbarkeit für den BGP-Peer

```
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
```

Stellen Sie sicher, dass der Ping an die benachbarte IP-Adresse von der Quell-IP des ACI-BGP aus funktioniert.

```
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. Überprüfen Sie die gleiche Sache auf dem externen Router

Nachfolgend finden Sie ein Konfigurationsbeispiel für den externen Router (Standalone NX-OS).

```
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. Zusätzlicher Schritt — tcpdump

Auf ACI-Leaf-Knoten kann das tcpdump-Tool die CPU-Schnittstelle "kpm_inb" abfragen, um zu überprüfen, ob die Protokollpakete die Leaf-CPU erreicht haben. Verwenden Sie den L4-Port 179 (BGP) als Filter.

```
f2-leaf3# tcpdump -ni kpm_inb port 179
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```

```
listening on kpm_inb, link-type EN10MB (Ethernet), capture size 65535 bytes
20:36:58.292903 IP 10.0.0.134.179 > 10.0.0.3.34873: Flags [P.], seq 3775831990:3775832009, ack
807595300, win 3650, length 19: BGP, length: 19
20:36:58.292962 IP 10.0.0.3.34873 > 10.0.0.134.179: Flags [.], ack 19, win 6945, length 0
20:36:58.430418 IP 10.0.0.3.34873 > 10.0.0.134.179: Flags [P.], seq 1:20, ack 19, win 6945,
length 19: BGP, length: 19
20:36:58.430534 IP 10.0.0.134.179 > 10.0.0.3.34873: Flags [.], ack 20, win 3650, length 0
```

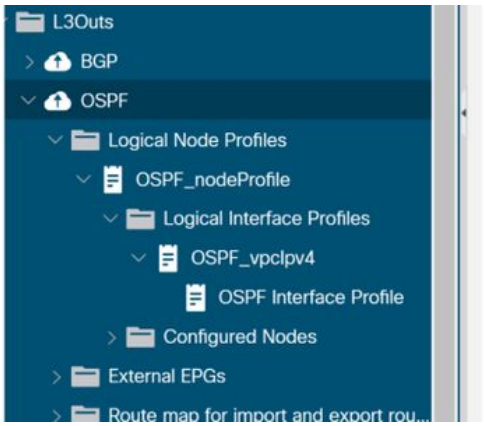
OSPF

In diesem Abschnitt wird ein Beispiel für OSPF-Nachbarschaften zwischen BL3, BL4 und R34 aus der Topologie im Abschnitt Overview mit OSPF AreaID 1 (NSSA) verwendet.

Im Folgenden sind die allgemeinen Kriterien für die Prüfung der OSPF-Adjacency-Einrichtung aufgeführt.

- OSPF-Area-ID und -Typ

L3Out - OSPF-Schnittstellenprofil - Area-ID und Typ



Wie jedes Routing-Gerät müssen OSPF-Area-ID und -Typ auf beiden Nachbarn übereinstimmen. Einige spezifische ACI-Einschränkungen für OSPF Area-ID-Konfigurationen:

- Ein L3Out kann nur eine OSPF-Area-ID haben.
- Zwei L3Outs können die gleiche OSPF Area-ID in derselben VRF-Instanz nur dann verwenden, wenn sie sich auf zwei verschiedenen Leaf-Knoten befinden.

Obwohl die OSPF-ID nicht Backbone 0 sein muss, ist sie beim Transit-Routing zwischen zwei OSPF-L3Outs auf demselben Leaf erforderlich. Einer von ihnen muss den OSPF-Bereich 0 verwenden, da jeder Routenaustausch zwischen OSPF-Bereichen über den OSPF-Bereich 0 erfolgen muss.

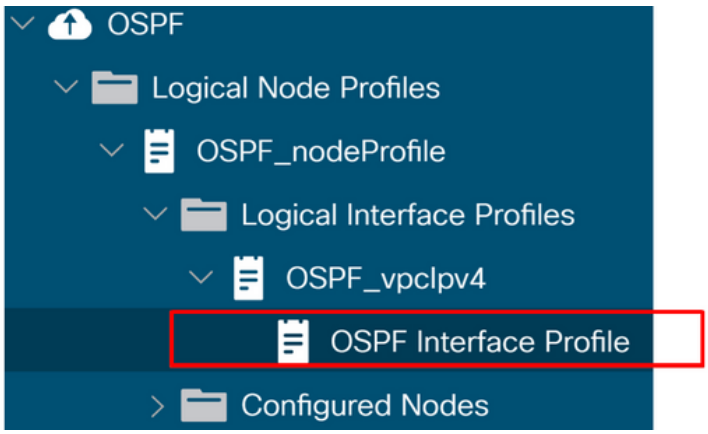
- MTU

Logisches Schnittstellenprofil - SVI

Der Standard-MTU-Wert für die ACI beträgt 9.000 Byte statt 1.500 Byte. Dies ist in der Regel der Standard für herkömmliche Routing-Geräte. Stellen Sie sicher, dass die MTU mit dem externen Gerät übereinstimmt. Wenn die Einrichtung von OSPF-Nachbarn aufgrund der MTU fehlschlägt, bleibt sie bei EXCHANGE/DROTHER hängen.

- IP-Subnetzmaske OSPF erfordert, dass die IP-Nachbaradresse dieselbe Subnetzmaske verwendet.
- OSPF-Schnittstellenprofil.

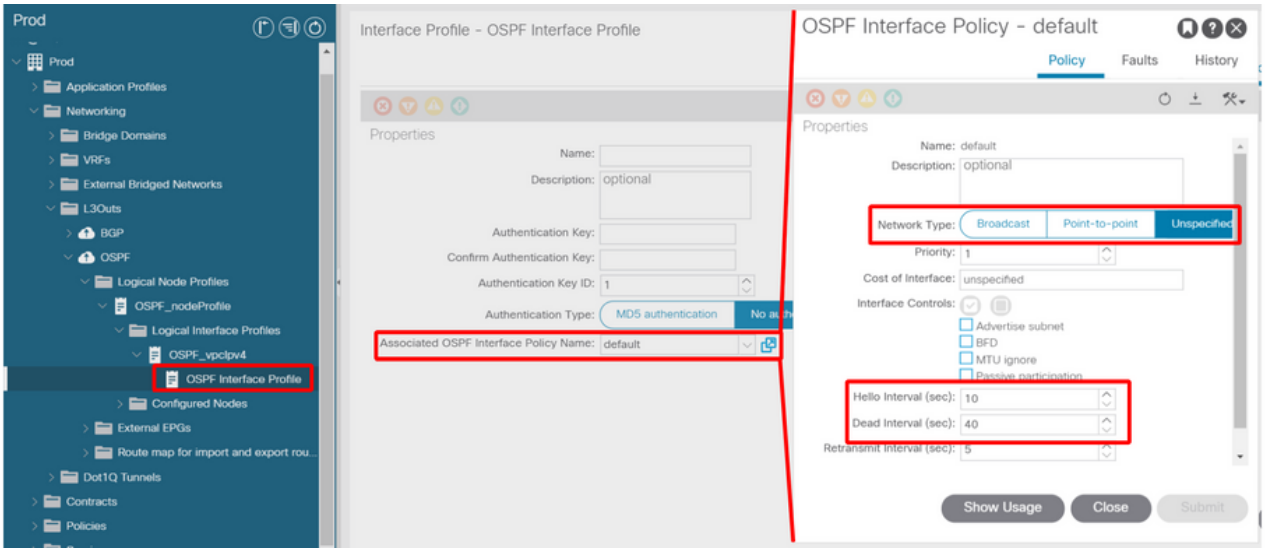
OSPF-Schnittstellenprofil



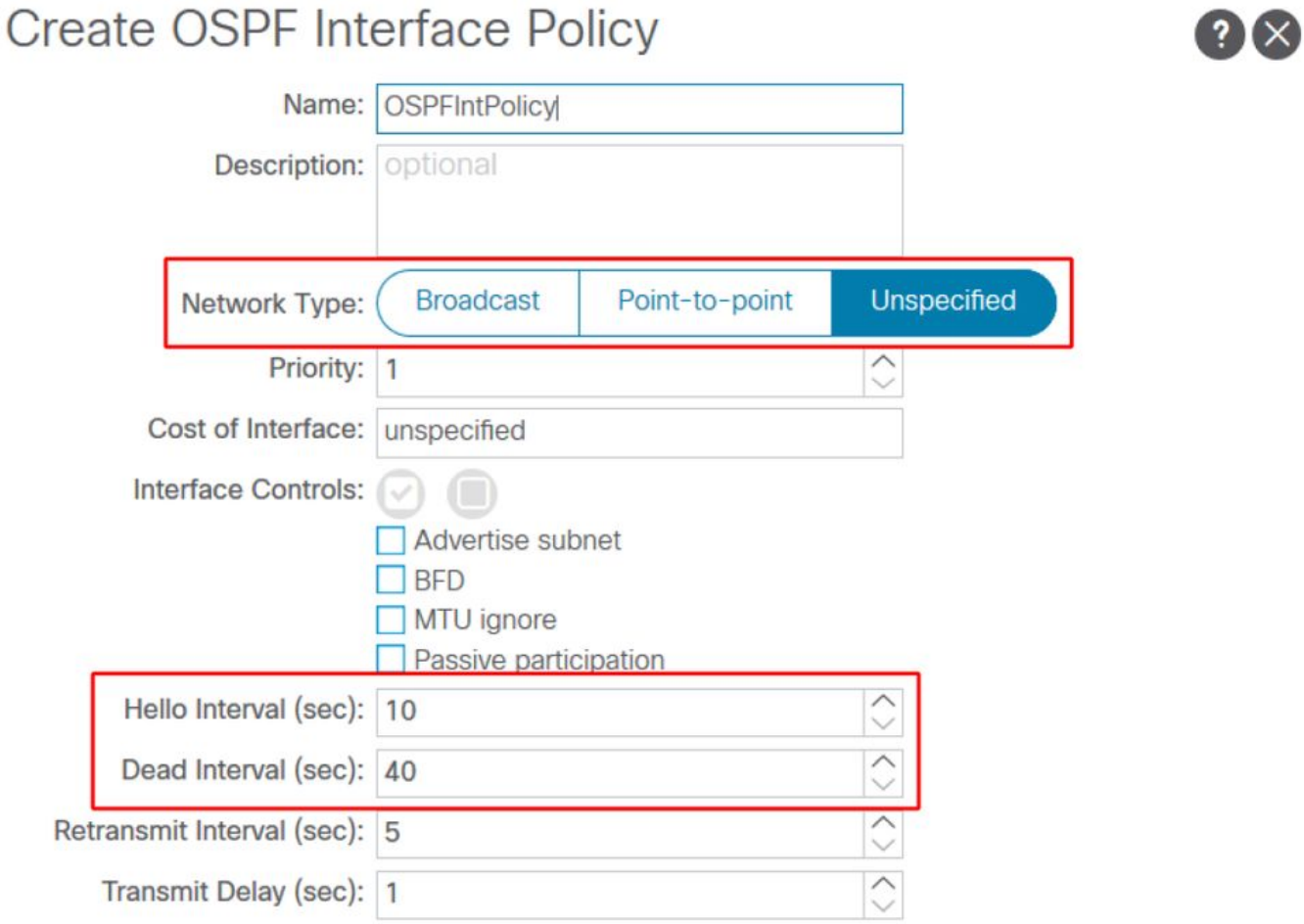
Dies entspricht "ip router ospf <tag> area <Area-ID>" in einer eigenständigen NX-OS-Konfiguration, um OSPF auf der Schnittstelle zu aktivieren. Andernfalls treten die Leaf-Schnittstellen nicht dem OSPF bei.

- OSPF Hello-/Dead-Timer, Netzwerktyp

OSPF-Schnittstellenprofil - Hello-/Dead-Timer und Netzwerktyp



Einzelheiten der OSPF-Schnittstellenrichtlinie



Für OSPF müssen die Hello- und Dead-Timer auf jedem benachbarten Gerät übereinstimmen. Diese werden im OSPF-Schnittstellenprofil konfiguriert.

Stellen Sie sicher, dass der Netzwerktyp der OSPF-Schnittstelle mit dem externen Gerät übereinstimmt. Wenn das externe Gerät den Typ Point-to-Point verwendet, muss auf ACI-Seite auch Point-to-Point explizit konfiguriert werden. Diese werden auch im OSPF-Schnittstellenprofil konfiguriert.

OSPF CLI-Verifizierung

Die CLI-Ausgaben in den folgenden Schritten werden aus BL3 im Abschnitt "Topologie" des Abschnitts "Übersicht" erfasst.

1. Überprüfen Sie den OSPF-Nachbarstatus.

Wenn der Status in der folgenden CLI "FULL" lautet, wird der OSPF-Nachbar korrekt eingerichtet. Andernfalls fahren Sie mit dem nächsten Schritt fort, um die Parameter zu überprüfen.

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

In der ACI bilden die BLs OSPF-Nachbarschaften miteinander über den externen Routern, wenn sie dieselbe VLAN-ID mit einer SVI verwenden. Der Grund hierfür ist, dass die ACI über eine interne Flooding-Domäne mit der Bezeichnung L3Out BD (oder External BD) für jede VLAN-ID in den L3Out-SVIs verfügt. Beachten Sie, dass die VLAN-ID 28 ein internes VLAN mit der Bezeichnung PI-VLAN (Platform-Independent VLAN) ist und nicht das tatsächliche VLAN (Access Encap VLAN). Verwenden Sie den folgenden Befehl, um das Access Encap-VLAN ('vlan-2502') zu überprüfen.

```
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
```

Die gleiche Ausgabe kann auch über die VLAN-ID des Access Encaps erzielt werden.

```
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. OSPF-Bereich überprüfen

Stellen Sie sicher, dass OSPF-Area-ID und -Type mit den Nachbarn identisch sind. Wenn das OSPF-Schnittstellenprofil fehlt, wird die Schnittstelle nicht zu OSPF hinzugefügt und nicht in der OSPF-CLI-Ausgabe angezeigt.

```
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. Überprüfen Sie die OSPF-Schnittstellendetails.

Stellen Sie sicher, dass die Parameter auf Schnittstellenebene die Anforderungen für die Einrichtung von OSPF-Nachbarn erfüllen, z. B. IP-Subnetz, Netzwerktyp und Hello/Dead Timer. Beachten Sie die VLAN-ID, um die SVI als IP-VLAN (vlan28) anzugeben.

```
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. IP-Erreichbarkeit des Nachbarn prüfen

Obwohl es sich bei OSPF-Hello-Paketen um lokale Link-Multicast-Pakete handelt, handelt es sich bei den für den ersten OSPF-LSDB-Austausch erforderlichen OSPF-DBD-Paketen um Unicast. Aus diesem Grund muss die Unicast-Erreichbarkeit auch für die OSPF-Nachbarschaft überprüft werden.

```
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. Dasselbe auf dem externen Router überprüfen

Nachfolgend finden Sie Beispiele für Konfigurationen auf dem externen Router (Standalone NX-OS).

```
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
```

Überprüfen Sie die MTU-Größe auch an der physischen Schnittstelle.

6. Zusätzlicher Schritt — tcpdump

Auf ACI-Leaf-Knoten kann der Benutzer tcpdump für die CPU-Schnittstelle "kpm_inb" ausführen, um zu überprüfen, ob die Protokollpakete die Leaf-CPU erreicht haben. Obwohl es mehrere Filter für OSPF gibt, ist die IP-Protokollnummer der umfassendste Filter.

- IP-Protokollnummer: proto 89 (IPv4) oder ip6 proto 0x59 (IPv6)
- IP-Adresse des Nachbarn: Host <ip>
- Lokale MCAST-IP für OSPF-Verbindung: Host 224.0.0.5 oder 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
```

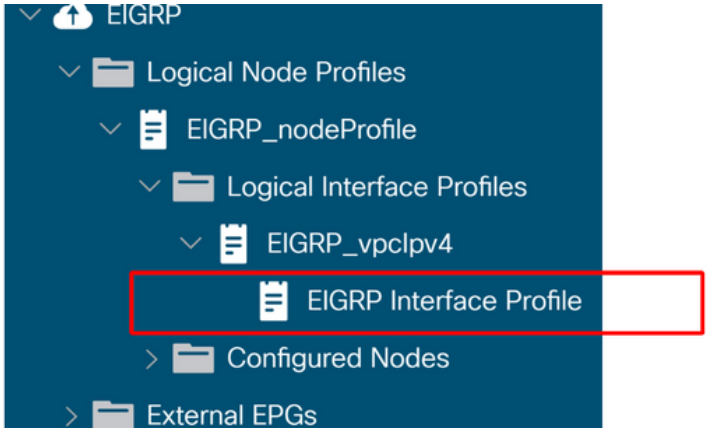
EIGRP

In diesem Abschnitt wird ein Beispiel für eine EIGRP-Nachbarschaft zwischen BL3, BL4 und R34 aus der Topologie im Abschnitt "Übersicht" mit EIGRP AS 10 verwendet.

Im Folgenden werden die allgemeinen Kriterien für den Aufbau der EIGRP-Adjacency aufgeführt.

- EIGRP AS: L3Out wird ein EIGRP-AS zugewiesen. Dies muss mit dem externen Gerät übereinstimmen.
- EIGRP-Schnittstellenprofil.

EIGRP-Schnittstellenprofil



Dies entspricht der Konfiguration "ip router eigrp <as>" auf einem eigenständigen NX-OS-Gerät. Andernfalls treten die Leaf-Schnittstellen nicht dem EIGRP bei.

- MTU

Obwohl dies nicht übereinstimmen muss, um einfach die EIGRP-Nachbarschaft einzurichten, können die EIGRP-Topologieaustauschpakete größer werden als die maximal zulässige MTU an den Schnittstellen zwischen den Peers. Da diese Pakete nicht fragmentiert werden dürfen, werden sie verworfen, und die EIGRP-Nachbarschaft flattert.

EIGRP CLI-Verifizierung

Die CLI-Ausgaben in den folgenden Schritten werden aus BL3 in der Topologie im Abschnitt "Overview" (Übersicht) erfasst.

1. EIGRP-Nachbarstatus überprüfen

```
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
```

Bei der ACI bilden die BLs eine EIGRP-Nachbarschaft zueinander auf den externen Routern, wenn sie dieselbe VLAN-ID mit der SVI verwenden. Der Grund hierfür ist, dass eine ACI über eine interne Flooding-Domäne mit der Bezeichnung L3Out BD (oder External BD) für jede VLAN-ID in L3Out-SVIs verfügt.

Beachten Sie, dass die VLAN-ID 29 ein internes VLAN mit der Bezeichnung PI-VLAN (Platform-Independent VLAN) ist und nicht das tatsächliche VLAN (Access Encap VLAN), das über eine Leitung verwendet wird. Verwenden Sie den folgenden Befehl, um das Access Encap-VLAN (vlan-2503) zu überprüfen.

```
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
```

Die gleiche Ausgabe kann auch über die VLAN-ID des Access Encaps erzielt werden.

```
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. Überprüfen Sie die EIGRP-Schnittstellendetails.

Stellen Sie sicher, dass EIGRP auf der erwarteten Schnittstelle ausgeführt wird. Wenn nicht, aktivieren Sie das Kontrollkästchen Logical Interface Profile (Logisches Schnittstellenprofil) und EIGRP Interface Profile (EIGRP-Schnittstellenprofil).

```
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. Überprüfen Sie dasselbe auf dem externen Router.

Nachfolgend finden Sie die Beispielkonfiguration für den externen Router (Standalone NX-OS).

```
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. Zusätzlicher Schritt — tcpdump

Auf ACI-Leaf-Knoten kann der Benutzer tcpdump für die CPU-Schnittstelle "kpm_inb" ausführen, um zu überprüfen, ob die Protokollpakete die CPU des Leaf erreicht haben. Verwenden Sie das IP-Protokoll 88 (EIGRP) als Filter.

```
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
```

Routenankündigung

Dieser Abschnitt befasst sich mit der Verifizierung und Fehlerbehebung von Routing-Meldungen in der ACI. Konkret geht es dabei um folgende Beispiele:

- Bridge-Domänen-Subnetzanzeige.
- Verkehrsweganzeige.
- Import- und Exportroutensteuerung

In diesem Abschnitt wird das Route Leaking für gemeinsam genutzte L3Outs in späteren Abschnitten beschrieben.

Bridge-Domänenrouten-Ankündigungsworkflow

Bevor Sie sich die gängige Fehlerbehebung ansehen, sollten Sie sich damit vertraut machen, wie die Bridge-Domänenankündigung funktionieren soll.

BD-Werbung, wenn sich BD und L3Out in derselben VRF-Instanz befinden, umfasst:

- Es besteht eine Vertragsbeziehung zwischen dem L3Out und der internen EPG.
- Verknüpfen des L3Out mit der Bridge-Domäne
- Wählen Sie im BD-Subnetz die Option "Extern anzeigen" aus.

Darüber hinaus ist es auch möglich, die Bridge-Domänenankündigung mithilfe von Export-Routenprofilen zu steuern, die verhindern, dass L3Out zugeordnet werden muss. Dennoch sollte 'Extern werben' ausgewählt werden. Dies ist ein weniger verbreiteter Anwendungsfall, daher wird hier nicht darauf eingegangen.

Die Vertragsbeziehung zwischen dem L3Out und der EPG ist erforderlich, um zu bewirken, dass die BD-weite statische Route an das BL übertragen wird. Die eigentliche Routen-Advertisement erfolgt über die Umverteilung der statischen Route in das externe Protokoll. Schließlich werden die Weiterverteilungs-Route-Maps nur innerhalb der L3Outs installiert, die dem BD zugeordnet sind. Auf diese Weise wird die Route nicht aus allen L3Outs bekannt gegeben.

In diesem Fall lautet das BD-Subnetz 192.168.1.0/24 und sollte über OSPF L3Out angekündigt werden.

Vor Anwendung des Vertrags zwischen dem L3Out und der internen EPG

```
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
```

Beachten Sie, dass die BD-Route im BL noch nicht vorhanden ist.

Nach Anwendung des Vertrags zwischen dem L3Out und der internen EPG

An diesem Punkt wurde keine andere Konfiguration vorgenommen. Das L3Out ist noch nicht mit dem BD verknüpft und das Flag 'Extern anzeigen' ist noch nicht gesetzt.

```
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
```

Beachten Sie, dass die BD-Subnetz-Route (gekennzeichnet durch das universelle Flag) jetzt auf dem BL bereitgestellt wird. Beachten Sie jedoch, dass die Route mit Tags versehen ist. Dieser Tag-Wert ist ein impliziter Wert, der BD-Routen vor der Konfiguration mit "Extern bekannt geben" zugewiesen wird. Alle externen Protokolle verweigern die Neuverteilung dieses Tags.

Nach der Auswahl von "Extern anzeigen" im BD-Subnetz

Das L3Out wurde noch nicht mit dem BD verknüpft. Beachten Sie jedoch, dass das Tag gelöscht wurde.

```
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
```

An diesem Punkt wird die Route immer noch nicht extern angekündigt, da es keine Route-Map und Präfix-Liste gibt, die mit diesem Präfix für die Neuverteilung in das externe Protokoll übereinstimmen. Dies kann mit den folgenden Befehlen überprüft werden:

```
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
```

Die BD-Route ist als statische Route programmiert. Überprüfen Sie daher die statische Weiterverteilungs-Route-Map, indem Sie 'show route-map <route-map name>' und dann 'show ip prefix-list <name>' auf allen Präfix-Listen ausführen, die in der Route-Map vorhanden sind. Führen Sie dies im nächsten Schritt durch.

Nach dem Zuordnen des L3Out zum BD

Wie bereits erwähnt, führt dieser Schritt dazu, dass die Präfixliste, die mit dem BD-Subnetz übereinstimmt, in der Route-Map für die Umverteilung zwischen statischem und externem Protokoll installiert wird.

```
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
```

Überprüfen Sie die Präfixliste:

```
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
```

Das BD-Subnetz wird für die Neuverteilung auf OSPF abgeglichen.

Zu diesem Zeitpunkt ist der Konfigurations- und Verifizierungs-Workflow für die Ankündigung des BD-Subnetzes aus L3Out abgeschlossen. Nach diesem Zeitpunkt ist die Verifizierung protokollspezifisch. Beispiel:

- Überprüfen Sie für EIGRP, ob die Route in der Topologietabelle mit "show ip eigrp topology vrf <name>" installiert wird.
- Überprüfen Sie für OSPF, ob die Route in der Datenbanktabelle als externes LSA mit "show ip ospf database vrf <name>" installiert wird.
- Überprüfen Sie für BGP, ob sich die Route in der BGP-RIB befindet, indem Sie "show bgp ipv4 unicast vrf <name>" eingeben.

BGP-Routenankündigung

Beim BGP sind alle statischen Routen implizit für die Neuverteilung zulässig. Die Route Map, die mit dem BD-Subnetz übereinstimmt, wird auf BGP-Nachbarebene angewendet.

```
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
```

Im obigen Beispiel ist 10.0.0.134 der im L3Out konfigurierte BGP-Nachbar.

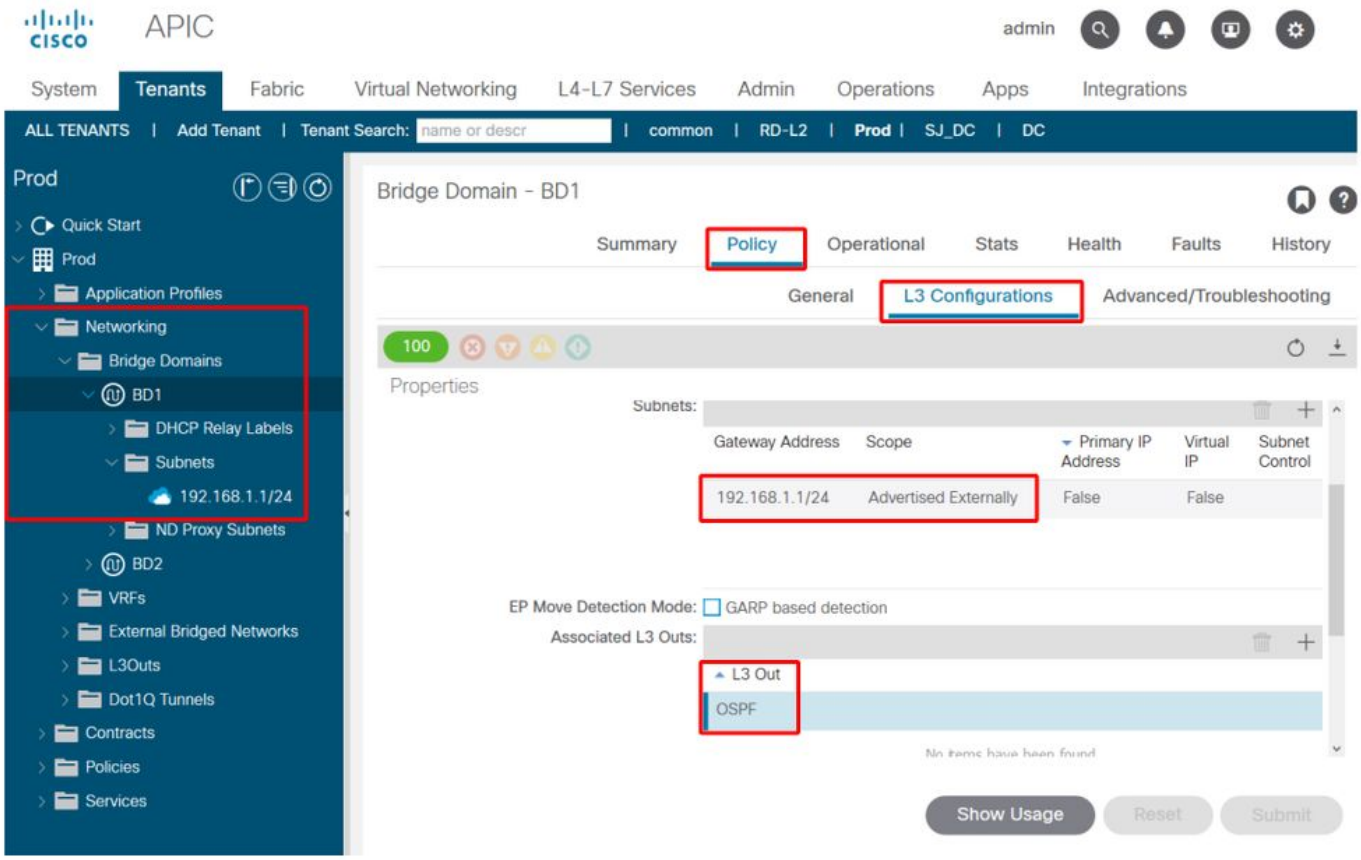
EIGRP-Routenankündigung

Wie OSPF wird eine Routing-Map verwendet, um die Umverteilung von statisch zu EIGRP zu steuern. Auf diese Weise sollten nur Subnetze, die mit dem L3Out verknüpft sind und auf "Extern anzeigen" gesetzt sind, neu verteilt werden. Dies kann mit dem folgenden Befehl überprüft werden:

```
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
```

Die endgültige funktionierende BD-Konfiguration ist unten dargestellt.

L3-Konfiguration der Bridge-Domäne



Fehlerbehebungsszenario: Routenankündigung für Bridge-Domänen

In diesem Fall besteht das typische Symptom normalerweise darin, dass ein konfiguriertes BD-Subnetz nicht von einem L3Out aus angekündigt wird. Folgen Sie dem vorherigen Workflow, um zu ermitteln, welche Komponente defekt ist.

Beginnen Sie mit der Konfiguration, bevor Sie zu niedrig angesetzt werden. Überprüfen Sie dazu Folgendes:

- Gibt es einen Vertrag zwischen der EPG und L3Out?
- Ist L3Out mit dem BD verbunden?
- Ist das BD-Subnetz so konfiguriert, dass es extern Werbung macht?
- Ist die externe Protokoll-Adjacency aktiv?

Mögliche Ursache: BD nicht bereitgestellt

Dieser Fall wäre in mehreren Szenarien anwendbar, z. B.:

- Die interne EPG verwendet die VMM-Integration mit der On-Demand-Option, und es wurden keine VM-Endpunkte mit der Port-Gruppe für die EPG verbunden.
- Die interne EPG wurde erstellt, es wurden jedoch keine statischen Pfadbindungen konfiguriert, oder die Schnittstelle, für die der statische Pfad konfiguriert wurde, ist ausgefallen.

In beiden Fällen würde der BD nicht bereitgestellt, und folglich würde die statische BD-Route nicht an den BL übertragen. Die Lösung besteht hier darin, einige aktive Ressourcen innerhalb einer EPG bereitzustellen, die mit diesem BD verknüpft ist, sodass das Subnetz bereitgestellt wird.

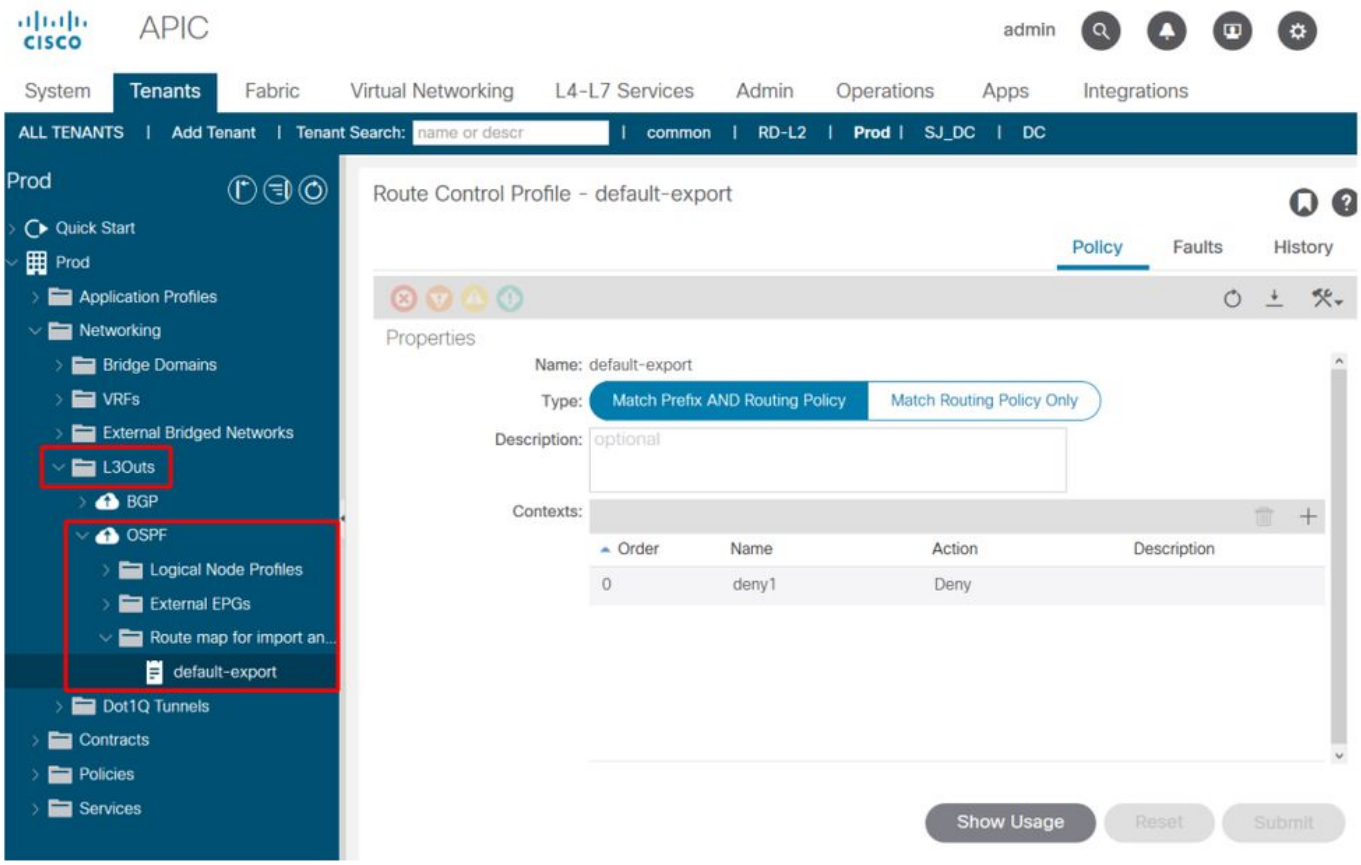
Mögliche Ursache: OSPF L3Out wird als 'Stub' oder 'NSSA' ohne Neuverteilung konfiguriert.

Wenn OSPF als L3Out-Protokoll verwendet wird, müssen die grundlegenden OSPF-Regeln befolgt werden. Stub-Bereiche erlauben keine umverteilten LSAs, können jedoch stattdessen eine Standardroute ankündigen. In NSSA-Bereichen sind umverteilte Pfade zulässig, aber auf dem L3Out muss die Option "Umverteilte LSAs in NSSA-Bereich senden" ausgewählt sein. NSSA kann auch eine Standardroute ankündigen, indem es auch "Originate Summary LSA" deaktiviert. Dies ist ein typisches Szenario, in dem "Send Redistributed LSA's into NSSA Area" deaktiviert würde.

Mögliche Ursache: "Default-Export"-Routenprofil mit konfigurierter Aktion "Deny" (Ablehnen) unter L3Out

Wenn Routenprofile unter einem L3Out mit den Namen "default-export" oder "default-import" konfiguriert werden, werden sie implizit auf das L3Out angewendet. Wenn außerdem für das Standard-Export-Routenprofil eine Verweigerungsaktion festgelegt und als "Match Prefix and Routing Policy" (Präfix und Routingrichtlinie abgleichen) konfiguriert ist, müssen BD-Subnetze aus diesem L3Out angekündigt werden und werden implizit abgelehnt:

Standard-Export - Routenprofil ablehnen



Präfix-Übereinstimmungen im Standard-Export-Routenprofil enthalten keine impliziten BD-Subnetze, wenn die Option "Nur Routing-Richtlinie zuordnen" aktiviert ist.

Workflow für externen Routenimport

In diesem Abschnitt wird erläutert, wie die ACI externe Routen über einen L3Out erlernt und an interne Leaf-Knoten verteilt. Sie umfasst auch Fälle von Verkehrsunfällen und undichten Stellen in späteren Abschnitten

Wie im vorherigen Abschnitt sollte der Benutzer wissen, was auf höherer Ebene geschieht.

Standardmäßig werden alle vom externen Protokoll empfangenen Routen im internen Fabric-BGP-Prozess neu verteilt. Dies gilt unabhängig davon, welche Subnetze unter der externen EPG konfiguriert und welche Markierungen ausgewählt werden. Es gibt zwei Beispiele, wo das nicht stimmt.

- Wenn die Option "Route Control Enforcement" (Durchsetzung der Routensteuerung) auf der obersten Ebene der L3Out-Richtlinie auf "Import" (Importieren) festgelegt ist. In diesem Fall würde das Routen-Importmodell von einem Sperrlistenmodell (nur angeben, was nicht zulässig ist) zu einem Permitlistenmodell (alles wird implizit abgelehnt, sofern nichts anderes konfiguriert wird).
- Wenn das externe Protokoll EIGRP oder OSPF ist und ein verwendetes Interleak-Routenprofil nicht mit den externen Routen übereinstimmt.

Damit eine externe Route an ein internes Leaf verteilt werden kann, muss Folgendes passieren:

- Die Route muss auf dem BL vom externen Router abgefragt werden. Um als Kandidat für die Neuverteilung über den Fabric-MP-BGP-Prozess fungieren zu können, muss die Route in der Routing-Tabelle und nicht nur im Protokoll RIB installiert werden.
- Die Route muss neu verteilt oder im internen BGP-Prozess angekündigt werden dürfen. Dies sollte immer erfolgen, es sei denn, es wird eine Durchsetzung der Importroutingkontrolle oder ein Interleak-Routenprofil verwendet.
- Eine BGP-Route-Reflector-Richtlinie muss konfiguriert und auf eine Pod-Richtliniengruppe angewendet werden, die auf das Pod-Profil angewendet wird. Wenn dies nicht angewendet wird, wird der BGP-Prozess auf den Switches nicht initialisiert.

Wenn sich die interne EPG/BD in derselben VRF-Instanz wie L3Out befindet, müssen nur die oben genannten drei Schritte ausgeführt werden, damit die interne EPG/BD externe Routen verwenden kann.

Route wird in BL-Routing-Tabelle installiert

In diesem Fall lautet die externe Route, die auf den BLs 103 und 104 erfasst werden sollte, 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 liegt auf der Hand, dass sie in der Routing-Tabelle installiert wird, wie dies über OSPF erlernt wird. Wenn hier nichts zu sehen ist, überprüfen Sie das individuelle Protokoll, und stellen Sie sicher, dass die Adjacencies aktiv sind. Route wird in BGP neu verteilt Die Weiterverteilungs-Route-Map kann überprüft werden, nachdem geprüft wurde, ob weder die Import-Durchsetzung noch Interleak-Routenprofile verwendet werden. Hierzu wird die Route-Map betrachtet, die für das externe Protokoll zur BGP-Neuverteilung verwendet wird. Siehe folgenden Befehl:

```
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
```

Hier wird deutlich, dass die "permit-all"-Routing-Map für die Umverteilung von OSPF zum BGP verwendet wird. Dies ist die Standardeinstellung. Von hier aus kann BL überprüft und die vom BGP stammende lokale Route überprüft werden:

```
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
```

In der obigen Ausgabe gibt 0.0.0.0/0 an, dass es lokal generiert wurde. Die Liste der Peers,

für die eine Benachrichtigung angekündigt wird, sind die Spine-Knoten im Fabric, die als Routen-Reflektoren fungieren.

Route auf internem Leaf überprüfen

Das BL sollte dies den Spine-Knoten über die VPNv4-BGP-Adressfamilie ankündigen. Die Spine-Knoten sollten dies allen Leaf-Knoten mit bereitgestellter VRF ankündigen (gilt für ein Beispiel ohne Route-Leaking). Führen Sie auf einem dieser Leaf-Knoten "show bgp vpnv4 unicast <route> vrf overlay-1" aus, um zu überprüfen, ob VPNv4 vorhanden ist.

Verwenden Sie den folgenden Befehl, um die Route auf dem internen Leaf zu überprüfen.

```
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
```

In der obigen Ausgabe wird die Route über BGP abgefragt, und die nächsten Hops sollten die physischen TEPs (PTEPs) der BLs sein.

```
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
```

Fehlerbehebung für externe Routen

In diesem Szenario erhält das interne Leaf (101) keine externe Route(n).

Überprüfen Sie wie immer zuerst die Grundlagen. Stellen Sie sicher, dass:

- Routing-Protokoll-Nachbarschaften sind auf den BLs vorhanden.
- Eine BGP-Route-Reflector-Richtlinie wird auf die Pod-Richtliniengruppe und das Pod-Profil angewendet.

Wenn die oben genannten Kriterien richtig sind, finden Sie im Folgenden einige weiterführende Beispiele für die Ursachen des Problems.

Mögliche Ursache: VRF nicht auf internem Leaf bereitgestellt

In diesem Fall besteht das Problem darin, dass keine EPGs mit Ressourcen auf dem internen Leaf bereitgestellt werden, auf dem die externe Route erwartet wird. Dies kann durch statische Pfadbindungen verursacht werden, die nur an Downschnittstellen konfiguriert sind oder nur über VMM-integrierte On-Demand-EPGs verfügen, ohne dass dynamische Anhänge erkannt werden.

Da das L3Out-VRF nicht auf dem internen Leaf bereitgestellt wird (überprüfen Sie dies mit "show vrf" auf dem internen Leaf), importiert das interne Leaf die BGP-Route nicht von VPNv4.

Um dieses Problem zu beheben, muss der Benutzer Ressourcen innerhalb des L3Out-VRF auf dem internen Leaf bereitstellen.

Mögliche Ursache: Import-Routendurchsetzung wird verwendet

Wie bereits erwähnt, akzeptiert L3Out bei aktivierter Durchsetzung der Importroutingkontrolle nur externe Routen, die explizit zulässig sind. In der Regel wird die Funktion als Tabellenzuordnung implementiert. Zwischen dem Protokoll RIB und der eigentlichen Routing-Tabelle befindet sich eine Table-Map, die sich nur auf den Inhalt der Routing-Tabelle auswirkt.

In der Ausgabe unten ist die Import Route Control (Routensteuerung importieren) aktiviert, es gibt jedoch keine explizit zulässigen Routen. Beachten Sie, dass sich das LSA in der OSPF-Datenbank, jedoch nicht in der Routing-Tabelle auf dem BL befindet:

```
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
```

Die jetzt installierte Tabellenzuordnung verursacht dieses Verhalten:

```
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:
```

Sämtliche Lerninhalte in Bereich 100, dem für diesen L3Out konfigurierten Bereich, werden von dieser Table-Map implizit abgelehnt, sodass sie nicht in der Routing-Tabelle installiert werden.

Um dieses Problem zu beheben, muss der Benutzer das Subnetz in der externen EPG mit der Markierung "Import Route Control Subnet" (Routensteuerungs-Subnetz importieren) definieren oder ein Import-Routenprofil erstellen, das mit den zu installierenden Präfixen übereinstimmt.

- Beachten Sie, dass die Importdurchsetzung für EIGRP nicht unterstützt wird.
- Beachten Sie außerdem, dass die Importdurchsetzung für BGP als eingehende Routing-Map implementiert wird, die auf den BGP-Nachbarn angewendet wird. Im Unterabschnitt "BGP Route Advertisement" finden Sie weitere Informationen zur Überprüfung.

Mögliche Ursache: ein Interleak-Profil verwendet wird.

Interleak-Routenprofile werden für EIGRP- und OSPF-L3Outs verwendet und sollen die Kontrolle darüber ermöglichen, was vom IGP in das BGP umverteilt wird. Außerdem ermöglichen sie die Anwendung von Richtlinien wie das Festlegen von BGP-Attributen.

Ohne ein Interleak-Routenprofil werden alle Routen implizit in das BGP importiert.

Ohne Interleak-Routenprofil:

```
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
```

Mit einem Interleak-Routenprofil:

```
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
```

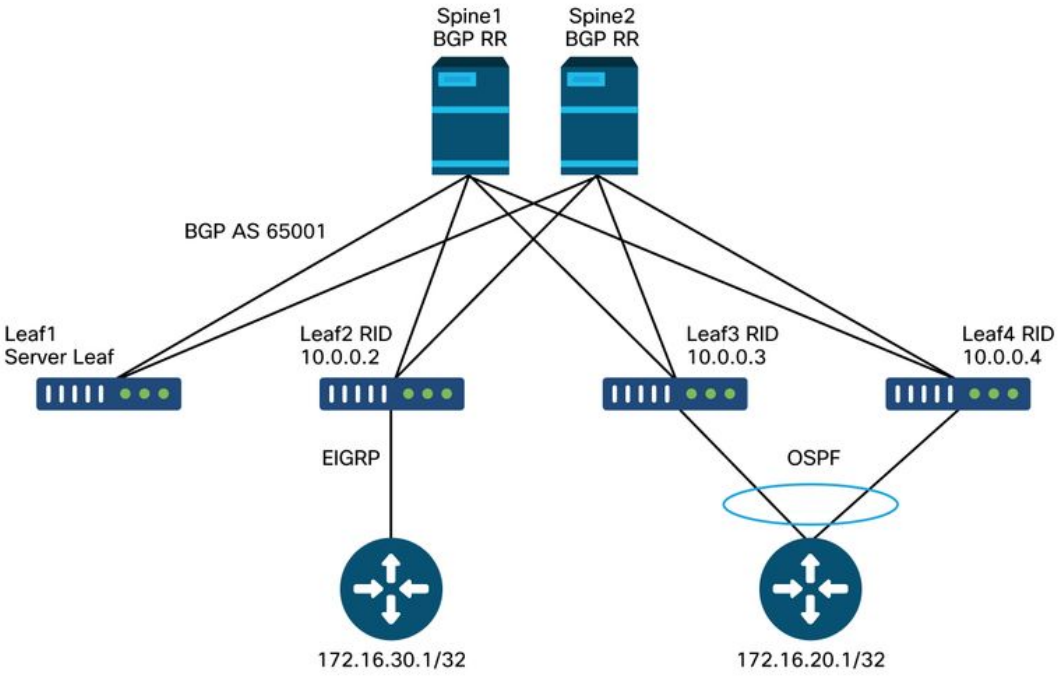
Die oben hervorgehobene Route Map lässt nur zu, was im konfigurierten Interleak-Profil explizit zugeordnet ist. Wenn die externe Route nicht übereinstimmt, wird sie nicht in das BGP umverteilt.

Workflow für die Transit-Routenankündigung

In diesem Abschnitt wird erläutert, wie Routen von einem L3Out über ein anderes L3Out angekündigt werden. Dies gilt auch für das Szenario, in dem statische Routen, die direkt in einem L3Out konfiguriert sind, angekündigt werden müssen. Dabei wird nicht jedes einzelne Protokoll berücksichtigt, sondern vielmehr, wie es in der ACI implementiert wird. Derzeit wird keine VRF-übergreifende Weiterleitung unterstützt.

In diesem Szenario wird die folgende Topologie verwendet:

Transit-Routing-Topologie



Im Folgenden wird erläutert, wie 172.16.20.1 aus OSPF abgerufen und dann in EIGRP angekündigt wird. Außerdem werden Verifizierungen des gesamten Prozesses und Fehlerbehebungsszenarien beschrieben.

Damit die Route 172.16.20.1 im EIGRP angekündigt wird, muss eine der folgenden Optionen konfiguriert werden:

- Das anzuzeigende Subnetz kann auf dem EIGRP-L3Out mit der Markierung "Export Route-Control Subnet" (Routen-Steuerungs-Subnetz exportieren) definiert werden. Wie im Übersichtsabschnitt erwähnt, wird dieses Flag hauptsächlich für das Transit-Routing verwendet und definiert die Subnetze, die aus diesem L3Out gemeldet werden sollen.
- Konfigurieren Sie 0.0.0.0/0, und wählen Sie sowohl "Aggregate Export" als auch "Export Route Control Subnet" aus. Dadurch wird eine Route Map für die Neuverteilung über das externe Protokoll erstellt, die mit 0.0.0.0/0 und allen spezifischeren Präfixen übereinstimmt (was eine effektive Übereinstimmung mit any darstellt). Beachten Sie, dass bei Verwendung von 0.0.0.0/0 mit "Aggregate Export" keine statischen Routen für die Neuverteilung zugeordnet werden. Damit sollen BD-Routen, die nicht angekündigt werden sollen, nicht versehentlich angekündigt werden.
- Schließlich kann ein Export-Routenprofil erstellt werden, das mit den anzuzeigenden Präfixen übereinstimmt. Mit dieser Methode kann die Aggregatoption mit Präfixen außer 0.0.0.0/0 konfiguriert werden.

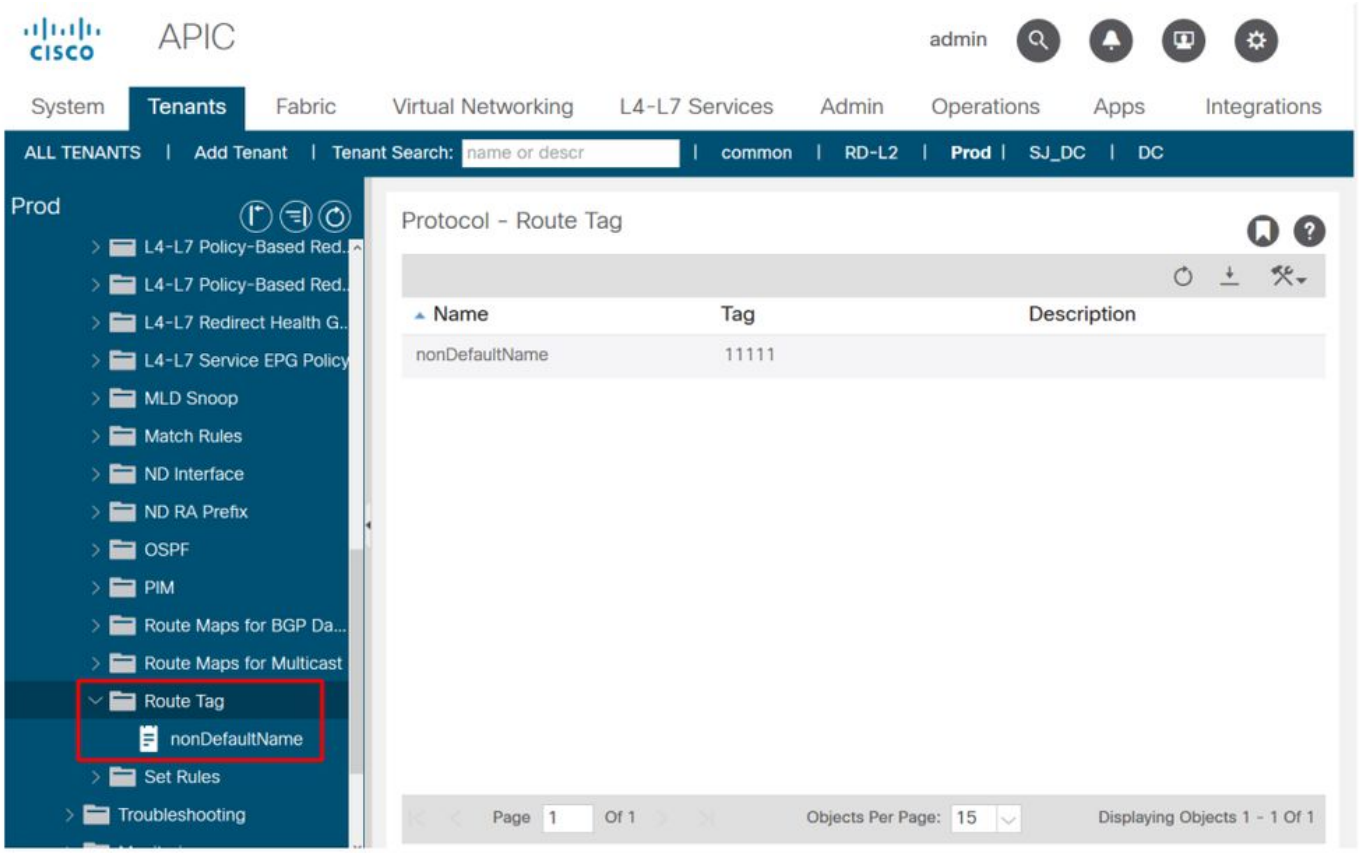
Die obigen Konfigurationen führen zur Meldung der Transitroute, benötigen jedoch weiterhin eine Sicherheitsrichtlinie, um den Datenverkehr auf dem Datenflugzeug zuzulassen. Wie bei jeder Kommunikation zwischen EPGs muss ein Vertrag vorliegen, bevor Datenverkehr zulässig ist.

> Beachten Sie, dass doppelte externe Subnetze mit dem "Externen Subnetz für externe EPG" nicht in derselben VRF-Instanz konfiguriert werden können. Bei der Konfiguration müssen Subnetze spezifischer sein als 0.0.0.0. Es ist wichtig, "Externes Subnetz für externe EPG" nur für das L3Out zu konfigurieren, von dem die Route empfangen wird. Konfigurieren Sie

dies nicht auf dem L3Out, das diese Route melden soll.

Es ist außerdem wichtig zu wissen, dass alle Transitstrecken mit einem spezifischen VRF-Tag versehen sind. Standardmäßig ist dieses Tag 4294967295. Die Route-Tag-Richtlinie wird unter "Tenant > Networking > Protocols > Route-Tag:

Route-Tag-Richtlinie



Diese Route Tag-Richtlinie wird dann auf die VRF-Instanz angewendet. Der Zweck dieses Tags ist im Wesentlichen, Schleifen zu verhindern. Dieses Routing-Tag wird angewendet, wenn die Transit-Route aus einem L3Out zurückgemeldet wird. Wenn diese Routen dann mit demselben Routen-Tag empfangen werden, wird die Route verworfen.

Prüfen, ob die Route über OSPF auf dem empfangenden BL vorhanden ist

Überprüfen Sie wie im letzten Abschnitt zuerst, dass das BL, das anfänglich die richtige Route empfangen soll.

```
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
```

Für den Moment nehmen Sie an, dass die Werbung L3Out ist auf einem anderen BL (wie in der Topologie) (später Szenarien werden diskutieren, wo es auf dem gleichen BL).

Überprüfen, ob die Route im BGP des empfangenden OSPF-BL vorhanden ist

Damit die OSPF-Route dem externen EIGRP-Router angekündigt wird, muss sie dem BGP auf der empfangenden OSPF-BL angekündigt werden.

```
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
```

Die Route befindet sich im BGP.

Überprüfen Sie auf der EIGRP-BL, die die installierte Route melden soll.

```
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
```

Es wird in der Routing-Tabelle mit Overlay Next-Hops installiert, die auf die ursprünglichen Border Leaf-Knoten zeigen.

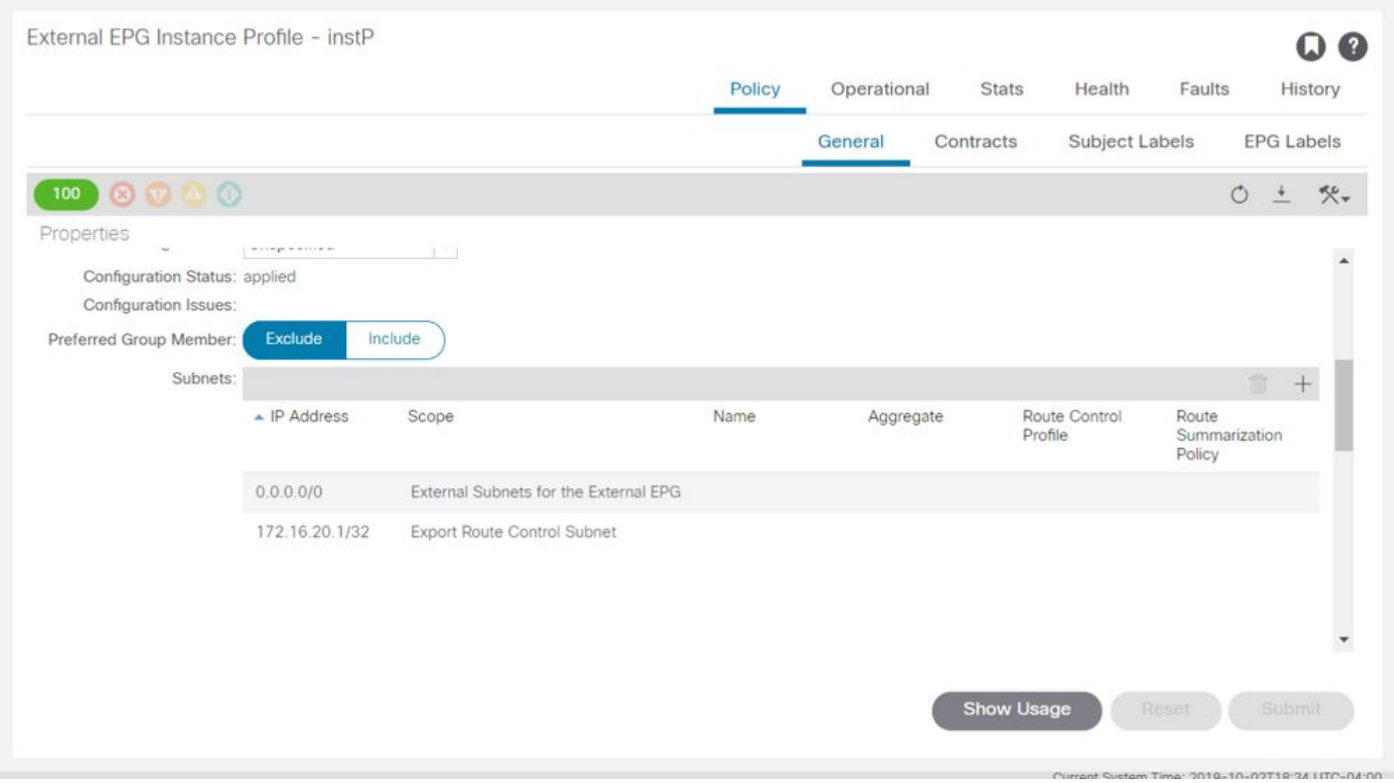
```
leaf102# acidiag fnvread

      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
```

Vergewissern Sie sich, dass die Route auf dem BL angekündigt wird.

Die Route wird von BL 102 als Ergebnis der Markierung "Export Route Control Subnet" (Subnetz für Exportroutensteuerung) im konfigurierten Subnetz angekündigt:

Routenkontrolle exportieren



Verwenden Sie den folgenden Befehl, um die Routenübersicht anzuzeigen, die als Ergebnis der Markierung "Export Route Control" (Routensteuerung exportieren) erstellt wird:

```
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
```

Um nach "BGP > EIGRP Redistribution" zu suchen, sehen Sie sich die Routing-Karte an. Die Route Map selbst sollte jedoch die gleiche sein, unabhängig davon, ob es sich um das Quellprotokoll OSPF, EIGRP oder BGP handelt. Statische Routen werden mit einem anderen Routenplan gesteuert.

```
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
```

In der obigen Ausgabe wird das VRF-Tag für dieses Präfix zur Loop-Verhinderung festgelegt, und das mit "Export Route Control" konfigurierte Subnetz wird explizit zugeordnet.

Transit-Routing bei identischem Empfang und gleicher Werbung für BL

Wenn sich die Empfangs- und Werbe-BLs unterscheiden, muss die Route, wie bereits erwähnt, mithilfe von BGP über die Fabric angekündigt werden. Wenn die BLs identisch sind, kann die Neuverteilung oder Ankündigung direkt zwischen den Protokollen auf dem Leaf erfolgen.

Im Folgenden finden Sie eine kurze Beschreibung der Implementierung:

- **Transit-Routing zwischen zwei OSPF-L3Outs auf demselben Leaf: Die** Routenankündigung wird über ein auf die OSPF-Prozessebene angewendetes "Area-Filter" gesteuert. Auf dem Leaf muss ein L3Out in Bereich 0 bereitgestellt werden, da die Routen nicht über Umverteilung, sondern zwischen Bereichen angekündigt werden. Verwenden Sie "show ip ospf vrf <Name>", um die Filterliste anzuzeigen. Zeigen Sie den Inhalt des Filters mit 'show route-map <Filtername>' an.
- **Transit-Routing zwischen OSPF und EIGRP-L3Outs auf demselben Leaf: Die** Routenankündigung wird über Weiterverteilungs-Routing-Maps gesteuert, die mit "show ip ospf" und "show ip eigrp" angezeigt werden. Wenn mehrere OSPF-L3Outs auf derselben BL vorhanden sind, besteht die einzige Möglichkeit zur Neuverteilung auf eine dieser OSPF-L3Outs darin, dass die andere ein Stub oder NSSA ist, bei dem "**Send redistributed LSAs into NSSA area" deaktiviert ist,** sodass keine externen LSAs zulässig sind.
- **Transit-Routing zwischen OSPF oder EIGRP und BGP auf demselben Leaf:** Die Routenankündigung im IGP wird über Weiterverteilungs-Routing-Maps gesteuert. Die Routenankündigung in das BGP wird über eine ausgehende Routenübersicht gesteuert, die direkt auf den BGP-Nachbarn angewendet wird, an den die Route gesendet werden soll. Dies kann mit dem Befehl "show bgp ipv4 unicast neighbor <Nachbar-Adresse> vrf <Name> | grep Outbound".

- **Transit-Routing zwischen zwei BGP-l3Outs auf demselben Leaf: Die** gesamte Ankündigung wird über Routing-Maps gesteuert, die direkt auf den BGP-Nachbarn angewendet werden, an den die Route gesendet werden soll. Dies kann mit dem Befehl "show bgp ipv4 unicast neighbor <Nachbar-Adresse> vrf <Name> | grep Outbound".

Fehlerbehebungsszenarien für das Transit-Routing #1: Transit-Route nicht angekündigt

Dieses Fehlerbehebungsszenario beinhaltet, dass Routen, die über einen L3Out abgefragt werden sollten, nicht über den anderen L3Out gesendet werden.

Überprüfen Sie wie gewohnt die Grundlagen, bevor Sie sich ACI-spezifische Aspekte ansehen.

- Sind Protokoll-Adjacencies aktiviert?
- Wird die Route, die die ACI propagieren sollte, von einem externen Protokoll überhaupt gelernt?
- Wird bei BGP der Pfad aufgrund eines BGP-Attributs verworfen? (as-path usw.).
- Verfügt das empfangende L3Out über eine OSPF-, EIGRP-Topologietabelle oder BGP-Tabelle?
- Wird eine BGP-Routen-Reflektorrichtlinie auf die Pod-Richtliniengruppe angewendet, die auf das Pod-Profil angewendet wird?

Wenn alle grundlegenden Protokollüberprüfungen richtig konfiguriert sind, finden Sie nachfolgend einige weitere häufige Ursachen für eine Transitroute, die nicht angekündigt wird.

Mögliche Ursache: Kein OSPF-Bereich 0

Wenn die betroffene Topologie zwei OSP L3Outs auf demselben Grenz-Leaf umfasst, muss es eine Area 0 geben, damit Routen von einer Area zu einer anderen angekündigt werden. Weitere Einzelheiten finden Sie im obigen Aufzählungspunkt "Transit-Routing zwischen zwei OSPF-L3Outs auf demselben Leaf".

Mögliche Ursache: OSPF-Bereich ist Stub oder NSSA

Dies wird angezeigt, wenn OSPF L3Out mit einem Stub- oder NSSA-Bereich konfiguriert ist, der nicht für die Ankündigung externer LSAs konfiguriert ist. Mit OSPF werden externe LSAs nie in Stub-Bereichen angekündigt. Sie werden in NSSA-Bereichen angekündigt, wenn die Option "Redistributed LSAs into NSSA Area senden" ausgewählt ist.

Fehlerbehebungsszenarien für das Transit-Routing #2: Transit-Route nicht empfangen

In diesem Szenario besteht das Problem darin, dass einige von einem ACI L3Out angekündigte Routen nicht in einem anderen L3Out empfangen werden. Dieses Szenario könnte anwendbar sein, wenn sich die L3Outs in zwei separaten Fabrics befinden und über externe Router verbunden sind, oder wenn sich die L3Outs in unterschiedlichen VRFs befinden und die Routen zwischen den VRFs von einem externen Router weitergeleitet werden.

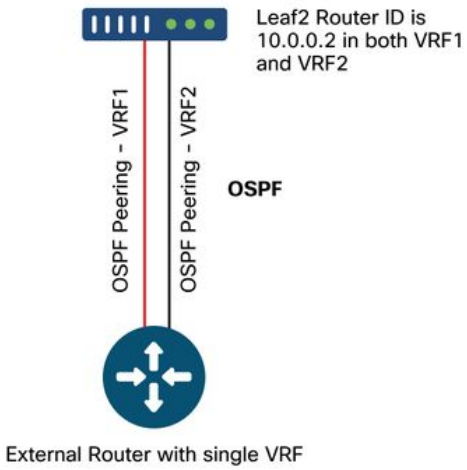
Mögliche Ursache: BL wird mit derselben Router-ID in mehreren VRFs konfiguriert

Aus Konfigurationsperspektive kann eine Router-ID nicht innerhalb derselben VRF-Instanz dupliziert werden. In der Regel ist es jedoch in Ordnung, dieselbe Router-ID in verschiedenen VRFs zu verwenden, solange die beiden VRFs nicht mit den gleichen Routing-Protokoll-Domänen

verbunden sind.

Berücksichtigen Sie die folgende Topologie:

Externer Router mit einzelnem VRF - Transit-Route nicht empfangen



Das Problem hierbei besteht darin, dass das ACI-Leaf LSAs mit einer eigenen Router-ID empfängt, sodass diese nicht in der OSPF-Datenbank installiert werden.

Wenn bei VPC-Paaren dieselbe Konfiguration auftritt, werden außerdem auf einigen Routern laufend LSAs hinzugefügt und gelöscht. Der Router sieht beispielsweise LSAs von seinem VPC-Peer mit VRF und LSAs von demselben Knoten (mit derselben Router-ID), die von der anderen VRF stammen.

Um dieses Problem zu beheben, muss der Benutzer sicherstellen, dass ein Knoten über eine andere, eindeutige Router-ID innerhalb jeder VRF-Instanz verfügt, in der ein L3Out vorhanden ist.

Mögliche Ursache: Routen von einem L3Out in einer ACI-Fabric, die in einer anderen Fabric mit demselben VRF-Tag empfangen werden

Das Standard-Routing-Tag in der ACI ist immer dasselbe, sofern es nicht geändert wird. Wenn Routen von einem L3Out in einer VRF- oder ACI-Fabric an ein anderes L3Out in einer anderen VRF- oder ACI-Fabric weitergegeben werden, ohne die Standard-VRF-Tags zu ändern, werden die Routen von den empfangenden BLs verworfen.

Die Lösung für dieses Szenario besteht einfach in der Verwendung einer eindeutigen Route-Tag-Richtlinie für jede VRF-Instanz der ACI.

Fehlerbehebungsszenarien für das Transit-Routing #3 — unerwartet gemeldete Transit-Routen

Dieses Szenario tritt ein, wenn Transit-Routen angekündigt werden, und L3Out, wenn sie nicht angekündigt werden sollen.

Mögliche Ursache: Nutzung von 0.0.0.0/0 mit "Aggregate Export"

Wenn ein externes Subnetz als 0.0.0.0/0 mit "Export Route Control Subnet" und "Aggregate

Export" konfiguriert wird, wird eine Übereinstimmung mit allen Weiterverteilungs-Routenzuordnungen installiert. In diesem Fall werden alle Routen im BL, die über OSPF, EIGRP oder BGP empfangen wurden, über das L3Out angekündigt, in dem dies konfiguriert ist.

Nachfolgend finden Sie die Routing-Map, die als Ergebnis des Aggregate-Exports auf dem Leaf bereitgestellt wird:

```
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
```

Dies ist die häufigste Ursache für Routing-Schleifen, die eine ACI-Umgebung betreffen.

Vertrag und L3Out

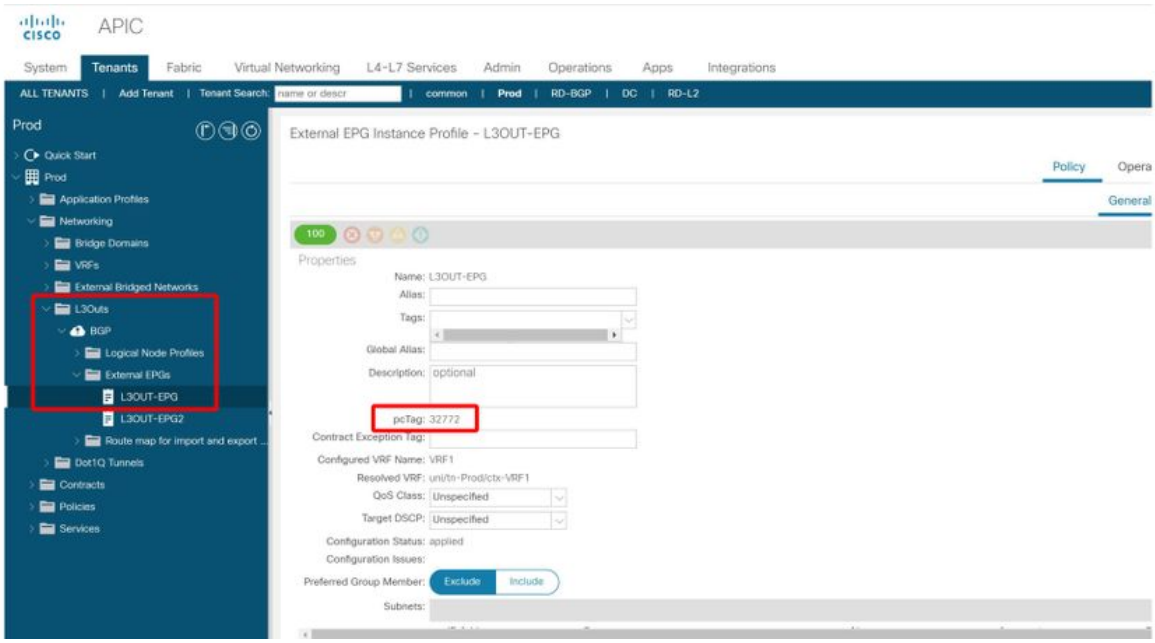
Präfixbasierte EPG auf L3Out

In einer internen EPG (nicht L3Out) werden Verträge erzwungen, nachdem das pcTag der Quell- und das pcTag der Ziel-EPG abgeleitet wurden. Das Kapselungs-VLAN/VXLAN des am Downlink-Port empfangenen Pakets dient dazu, das pcTag zu steuern, indem das Paket in die EPG klassifiziert wird. Beim Erlernen einer MAC- oder IP-Adresse wird diese zusammen mit der Zugriffskapselung und dem zugehörigen EPG pcTag erfasst. Weitere Einzelheiten zu pcTag und der Vertragsdurchsetzung finden Sie im Kapitel "Sicherheitsrichtlinien".

L3Outs steuern auch ein pcTag mit seiner L3Out EPG (External EPG) unter 'Tenant > Networking > L3OUT > Networks > L3OUT-EPG'. L3Outs nutzen jedoch keine VLANs und Schnittstellen, um Pakete als solche zu klassifizieren. Die Klassifizierung basiert stattdessen auf dem Quell-Präfix/Subnetz in der Art der längsten Präfixübereinstimmung. Daher kann eine L3Out-EPG als **präfixbasierte EPG** bezeichnet werden. Nachdem ein Paket basierend auf einem Subnetz in einen L3Out klassifiziert wurde, folgt es einem ähnlichen Richtliniendurchsetzungsmuster wie eine reguläre EPG.

Im folgenden Diagramm wird dargestellt, wo sich das pcTag einer bestimmten L3Out-EPG in der GUI befindet.

Position des pcTags für einen L3Out



Der Benutzer ist für die Definition der präfixbasierten EPG-Tabelle verantwortlich. Dies erfolgt über den Subnetzbereich "Externes Subnetz für externe EPG". Jedes Subnetzset mit diesem Bereich fügt einen Eintrag in einer statischen LPM-Tabelle (Longest Prefix Match) hinzu. Dieses Subnetz verweist auf den pcTag-Wert, der für alle IP-Adressen verwendet wird, die unter dieses Präfix fallen.

Die LPM-Tabelle präfixbasierter EPG-Subnetze kann mithilfe des folgenden Befehls auf Leaf-Switches überprüft werden:

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

Anmerkungen:

- Die Einträge in der LPM-Tabelle gelten für die VRF-VNID. Die Suche erfolgt per vrf_vnid/src pcTag/dst pcTag.

- Jeder Eintrag verweist auf ein einzelnes pcTag. Folglich können zwei L3Out-EPGs nicht dasselbe Subnetz mit derselben Maskenlänge innerhalb derselben VRF-Instanz verwenden.
- Subnetz 0.0.0.0/0 verwendet immer den speziellen pcTag 15. Daher kann es dupliziert werden, sollte jedoch nur mit einem vollen Verständnis der Auswirkungen der Richtliniendurchsetzung durchgeführt werden.
- Diese Tabelle wird in beide Richtungen verwendet. Von L3Out zu Leaf Local Endpoint wird das Quell-pcTag mithilfe dieser Tabelle abgeleitet.Von Leaf Local Endpoint zu L3Out wird das pcTag-Ziel mithilfe dieser Tabelle abgeleitet.
- Wenn für die VRF-Instanz die Durchsetzungseinstellung "Ingress" (Eingang) für "Policy Control Enforcement Direction" (Richtliniendurchsetzungsrichtung) festgelegt ist, ist die LPM-Präfixtabelle auf den L3Out-BLs sowie allen Leaf-Switches in der VRF-Instanz vorhanden, die einen Vertrag mit L3Out haben.

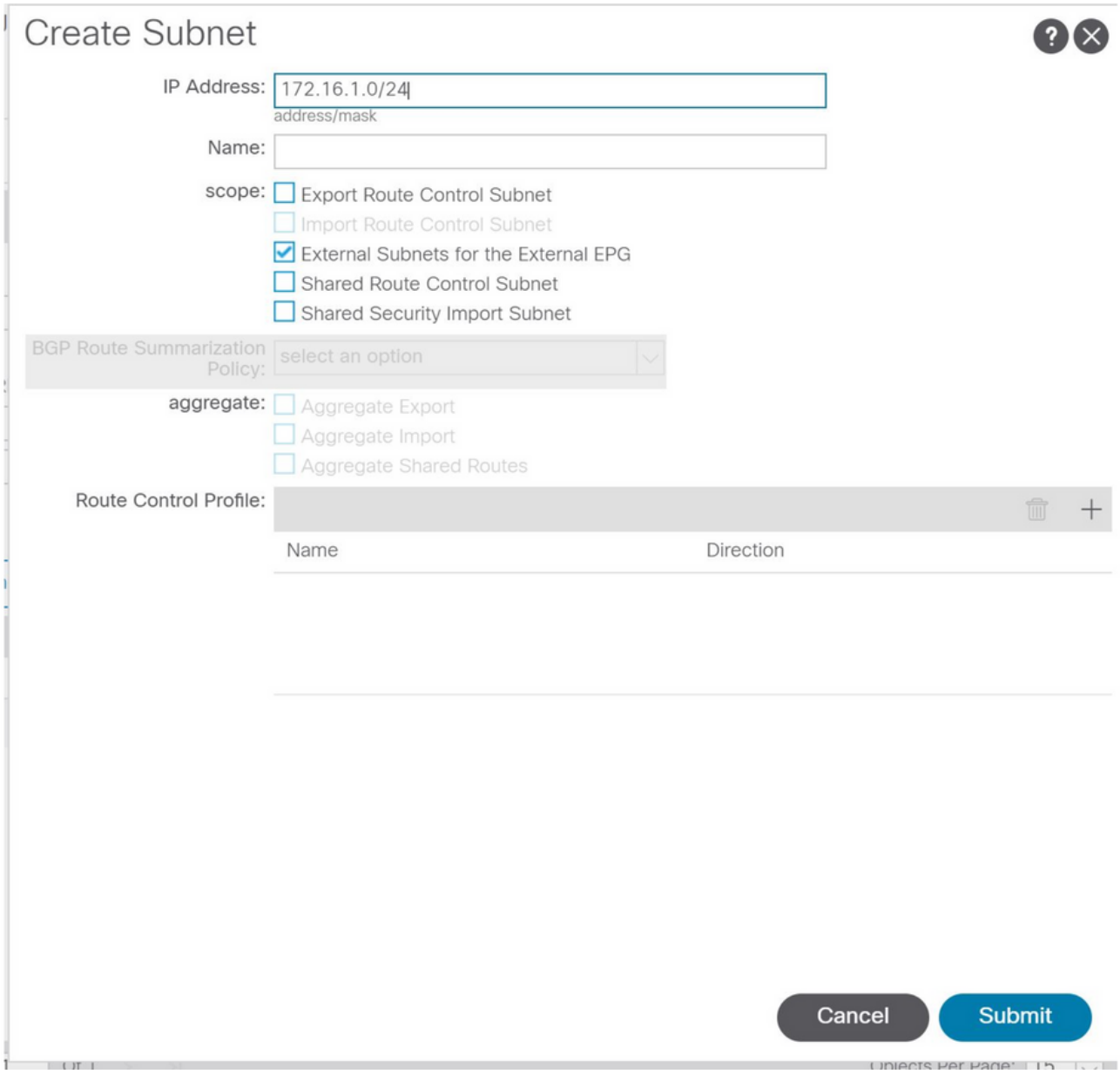
Beispiel 1: Einzel-L3Out mit spezifischem Präfix

Szenario: Ein BGP-L3Out in VRF-Prod:VRF1 mit einer L3Out-EPG. Das Präfix 172.16.1.0/24 wird von einer externen Quelle empfangen und muss daher in die L3Out-EPG klassifiziert werden.

```
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
```

Fügen Sie zunächst der Präfixtabelle das Subnetz hinzu.

Subnetz mit Bereich "Externe Subnetze für externe EPG"



Überprüfen Sie die Programmierung der Präfixliste auf den Leaf-Switches, die über die VRF-Instanz von L3Out verfügen:

```
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
```

Das pcTag der L3Out-EPG ist 32772 im VRF-Bereich 2097154.

Beispiel 2: Ein L3Out mit mehreren Präfixen

In diesem Szenario empfängt das L3Out mehrere Präfixe und geht damit auf das vorherige Beispiel zurück. Eine Alternative besteht darin, alle vom L3Out empfangenen Präfixe zu akzeptieren, während die Eingabe der Präfixe funktional fehlerfrei ist (je nach beabsichtigtem

Design).

Dies kann mit dem Präfix '0.0.0.0/0' erreicht werden.

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.

Daraus ergibt sich folgender Eintrag in der Policy-mgr-Präfixtabelle:

```
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
```

> Beachten Sie, dass der pcTag, der 0.0.0.0/0 zugewiesen ist, den Wert 15 und nicht 32772 verwendet. pcTag 15 ist ein reserviertes System-pcTag, das nur mit 0.0.0.0/0 verwendet wird, das als Platzhalter für alle Präfixe eines L3Out fungiert.

Verfügt die VRF-Instanz über ein einzelnes L3Out mit einer einzelnen L3Out-EPG unter Verwendung von 0.0.0.0/0, bleibt das Richtlinienpräfix eindeutig und stellt den einfachsten Ansatz zum Abfangen aller Daten dar.

Beispiel 3a: Mehrere L3Out-EPGs in einer VRF-Instanz

In diesem Szenario gibt es mehrere L3Out-EPGs in derselben VRF-Instanz.

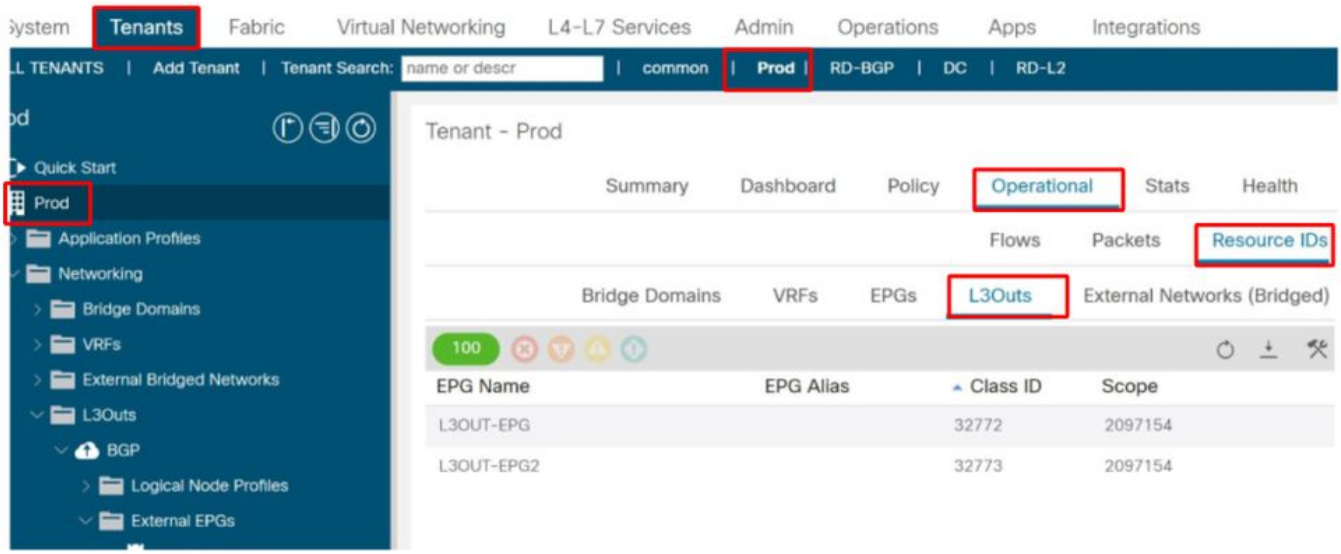
Anmerkung: Aus der präfixbasierten EPG-Perspektive ergeben die folgenden beiden Konfigurationen die entsprechenden Einträge in der LPM-Policy-mgr-Präfixtabelle:

1. Zwei L3Outs mit jeweils einer L3Out-EPG.
2. Ein L3Out mit zwei L3Out-EPGs

In beiden Szenarien sind insgesamt 2 L3Out-EPGs vorhanden. Das bedeutet, dass jedes EPG über ein eigenes pcTag und zugehörige Subnetze verfügt.

Alle pcTags einer bestimmten L3Out-EPG können in der GUI unter 'Tenant > Operational > Resource id > L3Outs' angezeigt werden.

Überprüfung des L3Out pcTag



In diesem Szenario empfängt die ACI-Fabric mehrere Präfixe von den externen Routern, und die L3Out-EPG-Definition lautet wie folgt:

- 172.16.1.0/24 der L3OUT-EPG zugewiesen.
- 172.16.2.0/24 zugewiesen an L3OUT-EPG2.
- 172.16.0.0/16 der L3OUT-EPG zugewiesen (zum Abfangen des Präfix 172.16.3.0/24).

Um dies abzugleichen, wird die Konfiguration wie folgt definiert:

- L3OUT-EPG hat das Subnetz 172.16.1.0/24 und 172.16.0.0/16 mit dem Bereich "Externes Subnetz für die externe EPG".
- L3OUT-EPG2 hat das Subnetz 172.16.2.0/24 mit dem Bereich "Externes Subnetz für die externe EPG".

Die Einträge in der Präfixtabelle lauten wie folgt:

```
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 ist dem pcTag 32773 (L3OUT-EPG2) und 172.16.0.0/16 dem 32772 (L3OUT-EPG) zugeordnet.

In diesem Szenario ist der Eintrag für 172.16.1.0/24 redundant, da das Supernet /16 derselben EPG zugewiesen ist.

Mehrere L3Out-EPGs sind nützlich, wenn das Ziel darin besteht, verschiedene Verträge auf Gruppen von Präfixen innerhalb eines einzelnen L3Out anzuwenden. Im nächsten Beispiel wird veranschaulicht, wie Verträge mit mehreren L3Out-EPGs zum Tragen kommen.

Beispiel 3b: mehrere L3Out-EPGs mit unterschiedlichen Verträgen

Dieses Szenario umfasst die folgende Konfiguration:

- ICMP-Vertrag, der nur ICMP zulässt.
- HTTP-Vertrag, der nur TCP-Zielport 80 zulässt.
- EPG1 (pcTag 32770) stellt den HTTP-Vertrag bereit, der von L3OUT-EPG (pcTag 32772) verwendet wird.
- EPG2 (pcTag 32771) stellt den ICMP-Vertrag bereit, der von L3OUT-EPG2 (pcTag 32773) verwendet wird.

Es werden die gleichen Policygr-Präfixe aus dem vorherigen Beispiel verwendet:

- 172.16.1.0/24 in L3OUT-EPG muss HTTP zu EPG1 zulassen.
- 172.16.2.0/24 in L3OUT-EPG2 muss ICMP zu EPG2 zulassen

policy-mgr-Präfix und Zoning-Regeln:

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

```
--------------------+
```

Datenpfadvalidierung mit fTriage — Fluss durch Richtlinie zugelassen

Mit einem ICMP-Datenstrom zwischen 172.16.2.1 im externen Netzwerk und 192.168.3.1 in EPG2 kann fTriage verwendet werden, um den Datenstrom zu erfassen und zu analysieren. Starten Sie in diesem Fall fTriage auf beiden Leaf-Switches 103 und 104, da der Datenverkehr in eines der beiden folgenden Bereiche eintreten kann:

```
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 bestätigt den Treffer der Zoning-Regel für die ICMP-Regel von L3OUT_EPG2 zu EPG:

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

Datenpfadvalidierung mit fTriage - Datenfluss, der von der Richtlinie nicht zugelassen ist

Bei ICMP-Datenverkehr, der von 172.16.1.1 (L3OUT-EPG) in Richtung 192.168.3.1 (EPG2)

stammt, ist ein Richtlinienverlust zu erwarten.

```
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"}}}
```

WennTriage bestätigt, dass das Paket mit dem Grund SECURITY_GROUP_DENY (Policy Drop) verworfen wurde und dass der abgeleitete Quell-pcTag 32772 und der Ziel-pcTag 32771 ist. Wenn dies anhand von Zoning-Regeln geprüft wird, gibt es eindeutig keine Einträge zwischen diesen EPGs.

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

Beispiel 4: mehrere L3Outs mit mehreren Präfixen

Das Szenario ist ähnlich wie in Beispiel 3 eingerichtet (L3Out- und L3Out-EPG-Definitionen), aber das auf beiden L3Out-EPGs definierte Netzwerk ist 0.0.0.0/0.

Die Vertragskonfiguration lautet wie folgt:

- ICMP1-Vertrag, der ICMP zulässt.
- ICMP2-Vertrag, der ICMP zulässt.
- EPG1 (pcTag 32770) stellt den ICMP1-Vertrag bereit, der von L3OUT-EPG (pcTag 32772) genutzt wird.
- EPG2 (pcTag 32771) stellt einen ICMP2-Vertrag bereit, der von L3OUT-EPG2 (pcTag 32773) genutzt wird.

Diese Konfiguration mag ideal aussehen, wenn das externe Netzwerk viele Präfixe ankündigt. Es gibt jedoch mindestens zwei Präfixe, die unterschiedlichen zulässigen Datenflussmustern folgen. In diesem Beispiel sollte ein Präfix nur ICMP1 und das andere nur ICMP2 zulassen.

Obwohl '0.0.0.0/0' zweimal in derselben VRF-Instanz verwendet wird, wird nur ein Präfix in die policy-mgr-Präfixtabelle programmiert:

```
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
```

Im Folgenden werden zwei Abläufe erneut untersucht. Basierend auf der obigen Vertragskonfiguration wird Folgendes erwartet:

1. 172.16.2.1 (L3OUT-EPG2) bis 192.168.3.1 (EPG2) **sollte** von ICMP2 zugelassen werden.
2. 172.16.2.1 (L3OUT-EPG2) bis 192.168.1.1 (EPG1) sind **nicht** zulässig, da zwischen EPG1 und L3OUT-EPG2 kein Vertrag besteht.

Datenpfadvalidierung mit fTriage - Datenfluss, der durch Richtlinie zugelassen wird

Führen Sie fTriage mit einem ICMP-Fluss von 172.16.2.1 (L3OUT-EPG2) bis 192.168.3.1 (EPG2 — pcTag 32771) aus.

```
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
```

Dieser Fluss wird (wie erwartet) von Zoning-Regel 4336 zugelassen.

Datenpfadvalidierung mit fTriage - Datenfluss, der von der Richtlinie nicht zugelassen ist

Führen Sie fTriage mit einem ICMP-Fluss von 172.16.2.1 (L3OUT-EPG2) bis 192.168.1.1 (EPG1 — pcTag 32770) aus:

```
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
```

Dieser Fluss wird durch Zoning-Regel 4341 zugelassen (unerwartet). Die Zonenregeln müssen nun analysiert werden, um zu verstehen, warum das so ist.

Datenpfadvalidierung - Zoning-Regeln

Die Zonenregeln für die letzten beiden Tests sind unten aufgeführt:

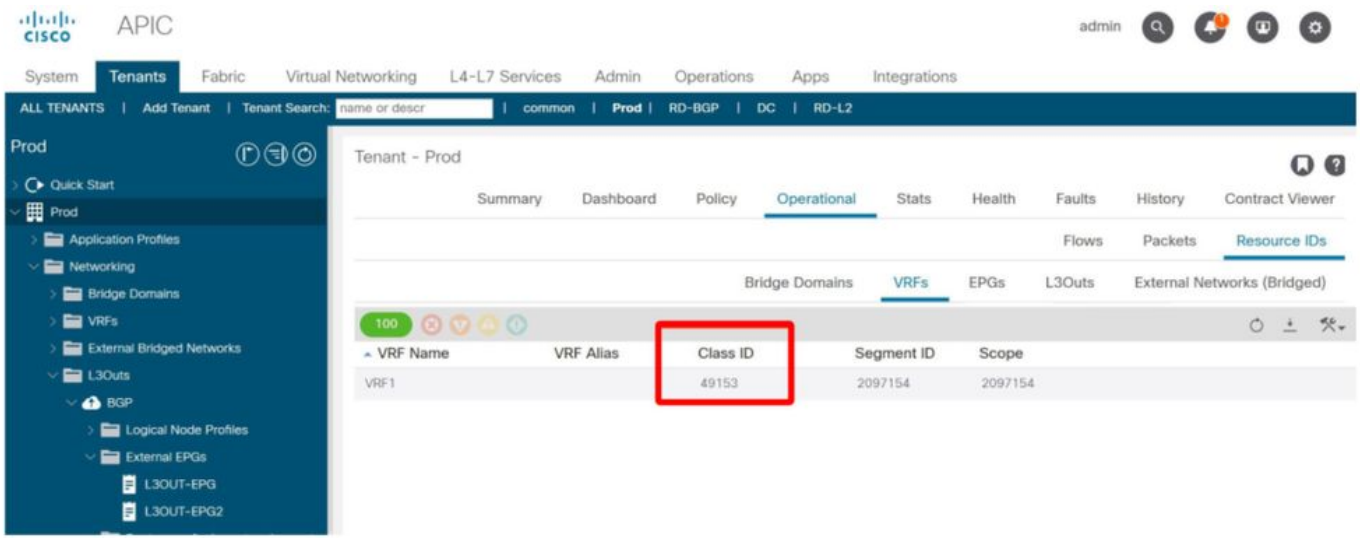
- Erwartet - Fluss trifft auf Zonenregelzeile 4336 (ICMP2-Vertrag).
- Unerwartet - Fluss trifft auf Zonenregelzeile 4341 (ICMP1-Vertrag).

```
+---------+--------+--------+----------+---------+---------+---------+-------+----------+-------
```

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

Beide Flüsse leiten den src pcTag von 49153 ab. Dies ist das pcTag der VRF. Dies kann in der Benutzeroberfläche überprüft werden:

Überprüfen des pcTag der VRF-Instanz



Folgendes geschieht, wenn das Präfix 0.0.0.0/0 mit einem L3Out verwendet wird:

- Der Datenverkehr von einer internen EPG zu einer L3Out-EPG mit 0.0.0.0/0 leitet einen pcTag-Zielwert von 15 ab.
- Der Datenverkehr von einer L3Out-EPG mit 0.0.0.0/0 zu einer internen ACI-EPG leitet einen Quell-PC-Tag der VRF-Instanz ab (49153).

Das contract_parser-Skript bietet eine ganzheitliche Ansicht der Zoning-Regeln:

```
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]
```

Bestätigen des vom Paket verwendeten pcTag mithilfe der ELAM Assistant-App

Die ELAM Assistant App bietet eine weitere Methode zur Bestätigung des Quell- und Ziel-PCtag von Live-Datenverkehrsflüssen.

Der folgende Screenshot zeigt das ELAM-Ergebnis für den Datenverkehr vom pcTag 32771 zum pcTag 49153.

ELAM Assistant App-Ausgabe für src 32771 bis 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)

Schlussfolgerung

Die Verwendung von 0.0.0.0/0 muss innerhalb einer VRF-Instanz sorgfältig überwacht werden, da jedes L3Out, das dieses Subnetz verwendet, die Verträge erbt, die auf jedes andere L3Out angewendet werden, das diese Instanz verwendet. Dies wird wahrscheinlich zu ungeplanten Genehmigungsflüssen führen.

Freigegebene L3Out

Überblick

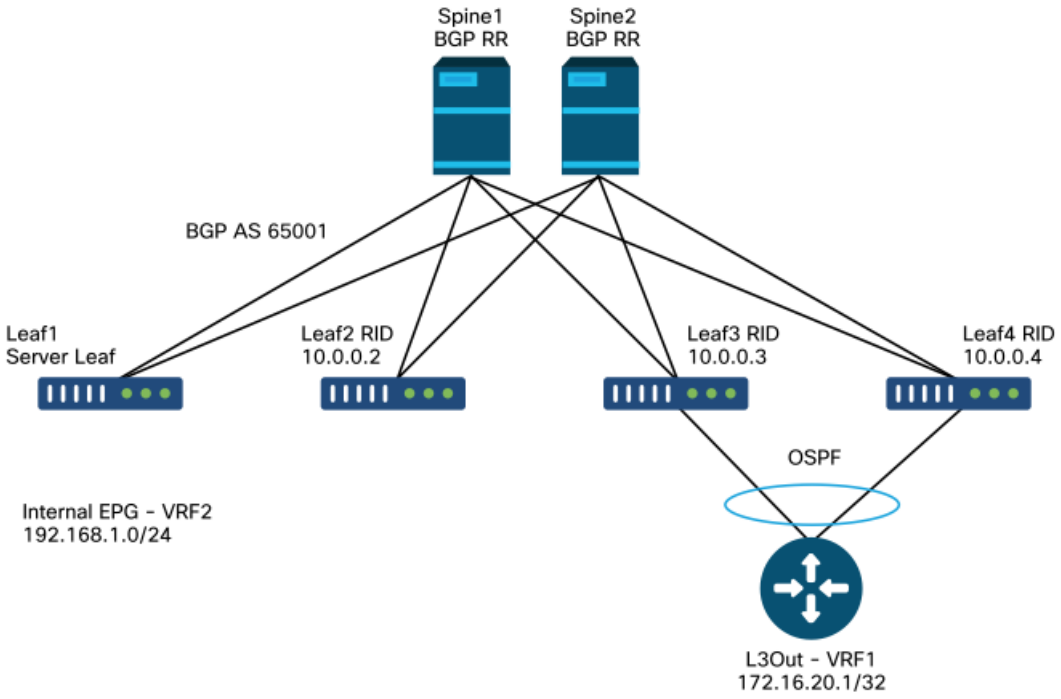
In diesem Abschnitt wird die Fehlerbehebung bei Routing-Advertisement-Nachrichten in Shared L3Out-Konfigurationen erläutert. Der Begriff "Shared L3Out" bezieht sich auf das Szenario, in dem sich ein L3Out in einer VRF-Instanz, eine interne EPG mit einem Vertrag mit dem L3Out jedoch in einer anderen VRF-Instanz befindet. Bei gemeinsam genutzten L3Outs erfolgt das Route Leaking

intern an die ACI-Fabric.

In diesem Abschnitt wird nicht im Detail auf die Fehlerbehebung für Sicherheitsrichtlinien eingegangen. Lesen Sie dazu das Kapitel "Sicherheitsrichtlinien" in diesem Buch. In diesem Abschnitt wird auch nicht im Detail auf die Präfix-Klassifizierung für externe Richtlinien zu Sicherheitszwecken eingegangen. Weitere Informationen finden Sie im Abschnitt "Vertrag und L3Out" im Kapitel "Externe Weiterleitung".

In diesem Abschnitt wird die folgende Topologie für unsere Beispiele verwendet.

Gemeinsam genutzte L3Out-Topologie



Auf oberster Ebene müssen die folgenden Konfigurationen vorhanden sein, damit ein Shared L3Out funktioniert:

- Ein L3Out-Subnetz muss mit dem Bereich "Shared Route Control Subnet" (Subnetz für gemeinsame Routenkontrolle) konfiguriert werden, um externe Routen an interne VRFs weiterzuleiten. Die Option "Aggregate Shared" (Gemeinsam genutzt aggregieren) kann ebenfalls ausgewählt werden, um alle Routen zu löschen, die spezifischer sind als das konfigurierte Subnetz.
- Ein L3Out-Subnetz muss mit dem Bereich "Shared Security Import Subnet" (Gemeinsames Sicherheitsimport-Subnetz) konfiguriert werden, um die Sicherheitsrichtlinien zu programmieren, die für die Kommunikation über dieses L3Out erforderlich sind.
- Das interne BD-Subnetz muss auf "Shared between VRFs" (Gemeinsam genutzte VRF-Instanzen) und "Advertise External" (Extern bewerben) gesetzt werden, damit das BD-Subnetz in der externen VRF-Instanz programmiert und angekündigt werden kann.

- Zwischen der internen EPG und der externen EPG des gemeinsam genutzten L3Out muss ein Tenant- oder globaler Bereichsvertrag konfiguriert werden.

Im nächsten Abschnitt wird detailliert beschrieben, wie ausgelaufene Routen in der ACI angekündigt und gelernt werden.

Gemeinsamer L3Out-Workflow - Lernen externer Routen

In diesem Abschnitt wird der Pfad einer erlernten externen Route beschrieben, wie sie im Fabric angekündigt wird.

Außenweg wie auf dem Grenzblatt zu sehen

Dieser Befehl zeigt die externe Route an, die vom OSPF empfangen wurde:

```
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
```

Anschließend muss die Route in das BGP importiert werden. Standardmäßig müssen alle externen Routen in das BGP importiert werden.

BGP-Überprüfungen auf dem Grenzblatt

Die Route muss zur BGP-VPNv4-Adressfamilie gehören, wobei ein Routing-Ziel über das gesamte Fabric verteilt werden muss. Das Route Target ist eine erweiterte BGP-Community, die von der externen VRF-Instanz exportiert und von allen internen VRF-Instanzen importiert wird, die den Pfad erhalten müssen.

Überprüfen Sie anschließend das Route Target, das von der externen VRF-Instanz des BL exportiert wird.

```
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
```

Die obige Ausgabe zeigt, dass alle Pfade, die von der externen VRF-Instanz in VPNv4 gemeldet werden, ein Routing-Ziel von 65001:2392068 erhalten sollten.

Überprüfen Sie anschließend den BGP-Pfad:

```
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
```

Die obige Ausgabe zeigt, dass der Pfad das richtige Routen-Ziel hat. Der VPNv4-Pfad kann auch mithilfe des Befehls "show bgp vpnv4 unicast 172.16.20.1 vrf overlay-1" überprüft werden.

Überprüfungen auf dem Server-Leaf

Damit das interne EPG-Leaf die vom BL angekündigte Route installieren kann, muss es das (oben erwähnte) Route-Target in die interne VRF-Instanz importieren. Der BGP-Prozess der internen VRF-Instanz kann überprüft werden, um Folgendes zu validieren:

```
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
```

Die obige Ausgabe zeigt die interne VRF-Instanz, die das Routing-Ziel importiert, das von der externen VRF-Instanz exportiert wird. Außerdem wird auf eine "Import Route Map" (Routenübersicht importieren) verwiesen. Die Import-Route-Map enthält die spezifischen Präfixe, die im gemeinsam genutzten L3Out mit dem Flag "Shared Route Control Subnet" definiert sind.

Der Inhalt der Routenübersicht kann überprüft werden, um sicherzustellen, dass er das externe Präfix enthält:

```
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
```

Die obige Ausgabe zeigt die Import-Route-Map, die das zu importierende Subnetz enthält.

Die abschließenden Überprüfungen umfassen die Überprüfung, ob die Route in der BGP-Tabelle und in der Routing-Tabelle installiert ist.

BGP-Tabelle auf Server-Leaf:

```
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
```

Die Route wird in die interne VRF-BGP-Tabelle importiert und hat das erwartete Routenziel.

Die installierten Routen können überprüft werden:

```
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
```

Die obige Ausgabe verwendet einen spezifischen 'vsh -c' Befehl, um die 'detail'-Ausgabe zu erhalten. Das Flag "detail" enthält die VXLAN-VNID zum Umschreiben. Dies ist die VXLAN-VNID der externen VRF-Instanz. Wenn das BL Datenverkehr über ein Datenflugzeug mit dieser VNID empfängt, weiß es, dass es die Weiterleitungsentscheidung in der externen VRF-Instanz treffen muss.

Der rw-vnid-Wert ist in Hex angegeben, sodass die Umwandlung in eine Dezimalzahl die VRF-VNID 2392068 ergibt. Suchen Sie mithilfe von "show system internal epm vrf all" nach der entsprechenden VRF-Instanz. | Grep 2392068' auf dem Blatt. Eine globale Suche auf einem APIC

kann mit dem Befehl 'moquery -c fvCtx -f 'fv.Ctx.seg=="2392068"' durchgeführt werden.

Die IP-Adresse des nächsten Hop sollte ebenfalls auf die BL-PTEPs verweisen, und "%overlay-1" gibt an, dass die Routensuche für den nächsten Hop in der Overlay-VRF-Instanz erfolgt.

Gemeinsamer L3Out-Workflow - Ankündigung interner Routen

Wie in den vorherigen Abschnitten wird die Werbung für interne BD-Subnetze in einem gemeinsam genutzten L3Out wie folgt gehandhabt:

- Das BD-Subnetz (internes VRF) wird auf dem BL (externes VRF) als statische Route installiert. Diese Bereitstellung statischer Routen ist das Ergebnis der Vertragsbeziehung zwischen der internen EPG und L3Out.
- Die statische Route wird in das externe Protokoll umverteilt, wenn der Bereich "Advertised External" im BD-Subnetz festgelegt wird.

Statische BD-Route auf BL überprüfen

```
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
```

Beachten Sie, dass in der obigen Ausgabe die VNID der internen VRF-Instanz für das Umschreiben festgelegt ist. Next-Hop wird ebenfalls auf die Proxy-v4-Anycast-Adresse festgelegt.

Die obige Route wird extern über dieselben Routenpläne bekannt gegeben, die im Abschnitt "Routenankündigung" vorgestellt werden.

Wenn ein BD-Subnetz auf "Extern bewerben" gesetzt ist, wird es in **jedes externe L3Out-Protokoll** umverteilt, mit dem die interne EPG eine Vertragsbeziehung hat.

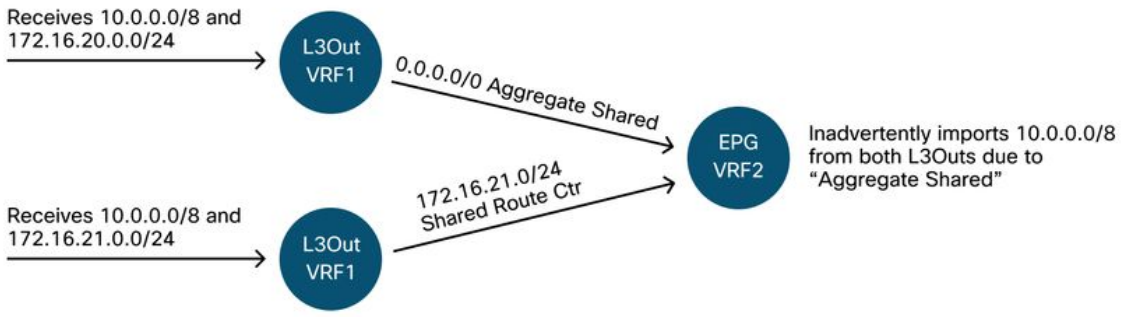
Shared L3Out-Fehlerbehebungsszenario - unerwartetes Durchlaufen der Route

Dieses Szenario enthält mehrere L3Outs im externen VRF, und eine interne EPG empfängt eine Route von einem L3Out, bei dem das Netzwerk **nicht** mit den Optionen für den gemeinsam genutzten Bereich definiert **ist**.

Verwendung von "Gesamt freigegeben"

Betrachten wir die folgende Zahl:

Unerwartete Route Leck



Die BGP-Import-Map mit der aus den Flags des **"Shared Route Control Subnet"** programmierten Präfixliste wird auf VRF-Ebene angewendet. Wenn ein L3Out in VRF1 über ein Subnetz mit "Shared Route Control Subnet" verfügt, werden alle über L3Outs innerhalb von VRF1 empfangenen Routen, die diesem Shared Route Control Subnet entsprechen, in VRF2 importiert.

Das obige Design kann zu unerwarteten Datenverkehrsflüssen führen. Wenn es keine Verträge zwischen der internen EPG und der unerwarteten L3Out-EPG für Werbung gibt, wird Datenverkehr verloren gehen.

Informationen zu dieser Übersetzung

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