

# Probleemoplossing voor ACI-extern doorsturen

## Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Overzicht](#)

[L3Out componenten](#)

[Belangrijke onderdelen van een L3Out](#)

[Externe routing](#)

[Externe routeringsstroom op hoog niveau](#)

[L3Out EPG-configuratieopties](#)

[Een L3Out-subnet wordt gedefinieerd inclusief 'scope'-definitie](#)

[L3Out topologie die in deze sectie wordt gebruikt](#)

[L3Out-topologie](#)

[Aangrenzingeren](#)

[BGP](#)

[Connectiviteitsprofiel van peers — Local-AS](#)

[Connectiviteitsprofiel van peers — Remote AS](#)

[L3Out — Connectiviteitsprofiel van BGP-peers](#)

[Profiel van logisch knooppunt — Node Association](#)

[BGP CLI-verificatie \(eBGP met loopback-voorbeeld\)](#)

[OSPF](#)

[L3Out — OSPF-interfaceprofiel — Area ID en type](#)

[Logisch interfaceprofiel — SVI](#)

[OSPF-interfaceprofiel](#)

[OSPF-interfaceprofiel — Hallo/dode timer en netwerktype](#)

[OSPF-interfacebeleidsdetails](#)

[OSPF CLI-verificatie](#)

[EIGRP](#)

[EIGRP-interfaceprofiel](#)

[EIGRP CLI-verificatie](#)

[Routespot](#)

[advertentieworkflow voor bridge-domeinroutes](#)

[Alvorens het contract tussen L3Out en interne EPG toe te passen](#)

[Na toepassing van het contract tussen L3Out en interne EPG](#)

[Na het selecteren van 'Extern adverteren' op BD Subnet](#)

[Nadat de L3Out aan de BD is gekoppeld](#)

[BGP-routeradvertenties](#)

[EIGRP-routeradvertenties](#)

[Configuratie van Bridge Domain L3](#)

[Probleemoplossing voor advertenties via Bridge Domain Route](#)

[Standaard-export routeprofiel met weigeringsrecht](#)

[Werkstroom voor externe routeinvoer](#)

[De route is geïnstalleerd in de BL-routeringstabel](#)  
[Controleer de route op het interne blad](#)  
[Externe route-probleemoplossing](#)  
[advertentieworkflow voor doorvoerroutes](#)  
[Doorvoerroutingtopologie](#)  
[Routetag-beleid](#)  
[Routebeheer voor export](#)  
[Transit Routing bij ontvangst en reclame BL zijn hetzelfde](#)  
[Transit routing probleemoplossing scenario's #1: Transit Route niet geadverteerd](#)  
[Transit routing probleemoplossing scenario's #2: Transit Route niet ontvangen](#)  
[Externe router met enkele VRF — Transit Route niet ontvangen](#)  
[Transit Routing Problemen oplossen scenario's #3 — Transit Routes onverwacht geadverteerd](#)  
[Contract en L3Out](#)  
[Op voorvoegsel gebaseerde EPG op L3Out](#)  
[Plaats van de pcTag voor een L3Out](#)  
[Voorbeeld 1: Single L3Out met specifieke prefix](#)  
[Subnet met 'Externe subnetten voor de externe EPG'-scope](#)  
[Voorbeeld 2: Single L3Out met meerdere prefixes](#)  
[Voorbeeld 3a: Meervoudige L3Out EPG's in een VRF](#)  
[Verificatie van de L3Out pcTag](#)  
[Voorbeeld 3b: meerdere L3Out EPG's met verschillende contracten](#)  
[Datapath-validatie met behulp van fTriage — flow toegestaan door beleid](#)  
[Datapath-validatie met fTriage — flow die niet is toegestaan volgens beleid](#)  
[Voorbeeld 4: meerdere L3Outs met meerdere prefixes](#)  
[Datapath-validatie met behulp van fTriage — flow die door beleid is toegestaan](#)  
[Datapath-validatie met fTriage — flow die niet is toegestaan volgens beleid](#)  
[Validatie van datapath — regels voor zonerings](#)  
[Verificatie van de pcTag van de VRF](#)  
[Bevestigen van pcTag gebruikt door pakket met ELAM Assistant-app](#)  
[ELAM Assistant-app-uitvoer voor src 32771 naar 49153](#)  
[Conclusie](#)  
[Gedeeld L3Out](#)  
[Overzicht](#)  
[Gedeelde L3Out-topologie](#)  
[Gedeelde L3Out workflow — externe trajecten leren](#)  
[Externe route zoals gezien op het grensblad](#)  
[BGP-verificaties op het grensblad](#)  
[Verificaties op de server](#)  
[Gedeelde L3Out workflow — reclame maken voor interne routes](#)  
[Controleer de BD statische route op de BL](#)  
[Gedeeld L3Out probleemoplossing scenario — onverwacht route lekken](#)  
[Gebruik van 'Gedeeld aggregaat'](#)  
[Onverwacht weglek](#)

## Inleiding

Dit document beschrijft stappen om een L3out in ACI te begrijpen en probleemoplossing te bieden

## Achtergrondinformatie

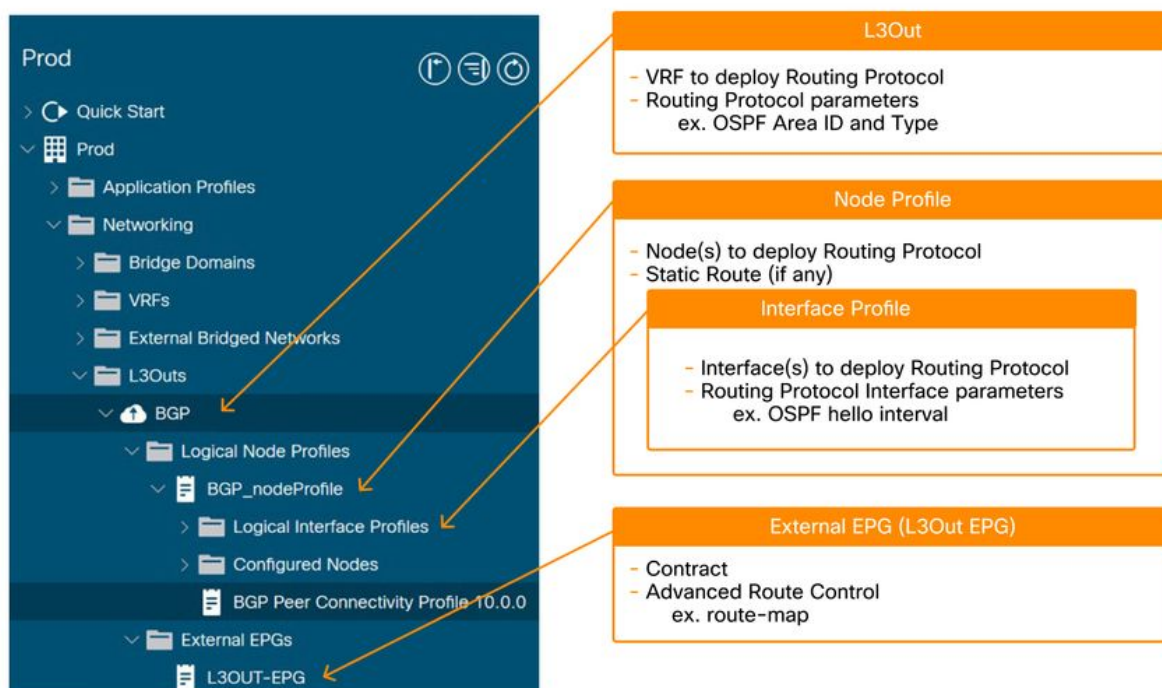
Het materiaal van dit document werd afgeleid uit de [Problemen oplossen Cisco Application Centric Infrastructure, Second Edition boek](#) specifiek het **Externe Forwarding - Overzicht**, **Extern Forwarding - Adjacencies**, **Externe Forwarding - Route advertentie**, **Extern Forwarding - Contract** en **L3out** en **Extern Forwarding - Share L3out** hoofdstukken.

## Overzicht

### L3Out componenten

Het volgende beeld illustreert de belangrijkste bouwstenen die nodig zijn om een L3 Outside (L3Out) te configureren.

### Belangrijke onderdelen van een L3Out



1. Root van L3Out: Selecteer een routeringsprotocol om te implementeren (zoals OSPF, BGP). Selecteer een VRF om het routeringsprotocol te implementeren. Selecteer een L3Out-domein om beschikbare bladinterfaces en VLAN voor de L3Out te definiëren.
2. Profiel knooppunt: Switch Selecteer bladprotocollen om het routingprotocol te implementeren. Deze worden doorgaans "Border Leaf Switches" (BL) genoemd. Configureer router-ID (RID) voor het routeringsprotocol op elk grensblad. In tegenstelling tot een normale router wijst ACI niet automatisch een router-ID toe op basis van een IP-adres op de switch. Configureer een statische route.
3. Interfaceprofiel: Configureer bladinterfaces om het routeringsprotocol uit te voeren. Bijvoorbeeld interfacetype (SVI, routed-port, subinterface), interface-ID en IP-adressen enz. Selecteer een beleid voor routingprotocolparameters op interfaceniveau (zoals hello-

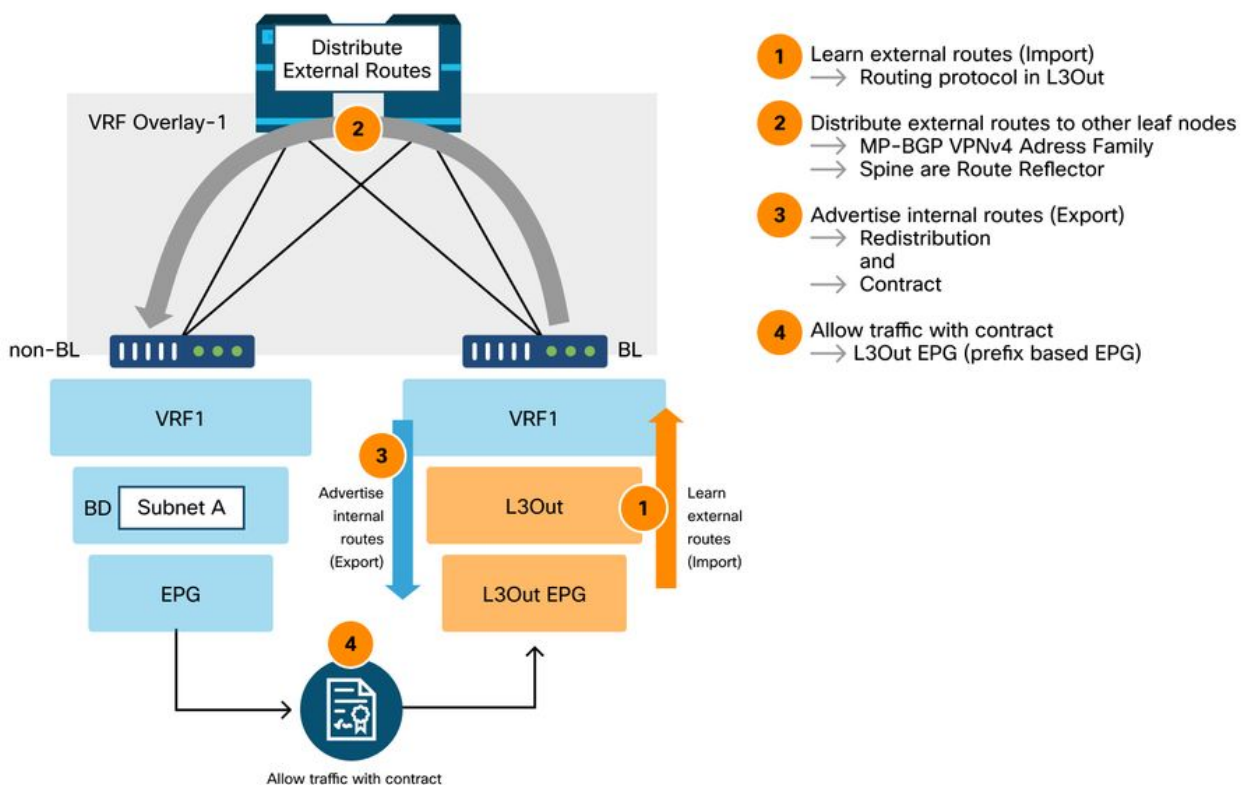
interval).

4. Externe EPG (L3Out EPG): Een 'Externe EPG' is een harde eis om al het beleid dat aan de L3Out is gekoppeld, zoals IP-adressen of SVI's, te implementeren om burens te vestigen. Nadere gegevens over het gebruik van externe EPG's komen later aan bod.

## Externe routing

Het volgende diagram toont de handeling op hoog niveau die betrokken is bij externe routing.

### Externe routeringsstroom op hoog niveau



1. De BL('s) zullen de routingprotocolnabijheid met externe routers duidelijk maken.
2. Routeprefixes worden ontvangen van externe routers en ingespoten in MP-BGP als VPNv4-adresfamiliepad. Minstens moeten twee wervelkolomknooppunten worden geconfigureerd als BGP-routerreflectoren om externe routes naar alle bladknooppunten weer te geven.
3. Interne prefixes (BD subnetten) en/of prefixes ontvangen van andere L3Out moeten expliciet opnieuw verdeeld worden in het routeringsprotocol om geadverteerd te worden naar de externe router.
4. Beveiliging: een L3Out bevat ten minste één L3Out EPG. Een contract moet worden geconsumeerd of geleverd op de L3Out EPG (ook wel l3extInstP genoemd vanuit de klassennaam) om verkeer in/uit de L3Out toe te staan.

## L3Out EPG-configuratieopties

In het L3Out EPG-gedeelte kunnen subnetten worden gedefinieerd met een reeks 'Scope'- en 'Aggregate'-opties, zoals hieronder wordt weergegeven:

## Een L3Out-subnet wordt gedefinieerd inclusief 'scope'-definitie

### Create Subnet



IP Address:   
address/mask

Name:

- scope:
- Export Route Control Subnet
  - Import Route Control Subnet
  - External Subnets for the External EPG
  - Shared Route Control Subnet
  - Shared Security Import Subnet

BGP Route Summarization Policy:

- aggregate:
- Aggregate Export
  - Aggregate Import
  - Aggregate Shared Routes

Route Control Profile:

Name	Direction
------	-----------

Cancel

Submit

"Toepassingsgebied":

- **Subnet van de Routecontrole van de uitvoer:** Dit werkingsgebied moet (de uitvoer) subnet van ACI aan buitenkant via L3Out adverteren. Hoewel dit voornamelijk voor Transit Routing is, kan dit ook worden gebruikt om een BD-subnetverbinding te adverteren zoals beschreven in de sectie "ACI BD-subnetreclame".
- **Subnet van de Route van de invoer:** Dit werkingsgebied is over het leren (het invoeren) van externe subnet van L3Out. Standaard is deze scope uitgeschakeld, vandaar dat het grijs wordt weergegeven, en een border leaf (BL) leert alle routes uit een routeringsprotocol. Dit werkingsgebied kan worden toegelaten wanneer het externe routes moet beperken die via OSPF en BGP worden geleerd. Dit wordt niet ondersteund voor EIGRP. Om dit bereik te gebruiken, moet 'Import Route Control Enforcement' eerst worden ingeschakeld op een bepaalde L3Out.
- **Externe subnetten voor de externe EPG (import-security):** Deze scope wordt gebruikt om pakketten met het geconfigureerde subnet van of naar de L3Out met een contract toe te staan. Het classificeert een pakket in de geconfigureerde L3Out EPG op basis van het subnetnet zodat een contract op de L3Out EPG kan worden toegepast op het pakket. Dit werkingsgebied is een Langste Prefix Gelijke in plaats van een nauwkeurige gelijke als ander werkingsgebied voor het verpletteren van lijst. Als 10.0.0.0/16 is geconfigureerd met 'Externe subnetten voor de externe EPG' in L3Out EPG A, worden alle pakketten met IP in dat subnet, zoals 10.0.1.1, geclassificeerd in de L3Out EPG A om er een contract op te gebruiken. Dit betekent niet dat 'Externe subnetten voor de Externe EPG'-scope een route 10.0.0.0/16 in een routingstabel installeert. Het zal een andere interne tabel maken om een subnetverbinding uitsluitend voor een contract aan een EPG (pcTag) toe te wijzen. Het heeft geen gevolgen voor het routeren van protocolgedrag. Deze scope moet worden geconfigureerd op een L3Out die het subnetnet leert.

- **Subnet van de gedeelde Routecontrole:** Dit werkingsgebied moet externe subnet aan een andere VRF lekken. ACI gebruikt MP-BGP en Route Target om een externe route van de ene naar de andere VRF te lekken. Dit werkingsgebied leidt tot een prefix-lijst met het Subnet, dat als filter wordt gebruikt om routes met routedoel in MP-BGP uit te voeren/in te voeren. Deze scope moet worden geconfigureerd op een L3Out die het subnetnet leert in de originele VRF.
- **Subnet voor gedeelde beveiliging:** dit bereik wordt gebruikt om pakketten toe te staan met het geconfigureerde subnet wanneer de pakketten over VRF's met een L3Out worden verplaatst. Een route in een routingstabel lekt uit naar een andere VRF met 'Shared Route Control Subnet' zoals hierboven vermeld. Een andere VRF moet echter nog weten tot welke EPG de uitgelekte route behoort. Het 'Shared Security Import Subnet' informeert een andere VRF over de L3Out EPG waartoe de gelekte route behoort. Daarom kan deze scope alleen worden gebruikt wanneer 'Externe Subnets voor de Externe EPG' ook wordt gebruikt, anders weet de originele VRF niet welke L3Out EPG het subnet tot één van beide behoort. Deze scope is ook de langste prefixmatch.

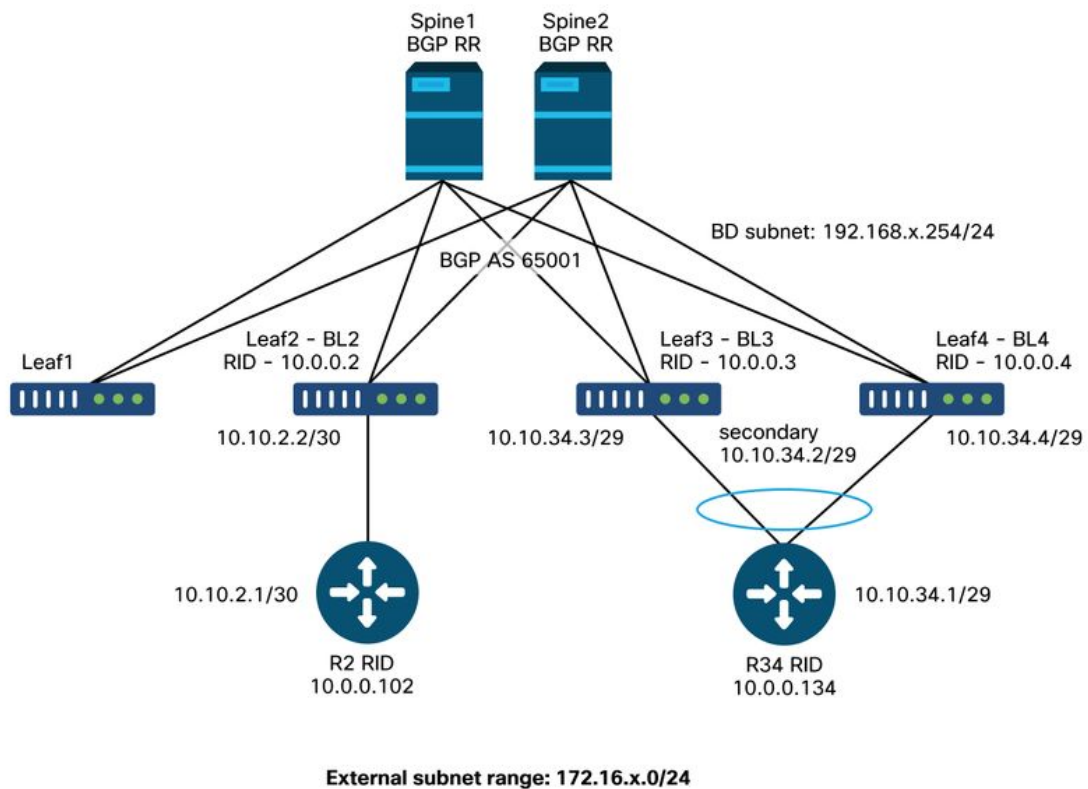
'Samengevoegde' opties:

- **Geaggregeerde export:** deze optie kan alleen worden gebruikt voor 0.0.0.0/0 met 'Export Route Control Subnet'. Wanneer zowel 'Export Route Control Subnet' als 'Aggregate Export' zijn ingeschakeld voor 0.0.0.0/0; het maakt een voorvoegsel-lijst met '0.0.0.0/0 le 32' die overeenkomt met alle subnetten. Daarom kan deze optie worden gebruikt wanneer een L3Out moet adverteren (exporteren) naar de buitenwereld. Wanneer meer korrelige aggregatie is vereist, kan routekaart/profiel met een expliciete prefixlijst worden gebruikt.
- **Geaggregeerde import:** deze optie kan alleen worden gebruikt voor 0.0.0.0/0 met 'Import Route Control Subnet'. Wanneer zowel 'Import Route Control Subnet' en 'Aggregate Import' zijn ingeschakeld voor 0.0.0.0/0, maakt het een voorvoegsel-lijst met '0.0.0.0/0 le 32' die overeenkomt met elk subnet. Daarom kan deze optie worden gebruikt wanneer een L3Out alle routes van buiten moet leren (importeren). Hetzelfde kan echter worden bereikt door 'Import Route Control Enforcement' uit te schakelen, wat de standaard is. Wanneer meer korrelige aggregatie is vereist, kan routekaart/profiel met een expliciete prefixlijst worden gebruikt.
- **Geaggregeerde gedeelde routers:** deze optie kan voor elke subnet met 'Shared Route Control Subnet' worden gebruikt. Wanneer zowel 'Shared Route Control Subnet' als 'Aggregate Shared Routes' zijn ingeschakeld voor 10.0.0.0/8 als voorbeeld, maakt het een voorvoegsel-lijst met '10.0.0.0/8 le 32' die overeenkomt met 10.0.0.0/8, 10.1.0.0/16 enzovoort.

## L3Out topologie die in deze sectie wordt gebruikt

De volgende topologie zal in deze sectie worden gebruikt:

### L3Out-topologie



## Aangrenzingen

Deze sectie legt uit hoe u problemen kunt oplossen en verifiëren bij routingprotocolnabijheid op L3Out interfaces.

Hieronder staan een aantal parameters om te controleren dat van toepassing zal zijn op alle ACI externe routeringsprotocollen:

- **Routerid:** in ACI moet elke L3Out dezelfde routerid in dezelfde VRF op hetzelfde blad gebruiken, zelfs als routerprotocollen verschillend zijn. Ook kan slechts een van die L3Outs op hetzelfde blad een loopback maken met de router-ID, wat doorgaans BGP is.
- **MTU:** Hoewel de harde eis van MTU alleen voor OSPF-nabijheid is, wordt aanbevolen om MTU aan te passen voor routeprotocollen om ervoor te zorgen dat jumbopakketten die voor routeuitwisseling/updates worden gebruikt zonder fragmentatie kunnen worden verzonden, aangezien de meeste frames van besturingsplane worden verzonden met de DF (don't fragment)-bitset, die het frame laat vallen als de grootte ervan de maximale MTU van de interface overschrijdt.
- **MP-BGP routerreflector:** zonder dit, zal het BGP-proces niet starten op bladknooppunten. Hoewel dit niet vereist is voor OSPF of EIGRP om alleen een buur te vestigen, is het nog steeds nodig voor BL's om externe routes naar andere bladknooppunten te distribueren.
- **Fouten:** Controleer altijd de fouten tijdens en na de configuratie.

## BGP

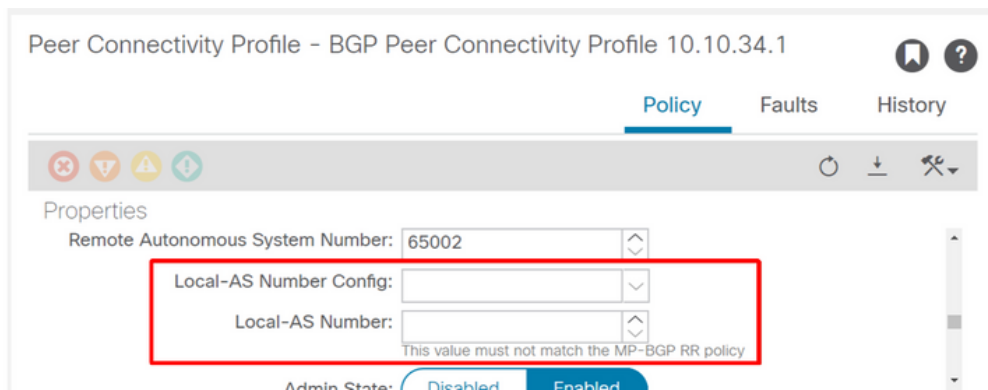
Deze sectie gebruikt een voorbeeld van een eBGP peering tussen de loopback op BL3, BL4, en

R34 van de topologie in de sectie Overzicht. De BGP AS op R34 is 65002.

Controleer de volgende criteria bij het instellen van een BGP-nabijheid.

- Lokaal BGP AS-nummer (ACI BL-kant).

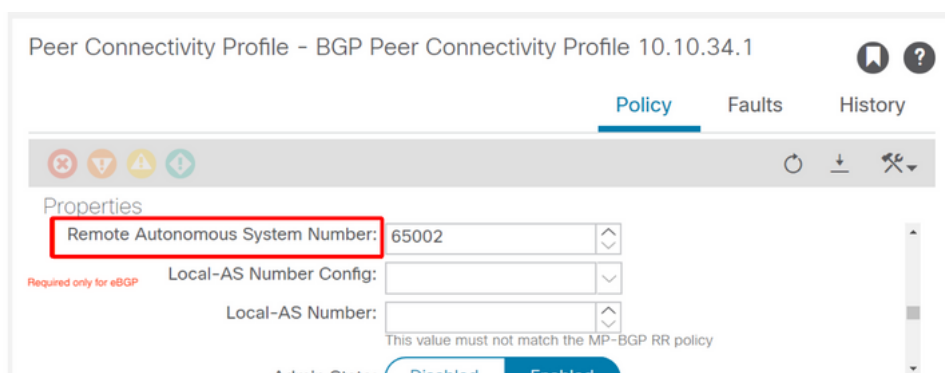
## Connectiviteitsprofiel van peers — Local-AS



Het BGP AS-nummer van een gebruiker L3Out zal automatisch hetzelfde zijn als de BGP AS voor de infra-MP-BGP die is geconfigureerd in het BGP-routerreflectorbeleid. De 'Local AS'-configuratie in het BGP Peer Connectivity Profile is niet vereist tenzij men de ACI BGP AS naar de buitenwereld moet verhullen. Dit betekent dat externe routers moeten verwijzen naar de BGP AS die in de BGP-routerreflector is geconfigureerd.

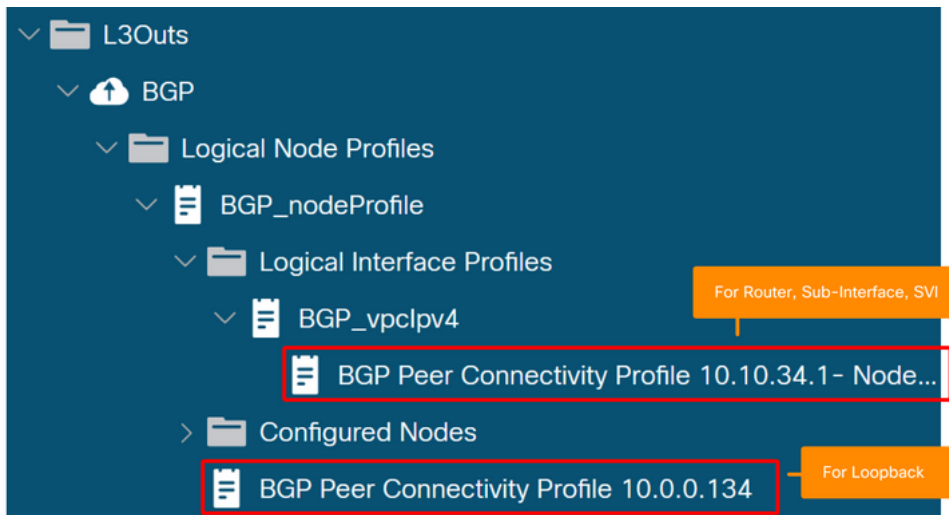
OPMERKING — Het scenario waarin lokale AS-configuratie is vereist, is hetzelfde als de zelfstandige opdracht NX-OS 'lokaal-als'.

- Remote BGP AS-nummer (externe kant) **Connectiviteitsprofiel van peers — Remote AS**

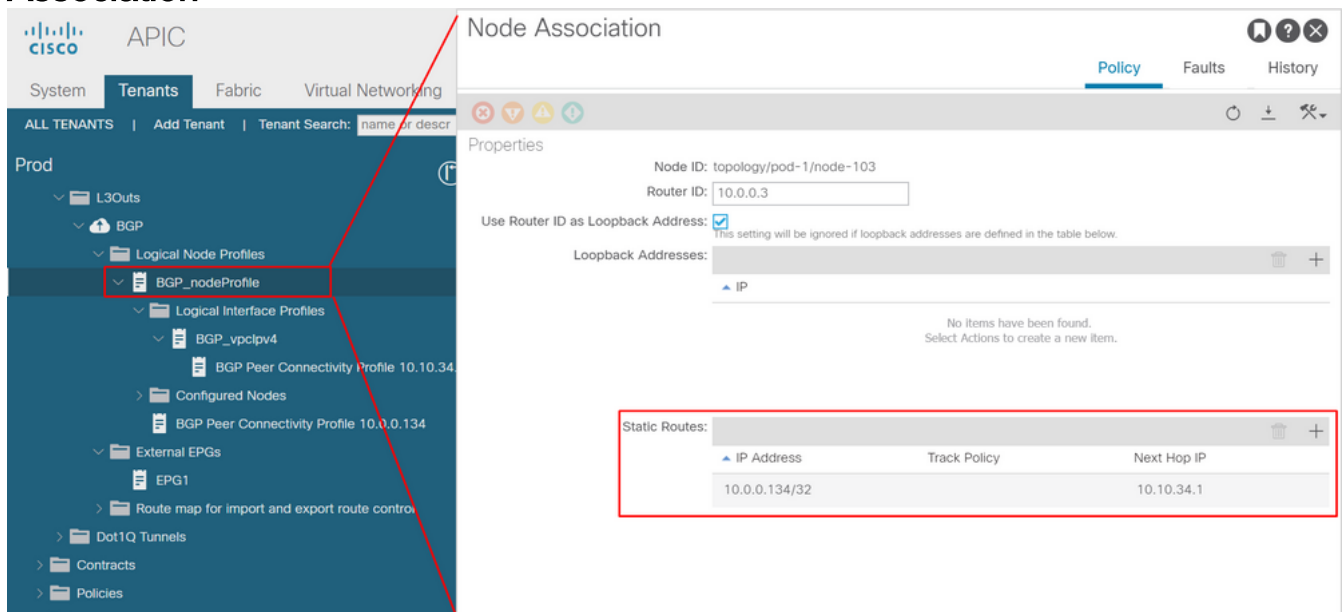


Het Remote BGP AS-nummer is alleen vereist voor eBGP waarbij de BGP AS van de buur verschilt van ACI BGP AS. Bron-IP voor BGP-peer sessie. **L3Out — Connectiviteitsprofiel van BGP-peers**





ACI ondersteunt het inkopen van een BGP-sessie via de loopback-interface bovenop een typisch ACI L3Out interfacetype (routed, sub-interface, SVI). Wanneer een BGP-sessie van een loopback moet worden afgeleid, configureer dan het BGP-peer-connectiviteitsprofiel onder het profiel van het logische knooppunt. Wanneer de BGP-sessie moet worden gebaseerd op een routing/subinterface/SVI, configureer dan het BGP-peer-connectiviteitsprofiel onder het logische interfaceprofiel. BGP peer-IP bereikbaarheid. **Profiel van logisch knooppunt — Node Association**



Wanneer de BGP peer IPs loopbacks zijn, zorg ervoor dat de BL en de externe router bereikbaar zijn voor het IP-adres van de peer. Statische routes of OSPF kunnen worden gebruikt om bereikbaarheid te bereiken voor de peer IP's. **BGP CLI-verificatie (eBGP met loopback-voorbeeld)** De CLI uitgangen voor de volgende stappen worden verzameld van BL3 in de topologie van de sectie Overzicht. **1. Controleer of de BGP-sessie is ingesteld** 'State/PfxRcd' in de volgende CLI-uitvoer betekent dat de BGP-sessie wordt ingesteld.

```
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

Als de 'State/PfxRcd' inactieveert of actief is, worden BGP-pakketten nog niet met de peer uitgewisseld. In een dergelijk scenario controleert u het volgende en gaat u verder met de volgende stap.

- Zorg ervoor dat de externe router correct naar de ACI BGP wijst (lokaal AS-nummer 65001).
- Zorg ervoor dat het ACI BGP-peer connectiviteitsprofiel de juiste buur-IP specificeert waarvan de externe router de BGP-sessie (10.0.0.134) opvraagt.
- Zorg ervoor dat het ACI BGP Peer Connectiviteitsprofiel de juiste buur AS van de externe router specificeert (Remote Autonomous System Number in GUI dat in CLI wordt weergegeven als AS 65002).

## 2. Controleer BGP-buurgegevens (BGP-peer connectiviteitsprofiel)

Het volgende bevel toont de parameters die voor BGP buuronderneming zeer belangrijk zijn.

- IP-buur: 10.0.0.134.
- Buurbuur BGP AS: extern AS 65002.
- Bron-IP: Het gebruik van loopback3 als updatebron.
- eBGP multihop: De externe peer van BGP zou tot 2 hop weg kunnen zijn.

```
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
```

Zodra de BGP peer correct wordt gevestigd, verschijnen de 'Local host' en 'Foreign host' onderaan de output.

## 3. Controleer IP-bereikbaarheid voor de 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
```

Zorg ervoor dat IP-adressering van de buur vanuit de bron-IP van ACI BGP pingt.

```
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. Controleer hetzelfde op de externe router

Het volgende is een voorbeeld van configuratie op de externe 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. Aanvullende stap — tcpdump

Op ACI-bladknooppunten kan het tcpdump-gereedschap de 'kpm\_inb' CPU-interface doorzoeken om te bevestigen of de protocolpakketten de blad-CPU hebben bereikt. Gebruik L4-poort 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
```

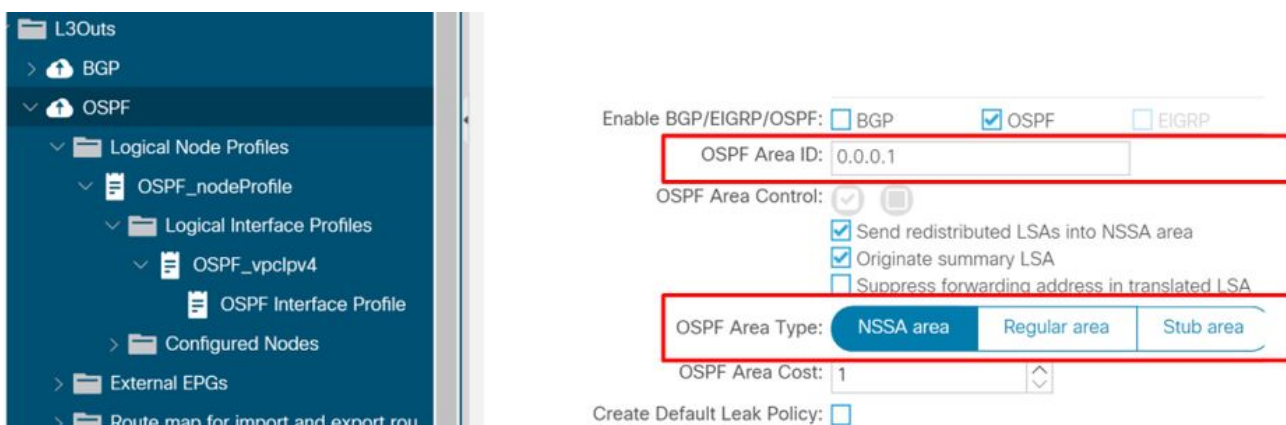
## OSPF

Deze sectie gebruikt een voorbeeld van burens OSPF tussen BL3, BL4, en R34 van de topologie in de sectie van het Overzicht met OSPF AreaID 1 (NSSA).

Het volgende zijn de gemeenschappelijke criteria om OSPF nabijheidsonderneming te controleren.

- OSPF-gebied-id en -type

## L3Out — OSPF-interfaceprofiel — Area ID en type



Net als elk routeringsapparaat, moeten OSPF Area ID en Type op beide burens overeenkomen. Sommige ACI-specifieke beperkingen op configuraties van OSPF Area ID omvatten:

- Eén L3Out kan slechts één OSPF Area ID hebben.
- Twee L3Outs kunnen dezelfde OSPF Area ID alleen in dezelfde VRF gebruiken als ze op twee verschillende bladknooppunten staan.

Ofschoon de OSPF-id geen backbone 0 hoeft te zijn, is het bij doorvoerrouting vereist tussen twee OSPF L3Outs op hetzelfde blad; één van hen moet OSPF Gebied 0 gebruiken omdat om het even welke routeuitwisseling tussen OSPF gebieden door OSPF Gebied 0 moet zijn.

- MTU

## Logisch interfaceprofiel — SVI

Logical Interface Profile - OSPF\_vpclpv4

Policy | Faults | History

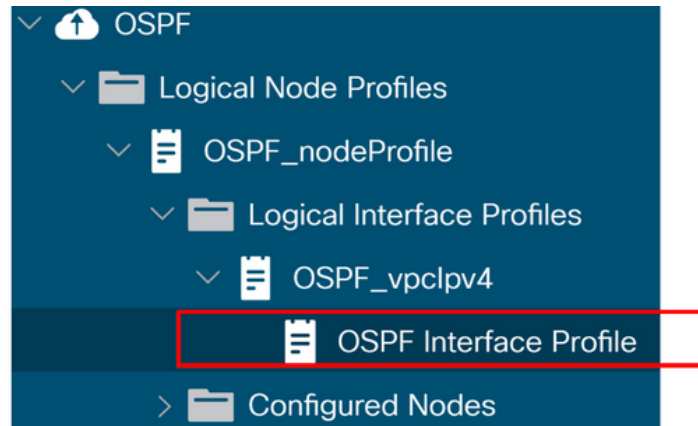
General | Routed Sub-Interfaces | Routed Interfaces | SVI | Floating SVI

Path	Side A IP	Side B IP	Secondary IP Address	IP Address	MAC Address	MTU (bytes)	Encap	Encap Scope
Pod-1/Node-103-104/N9K_VPC_3-4_13	10.10.34.3/29	10.10.34.4/29	10.10.34.2/29	0.0.0.0	00:22:BD:F8:19:FF	9000	vlan-2502	Local

De standaard MTU op ACI is 9000 bytes, in plaats van 1500 bytes, wat meestal het standaard is dat wordt gebruikt op traditionele routingapparaten. Zorg ervoor dat de MTU overeenkomt met het externe apparaat. Wanneer OSPF buuronderneming ontbreekt wegens MTU, wordt het geplakt bij UITWISSELING/DROTHER.

- IP-subnetmasker. OSPF vereist dat de IP-buur hetzelfde subnetmasker gebruikt.
- OSPF-interfaceprofiel

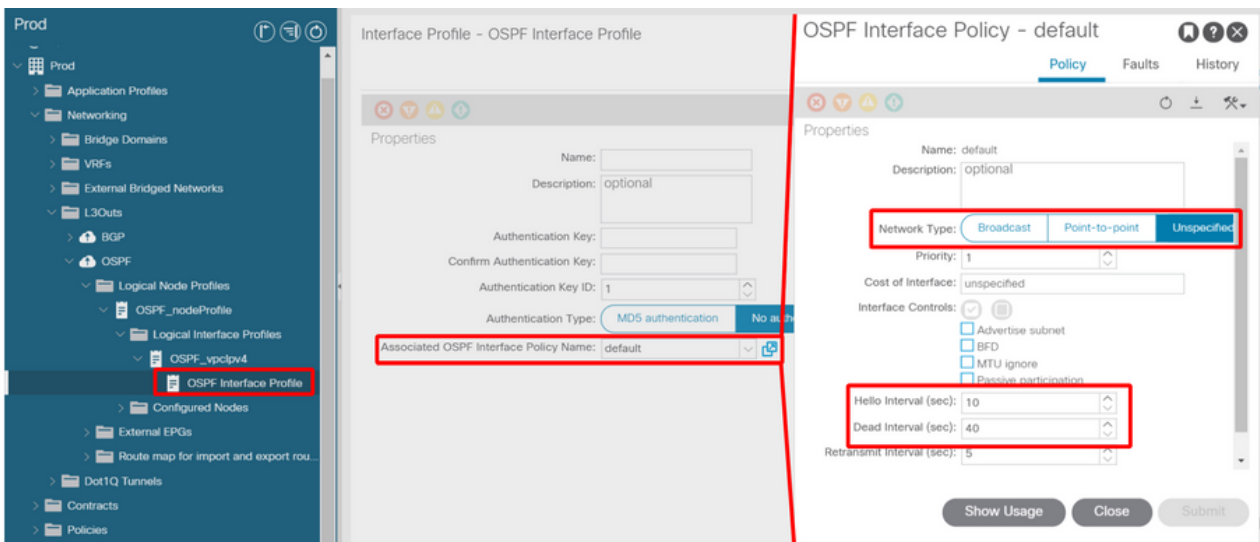
## OSPF-interfaceprofiel



Dit is gelijk aan 'ip router ospf <tag> gebied <area id>' op een standalone NX-OS-configuratie om OSPF in te schakelen op de interface. Zonder dit, zullen de bladinterfaces zich niet bij OSPF aansluiten.

- OSPF Hello / dode timer, netwerktype

## OSPF-interfaceprofiel — Hallo/dode timer en netwerktype



## OSPF-interfacebeleidsdetails

# Create OSPF Interface Policy



Name: OSPFIntPolicy

Description: optional

Network Type:  Broadcast  Point-to-point  Unspecified

Priority: 1

Cost of Interface: unspecified

Interface Controls:

- Advertise subnet
- BFD
- MTU ignore
- Passive participation

Hello Interval (sec): 10

Dead Interval (sec): 40

Retransmit Interval (sec): 5

Transmit Delay (sec): 1

OSPF vereist dat Hello en Dead Timers op elk buurapparaat overeenkomen. Deze worden geconfigureerd in het OSPF-interfaceprofiel.

Verzeker de overeenkomsten van het Type van OSPF-interfacenetwerk met het externe apparaat. Wanneer het externe apparaat type Point-to-Point gebruikt, moet de ACI-zijde Point-to-Point ook expliciet configureren. Deze worden ook geconfigureerd in het OSPF-interfaceprofiel.

## OSPF CLI-verificatie

De CLI uitgangen in de volgende stappen worden verzameld van BL3 in de topologie van de sectie "Overzicht".

### 1. Controleer OSPF-buurstatus

Als de 'Staat' in de volgende CLI 'FULL' is, wordt de OSPF-buur correct ingesteld. Anders gaat u door naar de volgende stap om de parameters te controleren.

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

In ACI, zullen BLs OSPF buurten met elkaar bovenop externe routers vormen wanneer het gebruiken van de zelfde ID van VLAN met een SVI. Dit komt doordat ACI een intern

overstromingsdomein heeft dat L3Out BD (of Externe BD) wordt genoemd voor elke VLAN-id in de L3Out SVI's. Merk op dat VLAN-id 28 een intern VLAN is dat PI-VLAN (Platform-Independent VLAN) wordt genoemd in plaats van het eigenlijke VLAN (Access Encap VLAN) dat op de bedrading wordt gebruikt. Gebruik het volgende commando om het access point VLAN te verifiëren ('VLAN-2502').

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

Men kon de zelfde output via access point VLAN ID ook krijgen.

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

## 2. Controleer het OSPF-gebied

Zorg ervoor dat de OSPF-gebied-id en het type identiek zijn aan de burens. Als het OSPF-interfaceprofiel ontbreekt, wordt de interface niet aangesloten bij OSPF en zal de interface niet verschijnen in de OSPF CLI-uitvoer.

```
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. Controleer OSPF-interfacedetails

Zorg ervoor dat de parameters op interfaceniveau voldoen aan de vereisten voor OSPF-buurinstelling zoals IP-Subnet, Netwerktipe, Hello/Dead Timer. Let op de VLAN-id om aan te geven dat SVI IP-VLAN is (VLAN28)

```
f2-leaf3# show ip ospf interface vrf Prod:VRF2
```

```
Vlan28 is up, line protocol is up
  IP address 10.10.34.3/29, Process ID default VRF Prod:VRF2, area 0.0.0.1
  Enabled by interface configuration
  State BDR, Network type BROADCAST, cost 4
  Index 94, Transmit delay 1 sec, Router Priority 1
  Designated Router ID: 10.0.0.4, address: 10.10.34.4
  Backup Designated Router ID: 10.0.0.3, address: 10.10.34.3
  2 Neighbors, flooding to 2, adjacent with 2
  Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello timer due in 0.000000
  No authentication
  Number of opaque link LSAs: 0, checksum sum 0
```

```
f2-leaf3# show interface vlan28
```

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

#### 4. Controleer IP-bereikbaarheid naar de buur

OSPF Hello-pakketten zijn Link Local Multicast-pakketten, maar OSPF DBD-pakketten die nodig zijn voor de eerste OSPF LSDB-uitwisseling zijn unicast. Daarom moet unicast bereikbaarheid ook voor de OSPF buuronderneming worden geverifieerd.

```
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. Controleer hetzelfde op de externe router

Hieronder vindt u voorbeelden van configuraties op de externe 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
```

Controleer de MTU ook op de fysieke interface.

#### 6. Extra trede — tcpdump

Op ACI-bladknooppunten kan de gebruiker tcpdump uitvoeren op de 'kpm\_inb' CPU-interface om te verifiëren of de protocolpakketten de blad-CPU hebben bereikt. Hoewel er meerdere filters voor OSPF zijn, is het IP-protocolnummer het meest uitgebreide filter.

- IP-protocolnummer: Proto 89 (IPv4) of ip6-protocol 0x59 (IPv6)
- IP-adres van de buur: host <ip>



- OSPF Link Local Mcast IP: host 24.0.0.5 of host 24.0.0.6

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

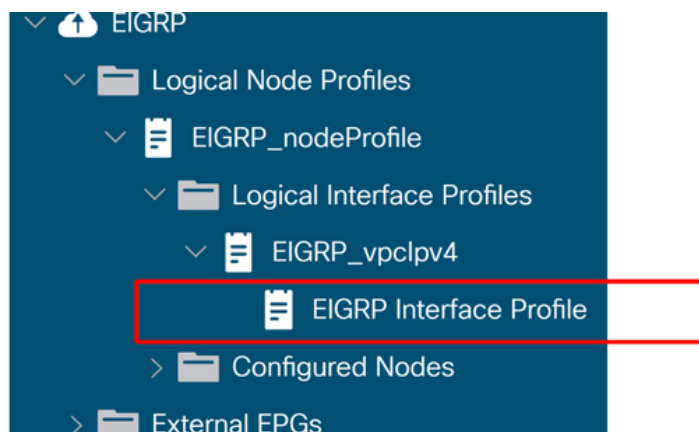
## EIGRP

In deze sectie wordt een voorbeeld gebruikt van de wijk EIGRP tussen BL3, BL4 en R34 vanuit de topologie in de sectie "Overzicht" met EIGRP AS 10.

Het volgende is de gemeenschappelijke criteria voor EIGRP nabijheidsonderneming.

- EIGRP AS: Een L3Out wordt toegewezen één EIGRP AS. Dit moet overeenkomen met het externe apparaat.
- EIGRP-interfaceprofiel.

## EIGRP-interfaceprofiel



Dit is gelijk aan de 'ip router eigrp <as>'-configuratie op een standalone NX-OS-apparaat. Zonder dit, zullen de bladinterfaces niet bij EIGRP aansluiten.

- MTU

Hoewel dit niet hoeft aan te passen om de EIGRP-wijk simpelweg te vestigen, kunnen de EIGRP-topologieuitwisselingspakketten groter worden dan de maximale MTU die is toegestaan op de interfaces tussen de peers, en omdat deze pakketten niet gefragmenteerd mogen zijn, worden ze kwijtgescholden en als gevolg zal de EIGRP-buurt flappen.

## EIGRP CLI-verificatie

De CLI uitgangen in de volgende stappen worden verzameld van BL3 in de topologie van de

sectie "Overzicht".

## 1. Controleer EIGRP-buurstatus

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

In ACI, zullen BLs een wijk EIGRP met elkaar bovenop externe routers vormen wanneer zij de zelfde ID van VLAN met SVI gebruiken. Dit komt doordat een ACI een intern overstromingsdomein heeft dat L3Out BD (of Externe BD) wordt genoemd voor elke VLAN-id in L3Out SVI's.

Houd er rekening mee dat VLAN-id 29 een intern VLAN is dat IP-VLAN (Platform-Independent VLAN) wordt genoemd, in plaats van het eigenlijke VLAN (Access Encap VLAN) dat op de bedrading wordt gebruikt. Gebruik het volgende commando om het access point VLAN (VLAN-2503) te verifiëren.

```
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
```

Men kon de zelfde output via access point VLAN ID ook krijgen.

```
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. Controleer EIGRP-interfacedetails

Verzeker EIGRP op de verwachte interface loopt. Als dit niet het geval is, controleert u het logische interfaceprofiel en het EIGRP-interfaceprofiel.

```
f2-leaf3# show ip eigrp interfaces vrf Prod:VRF3
EIGRP interfaces for process 10 VRF Prod:VRF3
Interface      Peers  Xmit Queue  Mean  Pacing Time  Multicast  Pending
              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. Controleer hetzelfde op de externe router

Het volgende is het voorbeeld config op de externe 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. Extra trede — tcpdump

Op ACI-bladknooppunten kan de gebruiker tcpdump uitvoeren op de 'kpm\_inb' CPU-interface om te bevestigen of de protocolpakketten de CPU van het blad hebben bereikt. Gebruik IP-protocolnummer 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
```

## Routespot

Deze sectie concentreert zich op de verificatie en het oplossen van problemen van routereclame in ACI. Er worden met name voorbeelden onderzocht van:

- Subnetadvertenties voor Bridge Domains.
- Aanmelding transitoroute.
- Route voor importeren en exporteren.

In deze paragraaf wordt routelekken besproken, aangezien het gaat om gedeelde L3Outs in latere secties.

### advertentieworkflow voor bridge-domeinroutes

Alvorens te kijken naar de algemene probleemoplossing moet de gebruiker zich vertrouwd maken met hoe Bridge Domain-advertenties moeten werken.

BD reclame, wanneer BD en L3Out in zelfde VRF zijn, omvat:

- Het hebben van een contractverhouding tussen L3Out en de interne EPG.
- L3Out koppelen aan het Bridge Domain.
- Selecteer 'Extern adverteren' op het BD-subnetje.

Daarnaast is het ook mogelijk om de Bridge Domain-advertenties te controleren met behulp van routeprofielen die voorkomen dat de L3Out moet worden gekoppeld. 'Extern adverteren' moet echter nog steeds worden geselecteerd. Dit is een minder gebruikelijk geval, dus het zal hier niet worden besproken.

De contractrelatie tussen de L3Out en de EPG is vereist om ervoor te zorgen dat de BD doordringende statische route naar de BL wordt geduwd. De daadwerkelijke route-reclame wordt behandeld via herdistributie van de statische route in het externe protocol. Ten slotte zullen de herverdelingsroutekaarten alleen worden geïnstalleerd binnen de L3Outs die zijn gekoppeld aan de BD. Op deze manier wordt de route niet geadverteerd alle L3Outs.

In dit geval is het BD-netwerk 192.168.1.0/24 en moet het worden geadverteerd via OSPF L3Out.

### **Alvorens het contract tussen L3Out en interne EPG toe te passen**

```
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
```

Merk op dat de BD route nog niet aanwezig is op de BL.

### **Na toepassing van het contract tussen L3Out en interne EPG**

Op dit punt is geen andere configuratie uitgevoerd. De L3Out is nog niet gekoppeld aan de BD en de vlag 'Extern adverteren' is niet ingesteld.

```
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
```

Bericht dat de BD subnetroute (die door de doordringende vlag wordt vermeld) nu op BL wordt opgesteld. Merk echter op dat de route is gelabeld. Deze tag-waarde is een impliciete waarde die wordt toegewezen aan BD-routes voordat deze wordt geconfigureerd met 'Extern adverteren'. Alle externe protocollen ontkennen dat deze tag opnieuw wordt gedistribueerd.

### **Na het selecteren van 'Extern adverteren' op BD Subnet**

De L3Out is nog steeds niet gekoppeld aan de BD. Let er echter op dat de tag is verwijderd.

```
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
```

Op dit punt wordt de route nog steeds niet extern geadverteerd omdat er geen route-kaart en prefixlijst zijn die dit prefix voor herverdeling in het externe protocol aanpast. Dit kan met de volgende opdrachten worden geverifieerd:

```
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
```

De BD route is geprogrammeerd als een statische route, dus controleer de statische her distributie route-kaart door 'show route-map <route-map name>' en 'toon ip prefix-lijst <name>' op alle prefix-lijsten die aanwezig zijn in de route-kaart. Doe dit in de volgende stap.

## Nadat de L3Out aan de BD is gekoppeld

Zoals eerder vermeld, resulteert deze stap in de prefix-lijst die BD-subnet die in de statische aan externe routekaart van de protocolherdistributie wordt geïnstalleerd aanpast.

```
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
```

Controleer de prefixlijst:

```
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
```

Subnet BD wordt aangepast om in OSPF opnieuw te verdelen.

Op dit punt is de configuratie- en verificatieworkflow compleet voor de advertentie van het BD-subnetnet uit de L3Out. Na dit punt zou de controle protocolspecifiek zijn. Bijvoorbeeld:

- Voor EIGRP, verifieer dat de route in de topologielijst met "toon ip eigrp topologie vrf <name>" wordt geïnstalleerd
- Voor OSPF, verifieer dat de route in de gegevensbestandlijst als Externe LSA met "toon ip ospf- gegevensbestand vrf <name>" wordt geïnstalleerd
- Controleer voor BGP dat de route in de BGP RIB staat met 'toon bgp ipv4 unicast vrf <name>'

## BGP-routeradvertenties

Voor BGP zijn alle statische routes impliciet toegestaan voor herverdeling. De routekaart die overeenkomt met het BD-netwerk wordt toegepast op het BGP-buurniveau.

```
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
```

In het bovenstaande voorbeeld, 10.0.0.134 is de BGP buur die binnen L3Out wordt gevormd.

## EIGRP-routeradvertenties

Als OSPF, wordt een route-kaart gebruikt om Statische aan her distributie te controleren EIGRP. Op deze manier worden alleen subnetten die gekoppeld zijn aan de L3Out en ingesteld zijn op 'Extern adverteren' opnieuw verdeeld. Dit kan met deze opdracht worden geverifieerd:

```
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
```

De definitieve BD configuratie wordt hieronder getoond.

## Configuratie van Bridge Domain L3

## Probleemoplossing voor advertenties via Bridge Domain Route

In dit geval, het typische symptoom zou normaal zijn dat een gevormde BD-subnet niet uit een L3Out wordt geadverteerd. Volg de vorige workflow om te begrijpen welke component is gebroken.

Begin met de configuratie voordat u te laag wordt door het volgende te verifiëren:

- Is er een contract tussen de EPG en L3Out?
- Is de L3Out geassocieerd met de BD?
- Is het BD-subnet ingesteld om extern te adverteren?
- Is de externe protocolnabijheid omhoog?

### Mogelijke oorzaak: BD niet geïmplementeerd

Dit geval zou van toepassing zijn in een aantal verschillende scenario's, zoals:

- De interne EPG maakt gebruik van VMM-integratie met On Demand-optie en er zijn geen VM-endpoints gekoppeld aan de poortgroep voor de EPG.
- De interne EPG is gemaakt, maar er zijn geen statische padbindingen geconfigureerd of de interface waarop het statische pad is geconfigureerd, is niet beschikbaar.

In beide gevallen zou de BD niet worden ingezet en als gevolg daarvan zou de BD statische route niet naar de BL worden geduwd. De oplossing hier is om een aantal actieve bronnen te implementeren binnen een EPG die is gekoppeld aan deze BD, zodat het subnetnetwork wordt geïmplementeerd.

### Mogelijke oorzaak: OSPF L3Out wordt geconfigureerd als 'Stub' of 'NSSA' zonder herdistributie

Wanneer OSPF wordt gebruikt als L3Out protocol, moeten basisregels OSPF nog worden gevolgd. Stub-gebieden staan geen herverdeelde LSA's toe, maar kunnen in plaats daarvan een standaardroute adverteren. In NSSA-gebieden zijn herverdeelde paden wel toegestaan, maar 'Verzend herverdeelde LSA's naar NSSA-gebied' moet op de L3Out worden geselecteerd. Of NSSA kan ook een standaardroute adverteren door 'Originele Samenvatting LSA' uit te schakelen, wat ook een typisch scenario is waarbij 'Verzend herverdeelde LSA's naar NSSA-gebied' zou worden uitgeschakeld.

## Mogelijke oorzaak: 'Default-Export' routeprofiel met een 'Deny'-actie geconfigureerd onder de L3Out

Wanneer routeprofielen worden geconfigureerd onder een L3Out met de namen 'standaard-export' of 'standaard-import' worden ze impliciet toegepast op de L3Out. Als het standaard-export route-profiel is ingesteld op een deny action en geconfigureerd als 'Match Prefix and Routing Policy', dan moeten BD subnetten worden geadverteerd uit deze L3Out en zou impliciet worden geweigerd:

## Standaard-export routeprofiel met weigeringsrecht

The screenshot shows the Cisco APIC interface. The left sidebar displays a navigation tree with 'L3Outs' and 'OSPF' highlighted. The main panel shows the configuration for the 'Route Control Profile - default-export'. The 'Policy' tab is active, showing the following configuration:

- Name: default-export
- Type: Match Prefix AND Routing Policy (selected), Match Routing Policy Only
- Description: optional
- Contexts: A table with one entry:

Order	Name	Action	Description
0	deny1	Deny	

Buttons at the bottom include 'Show Usage', 'Reset', and 'Submit'.

De prefix-overeenkomsten binnen het standaard-export route-profiel zullen niet impliciet BD Subnets omvatten als de "Match Routing Policy Only" optie is geselecteerd.

## Werkstroom voor externe routeinvoer

In deze sectie wordt besproken hoe ACI externe routes leert via een L3Out en dit verdeelt naar interne bladknooppunten. Zij heeft ook betrekking op doorvoer- en routelekkende gebruikgevallen in latere secties



Net als bij de vorige paragraaf dient de gebruiker zich bewust te zijn van wat er op een hoger niveau gebeurt.

Standaard worden alle routes die door het externe protocol worden geleerd, opnieuw verdeeld in het interne BGP-proces. Dit is waar ongeacht welke subnetten onder externe EPG worden gevormd en welke vlaggen worden geselecteerd. Er zijn twee voorbeelden waar dit niet waar is.

- Als de 'Route Control Enforcement' optie op het hoogste niveau L3Out beleid is ingesteld op 'Import'. In dit geval zou het model van de routeinvoer van een blocklist model (specificeer slechts wat niet zou moeten worden toegestaan) naar een permitlist model gaan (alles wordt impliciet ontkend tenzij anders gevormd).
- Als het externe protocol EIGRP of OSPF is en een gebruikt Interleak-routeprofiel niet overeenkomt met de externe routes.

Voor een externe route die over een intern blad wordt verdeeld moet het volgende gebeuren:

- De route moet op de BL van de externe router worden geleerd. Om een kandidaat te zijn om in het fabric MP-BGP-proces opnieuw te verdelen moet de route in de routingstabel worden geïnstalleerd in plaats van alleen in het protocol RIB.
- Het moet zijn toegestaan dat de route wordt herverdeeld of geadverteerd in het interne BGP-proces. Dit moet altijd gebeuren tenzij een routebeheershandhaving of een interlek routeprofiel wordt gebruikt.
- Een BGP Route-Reflector Beleid moet worden geconfigureerd en toegepast op een Pod Policy Group die wordt toegepast op het Pod Profile. Als dit niet wordt toegepast, dan zal het BGP-proces niet op de switches initialiseren.

Als de interne EPG/BD in dezelfde VRF zit als de L3Out dan zijn de drie bovenstaande stappen alles wat nodig is om de interne EPG/BD externe routes te laten gebruiken.

## De route is geïnstalleerd in de BL-routingstabel

In dit geval is de externe route die op BLs 103 en 104 moet worden geleerd 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
```

Het is duidelijk dat het in de routingstabel is geïnstalleerd zoals geleerd door OSPF. Als het hier niet is gezien, controleer dan het afzonderlijke protocol en controleer of er iets aan de hand is. Route wordt opnieuw verdeeld in BGP De her distributie route-kaart kan worden geverifieerd, na te hebben gecontroleerd dat geen 'Import' handhaving of Interleak Route-Profiles worden gebruikt, door te kijken naar de route-kaart die wordt gebruikt voor externe protocol naar BGP her distributie. Zie de volgende opdracht:

```
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 is het duidelijk dat de 'vergunning-alle' route-kaart wordt gebruikt voor OSPF aan BGP herdistributie. Dit is de standaardinstelling. Van hieruit kan BL worden geverifieerd en kan de lokale route vanuit BGP worden gecontroleerd:

```
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: redistrib 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 de bovengenoemde output, 0.0.0.0/0 wijst erop het plaatselijk voortgekomen is. De lijst van geadverteerde peers zijn de wervelkolom knooppunten in de stof die als Route-

Reflectoren dienst doen.

## Controleer de route op het interne blad

De BL moet dit via de VPNv4 BGP-adresfamilie bekendmaken bij de wervelkolomknooppunten. De wervelkolomknooppunten moeten dit op alle bladknooppunten met de ingezette VRF (waar van niet-route-lekkende voorbeeld) bekendmaken. Op elk van deze bladknooppunten wordt 'toon bgp vpnv4 unicast <route> vrf overlay-1' uitgevoerd om te controleren of dit in VPNv4 is

Gebruik de onderstaande opdracht om de route op het interne blad te controleren.

```
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 de bovengenoemde output wordt de route geleerd door BGP en de volgende-hop zou de Fysieke TEPs (PTEP) van BLs moeten zijn.

```
leaf101# acidiag fmvread
      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
```

## Externe route-probleemoplossing

In dit scenario krijgt het interne blad (101) geen externe route(s).

Zoals altijd, eerst de basis controleren. Zorg ervoor dat:

- De Routing-protocolnabijheid is ingesteld op de BL's.
- Een BGP Route-Reflector-beleid wordt toegepast op de Pod Policy-groep en het Pod Profile.

Als de bovenstaande criteria juist zijn, zijn hieronder enkele meer geavanceerde voorbeelden van wat de oorzaak van de kwestie zou kunnen zijn.

### Mogelijke oorzaak: VRF niet toegepast op het interne blad

In dit geval zou het probleem zijn dat er geen EPG's zijn met middelen die worden ingezet op het interne blad waar de externe route wordt verwacht. Dit kan worden veroorzaakt door statische

padbindingen die alleen zijn geconfigureerd op down-interfaces of alleen door VMM geïntegreerde EPG's in On Demand-modus hebben zonder dynamische bijlagen gedetecteerd.

Omdat L3Out VRF niet op het interne blad wordt geïmplementeerd (verifiëren met 'toon vrf' op intern blad) zal het interne blad de BGP-route niet van VPNv4 importeren.

Om dit probleem op te lossen, moet de gebruiker resources inzetten binnen de L3Out VRF op het interne blad.

### Mogelijke oorzaak: Er wordt gebruik gemaakt van importrouthandhaving

Zoals eerder vermeld, wanneer de import route-controle handhaving is ingeschakeld accepteert de L3Out alleen externe routes die expliciet zijn toegestaan. De functie wordt meestal geïmplementeerd als een tabel-map. Een tabel-kaart ligt tussen het protocol RIB en de eigenlijke routingstabel zodat het alleen invloed heeft op wat in de routingstabel staat.

In de output onder wordt de Import Route-Control ingeschakeld, maar er zijn geen expliciet toegestane routes. Bericht dat LSA in het OSPF-gegevensbestand maar niet in de routingstabel op de BL is:

```
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

Hier is de tabel-kaart die nu is geïnstalleerd die dit gedrag veroorzaakt:

```
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:
```

Om het even wat die op gebied 100 leren, dat het gebied is op dit L3Out wordt gevormd, wordt impliciet ontkend door deze lijst-kaart zodat het niet geïnstalleerd in de routingstabel is.

Om dit probleem op te lossen, moet de gebruiker het subnet op de externe EPG definiëren met de vlag 'Import Route Control Subnet' of een importroute-profiel maken dat overeenkomt met de te installeren prefixes.

- Merk op dat de de invoerhandhaving niet voor EIGRP wordt gesteund.
- Merk ook op dat voor BGP de invoerhandhaving als inkomende route-kaart wordt uitgevoerd die op de buur BGP wordt toegepast. Controleer de subsectie "BGP Route Advertisement" voor details hoe u dit kunt controleren.

### Mogelijke oorzaak: er wordt een interlekprofiel gebruikt

Interleak-route-profielen worden gebruikt voor EIGRP en OSPF L3Outs en zijn bedoeld om controle mogelijk te maken over wat van IGP in BGP wordt herverdeeld alsook om de toepassing van beleid mogelijk te maken zoals het instellen van BGP-kenmerken.

Zonder een interlek-route-profiel worden alle routes impliciet geïmporteerd naar BGP.

Zonder interlek-route-profiel:

```
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 refcnt         : 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
```

Met een profiel voor een interlekroute:

```
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
```

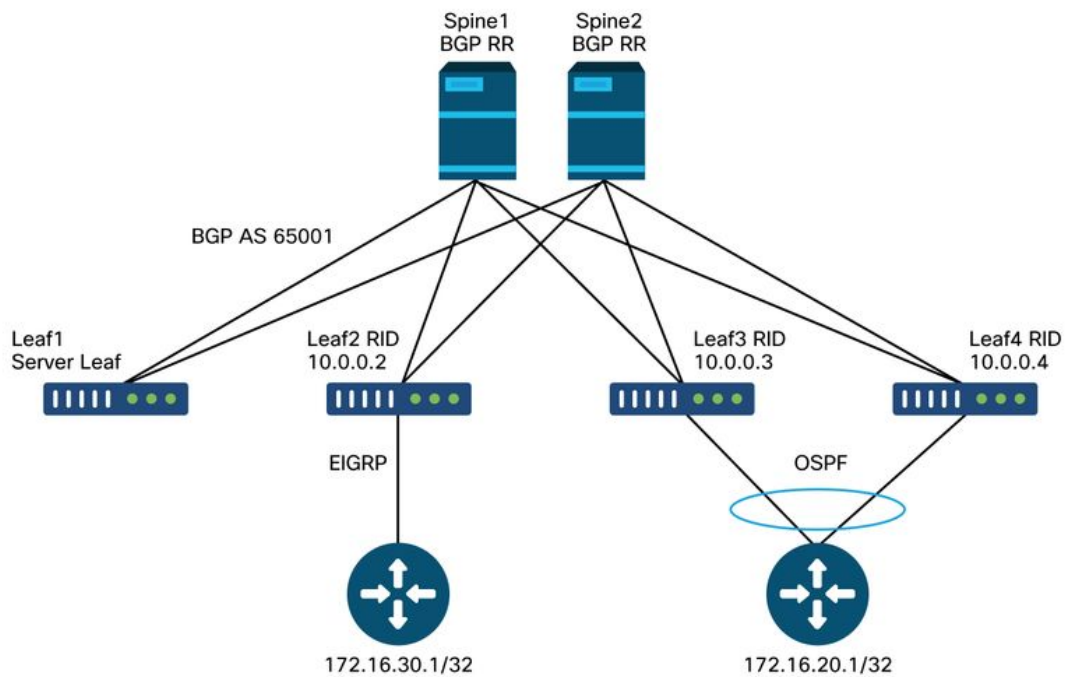
De hierboven benadrukte route-kaart zou alleen toestaan wat expliciet is afgestemd in het geconfigureerde interlek profiel. Als de externe route niet wordt aangepast, wordt deze niet herverdeeld in BGP.

## advertentieworkflow voor doorvoerroutes

In deze paragraaf wordt besproken hoe routes van één L3Out geadverteerd worden met een andere L3Out. Dit zou ook het scenario omvatten waar statische routes die direct op een L3Out worden gevormd moeten worden geadverteerd. Het zal niet ingaan op elke specifieke protocoloverweging, maar veeleer op de manier waarop dit in ACI wordt uitgevoerd. Het zal op dit moment niet in de routing van de interVRF-doorvoer gaan.

Dit scenario zal de volgende topologie gebruiken:

## Doorvoerroutingtopologie



De stroom op hoog niveau van hoe 172.16.20.1 van OSPF zou worden geleerd en dan in EIGRP geadverteerd, en controles van het gehele proces en het oplossen van problemen scenario's, worden hieronder besproken.

Voor de route 172.16.20.1 om in EIGRP geadverteerd te worden, moet één van het volgende worden gevormd:

- Het te adverteren subnet kan op de EIGRP L3Out met de vlag 'Export Route-Control Subnet' worden gedefinieerd. Zoals vermeld in het overzichtsgedeelte, wordt deze vlag voornamelijk gebruikt voor doorvoerrouting en definieert de subnetten die moeten worden geadverteerd vanuit die L3Out.
- Configureer 0.0.0.0/0 en selecteer zowel 'Aggregate Export' als 'Export Route Control Subnet'. Dit leidt tot een route-kaart voor her distributie in het externe protocol dat 0.0.0.0/0 en alle prefixes aanpast die specifieker zijn (die een efficiënte gelijke om het even welk) is. Merk op dat wanneer 0.0.0.0/0 wordt gebruikt met 'Aggregate Export', statische routes niet worden aangepast voor her distributie. Dit om onbedoeld reclame te voorkomen voor BD-routes die niet mogen worden geadverteerd.
- Tot slot is het mogelijk om een export route-profiel te maken dat overeenkomt met de prefixes die geadverteerd worden. Met behulp van deze methode kon de 'Aggregate' optie configureren met prefixes naast 0.0.0.0/0.

De bovenstaande configuraties zouden ertoe leiden dat de transitroute wordt geadverteerd, maar er moet nog steeds een beveiligingsbeleid zijn om dataplane-verkeer te laten stromen. Zoals bij elke EPG-naar-EPG-communicatie moet er een contract zijn voordat verkeer wordt toegestaan.

Merk op dat het dupliceren van externe subnetten met het 'Externe Subnet voor Externe EPG' niet kan worden geconfigureerd in dezelfde VRF. Indien geconfigureerd moeten subnetten specifieker zijn dan 0.0.0.0 Het is belangrijk om 'Externe Subnet voor Externe EPG' alleen te configureren voor de L3Out waar de route wordt ontvangen. Stel dit niet in op de L3Out die deze route zou moeten adverteren.

Het is ook belangrijk om te begrijpen dat alle transitroutes zijn voorzien van een specifieke VRF-tag. Standaard is deze tag 4294967295. Het Route-Tag-beleid is geconfigureerd onder 'Wandelaar > Netwerken > Protocollen > Route-Tag:

## Routetag-beleid

The screenshot shows the Cisco APIC interface. The top navigation bar includes 'System', 'Tenants', 'Fabric', 'Virtual Networking', 'L4-L7 Services', 'Admin', 'Operations', 'Apps', and 'Integrations'. The 'Tenants' tab is active, and the 'Prod' tenant is selected. The left sidebar shows a tree view of configuration objects, with 'Route Tag' selected and 'nonDefaultName' highlighted. The main panel displays a table titled 'Protocol - Route Tag' with the following data:

Name	Tag	Description
nonDefaultName	11111	

Dit beleid van de Routetag wordt dan toegepast op VRF. Het doel van deze tag is in wezen om loops te voorkomen. Deze routemarkering wordt toegepast wanneer de transitroute wordt teruggeadvertiseerd uit een L3Out. Als deze routes dan terug met de zelfde routemarkering worden ontvangen dan wordt de route verworpen.

### Controleer dat de route op de ontvangende BL via OSPF aanwezig is

Net als de laatste sectie, eerst controleren dat de BL die in eerste instantie de juiste route moet ontvangen.

```
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
```

Voorlopig, veronderstel dat de reclame L3Out op een andere BL (zoals in de topologie) is (de latere scenario's zullen bespreken waar het op de zelfde BL is).

### Controleer of de route in BGP aanwezig is op de ontvangende OSPF BL



Opdat de OSPF-route aan de externe EIGRP-router wordt geadverteerd, moet de route in BGP worden geadverteerd op de ontvangende OSPF BL.

```
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: redistrib 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
```

De route is in BGP.

**Controleer op de EIGRP BL die de route zou moeten adverteren dat het geïnstalleerd is**

```
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
```

Het is geïnstalleerd in de routingstabel met overlay next-hops gericht op de voortkomende grensbladknooppunten.

```
leaf102# acidiag fmvread

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
```

## Controleer of de route op de BL wordt geadverteerd

De route zal door BL 102 worden geadverteerd als resultaat van de "Subnet van de Route van de Uitvoer"vlag die op gevormde subnets wordt geplaatst:

## Routebeheer voor export

External EPG Instance Profile - instP

Policy | Operational | Stats | Health | Faults | History

General | Contracts | Subject Labels | EPG Labels

100

Properties

Configuration Status: applied

Configuration Issues:

Preferred Group Member: Exclude Include

Subnets:

IP Address	Scope	Name	Aggregate	Route Control Profile	Route Summarization Policy
0.0.0.0/0		External Subnets for the External EPG			
172.16.20.1/32		Export Route Control Subnet			

Show Usage | Reset | Submit

Current System Time: 2019-10-02T18:24:04:00

Gebruik de volgende opdracht om de routekaart te bekijken die is gemaakt als resultaat van deze vlag 'Exportroutecontrole':

```
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
```

Om de 'BGP > EIGRP-herverdeling' te zoeken, kijkt u naar de routekaart. Maar de route-kaart zelf moet hetzelfde zijn, ongeacht of het bronprotocol OSPF, EIGRP of BGP is. Statische routes worden gecontroleerd met een andere routekaart.

```
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 de bovenstaande uitvoer wordt de VRF-tag op dit prefix voor luspreventie ingesteld en wordt het subnetbestand dat met 'Export Route Control' is geconfigureerd, expliciet aangepast.

## Transit Routing bij ontvangst en reclame BL zijn hetzelfde

Zoals eerder besproken, wanneer de ontvangst en reclame BL's verschillend zijn, moet de route worden geadverteerd door de stof met behulp van BGP. Als de BL's hetzelfde zijn, kan de herverdeling of de reclame direct tussen de protocollen op het blad gebeuren.

Hieronder vindt u een korte beschrijving van de implementatie:

- **Transit routing tussen twee OSPF L3Outs op hetzelfde blad:** Routeradvertentie wordt bestuurd via een 'area-filter' toegepast op het OSPF-procesniveau. Een L3Out in gebied 0 moet op het blad worden ingezet, aangezien de routes tussen gebieden worden geadverteerd in plaats van door herverdeling. Gebruik 'toon ip ospf vrf <name>' om de filterlijst te bekijken. Geef de inhoud van het filter weer met 'toon route-map <filternaam>'.
- **Transit routing tussen OSPF en EIGRP L3Outs op hetzelfde blad:** Route-advertentie wordt gecontroleerd via herdistributie routekaarten die kunnen worden gezien met 'toon ip ospf' en 'toon ip eigrp'. Merk op dat als meerdere OSPF L3Outs op dezelfde BL bestaan de enige manier om te herverdelen in slechts een van die OSPF L3Outs is als de andere een Stub of NSSA is met '**Verzend herverdeelde LSAs in NSSA gebied**' uitgeschakeld zodat het geen externe LSA's toestaat.
- **Doorvoerrouting tussen OSPF of EIGRP en BGP op hetzelfde blad:** routeradvertenties in de IGP worden gecontroleerd via routekaarten voor herdistributie. Route-reclame in BGP wordt gecontroleerd via een uitgaande route-kaart die direct op de bgp buur wordt toegepast dat de route zou moeten worden verzonden doen. Dit kan worden geverifieerd met 'toon bgp ipv4 unicast buurman <buuradres> vrf <name> | grep Outbound'.
- **Transit routing tussen twee BGP I3Outs op hetzelfde blad:** Alle advertenties worden gecontroleerd via routekaarten die direct worden toegepast op de bgp buurman waarnaar de route moet worden verzonden. Dit kan worden geverifieerd met 'toon bgp ipv4 unicast buurman <buuradres> vrf <name> | grep Outbound'.

## Transit routing probleemoplossing scenario's #1: Transit Route niet geadverteerd

Dit probleemoplossingsscenario omvat routes die door één L3Out moeten worden geleerd die niet door de andere L3Out worden verzonden.

Kijk zoals altijd eerst naar de basisgegevens voordat u naar iets specifieks van de ACI kijkt.

- Zijn protocolnabijheid opgeheven?
- Is de route, dat ACI reclame zou moeten zijn, in de eerste plaats geleerd van een extern protocol?
- Voor BGP: wordt het pad verbroken vanwege een of ander BGP-kenmerk? (as-pad etc.).
- Heeft de ontvangende L3Out het in de OSPF-database, de EIGRP-topologietabel of de BGP-tabel?
- Wordt een BGP-routerreflectorbeleid toegepast op de Pod Policy Group die wordt toegepast op het Pod-profiel?

Als alle basis protocol verificaties correct zijn geconfigureerd, hieronder zijn enkele andere gemeenschappelijke oorzaken voor een doorvoerroute die niet wordt geadverteerd.

### Mogelijke oorzaak: Geen OSPF-gebied 0

Als de betrokken topologie twee OSP L3Outs op hetzelfde grensblad impliceert, dan moet er een Gebied 0 zijn voor routes die van één gebied aan een ander moeten worden geadverteerd. Bekijk de "Transit routing tussen twee OSPF L3Outs op hetzelfde blad" hierboven voor meer informatie.

### Mogelijke oorzaak: OSPF-gebied is stub of NSSA

Dit zou worden gezien als OSPF L3Out met een gebied wordt gevormd Stub of NSSA dat niet wordt gevormd om externe LSAs te adverteren. Met OSPF worden externe LSA's nooit geadverteerd in Stub-gebieden. Ze worden geadverteerd in NSSA-gebieden als 'Verzend opnieuw gedistribueerde LSA's naar NSSA-gebied' is geselecteerd.

## Transit routing probleemoplossing scenario's #2: Transit Route niet ontvangen

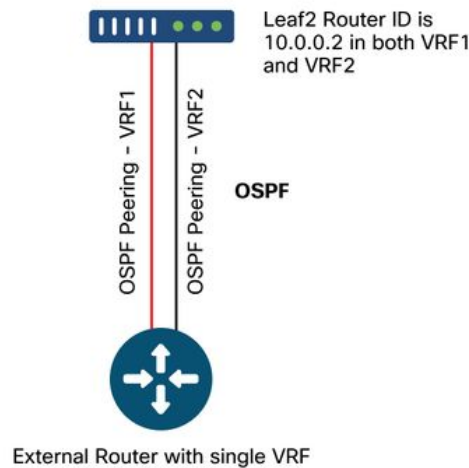
In dit scenario is het probleem dat sommige routes geadverteerd door een ACI L3Out niet worden terugontvangen in een andere L3Out. Dit scenario zou van toepassing kunnen zijn als L3Outs in twee afzonderlijke stoffen zijn en verbonden worden door externe routers of als L3Outs in verschillende VRFs zijn en de routes tussen VRFs door een externe router worden doorgegeven.

### Mogelijke oorzaak: BL wordt geconfigureerd met dezelfde router-id in meerdere VRF-systemen

Vanuit een configuratieperspectief kan een router-id niet worden gedupliceerd binnen dezelfde VRF. Het is echter meestal fijn om dezelfde router-id in verschillende VRF's te gebruiken zolang de twee VRF's niet aan dezelfde routerprotocoldomeinen verbonden zijn.

Overweeg de volgende topologie:

### Externe router met enkele VRF — Transit Route niet ontvangen



Het probleem zou hier zijn dat het ACI-blad LSA's ziet met zijn eigen router-ID die worden ontvangen, wat er in zou resulteren dat deze niet in de OSPF-database worden geïnstalleerd.

Bovendien als de zelfde opstelling met paren VPC werd gezien, zou LSAs onophoudelijk op sommige routers worden toegevoegd en worden geschrapt. De router zou bijvoorbeeld LSA's zien die afkomstig zijn van zijn VPC-peer met VRF en LSA's die afkomstig zijn van dezelfde knooppunt (met dezelfde router-ID) die in de andere VRF zijn gegenereerd.

Om dit probleem op te lossen, dient de gebruiker ervoor te zorgen dat een knooppunt binnen elke VRF een verschillende, unieke router-id heeft waarin het een L3Out heeft.

### **Mogelijke oorzaak: routes van één L3Out in één ACI stof ontvangen op een andere stof met de zelfde VRF markering**

De standaardroutemarkering in ACI is altijd hetzelfde, tenzij deze wordt gewijzigd. Als routes worden geadverteerd van één L3Out in één VRF of ACI stof aan een andere L3Out in een andere VRF of ACI stof zonder de standaard VRF markeringen te veranderen, zullen de routes door de ontvangende BLs worden gelaten vallen.

De oplossing voor dit scenario is simpelweg om een uniek Route-Tag beleid te gebruiken voor elke VRF in ACI.

### **Transit Routing Problemen oplossen scenario's #3 — Transit Routes onverwacht geadverteerd**

Dit scenario zou zich voordoen wanneer transitroutes worden geadverteerd met een L3Out waar ze niet geadverteerd worden.

### **Mogelijke oorzaak: gebruik van 0.0.0.0/0 met 'Aggregate Export'**

Wanneer een externe subnetconfiguratie is geconfigureerd als 0.0.0.0/0 met 'Export Route Control Subnet' en 'Aggregate Export', is het resultaat dat er een overeenkomst is geïnstalleerd voor alle herdistributie routekaart. In dit geval worden alle routes op de BL die via OSPF, EIGRP of BGP zijn geleerd, geadverteerd vanuit de L3Out waar dit is geconfigureerd.

Hieronder is de routekaart die aan het blad als resultaat van de Samengevoegde Uitvoer wordt opgesteld:

```

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

```

Dit is de belangrijkste oorzaak van het routing van lusjes die een ACI-omgeving omvatten.

## Contract en L3Out

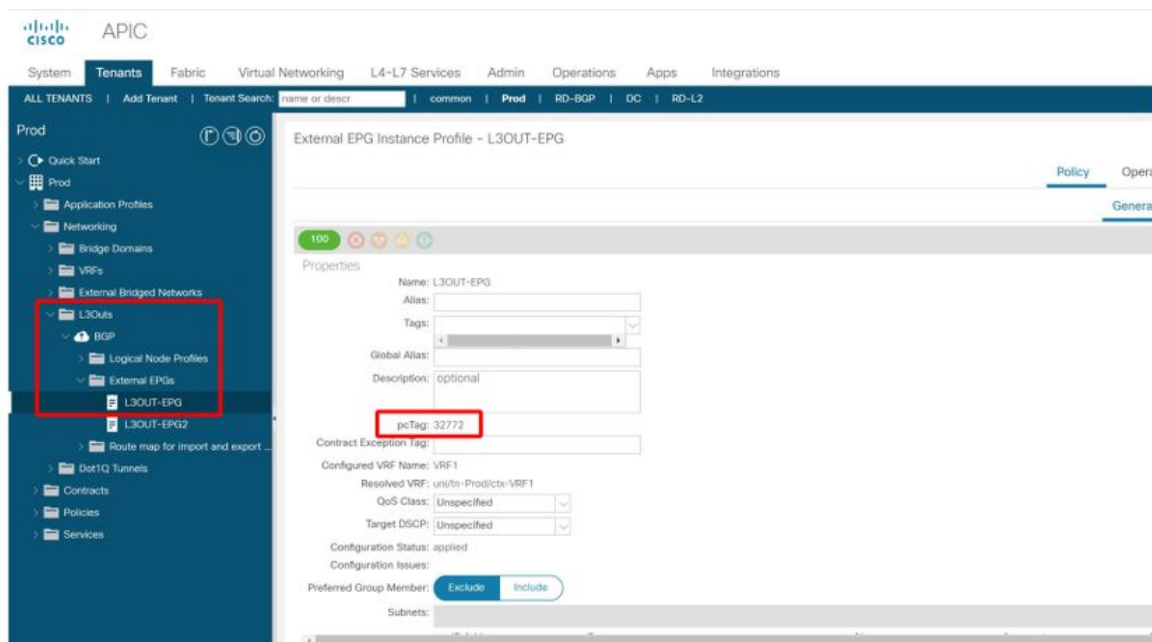
### Op voorvoegsel gebaseerde EPG op L3Out

In een interne EPG (niet-L3Out) worden contracten afgedwongen nadat de pcTag van de bron en de pcTag van de bestemming EPG zijn afgeleid. De insluiting VLAN/VXLAN van het pakket dat op de downlink-poort wordt ontvangen, wordt gebruikt om deze pcTag aan te drijven door het pakket in de EPG te classificeren. Wanneer het leren van een MAC-adres of een IP-adres, wordt het geleerd samen met zijn toegangsinkapseling en de bijbehorende EPG pcTag. Raadpleeg voor meer informatie over pcTag en contracthandhaving het hoofdstuk "Beveiligingsbeleid".

L3Outs bestuurt ook een pcTag met behulp van zijn L3Out EPG (Externe EPG) onder 'Huurder > Netwerken > L3OUT > Netwerken > L3OUT-EPG'. L3Outs vertrouwt echter niet op VLAN's en interfaces om pakketten als zodanig te classificeren. De classificatie is in plaats daarvan gebaseerd op bronvoorvoegsel/subnet op een 'Langste Prefix Match' manier. Vandaar, kan een L3Out EPG als **prefix-gebaseerde EPG** worden bedoeld. Nadat een pakket is geclassificeerd in een L3Out gebaseerd op een subnet, volgt het een gelijkaardig patroon van de beleidshandhaving als regelmatige EPG.

Het volgende diagram schetst waar pcTag van een bepaalde L3Out EPG binnen GUI kan worden gevonden.

## Plaats van de pcTag voor een L3Out



De gebruiker is verantwoordelijk voor het definiëren van de op prefix gebaseerde EPG-tabel. Dit gebeurt met behulp van het 'Externe Subnet voor Externe EPG'-subnetbereik. Elke subnetset met die scope wordt toegevoegd in een statische LPM-tabel (Longest Prefix Match). Dit subnet zal naar de pcTag waarde wijzen die gebruikt zal worden voor elk IP-adres dat binnen dat prefix valt.

Switch De LPM-tabel van op prefix gebaseerde EPG-subnetten kan op bladmodules worden geverifieerd met behulp van de volgende opdracht:

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

Opmerkingen:

- LPM-tabelvermeldingen worden bestreken door VRF-VNID. De raadpleging gebeurt per vrf\_vnid/src pcTag/dst pcTag.
- Elke ingang wijst naar één pcTag. Dientengevolge, kunnen twee L3Out EPGs niet zelfde subnet met de zelfde maskerlengte binnen zelfde VRF gebruiken.
- Subnet 0.0.0.0/0 gebruikt altijd speciale pcTag 15. Als zodanig kan het worden gedupliceerd, maar moet dit alleen worden gedaan met een volledig begrip van de implicaties voor beleidshandhaving.
- Deze tabel wordt in beide richtingen gebruikt. Van L3Out tot Leaf Local Endpoint, wordt de bron pcTag afgeleid met behulp van deze tabel. Van Leaf Local Endpoint tot L3Out, de

bestemming pcTag wordt afgeleid met behulp van deze tabel.

- Als de VRF de 'Ingress' handhavinginstelling heeft voor 'Policy Control Enforcement Direction', dan zal de LPM prefixtabel aanwezig zijn op de L3Out BL's, evenals eventuele switches in de VRF die een contract hebben met de L3Out.

## Voorbeeld 1: Single L3Out met specifieke prefix

**Scenario:** Eén BGP L3Out in VRF-proxy:VRF1 met één L3Out EPG. Prefix 172.16.1.0/24 wordt ontvangen van een externe bron dus het moet worden geclassificeerd in de L3Out EPG.

```
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
```

Voeg eerst het subnetnummer toe aan de prefixtabel.

## Subnet met 'Externe subnetten voor de externe EPG'-scope



## Create Subnet

IP Address:   
address/mask

Name:

scope:  Export Route Control Subnet  
 Import Route Control Subnet  
 External Subnets for the External EPG  
 Shared Route Control Subnet  
 Shared Security Import Subnet

BGP Route Summarization Policy:

aggregate:  Aggregate Export  
 Aggregate Import  
 Aggregate Shared Routes

Route Control Profile:

Name	Direction

Controleer de programmering van de prefixlijst op de switches die de VRF van de L3Out hebben:

```
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
```

De pcTag van de L3Out EPG is 32772 in vrf scope 2097154.

## Voorbeeld 2: Single L3Out met meerdere prefixes

Uitbreidend op het vorige voorbeeld, in dit scenario ontvangt L3Out meerdere prefixes. Terwijl het invoeren van elk prefix functioneel correct is, is een alternatieve optie (afhankelijk van het voorgenomen ontwerp) om alle prefixes ontvangen op de L3Out te accepteren.

Dit kan worden bereikt met het '0.0.0.0/0' prefix.

# 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
  - 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:

Route Control Profile:

Name ▲ Direction

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

Dit resulteert in de volgende ingang van de prefixtabel:

```
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
```

Merk op dat pcTag toegewezen aan 0.0.0.0/0 waarde 15 gebruikt, niet 32772. pcTag 15 is een gereserveerd systeem pcTag die alleen wordt gebruikt met 0.0.0.0/0 die fungeert als wildcard voor alle prefixes op een L3Out.

Als de VRF een enkele L3Out met een enkele L3Out EPG met behulp van de 0.0.0.0/0 heeft, dan blijft het beleidsvoorvoegsel uniek en is de eenvoudigste benadering om alles te vangen.

### Voorbeeld 3a: Meervoudige L3Out EPG's in een VRF

In dit scenario zijn er meerdere L3Out EPG's in dezelfde VRF.

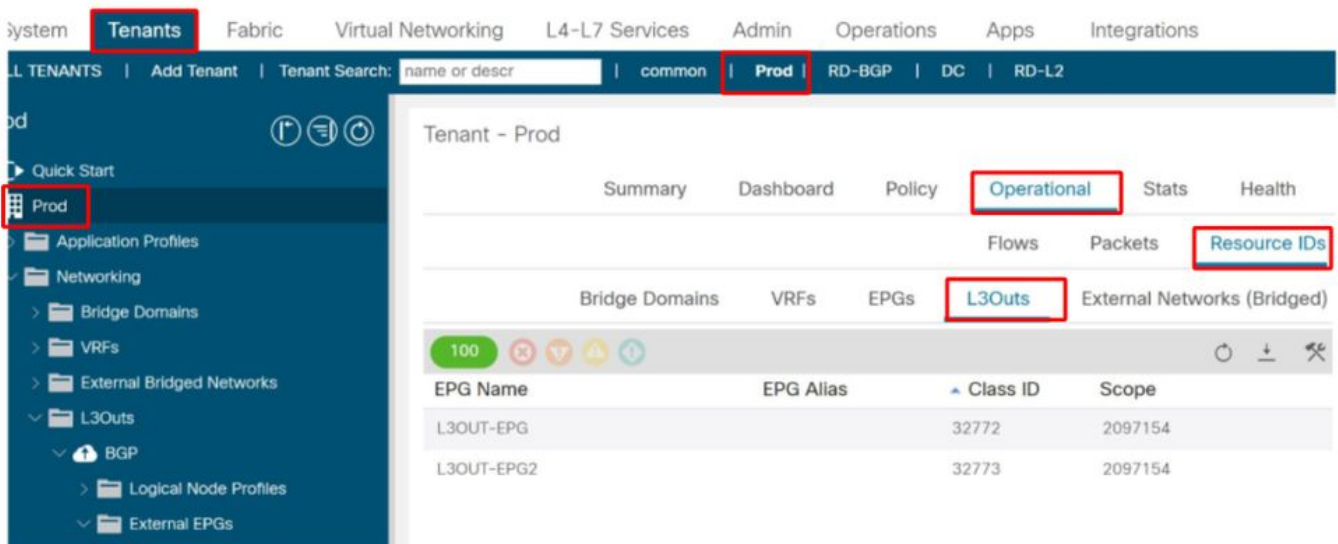
Opmerking: Vanuit een op voorvoegsel gebaseerd EPG-perspectief, zullen de volgende twee configuraties resulteren in gelijkwaardige LPM-policy-mgr-tabelvermeldingen:

1. Twee L3Outs met elk één L3Out EPG.
2. Eén L3Out met twee L3Out EPG's

In beide scenario's is het totale aantal L3Out EPG's 2. Dit betekent dat elke één zijn eigen pcTag en bijbehorende subnetten zal hebben.

Alle pcTags van een gegeven L3Out EPG kunnen worden bekeken in de GUI bij 'Tenant > Operational > Resource id > L3Outs'

### Verificatie van de L3Out pcTag



In dit scenario ontvangt de ACI-fabric meerdere prefixes van de externe routers en is de L3Out EPG-definitie als volgt:

- 172.16.1.0/24 toegewezen aan L3OUT-EPG.
- 172.16.2.0/24 toegewezen aan L3OUT-EPG2.
- 172.16.0.0/16 toegewezen aan L3OUT-EPG (om het 172.16.3.0/24 prefix te vangen).

Om dit aan te passen, wordt de configuratie als volgt gedefinieerd:

- L3OUT-EPG heeft subnetnummers 172.16.1.0/24 en 172.16.0.0/16, beide met scope 'Externe Subnet voor de Externe EPG'.
- L3OUT-EPG2 heeft subnet 172.16.2.0/24 met scope 'Externe Subnet voor Externe EPG'.

De resulterende vermeldingen in de prefixtabel zijn:

```
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 is toegewezen aan pcTag 32773 (L3OUT-EPG2) en 172.16.0.0/16 is toegewezen aan 32772 (L3OUT-EPG).

In dit scenario is de vermelding voor 172.16.1.0/24 overbodig omdat de /16 supernet aan dezelfde EPG is toegewezen.

Meervoudige L3Out EPG's zijn nuttig wanneer het doel is om verschillende contracten toe te passen op groepen prefixes binnen één L3Out. Het volgende voorbeeld zal illustreren hoe contracten in het spel komen met meerdere L3Out EPG's.

### Voorbeeld 3b: meerdere L3Out EPG's met verschillende contracten

Dit scenario bevat de volgende instellingen:

- ICMP-contract dat alleen ICMP toestaat.
- HTTP-contract dat alleen TCP-bestemmingspoort 80 toestaat.
- EPG1 (pcTag 32770) biedt het HTTP-contract dat wordt verbruikt door L3OUT-EPG (pcTag 32772).
- EPG2 (pcTag 32771) biedt het ICMP-contract dat wordt verbruikt door L3OUT-EPG2 (pcTag 32773).

Dezelfde beleidsvoorvoegsels als in het vorige voorbeeld worden gebruikt:

- 172.16.1.0/24 in L3OUT-EPG moet HTTP naar EPG1 toestaan
- 172.16.2.0/24 in L3OUT-EPG2 zou ICMP aan EPG2 moeten toestaan

## voorvoegsel en zoneregels van beleidsbepaler:

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

## Datapath-validatie met behulp van fTriage — flow toegestaan door beleid

Met een ICMP-stroom tussen 172.16.2.1 op het externe netwerk en 192.168.3.1 in EPG2 kan fTriage worden gebruikt om de stroom te vangen en te analyseren. In dit geval, start fTriage op zowel blad switch 103 als 104 als verkeer kan binnenkomen één van beiden:

```
admin@apic1:~> ftriage route -ii LEAF:103,104 -sip 172.16.2.1 -dip 192.168.3.1
fTriage Status: {"dbgFtrriage": {"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 bevestigt dat de zoning-regel tegen de ICMP-regel van L3OUT\_EPG2 tot EPG is geraakt:

```

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

```

## Datapath-validatie met fTriage — flow die niet is toegestaan volgens beleid

Verwacht een beleidsdaling met ICMP-verkeer dat afkomstig is van 172.16.1.1 (L3OUT-EPG) naar 192.168.3.1 (EPG2).

```

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"}}}
```

Als Triage bevestigt dat het pakket wordt gelaten vallen met de Security\_GROUP\_DENY (beleidsdruppel) reden en dat de afgeleide bron pcTag is 32772 en de bestemming pcTag is 32771. Als u dit controleert aan de hand van regels voor zonering, zijn er duidelijk geen items tussen die EPG.

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

### Voorbeeld 4: meerdere L3Outs met meerdere prefixes

Het scenario is op dezelfde manier ingesteld als voorbeeld 3 (L3Out en L3Out EPG definities), maar het netwerk dat op beide L3Out EPG's is gedefinieerd, is 0.0.0.0/0.

De contractconfiguratie is als volgt:

- ICMP1-contract dat ICMP toestaat.
- ICMP2-contract dat ICMP toestaat.
- EPG1 (pcTag 32770) biedt ICMP1-contract dat wordt verbruikt door L3OUT-EPG (pcTag 32772).
- EPG2 (pcTag 32771) biedt ICMP2-contract dat wordt verbruikt door L3OUT-EPG2 (pcTag 32773).

Deze configuratie kan ideaal lijken in het geval dat het externe netwerk vele prefixes adverteert, maar er zijn ten minste twee blokken van prefixes die verschillende toegestane stroompatronen volgen. In dit voorbeeld, zou één prefix slechts ICMP1 moeten toestaan en andere zou ICMP2 slechts moeten toestaan.

Ondanks het feit dat '0.0.0.0/0' tweemaal in dezelfde VRF wordt gebruikt, wordt slechts één voorvoegsel geprogrammeerd in de policy-mgr prefixtabel:

```
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
```

Twee stromen worden hieronder opnieuw onderzocht. Op basis van de bovenstaande contractconfiguratie wordt het volgende verwacht:

1. 172.16.2.1 (L3OUT-EPG2) tot 192.168.3.1 (EPG2) **moet** worden toegestaan door ICMP2.
2. 172.16.2.1 (L3OUT-EPG2) tot en met 192.168.1.1 (EPG1) **niet** worden toegestaan, aangezien er geen contract bestaat tussen EPG1 en L3OUT-EPG2

### Datath-validatie met behulp van fTriage — flow die door beleid is toegestaan



Triage met een ICMP-stroom van 172.16.2.1 (L3OUT-EPG2) tot 192.168.3.1 (EPG2 — pcTag 32771).

Starting ftriage

Log file name for the current run is: ftlog\_2019-10-02-23-11-14-298.txt

```
2019-10-02 23:11:14,302 INFO      /controller/bin/ftriage route -ii LEAF:103,104 -sip 172.16.2.1
-dip 192.168.3.1
2019-10-02 23:12:00,887 INFO      ftriage:      main:1165 Invoking ftriage with default password
and default username: apic#fallback\admin
2019-10-02 23:12:44,565 INFO      ftriage:      main:839 L3 packet Seen on bdsol-aci32-leaf3
Ingress: Eth1/12 (Pol) Egress: Eth1/12 (Pol) 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(Pol) same as
egr if(Pol)
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
```

Deze stroom is toegestaan (zoals verwacht) door zoning-regel 4336.

## Datapath-validatie met fTriage — flow die niet is toegestaan volgens beleid

Triage met een ICMP-stroom van 172.16.2.1 (L3OUT-EPG2) tot 192.168.1.1 (EPG1 — pcTag 32770):

```
admin@apic1:~> ftriage route -ii LEAF:103,104 -sip 172.16.2.1 -dip 192.168.1.1
```

```
fTriage Status: {"dbgFtriage": {"attributes": {"operState": "InProgress", "pid": "31500",
"apicId": "1", "id": "0"}}}
```

Starting ftriage

Log file name for the current run is: ftlog\_2019-10-02-23-53-03-478.txt

```
2019-10-02 23:53:03,482 INFO      /controller/bin/ftriage route -ii LEAF:103,104 -sip 172.16.2.1
-dip 192.168.1.1
2019-10-02 23:53:50,014 INFO      ftriage:      main:1165 Invoking ftriage with default password
and default username: apic#fallback\admin
2019-10-02 23:54:39,199 INFO      ftriage:      main:839 L3 packet Seen on bdsol-aci32-leaf3
Ingress: Eth1/12 (Pol) Egress: Eth1/12 (Pol) 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

```

Deze stroom is toegestaan (onverwacht) door zoning-regel 4341. De regels voor de indeling in zones moeten nu worden geanalyseerd om te begrijpen waarom.

## Validatie van datapath — regels voor zoning

Hieronder staan de zoningregels voor de laatste 2 tests:

- Verwacht — stroom raakt lijn 4336 van de zoningregel (contract ICMP2).
- Onverwacht — stroomstoot op lijn 4341 (ICMP1-contract) volgens de zoningregel.

```

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

```

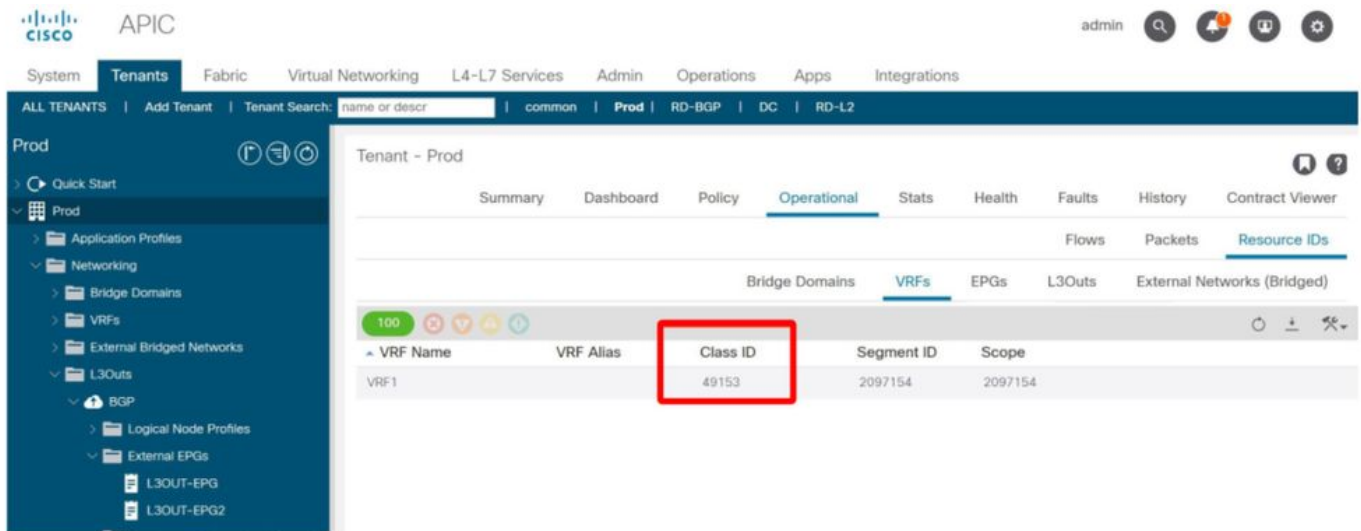
```

| 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 stromen leiden uit de src pcTag van 49153. Dit is de pcTag van de VRF. Dit kan in de BU worden geverifieerd:

## Verificatie van de pcTag van de VRF



Het volgende gebeurt wanneer de 0.0.0.0/0 prefix in gebruik is met een L3Out:

- Verkeer van een interne EPG naar een L3Out EPG met 0.0.0.0/0 zal een bestemming pcTag van 15 afleiden.
- Het verkeer van een L3Out EPG met 0.0.0.0/0 aan een ACI interne EPG zal een bron pcTag van VRF (49153) afleiden.

Het contract\_parser script geeft een holistische kijk op de zonering-regels:

```
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]

```

## Bevestigen van pcTag gebruikt door pakket met ELAM Assistant-app

De ELAM Assistant App geeft een andere methode om de bron en bestemming pcTag van live verkeersstromen te bevestigen.

De screenshot hieronder toont het ELAM resultaat voor verkeer van pcTag 32771 naar pcTag 49153.

## ELAM Assistant-app-uitvoer voor src 32771 naar 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)

### Conclusie

Het gebruik van 0.0.0.0/0 moet zorgvuldig worden getraceerd binnen een VRF als elke L3Out met behulp van dat net de contracten erft die op elke andere L3Out met behulp van het worden toegepast. Dit zal waarschijnlijk leiden tot ongeplande stromen van vergunningen.

## Gedeeld L3Out

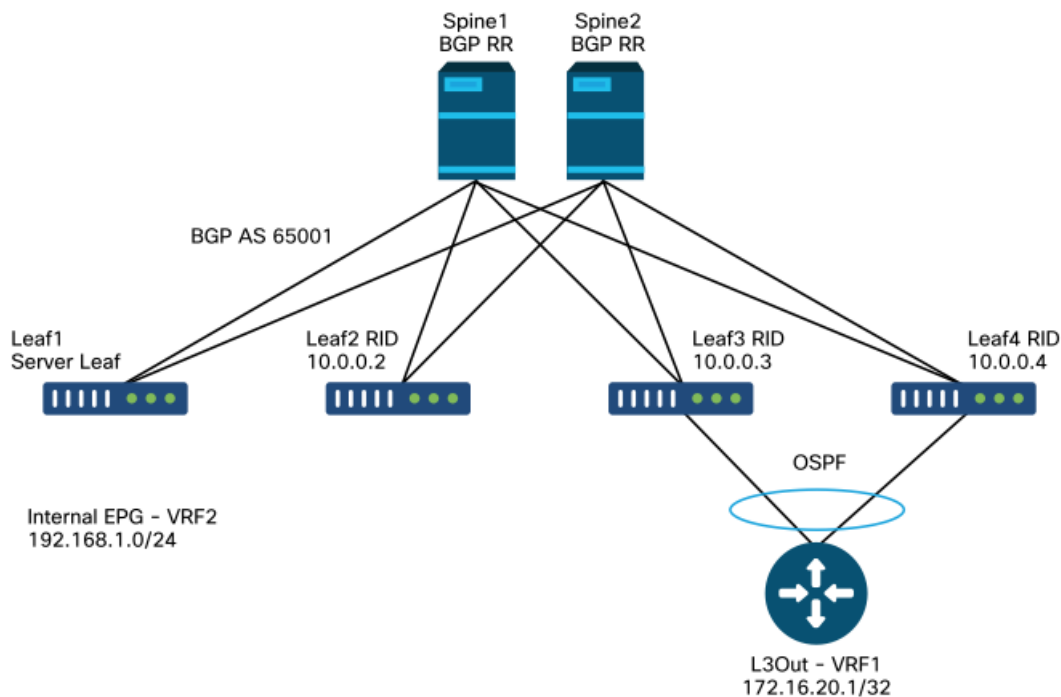
### Overzicht

Deze sectie zal bespreken hoe u routeradvertenties kunt oplossen in gedeelde L3Out-configuraties. De term 'shared L3Out' verwijst naar het scenario waarbij een L3Out in een VRF zit, maar een interne EPG met een contract met de L3Out in een andere VRF zit. Met Shared L3Outs wordt het weglekken intern uitgevoerd naar het ACI-weefsel.

Deze sectie gaat niet diepgaand in detail over problemen oplossen bij beveiligingsbeleid. Zie daarvoor het hoofdstuk "Veiligheidsbeleid" van dit boek. Deze paragraaf zal ook niet in detail ingaan op de classificatie van de prefix voor extern beleid voor beveiligingsdoeleinden. Raadpleeg het gedeelte "Contract en L3Out" in het hoofdstuk "Extern doorsturen".

Deze sectie gebruikt de volgende topologie voor onze voorbeelden.

### Gedeelde L3Out-topologie



Op een hoog niveau moeten de volgende configuraties aanwezig zijn om een gedeelde L3Out te laten functioneren:

- Een L3Out-subnet moet worden geconfigureerd met het bereik 'Shared Route Control Subnet' om externe routes naar interne VRF's te lekken. De optie 'Geaggregeerd Gedeeld' kan ook worden geselecteerd om alle routes te lekken die specifiek zijn dan het geconfigureerde subnet.
- Een L3Out-subnet moet worden geconfigureerd met het bereik 'Shared Security Import Subnet' om het beveiligingsbeleid te programmeren dat nodig is om communicatie via deze L3Out mogelijk te maken.
- Het interne BD-subnet moet worden ingesteld op 'Gedeeld tussen VRF's' en 'Extern adverteren' om het BD-subnet in de externe VRF te programmeren en er reclame voor te maken.
- Een 'huurder' of 'globaal' werkingscontract moet worden geconfigureerd tussen de interne EPG en de externe EPG van de gedeelde L3Out.

In het volgende gedeelte wordt in detail beschreven hoe uitgelekte routes worden geadverteerd en aangeleerd in ACI.

## Gedeelde L3Out workflow — externe trajecten leren

In dit gedeelte wordt het pad van een aangeleerde externe route beschreven zoals deze in de stof wordt geadverteerd.

### Externe route zoals gezien op het grensblad

Dit bevel zal de externe route tonen die van OSPF wordt geleerd:

```
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
```

Vervolgens moet de route worden geïmporteerd in BGP. Standaard moeten alle externe routes in BGP worden geïmporteerd.

## BGP-verificaties op het grensblad

De route moet in de BGP VPNv4-adresfamilie zijn opgenomen met een routedoel dat in de hele fabric moet worden verdeeld. De route-doel is een BGP uitgebreide gemeenschap die door externe VRF wordt uitgevoerd en door om het even welke interne VRFs wordt ingevoerd die de weg moet ontvangen.

Controleer vervolgens het routedoel dat wordt geëxporteerd door de externe VRF op de BL.

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

Information regarding configured VRFs:

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

...

```
Wait for IGP convergence is not configured
Export RT list:
  65001:2392068
Import RT list:
  65001:2392068
Label mode: per-prefix
```

De bovenstaande output toont aan dat alle paden die van de externe VRF naar VPNv4 worden geadvertiseerd, een route-doel van 65001:2392068 moeten ontvangen.

Controleer vervolgens het snijpad:

```

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

```

De bovenstaande output toont aan dat het pad de juiste route-doelstelling heeft. Het VPNv4-pad kan ook worden geverifieerd met de opdracht 'show bgp vpnv4 unicast 172.16.20.1 vrf overlay-1'.

## Verificaties op de server

Als het interne EPG-blad de BL-geadverteerde route wil installeren, moet het het route-doel (hierboven genoemd) importeren in de interne VRF. Het BGP-proces van de interne VRF kan worden gecontroleerd om dit te valideren:

```

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
```

De bovenstaande output laat de interne VRF zien die het route-doel importeert dat door de externe VRF wordt geëxporteerd. Bovendien is er een 'Import Route-Map' waarnaar wordt verwezen. De import route-map bevat de specifieke prefixes die zijn gedefinieerd in de gedeelde L3Out met de 'Shared Route Control Subnet'-vlag.

De inhoud van de routekaart kan worden gecontroleerd om te verzekeren het externe prefix omvat:

```
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
```

De bovenstaande output toont de route-kaart van de import die het te importeren subnet bevat.

De definitieve controles omvatten het controleren dat de route in de BGP-tabel staat en dat deze in de routeringstabel is geïnstalleerd.

BGP-tabel op serverblad:

```
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
```

De route wordt geïmporteerd in de interne VRF BGP-tabel en heeft het verwachte routedoel.

De geïnstalleerde routes kunnen worden geverifieerd:

```
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
```

De bovenstaande output gebruikt een specifieke 'vsh -c' opdracht om de 'detail' output te krijgen. De 'detail' vlag omvat de herschrijven VXLAN VNID. Dit is het VXLAN-algoritme van de externe VRF. Wanneer de BL dataplane-verkeer ontvangt met dit VNID, weet het de doorsturen beslissing te nemen in de externe VRF.

De rw-vnid waarde is in hexuitdraai, dus het omzetten in decimale zal de VRF VNID van 2392068 krijgen. | grep 2392068' op het blad. Een globale zoekopdracht kan uitgevoerd worden op een APIC met de 'moquery -c fvCtx -f 'fv.Ctx.seg=="2392068" opdracht.

IP van de volgende hop zou ook aan BL PTEPs moeten richten en "%overlay-1"wijst erop dat de routeraadpleging voor de volgende-hop in de overlay VRF is.

## Gedeelde L3Out workflow — reclame maken voor interne routes

Net als in voorgaande secties wordt een gedeelde L3Out als volgt verwerkt:

- Het BD-subnet (interne VRF) is als statische route op de BL (externe VRF) geïnstalleerd. Deze statische routeplaatsing is een resultaat van de contractverhouding tussen interne EPG en L3Out.
- De statische route wordt opnieuw verdeeld in het externe protocol wanneer het 'Extern geadverteerde' bereik is ingesteld op het BD-subnet.

## Controleer de BD statische route op de BL

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

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

Bericht dat in de bovengenoemde output de VNID van interne VRF voor herschrijft wordt geplaatst. De next-hop is ook ingesteld op het proxy-v4-anycast adres.

Bovenstaande route wordt extern geadverteerd via dezelfde routekaarten die worden getoond in de sectie "Routeadvertenties".

Als een BD-subnet is ingesteld op 'Extern adverteren', wordt het opnieuw verdeeld in **elk extern L3Out-protocol** waarmee de interne EPG een contractuele relatie heeft.

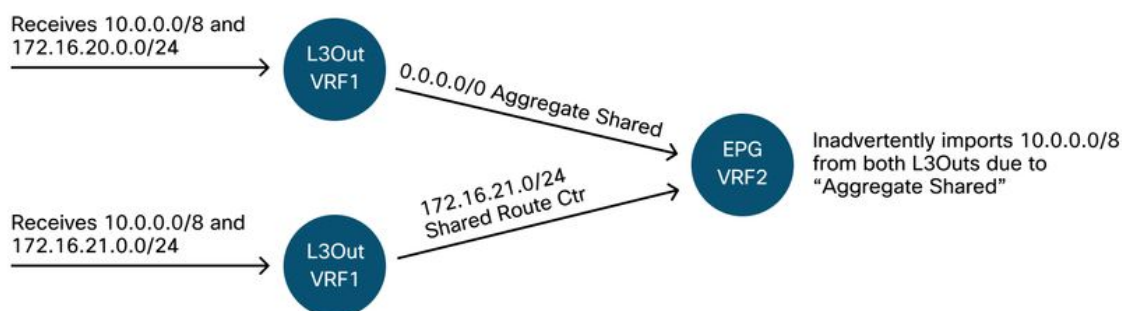
## Gedeeld L3Out probleemoplossing scenario — onverwacht route lekken

Dit scenario heeft meerdere L3Outs in de externe VRF en een interne EPG ontvangt een route van een L3Out waar het netwerk **niet is** gedefinieerd met de 'gedeelde' scope opties.

### Gebruik van 'Gedeeld aggregaat'

Neem het volgende cijfer:

### Onverwacht wegtek



De BGP import-map met de voorvoegsel-lijst geprogrammeerd vanuit de vlaggen **'Shared Route Control Subnet'** wordt toegepast op VRF-niveau. Als één L3Out in VRF1 een subnetverbinding heeft met 'Shared Route Control Subnet', worden alle routes die binnen VRF1 worden ontvangen op L3Outs die overeenkomen met dit gedeelde Route Control Subnet geïmporteerd in VRF2.

Het bovenstaande ontwerp kan leiden tot onverwachte verkeersstromen. Als er geen contracten zijn tussen de interne EPG en de onverwachte reclame L3Out EPG, dan zal er een verkeersdaling zijn.

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.