ACI 외부 포워딩 문제 해결

목차

소개

이 문서에서는 ACI에서 L3out을 이해하고 문제를 해결하는 단계를 설명합니다

배경 정보

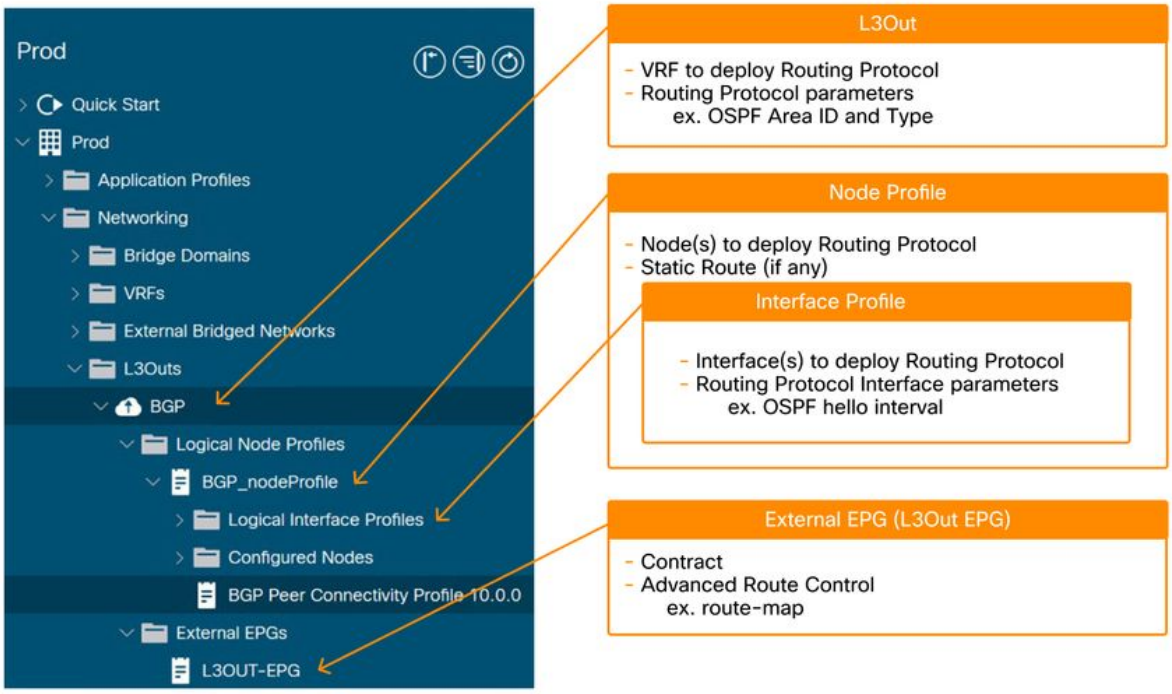
이 문서의 자료는 Troubleshooting Cisco Application Centric Infrastructure, Second Edition Book에서 특히 **External Forwarding- Overview, External Forwarding - Adjacances, External Forwarding - Route Advertisement, External Forwarding - Contract and L3out and External Forwarding - Share L3out** 장과 **관련된 내용을 발췌했습니다**.

개요

L3Out 구성 요소

다음 그림은 L3 Outside(L3Out)를 구성하는 데 필요한 주요 구성 요소를 보여줍니다.

L3Out의 주요 구성 요소



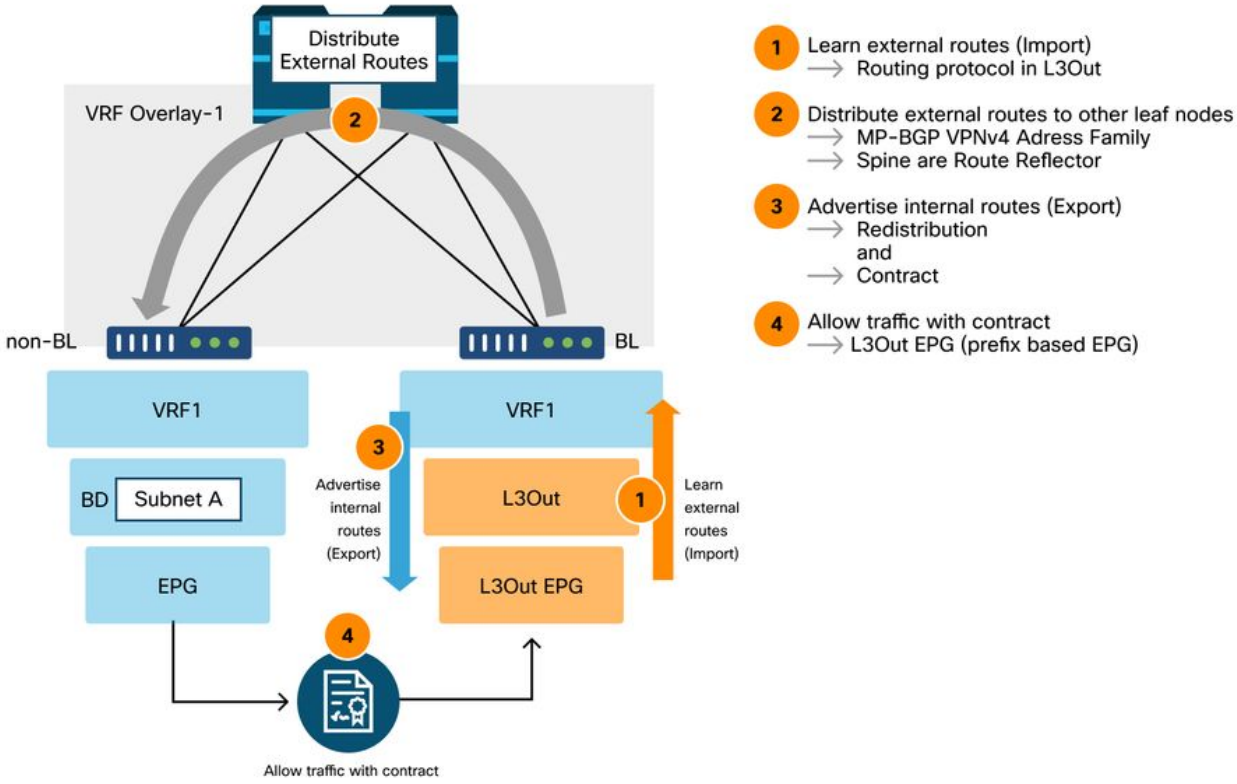
1. L3Out 루트: 구축할 라우팅 프로토콜(예: OSPF, BGP)을 선택합니다.라우팅 프로토콜을 구축할 VRF를 선택합니다.L3Out 도메인을 선택하여 L3Out에 사용 가능한 리프 인터페이스와 VLAN을 정의합니다.
2. 노드 프로파일: 라우팅 프로토콜을 구축할 리프 스위치를 선택합니다. 이러한 스위치를 일반적으로 'BL(Border Leaf Switch)'이라고 합니다.각 보더 리프에 라우팅 프로토콜의 RID(Router-ID)를 구성합니다. 일반 라우터와 달리 ACI는 스위치의 IP 주소를 기반으로 라우터 ID를 자동으로 할당하지 않습니다.고정 경로를 구성합니다.
3. 인터페이스 프로필: 라우팅 프로토콜을 실행하도록 리프 인터페이스를 구성합니다. 예: 인터페이스 유형(SVI, 라우팅된 포트, 하위 인터페이스), 인터페이스 ID 및 IP 주소 등인터페이스 레벨 라우팅 프로토콜 매개변수(예: hello 간격)에 대한 정책을 선택합니다.
4. 외부 EPG(L3Out EPG): '외부 EPG'는 인접 디바이스를 설정하기 위해 IP 주소 또는 SVI와 같이 L3Out에 연결된 모든 정책을 배포하기 위한 까다로운 요구 사항입니다. 외부 EPG 사용 방

법에 대한 자세한 내용은 나중에 다룹니다.

외부 라우팅

다음 다이어그램은 외부 라우팅과 관련된 상위 레벨 공정을 보여줍니다.

상위 레벨 외부 라우팅 흐름

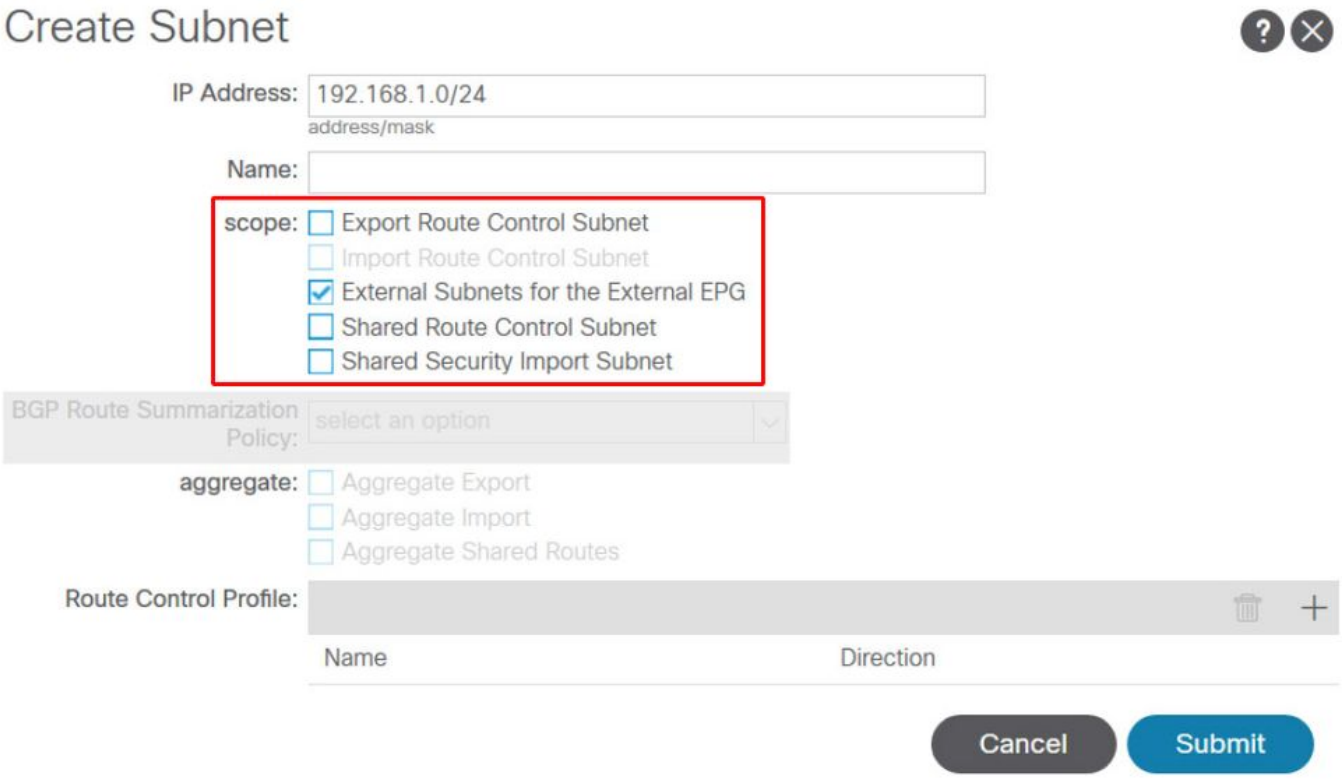


1. BL은 외부 라우터와의 라우팅 프로토콜 인접성을 설정합니다.
2. 경로 접두사는 외부 라우터에서 수신되며 VPNv4 주소군 경로로 MP-BGP에 삽입됩니다. 적어도 2개의 스파인 노드는 모든 리프 노드에 대한 외부 경로를 반영하도록 BGP 경로 리플렉터로 구성해야 합니다.
3. 다른 L3Out에서 받은 내부 접두사(BD 서브넷) 및/또는 접두사는 외부 라우터로 광고하기 위해 라우팅 프로토콜에 명시적으로 재배포해야 합니다.
4. 보안 시행: l3Out에는 하나 이상의 L3Out EPG가 포함되어 있습니다. L3Out에서 트래픽을 허용하려면 L3Out EPG에서 contract를 사용하거나 제공해야 합니다(클래스 이름에서 l3extInstP라고도 함).

L3Out EPG 컨피그레이션 옵션

L3Out EPG 섹션에서 서브넷은 아래 그림과 같이 일련의 'Scope' 및 'Aggregate' 옵션으로 정의할 수 있습니다.

'범위' 정의를 포함하여 정의되는 L3Out 서브넷



'범위' 옵션:

- **경로 제어 서브넷 내보내기:** 이 범위는 ACI에서 L3Out을 통해 외부로 서브넷을 알림(내보내기)하는 것입니다. 주로 전송 라우팅을 위한 것이지만 "ACI BD 서브넷 광고" 섹션에 설명된 대로 BD 서브넷을 광고하는 데에도 사용할 수 있습니다.
- **경로 제어 서브넷 가져오기:** 이 범위는 L3Out에서 외부 서브넷을 학습(가져오기)하는 것입니다. 기본적으로 이 범위는 비활성화되어 회색으로 표시되며, BL(Border Leaf)이 라우팅 프로토콜에서 경로를 학습합니다. 이 범위는 OSPF 및 BGP를 통해 학습된 외부 경로를 제한해야 할 때 활성화할 수 있습니다. EIGRP에서는 지원되지 않습니다. 이 범위를 사용하려면 지정된 L3Out에서 'Import Route Control Enforcement'를 먼저 활성화해야 합니다.
- **외부 EPG를 위한 외부 서브넷(import-security):** 이 범위는 구성된 서브넷을 가진 패킷이 contract를 가진 L3Out에서 오도록 허용하는 데 사용됩니다. 서브넷을 기준으로 패킷을 구성된 L3Out EPG로 분류하여 L3Out EPG의 계약이 패킷에 적용될 수 있도록 합니다. 이 범위는 라우팅 테이블의 다른 범위와 마찬가지로 정확한 일치 대신 최장 접두사 일치입니다. L3Out EPG A에서 10.0.0.0/16이 '외부 EPG용 외부 서브넷'으로 구성된 경우, 해당 서브넷에 IP가 있는 패킷(예: 10.0.1.1)은 L3Out EPG A에서 계약을 사용하기 위해 L3Out EPG A로 분류됩니다. 이는 '외부 EPG를 위한 외부 서브넷' 범위가 라우팅 테이블에 경로 10.0.0.0/16을 설치한다는 의미는 아닙니다. 서브넷을 계약의 EPG(pcTag)에 매핑하기 위해 다른 내부 테이블을 생성합니다. 라우팅 프로토콜 동작에 영향을 미치지 않습니다. 이 범위는 서브넷을 학습 중인 L3Out에서 구성됩니다.
- **공유 경로 제어 서브넷:** 이 범위는 외부 서브넷을 다른 VRF로 유출하는 것입니다. ACI는 MP-BGP 및 Route Target을 사용하여 한 VRF에서 다른 VRF로 외부 경로를 유출합니다. 이 범위는 MP-BGP에서 경로 대상으로 경로를 내보내거나 가져오기 위한 필터로 사용되는 서브넷을 포함하는 접두사 목록을 생성합니다. 이 범위는 원래 VRF에서 서브넷을 학습하는 L3Out에서 구성됩니다.
- **공유 보안 가져오기 서브넷:** 이 범위는 패킷이 L3Out을 사용하는 VRF를 통해 이동할 때 구성된 서브넷을 사용하는 패킷을 허용하는 데 사용됩니다. 라우팅 테이블의 경로가 위에서 설명한 대로 '공유 경로 제어 서브넷'을 사용하여 다른 VRF로 유출됩니다. 그러나 또 다른 VRF는 유출된

경로가 어떤 EPG에 속해야 하는지 아직 모릅니다. '공유 보안 가져오기 서브넷'은 다른 VRF에게 유출된 경로가 속한 L3Out EPG를 알려줍니다. 따라서 이 범위는 '외부 EPG를 위한 외부 서브넷'도 사용되는 경우에만 사용할 수 있습니다. 그렇지 않으면 원래 VRF가 서브넷이 어느 L3Out EPG에 속하는지 알지 못합니다. 이 범위는 Longest Prefix Match이기도 합니다.

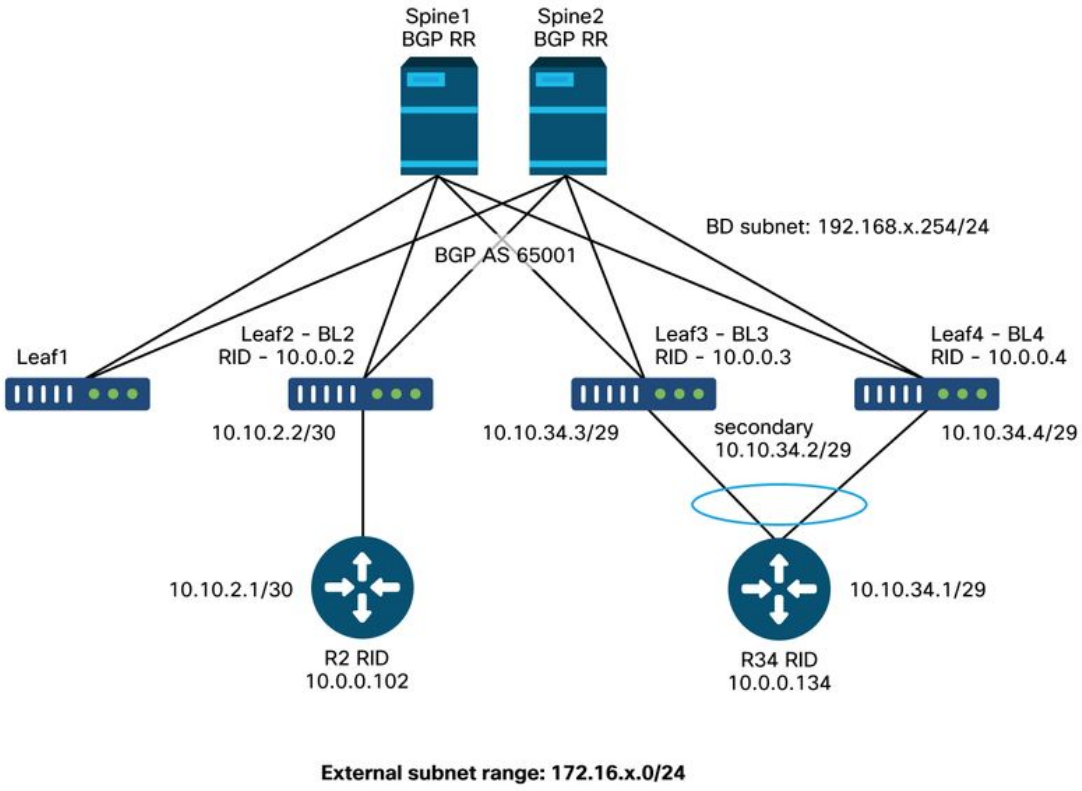
'집계' 옵션:

- **집계 내보내기:** 이 옵션은 'Export Route Control Subnet'을 사용하는 0.0.0.0/0에만 사용할 수 있습니다. 0.0.0.0/0에 대해 'Export Route Control Subnet' 및 'Aggregate Export'가 모두 활성화된 경우; 서브넷과 일치하는 '0.0.0.0/0 le 32'가 포함된 접두사 목록을 생성합니다. 따라서 이 옵션은 L3Out에서 어떤 경로든 외부로 알림(내보내기)해야 할 때 사용할 수 있습니다. 보다 세분화된 집계가 필요한 경우, 명시적 접두사 목록이 있는 경로 맵/프로파일을 사용할 수 있습니다.
- **집계 가져오기:** 이 옵션은 'Import Route Control Subnet'을 사용하는 0.0.0.0/0에만 사용할 수 있습니다. 0.0.0.0/0에 대해 'Import Route Control Subnet' 및 'Aggregate Import'를 모두 활성화하면, 모든 서브넷과 일치하는 '0.0.0.0/0 le 32'가 포함된 접두사 목록이 생성됩니다. 따라서 이 옵션은 L3Out이 외부에서 경로를 학습(가져오기)해야 할 때 사용할 수 있습니다. 그러나 기본값인 'Import Route Control Enforcement'를 비활성화하면 동일한 작업을 수행할 수 있습니다. 보다 세분화된 집계가 필요한 경우, 명시적 접두사 목록이 있는 경로 맵/프로파일을 사용할 수 있습니다.
- **공유 경로 집계:** 이 옵션은 '공유 경로 제어 서브넷'이 있는 서브넷에 사용할 수 있습니다. 예를 들어 10.0.0.0/8에 대해 '공유 경로 제어 서브넷'과 '종합 공유 경로'를 모두 사용하도록 설정하면 10.0.0.0/8, 10.1.0.0/16 등과 일치하는 '10.0.0.0/8 le 32'가 포함된 접두사 목록이 생성됩니다.

이 섹션에서 사용되는 L3Out 토폴로지

이 섹션에서는 다음 토폴로지를 사용합니다.

L3Out 토폴로지



인접성

이 섹션에서는 L3Out 인터페이스의 라우팅 프로토콜 인접성을 트러블슈팅하고 확인하는 방법에 대해 설명합니다.

다음은 모든 ACI 외부 라우팅 프로토콜에 적용할 수 있는 몇 가지 매개변수입니다.

- **라우터 ID:** ACI에서 각 L3Out은 라우팅 프로토콜이 다르더라도 동일한 리프의 동일한 VRF에서 동일한 라우터 ID를 사용해야 합니다. 또한 동일한 리프에 있는 L3Out 중 하나만 일반적으로 BGP인 라우터 ID로 루프백을 생성할 수 있습니다.
- **MTU:** MTU라는 까다로운 요구 사항은 OSPF 인접성에만 적용되지만, 경로 교환/업데이트에 사용되는 점보 패킷을 단편화 없이 전송할 수 있도록 모든 라우팅 프로토콜에 대해 MTU를 일치시키는 것이 좋습니다. 대부분의 컨트롤 플레인 프레임은 DF(조각화 안 함) 비트 설정으로 전송되기 때문에, 해당 크기가 인터페이스의 최대 MTU를 초과하면 프레임이 삭제됩니다.
- **MP-BGP 라우터 리플렉터:** 이 기능이 없으면 리프 노드에서 BGP 프로세스가 시작되지 않습니다. OSPF 또는 EIGRP가 인접 디바이스를 설정하는 데에만 이 기능이 필요하지는 않지만, BL이 외부 경로를 다른 리프 노드에 배포하는 데에도 이 기능이 필요합니다.
- **Faults(결함):** 컨피그레이션이 완료되는 동안과 완료된 후에 항상 결함을 확인하십시오.

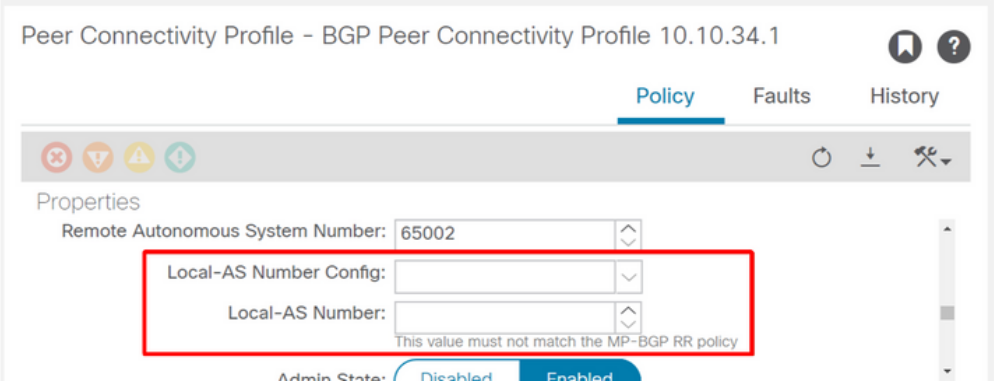
BGP

이 섹션에서는 Overview 섹션의 토폴로지에서 BL3, BL4 및 R34의 루프백 간 eBGP 피어링 예를 사용합니다. R34의 BGP AS가 65002.

BGP 인접성을 설정할 때 다음 기준을 확인합니다.

- 로컬 BGP AS 번호(ACI BL 측).

피어 연결 프로파일 — Local-AS

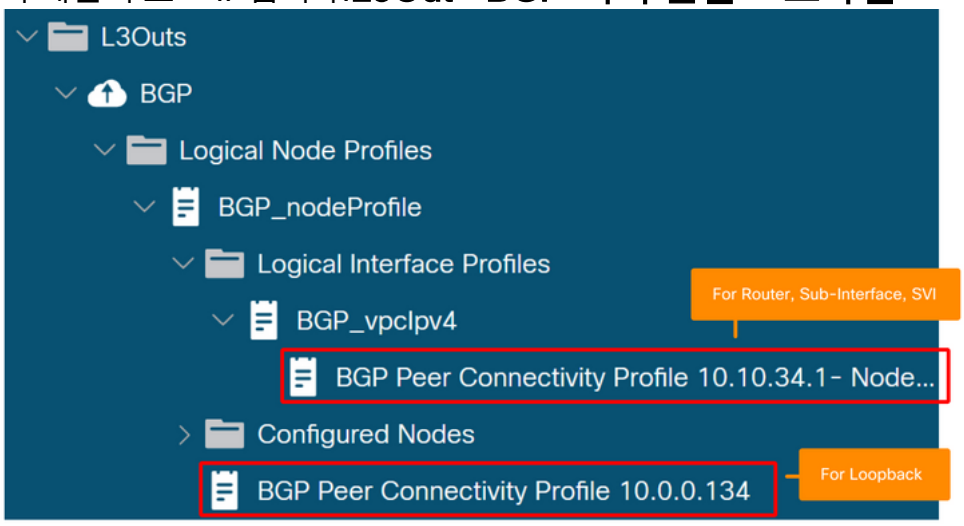


사용자 L3Out의 BGP AS 번호는 BGP 경로 리플렉터 정책에 구성된 infra-MP-BGP의 BGP AS와 자동으로 동일합니다. ACI BGP AS를 외부 영역으로 가장해야 하는 경우가 아니면 BGP 피어 연결 프로파일의 '로컬 AS' 컨피그레이션이 필요하지 않습니다. 이는 외부 라우터가 BGP Route Reflector에 구성된 BGP AS를 가리켜야 함을 의미합니다.

참고 — 로컬 AS 컨피그레이션이 필요한 시나리오는 독립형 NX-OS 'local-as' 명령과 동일합니다.

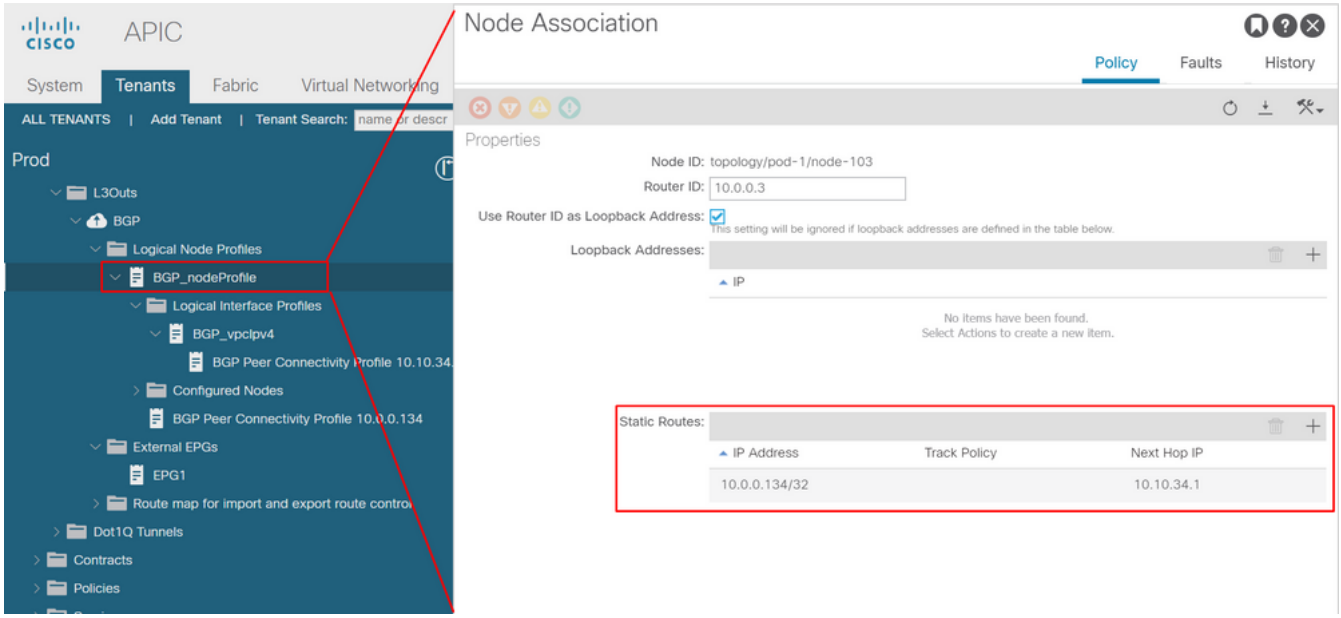
- 원격 BGP AS 번호(외부) **피어 연결 프로파일 — 원격 AS**

Remote BGP AS 번호는 인접 디바이스의 BGP AS가 ACI BGP AS와 다른 eBGP에만 필요합니다.BGP 피어 세션의 소스 IP입니다.**L3Out - BGP 피어 연결 프로파일**



ACI는 일반적인 ACI L3Out 인터페이스 유형(라우티드, 하위 인터페이스, SVI) 위에 루프백 인

터페이스에서 BGP 세션을 소싱할 수 있도록 지원합니다.루프백에서 BGP 세션을 소싱해야 하는 경우 Logical **Node** Profile(논리적 노드 프로파일) 아래에 BGP Peer Connectivity Profile(BGP 피어 연결 프로파일)**을** 구성합니다.BGP 세션을 라우티드/하위 인터페이스/SVI에서 소싱해야 하는 경우 논리적 인터페이스 프로파일 아래에 BGP 피어 연결 **프로파일을** 구성합니다.BGP 피어 IP 연결성.**논리 노드 프로파일 — 노드 연결**



BGP 피어 IP가 루프백인 경우 BL과 외부 라우터가 피어의 IP 주소에 연결할 수 있는지 확인합니다. 고정 경로 또는 OSPF를 사용하여 피어 IP에 연결할 수 있습니다.**BGP CLI 확인(eBGP with loopback 예)**다음 단계에 대한 CLI 출력은 Overview(개요) 섹션의 토폴로지에 있는 BL3에서 수집됩니다.**1. BGP 세션이 설정되었는지 확인합니다**다음 CLI 출력의 'State/PfxRcd'는 BGP 세션이 설정되었음을 의미합니다.

```
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
```

'State/PfxRcd'에 Idle 또는 Active가 표시되면 BGP 패킷이 아직 피어와 교환되지 않은 것입니다. 이러한 시나리오에서는 다음을 확인하고 다음 단계로 진행합니다.

- 외부 라우터가 ACI BGP AS를 올바르게 가리키는지 확인합니다(로컬 AS 번호 65001).
- ACI BGP 피어 연결 프로파일이 외부 라우터가 BGP 세션을 소싱하는 올바른 인접 디바이스 IP를 지정하는지 확인합니다(10.0.0.134).
- ACI BGP 피어 연결 프로파일이 외부 라우터의 올바른 인접 디바이스 AS(CLI에 AS 번호로 표시되는 GUI의 원격 자동 시스템 번호)를 65002.

2. BGP 네이버 세부 정보 확인(BGP 피어 연결 프로파일)

다음 명령은 BGP 네이버 설정에 대한 키인 매개변수를 보여줍니다.

- 네이버 IP: 10.0.0.134 .
- 인접 BGP AS: 원격 AS 65002.
- 소스 IP: 루프백3을 업데이트 소스로 사용합니다.

- eBGP 멀티 홉: 외부 BGP 피어는 최대 2홉 떨어져 있을 수 있습니다.

```
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
```

BGP 피어가 올바르게 설정되면 '로컬 호스트' 및 '외부 호스트'가 출력의 맨 아래에 나타납니다.

3. BGP 피어에 대한 IP 연결성 확인

```
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
```

인접 디바이스 IP에 대한 ping이 ACI BGP의 소스 IP에서 작동하는지 확인합니다.

```
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. 외부 라우터에서 동일한 항목을 확인합니다

다음은 외부 라우터(독립형 NX-OS)의 컨피그레이션 예입니다.

```
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. 추가 단계 — tcpdump

ACI 리프 노드에서 tcpdump 툴은 'kpm_inb' CPU 인터페이스를 스니핑하여 프로토콜 패킷이 리프 CPU에 도달했는지 확인할 수 있습니다. L4 포트 179(BGP)를 필터로 사용합니다.

```
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
```

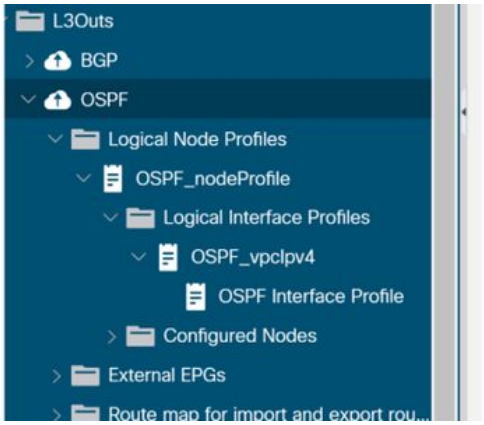
OSPF

이 섹션에서는 OSPF NSSA(AreaID 1)가 포함된 Overview(개요) 섹션의 토폴로지에서 BL3, BL4 및 R34 간의 OSPF 네이버 예를 사용합니다.

다음은 OSPF 인접성 설정을 확인하는 일반적인 기준입니다.

- OSPF 영역 ID 및 유형

L3Out — OSPF 인터페이스 프로파일 — 영역 ID 및 유형



다른 라우팅 디바이스와 마찬가지로 OSPF Area ID 및 Type도 두 네이버에서 일치해야 합니다. OSPF 영역 ID 컨피그레이션의 일부 ACI 관련 제한은 다음과 같습니다.

- 하나의 L3Out에는 하나의 OSPF 영역 ID만 사용할 수 있습니다.
- 두 개의 L3Out은 두 개의 서로 다른 리프 노드에 있는 경우에만 동일한 VRF에서 동일한 OSPF 영역 ID를 사용할 수 있습니다.

OSPF ID가 백본 0일 필요는 없지만 트랜짓 라우팅의 경우 동일한 리프에 있는 두 OSPF L3Out 사이에 필요합니다. OSPF 영역 간의 경로 교환은 OSPF 영역 0을 통과해야 하므로 그중 하나는 OSPF 영역 0을 사용해야 합니다.

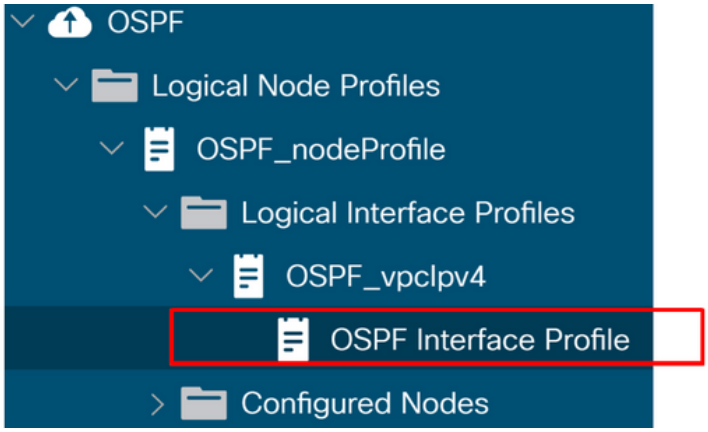
- MTU

논리적 인터페이스 프로파일 — SVI

ACI의 기본 MTU는 1500바이트가 아닌 9000바이트이며, 이는 일반적으로 기존 라우팅 디바이스에서 사용되는 기본값입니다. MTU가 외부 디바이스와 일치하는지 확인합니다. OSPF 네이버 설정이 MTU로 인해 실패할 경우 EXCHANGE/DROTHER에서 중단됩니다.

- IP 서브넷 마스크입니다. OSPF에서는 인접 디바이스 IP가 동일한 서브넷 마스크를 사용해야 합니다.
- OSPF 인터페이스 프로파일

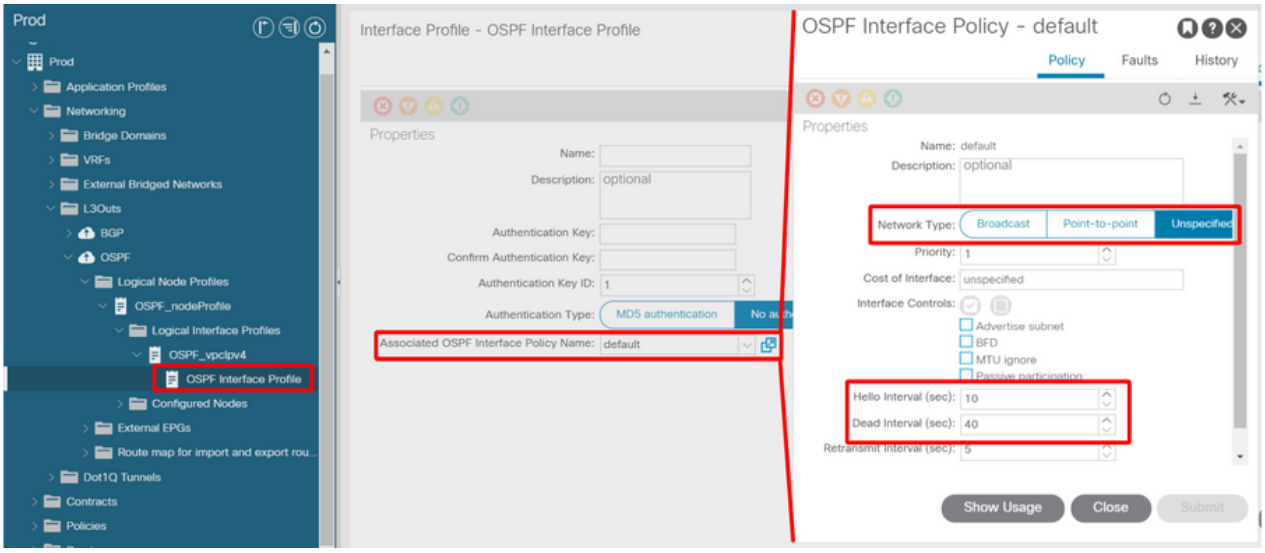
OSPF 인터페이스 프로파일



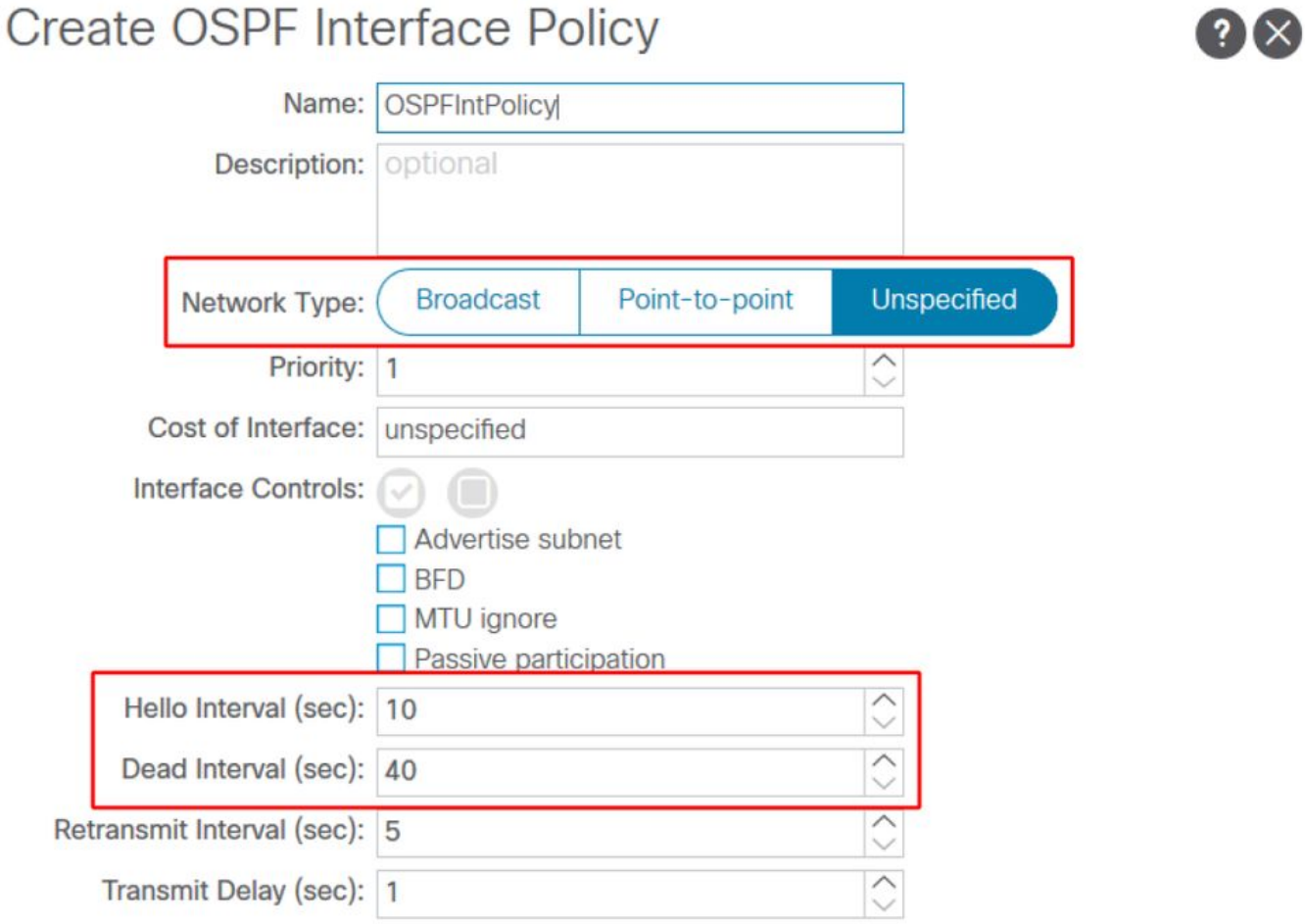
이는 독립형 NX-OS 컨피그레이션의 'ip router ospf <tag> area <area id>'가 인터페이스에서 OSPF를 활성화하는 것과 같습니다. 이를 사용하지 않으면 리프 인터페이스가 OSPF에 조인하지 않습니다.

- OSPF Hello/Dead Timer, 네트워크 유형

OSPF 인터페이스 프로파일 — Hello/Dead 타이머 및 네트워크 유형



OSPF 인터페이스 정책 세부 정보



OSPF에서는 Hello 및 Dead 타이머가 각 네이버 디바이스에서 일치해야 합니다. OSPF 인터페이스 프로파일에서 구성합니다.

OSPF 인터페이스 네트워크 유형이 외부 디바이스와 일치하는지 확인합니다. 외부 디바이스에서 Point-to-Point 유형을 사용하는 경우 ACI 측에서 Point-to-Point도 명시적으로 구성해야 합니다. OSPF 인터페이스 프로파일에서도 구성됩니다.

OSPF CLI 확인

다음 단계의 CLI 출력은 "개요" 섹션의 토폴로지에 있는 BL3에서 수집됩니다.

1. OSPF 네이버 상태 확인

다음 CLI에서 'State'가 'FULL'이면 OSPF 인접 디바이스가 올바르게 설정됩니다. 그렇지 않으면 다음 단계로 이동하여 매개변수를 확인합니다.

```
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
```

ACI에서는 SVI와 동일한 VLAN ID를 사용할 때 BL이 외부 라우터 위에 서로 OSPF 네이버를 형성합니다. 이는 ACI에 L3Out SVI의 각 VLAN ID에 대해 L3Out BD(또는 External BD)라는 내부 플러딩 도메인이 있기 때문입니다. VLAN ID 28은 유선에서 사용되는 실제 VLAN(Access Encap

VLAN)이 아닌 PI-VLAN(Platform-Independent VLAN)이라는 내부 VLAN입니다. 다음 명령을 사용하여 액세스 캡슐화 VLAN('vlan-2502')을 확인합니다.

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

액세스 캡슐화 VLAN ID를 통해 동일한 출력을 얻을 수도 있습니다.

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

2. OSPF 영역 확인

OSPF 영역 ID 및 유형이 네이버와 동일한지 확인합니다. OSPF 인터페이스 프로파일이 없는 경우 인터페이스는 OSPF에 조인하지 않으며 OSPF CLI 출력에 표시되지 않습니다.

```
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. OSPF 인터페이스 세부사항 확인

인터페이스 레벨 매개변수가 IP 서브넷, 네트워크 유형, Hello/Dead 타이머와 같은 OSPF 네이버 설정에 대한 요구 사항을 충족하는지 확인합니다. SVI를 PI-VLAN(vlan28)으로 지정하려면 VLAN ID를 확인하십시오

```
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. 네이버에 대한 IP 연결 가능성 확인

OSPF Hello 패킷은 링크 로컬 멀티캐스트 패킷이지만 첫 번째 OSPF LSDB 교환에 필요한 OSPF DBD 패킷은 유니캐스트입니다. 따라서 OSPF 인접 디바이스 설정에 대해서도 유니캐스트 연결성을 확인해야 합니다.

```
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. 외부 라우터에서 동일한 항목을 확인합니다

다음은 외부 라우터(독립형 NX-OS)의 컨피그레이션 예입니다

```
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
```

물리적 인터페이스에서도 MTU를 확인해야 합니다.

6. 추가 단계 — tcpdump

ACI 리프 노드에서 사용자는 'kpm_inb' CPU 인터페이스에서 tcpdump를 수행하여 프로토콜 패킷이 리프 CPU에 도달했는지 확인할 수 있습니다. OSPF에는 여러 필터가 있지만 IP Protocol Number(IP 프로토콜 번호)가 가장 포괄적인 필터입니다.

- IP 프로토콜 번호: proto 89(IPv4) 또는 ip6 proto 0x59(IPv6)
- 인접 디바이스의 IP 주소: 호스트 <ip>
- OSPF 링크 로컬 멀티캐스트 IP: host 224.0.0.5 또는 host 224.0.0.6

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

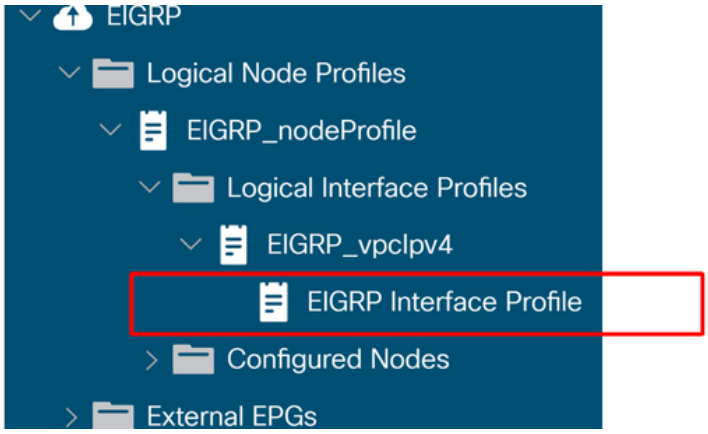
EIGRP

이 섹션에서는 "Overview(개요)" 섹션의 토폴로지에서 EIGRP AS 10으로 BL3, BL4 및 R34 간 EIGRP 네이버십의 예를 사용합니다.

다음은 EIGRP 인접성 설정의 일반적인 기준입니다.

- EIGRP AS: l3Out에는 하나의 EIGRP AS가 할당됩니다. 외부 장치와 일치해야 합니다.
- EIGRP 인터페이스 프로파일

EIGRP 인터페이스 프로파일



이는 독립형 NX-OS 디바이스의 'ip router eigrp <as>' 컨피그레이션과 동일합니다. 이를 사용하지 않으면 리프 인터페이스가 EIGRP에 조인하지 않습니다.

- MTU

단순히 EIGRP 네이버십을 설정하기 위해 일치할 필요는 없지만 EIGRP 토폴로지 교환 패킷은 피어 간의 인터페이스에 허용되는 최대 MTU보다 클 수 있으며, 이러한 패킷은 프래그먼트화될 수 없으므로 삭제되고 결과적으로 EIGRP 네이버십이 플랩됩니다.

EIGRP CLI 확인

다음 단계의 CLI 출력은 "개요" 섹션의 토폴로지에 있는 BL3에서 수집됩니다.

1. EIGRP 네이버 상태 확인

```
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
```

ACI에서 BL은 SVI와 동일한 VLAN ID를 사용할 때 외부 라우터 위에 서로 EIGRP 네이버를 형성합니다. 이는 ACI에 L3Out SVI의 각 VLAN ID에 대한 L3Out BD(또는 External BD)라는 내부 플러딩 도메인이 있기 때문입니다.

VLAN ID 29는 유선에서 사용되는 실제 VLAN(Access Encap VLAN)이 아닌 PI-VLAN(Platform-Independent VLAN)이라는 내부 VLAN입니다. 다음 명령을 사용하여 액세스 캡슐화 VLAN(vlan-2503)을 확인합니다.

```
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
```

액세스 캡슐화 VLAN ID를 통해 동일한 출력을 얻을 수도 있습니다.

```
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. EIGRP 인터페이스 세부사항 확인

EIGRP가 예상 인터페이스에서 실행 중인지 확인합니다. 그렇지 않은 경우 Logical Interface Profile(논리적 인터페이스 프로파일) 및 EIGRP Interface Profile(EIGRP 인터페이스 프로파일)을 선택합니다.

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

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

3. 외부 라우터에서 확인하십시오

다음은 외부 라우터(독립형 NX-OS)의 컨피그레이션 예입니다.

```
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. 추가 단계 — tcpdump

ACI 리프 노드에서 사용자는 'kpm_inb' CPU 인터페이스에서 tcpdump를 수행하여 프로토콜 패킷이 리프의 CPU에 도달했는지 확인할 수 있습니다. EIGRP(IP 프로토콜 번호 88)를 필터로 사용합니다.

```
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
```

경로 광고

이 섹션에서는 ACI의 경로 광고 확인 및 트러블슈팅을 중점적으로 다룹니다. 특히 다음과 관련된 예를 살펴봅니다.

- 브리지 도메인 서브넷 광고
- 이동 경로 알림
- 경로 제어 가져오기 및 내보내기

이 섹션에서는 이후의 섹션에서 공유 L3Out과 관련된 경로 누출에 대해 설명합니다.

브리지 도메인 경로 알림 워크플로

일반적인 트러블슈팅을 살펴보기 전에 사용자는 Bridge 도메인 광고의 작동 방식을 숙지해야 합니다.

BD 광고는 BD와 L3Out이 동일한 VRF에 있을 때 다음을 포함합니다.

- L3Out과 내부 EPG 간의 계약 관계
- L3Out을 브리지 도메인에 연결
- BD 서브넷에서 '외부에 알림'을 선택합니다.

또한 L3Out을 연결할 필요가 없는 내보내기 경로 프로파일을 사용하여 브리지 도메인 광고를 제어할 수도 있습니다. 그러나 'Advertise Externally'는 계속 선택해야 합니다. 이것은 덜 일반적인 활용 사례이므로 여기서는 논의하지 않습니다.

BD 퍼베이시브 고정 경로가 BL로 푸시되도록 하려면 L3Out과 EPG 간의 계약 관계가 필요합니다. 실제 경로 알림은 고정 경로를 외부 프로토콜로 재배포하여 처리됩니다. 마지막으로, 재배포 경로 맵은 BD와 연결된 L3Out 내에서만 설치됩니다. 이 방법으로 경로가 모든 L3Out에 광고되지 않습니다.

이 경우 BD 서브넷은 192.168.1.0/24이며 OSPF L3Out을 통해 광고해야 합니다.

L3Out과 내부 EPG 간에 계약을 적용하기 전

```
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
```

BL에 BD 경로가 아직 없습니다.

L3Out과 내부 EPG 간에 계약을 적용한 후

이 시점에서 다른 컨피그레이션은 수행되지 않았습니다. L3Out이 아직 BD에 연결되지 않았고 '외부에 알림' 플래그가 설정되지 않았습니다.

```
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
```

이제 BD 서브넷 경로(퍼베이시브 플래그로 표시됨)가 BL에 구축됩니다. 그러나 경로에 태그가 지정되어 있습니다. 이 태그 값은 'Advertise Externally'로 구성되기 전에 BD 경로에 할당된 암시적 값입니다. 모든 외부 프로토콜은 이 태그의 재배포를 거부합니다.

BD 서브넷에서 '외부 알림'을 선택한 후

L3Out이 여전히 BD에 연결되지 않았습니다. 그러나 태그가 지워졌습니다.

```
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
```

이 시점에서는 외부 프로토콜로 재배포할 이 접두사와 일치하는 경로 맵 및 접두사 목록이 없기 때문에 경로가 여전히 외부에 알려지지 않습니다. 다음 명령으로 확인할 수 있습니다.

```
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
```

BD 경로는 고정 경로로 프로그래밍되므로, 경로 맵에 있는 접두사 목록에서 'show route-map <route-map name>'을 실행한 다음 'show ip prefix-list <name>'을 실행하여 고정 재배포 경로 맵을 확인하십시오. 다음 단계에서 이를 수행합니다.

L3Out을 BD에 연결한 후

앞에서 설명한 것처럼 이 단계에서는 고정-외부 프로토콜 재배포 경로 맵에 설치 중인 BD 서브넷과 일치하는 접두사 목록이 생성됩니다.

```
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
```

접두사 목록을 확인합니다.

```
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
```

BD 서브넷이 OSPF에 재배포되도록 일치됩니다.

이 시점에서 L3Out에서 BD 서브넷을 알리는 컨피그레이션 및 확인 워크플로가 완료되었습니다. 이 시점이 지나면 검증은 프로토콜에 따라 달라집니다. 예를 들면 다음과 같습니다.

- EIGRP의 경우 경로가 토폴로지 테이블에 'show ip eigrp topology vrf <name>'으로 설치되어 있는지 확인합니다
- OSPF의 경우 경로가 'show ip ospf database vrf <name>'을 사용하여 데이터베이스 테이블에 외부 LSA로 설치되어 있는지 확인합니다
- BGP의 경우 경로가 'show bgp ipv4 unicast vrf <name>'으로 BGP RIB에 있는지 확인합니다.

BGP 경로 알림

BGP의 경우 모든 고정 경로는 재배포가 암시적으로 허용됩니다. BD 서브넷과 일치하는 경로 맵은 BGP 네이버 레벨에 적용됩니다.

```
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
```

위 예에서 10.0.0.134는 L3Out 내에 구성된 BGP 인접 디바이스입니다.

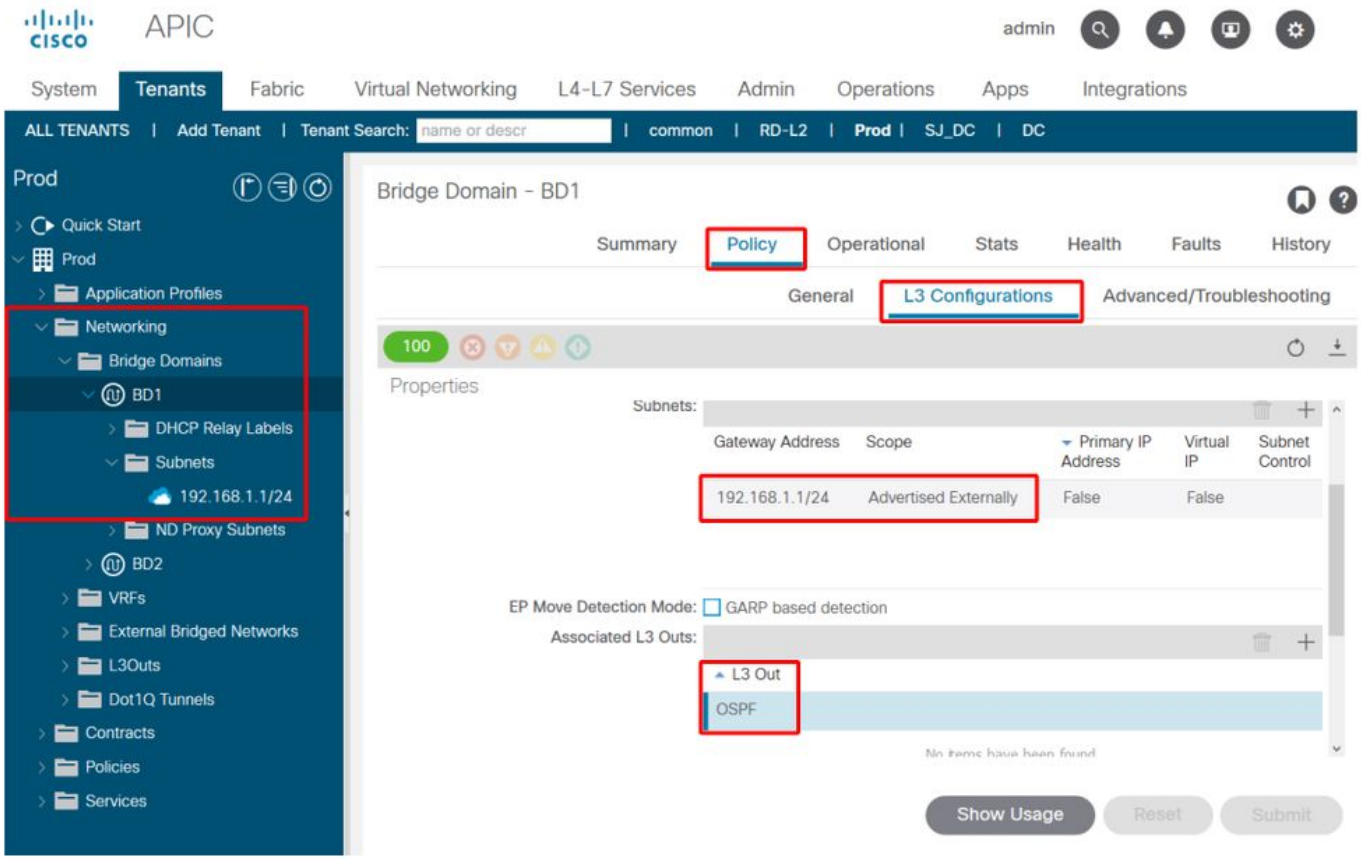
EIGRP 경로 알림

OSPF와 마찬가지로 경로 맵을 사용하여 Static에서 EIGRP로의 재배포를 제어합니다. 이렇게 하면 L3Out에 연결되어 있고 '외부에서 알림'으로 설정된 서브넷만 재배포되어야 합니다. 이 명령은 다음 명령으로 확인할 수 있습니다.

```
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
```

최종 작업 BD 컨피그레이션은 아래와 같습니다.

브리지 도메인 L3 컨피그레이션



브리지 도메인 경로 광고 문제 해결 시나리오

이 경우 일반적인 증상은 일반적으로 구성된 BD 서브넷이 L3Out에서 광고되지 않는 것입니다. 어떤 구성 요소가 손상되었는지 파악하려면 이전 워크플로를 따릅니다.

컨피그레이션으로 시작한 후 다음을 확인하여 너무 낮은 수준으로 설정합니다.

- EPG와 L3Out 사이에 계약이 있습니까?
- L3Out이 BD와 연결되어 있습니까?
- BD 서브넷이 외부에 알리도록 설정되었습니까?
- 외부 프로토콜 인접성이 향상되었습니까?

가능한 원인: BD가 구축되지 않음

이 사례는 다음과 같은 몇 가지 시나리오에 적용됩니다.

- 내부 EPG가 VMM과 온디맨드 통합 옵션을 사용하고 있으며 EPG의 포트 그룹에 연결된 VM 엔드포인트가 없습니다.
- 내부 EPG가 생성되었지만 고정 경로 바인딩이 구성되지 않았거나 고정 경로가 구성된 인터페이스가 다운되었습니다.

두 경우 모두 BD가 구축되지 않으므로 BD 고정 경로가 BL로 푸시되지 않습니다. 여기서 해결 방법은 서브넷이 구축되도록 이 BD에 연결된 EPG 내에 일부 활성 리소스를 구축하는 것입니다.

가능한 원인: OSPF L3Out이 재배포 없이 '스텁' 또는 'NSSA'로 구성됨

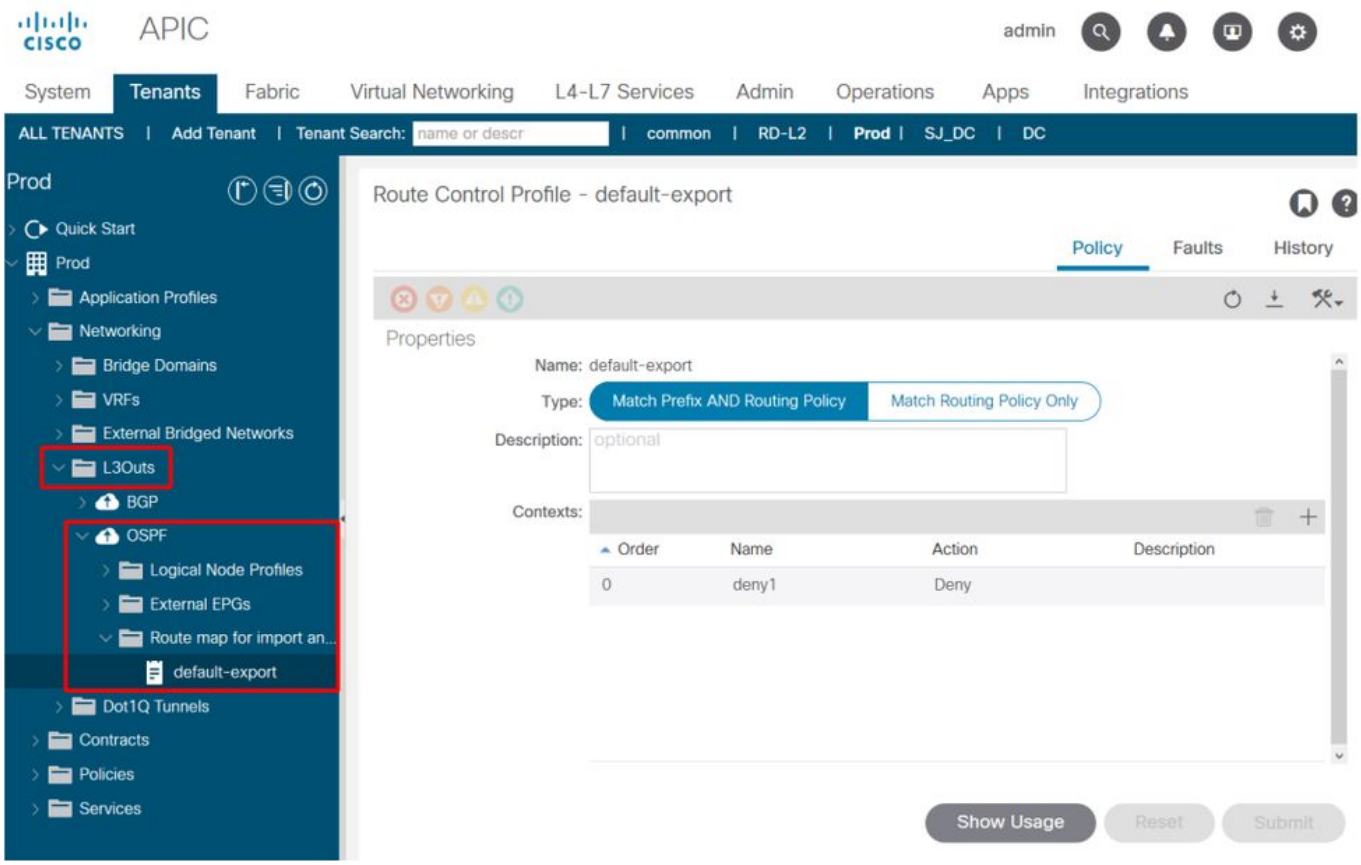
OSPF가 L3Out 프로토콜로 사용되는 경우에도 기본 OSPF 규칙을 따라야 합니다. 스텁 영역은 재배포된 LSA를 허용하지 않지만 대신 기본 경로를 광고할 수 있습니다. NSSA 영역은 재배포된 경로를 허용하지만 L3Out에서 'Send Redistributed LSAs into NSSA Area(NSSA 영역으로 재배포된

LSA 보내기)'를 선택해야 합니다. 또는 NSSA는 'Originate Summary LSA'를 비활성화하는 대신 기본 경로를 광고할 수도 있습니다. 이는 'Send Redistributed LSA's into NSSA Area'가 비활성화되는 일반적인 시나리오이기도 합니다.

가능한 원인: L3Out에 'Deny' 작업이 구성된 'Default-Export' 경로 프로파일

경로 프로파일이 'default-export' 또는 'default-import' 이름으로 L3Out에 구성된 경우 L3Out에 암시적으로 적용됩니다. 또한 default-export 경로 프로파일이 거부 작업으로 설정되고 'Match Prefix and Routing Policy'로 구성된 경우 BD 서브넷은 이 L3Out에서 광고되어야 하며 암시적으로 거부됩니다
.

Default-export 거부 경로 프로파일



'Match Routing Policy Only' 옵션을 선택한 경우 default-export 경로 프로필 내의 접두사 일치에 BD 서브넷이 암시적으로 포함되지 않습니다.

외부 경로 가져오기 워크플로

이 섹션에서는 ACI가 L3Out을 통해 외부 경로를 학습하고 이를 내부 리프 노드에 배포하는 방법에 대해 설명합니다. 또한, 이후 섹션에서 수송 및 경로 유출 활용 사례도 다룹니다

이전 섹션과 마찬가지로, 사용자는 상위 레벨에서 발생하는 상황을 인식해야 합니다.

기본적으로 외부 프로토콜을 통해 학습된 모든 경로는 내부 패브릭 BGP 프로세스로 재배포됩니다. 이는 외부 EPG에 어떤 서브넷이 구성되어 있는지, 어떤 플래그가 선택되어 있는지에 관계없이 마찬가지입니다. 이것이 사실이 아닌 두 가지 예가 있다.

- 최상위 L3Out 정책의 'Route Control Enforcement' 옵션이 'Import'로 설정된 경우 이 경우 경로

가져오기 모델은 차단 목록 모델(허용해서는 안 되는 항목만 지정)에서 허용 목록 모델(달리 구성하지 않는 한 모든 항목이 암시적으로 거부됨)로 바뀝니다.
- 외부 프로토콜이 EIGRP 또는 OSPF이고 사용된 Interleak Route-Profile이 외부 경로와 일치하지 않는 경우

외부 경로를 내부 리프에 배포하려면 다음 작업이 수행되어야 합니다.

- 외부 라우터에서 BL에서 경로를 학습해야 합니다. 패브릭 MP-BGP 프로세스에 재배포할 후보가 되려면 프로토콜 RIB가 아닌 라우팅 테이블에 경로를 설치해야 합니다.
- 경로를 내부 BGP 프로세스로 재배포하거나 광고하도록 허용해야 합니다. 이는 가져오기 경로 제어 적용 또는 Interleak Route-Profile이 사용되지 않는 한 항상 발생해야 합니다.
- BGP 경로 리플렉터 정책을 구성하고 포드 프로필에 적용되는 포드 정책 그룹에 적용해야 합니다. 이를 적용하지 않으면 스위치에서 BGP 프로세스가 초기화되지 않습니다.

내부 EPG/BD가 L3Out과 동일한 VRF에 있는 경우, 위의 세 단계는 내부 EPG/BD가 외부 경로를 사용하는 데 필요한 전부입니다.

경로가 BL 라우팅 테이블에 설치되어 있습니다.

이 경우 BL들(103, 104)에서 학습되어야 하는 외부 경로는 172.16.20.1/32이다.

```
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
```

OSPF를 통해 학습되는 것으로 라우팅 테이블에 설치되어 있음이 분명합니다. 여기에 표시되지 않으면 개별 프로토콜을 확인하고 인접성이 있는지 확인합니다. 경로가 BGP로 재배포됨 BGP 재배포에 대한 외부 프로토콜에 사용된 경로 맵을 확인하여 '가져오기' 시행이나 Interleak Route-Profiles가 사용되지 않는지 확인한 후 재배포 경로 맵을 확인할 수 있습니다. 다음 명령을 참조하십시오.

```
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
```

여기서 'permit-all' 경로 맵은 OSPF-to-BGP 재배포에 사용됩니다. 이는 기본값입니다. 여기에서 BL을 확인하고 BGP에서 시작되는 로컬 경로를 확인할 수 있습니다.

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


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

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

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

위 출력에서 0.0.0.0/0은 로컬에서 시작되었음을 나타냅니다. 알려지는 피어 목록은 Route-Reflector 역할을 하는 패브릭의 스파인 노드입니다.

내부 leaf에서 경로 확인

BL은 VPNv4 BGP 주소군을 통해 스파인 노드에 이를 광고해야 합니다. 스파인 노드는 VRF가 구축된 모든 리프 노드에 이를 광고해야 합니다(경로 유출 방지 예제의 경우 참). 이러한 리프 노드 중 하나에서 'show bgp vpnv4 unicast <route> vrf overlay-1'을 실행하여 VPNv4에 있는지 확인합니다

내부 leaf에서 경로를 확인하려면 아래 명령을 사용합니다.

```
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
```

위의 출력에서 경로는 BGP를 통해 학습되며 next-hop은 BL의 PTEP(Physical TEP)여야 합니다.

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

외부 경로 문제 해결 시나리오

이 시나리오에서 내부 리프(101)는 외부 경로를 수신하지 않습니다.

늘 그렇듯이, 먼저 기본을 점검하세요. 다음을 확인하십시오.

- 라우팅 프로토콜 인접성이 BL에 설정되어 있습니다.
- BGP 경로 리플렉터 정책은 Pod Policy-Group 및 Pod Profile에 적용됩니다.

위 기준이 올바르면 문제의 원인을 보여주는 몇 가지 더 발전된 예가 아래에 나와 있습니다.

가능한 원인: 내부 리프에 VRF가 구축되지 않음

이 경우 외부 경로가 예상되는 내부 leaf에 리소스가 구축된 EPG가 없는 것이 문제입니다. 이는 고정 경로 바인딩이 다운 인터페이스에만 구성되었거나 온디맨드 모드 VMM 통합 EPG만 있고 동적 첨부 파일은 탐지되지 않았기 때문에 발생할 수 있습니다.

L3Out VRF는 내부 leaf에 구축되지 않으므로(내부 leaf에서 'show vrf'로 확인) 내부 leaf는 VPNv4에서 BGP 경로를 가져오지 않습니다.

이 문제를 해결하려면 사용자는 내부 리프의 L3Out VRF 내에 리소스를 구축해야 합니다.

가능한 원인: 가져오기 경로 적용이 사용 중입니다.

앞에서 언급한 대로 가져오기 경로 제어 적용이 활성화된 경우 L3Out은 명시적으로 허용된 외부 경로만 허용합니다. 일반적으로 이 기능은 table-map으로 구현됩니다. 테이블 맵은 프로토콜 RIB와 실제 라우팅 테이블 사이에 있으므로 라우팅 테이블의 내용에만 영향을 줍니다.

Import Route-Control 아래의 출력에서 Enable되어 있지만 명시적으로 허용된 경로가 없습니다. LSA는 OSPF 데이터베이스에 있지만 BL의 라우팅 테이블에 없습니다.

```
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
```

다음은 이러한 동작을 유발하도록 설치된 테이블 맵입니다.

```
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:
```

이 L3Out에 구성된 영역인 영역 100에서 학습하는 모든 내용은 이 테이블 맵에 의해 암시적으로 거부되므로 라우팅 테이블에 설치되지 않습니다.

이 문제를 해결하려면 사용자는 'Import Route Control Subnet' 플래그로 외부 EPG의 서브넷을 정의하거나 설치할 접두사와 일치하는 Import Route-Profile을 만들어야 합니다.

- EIGRP에는 가져오기 적용이 지원되지 않습니다.
- BGP의 경우 가져오기 시행은 BGP 인접 디바이스에 적용되는 인바운드 경로 맵으로 구현됩니다. 이를 확인하는 방법에 대한 자세한 내용은 "BGP 경로 광고" 하위 섹션을 참조하십시오.

가능한 원인: Interleak Profile이 사용되고 있습니다.

Interleak Route-Profiles는 EIGRP 및 OSPF L3Outs에 사용되며 IGP에서 BGP로 재배포되는 항목을 제어할 수 있도록 하고 BGP 특성 설정과 같은 정책 적용을 허용하도록 합니다.

Interleak Route-Profile이 없으면 모든 경로를 BGP로 암시적으로 가져옵니다.

Interleak Route-Profile이 없는 경우:

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

Information regarding configured VRFs:

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

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

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

Interleak 경로 프로파일 사용:

```
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
```

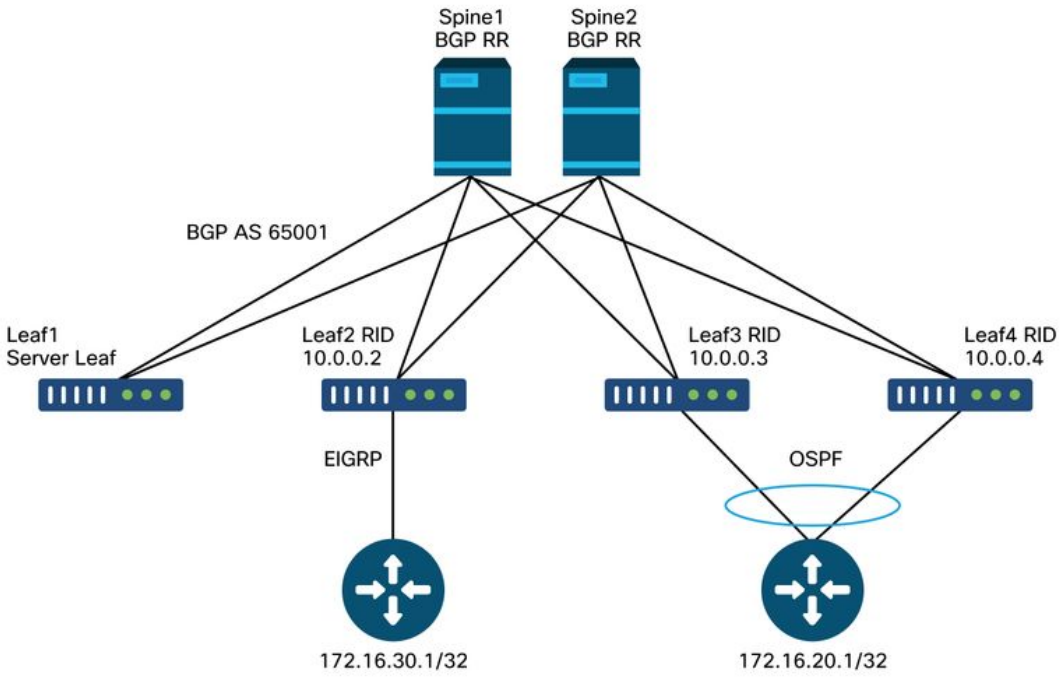
위에서 강조 표시된 경로 맵은 구성된 Interleak Profile에서 명시적으로 일치하는 항목만 허용합니다. 외부 경로가 일치하지 않으면 BGP로 재배포되지 않습니다.

이동 경로 알림 워크플로

이 섹션에서는 하나의 L3Out에서 다른 L3Out으로 경로를 광고하는 방법에 대해 설명합니다. 또한 L3Out에서 직접 구성된 고정 경로를 광고해야 하는 시나리오도 다룹니다. 모든 특정 프로토콜 고려 사항을 검토하는 것이 아니라 ACI에서 이를 구현하는 방법을 살펴봅니다. 현재는 VRF 간 전송 라우팅으로 이동하지 않습니다.

이 시나리오에서는 다음 토폴로지를 사용합니다.

트랜짓 라우팅 토폴로지



OSPF에서 172.16.20.1을 학습한 다음 EIGRP로 광고하는 방법에 대한 상위 레벨 흐름과 전체 프로세스 및 문제 해결 시나리오의 검증은 아래에서 설명합니다.

172.16.20.1 경로가 EIGRP로 알려지려면 다음 중 하나를 구성해야 합니다.

- 알릴 서브넷은 EIGRP L3Out에서 'Export Route-Control Subnet' 플래그로 정의할 수 있습니다. 개요 섹션에서 설명한 것처럼 이 플래그는 주로 전송 라우팅에 사용되며 해당 L3Out에서 광고해야 하는 서브넷을 정의합니다.
- 0.0.0.0/0을 구성하고 'Aggregate Export(집계 내보내기)' 및 'Export Route Control Subnet(경로 제어 서브넷 내보내기)'을 모두 선택합니다. 이렇게 하면 0.0.0.0/0과 일치하는 외부 프로토콜 및 더 구체적인(any와 일치하는 효과적인) 모든 접두사로 재배포하기 위한 경로 맵이 생성됩니다. 0.0.0.0/0을 'Aggregate Export'와 함께 사용하면 고정 경로가 재배포에 일치하지 않습니다.

이는 알리지 말아야 할 BD 경로를 부주의하게 광고하는 것을 방지하기 위함이다.

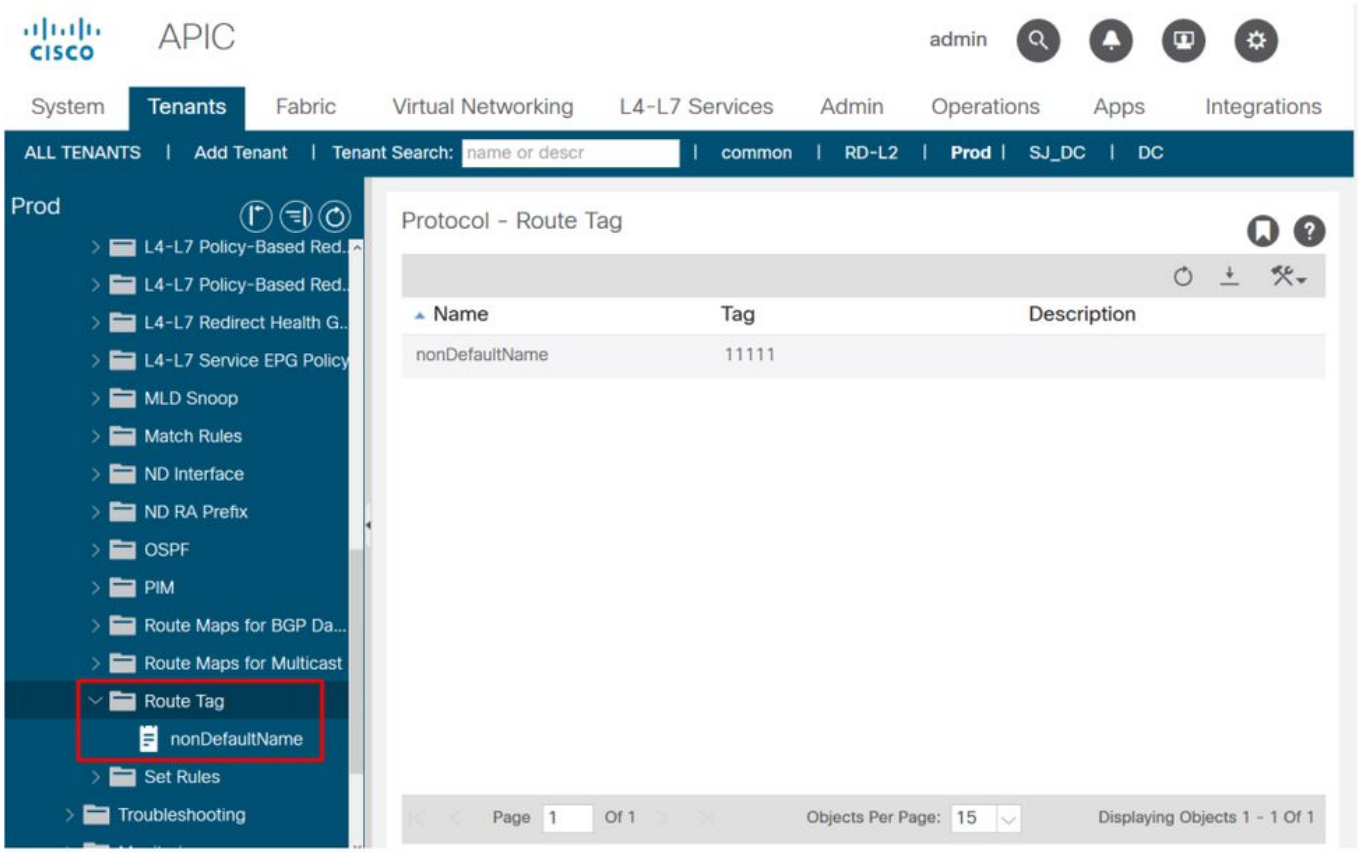
- 마지막으로, 알릴 접두사와 일치하는 내보내기 경로 프로파일을 생성할 수 있습니다. 이 메서드를 사용하면 0.0.0.0/0 이외의 접두사와 함께 'Aggregate' 옵션을 구성할 수 있습니다.

위의 컨피그레이션으로 인해 트랜짓 경로가 광고되지만 데이터플레인 트래픽이 흐르도록 허용하려면 보안 정책이 있어야 합니다. EPG 간 통신과 마찬가지로, 트래픽이 허용되기 전에 계약이 있어야 합니다.

'외부 EPG용 외부 서브넷'이 포함된 중복 외부 서브넷은 동일한 VRF에서 구성할 수 없습니다. 서브넷을 구성할 경우 서브넷은 0.0.0.0보다 구체적이어야 합니다. 경로를 수신하는 L3Out에 대해서만 '외부 EPG용 외부 서브넷'을 구성하는 것이 중요합니다. 이 경로를 광고해야 하는 L3Out에서 구성하지 마십시오.

또한 모든 통과 경로가 특정 VRF 태그로 태그되어 있다는 것을 이해하는 것이 중요합니다. 기본적으로 이 태그는 4294967295. Route-Tag 정책은 'Tenant(테넌트) > Networking(네트워킹) > Protocols(프로토콜) > Route-Tag(경로 태그):

경로 태그 정책



그런 다음 이 경로 태그 정책이 VRF에 적용됩니다. 이 태그의 목적은 기본적으로 루프를 방지하는 것입니다. 이 경로 태그는 전송 경로가 L3Out에서 다시 광고될 때 적용됩니다. 이러한 경로가 동일한 경로 태그로 다시 수신될 경우 경로는 무시됩니다.

OSPF를 통해 수신 BL에 경로가 있는지 확인합니다.

마지막 섹션과 마찬가지로, 먼저 올바른 경로를 처음 수신해야 하는 BL이 있는지 확인합니다.

```
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
```

지금은 광고 L3Out이 다른 BL에 있다고 가정합니다(토폴로지에서와 같이)(이후의 시나리오에서는 동일한 BL의 어디에 있는지 설명합니다).

수신 OSPF BL의 BGP에 경로가 있는지 확인합니다.

OSPF 경로를 외부 EIGRP 라우터로 알리려면 수신 OSPF BL의 BGP로 알려줘야 합니다.

```
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
```

경로가 BGP에 있습니다.

EIGRP BL에서 해당 EIGRP BL이 설치된 경로를 광고할지 확인합니다

```
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
```

라우팅 테이블에 설치되며, 원래 경계 리프 노드를 가리키는 오버레이 다음 홉이 있습니다.

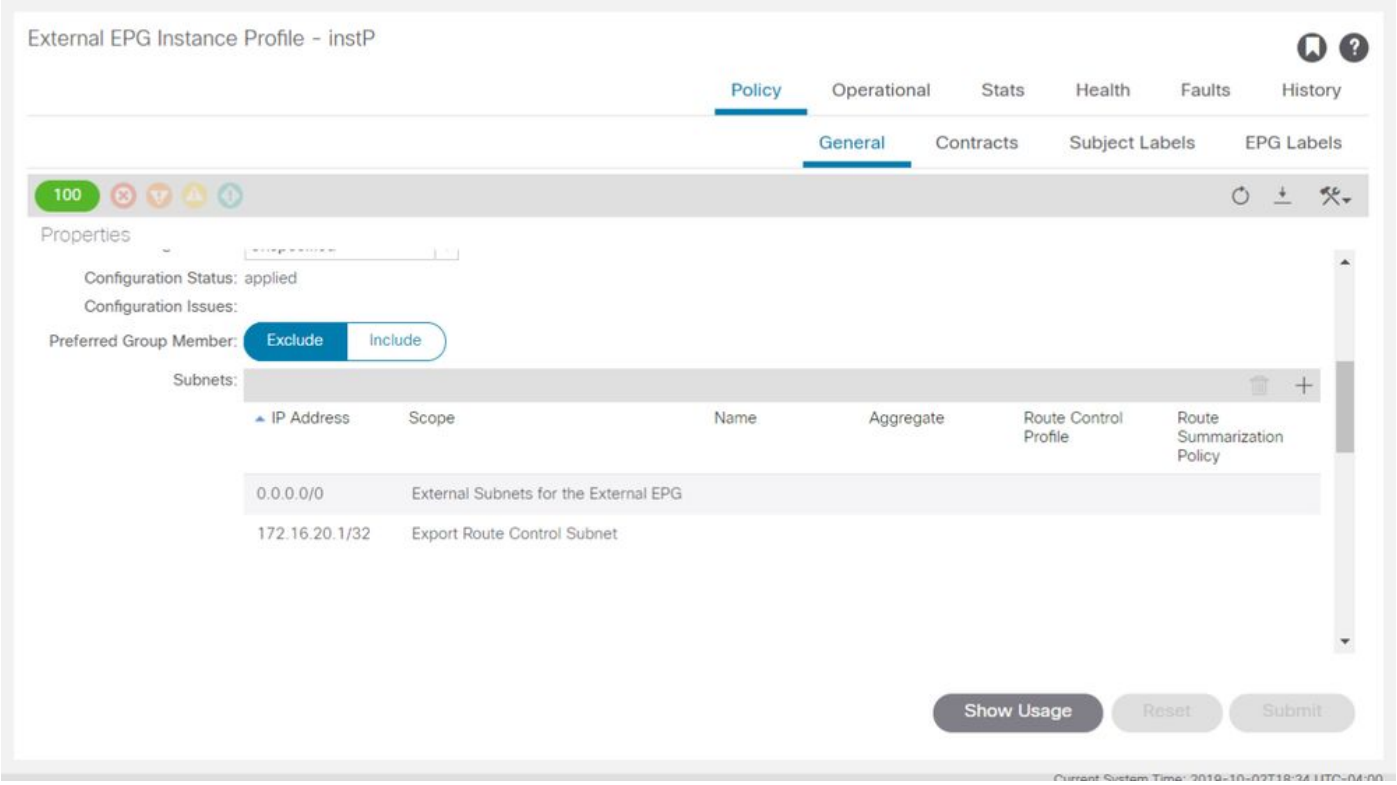
```
leaf102# acidiag fnvread

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

경로가 BL에 광고되는지 확인합니다.

구성된 서브넷에 'Export Route Control Subnet' 플래그가 설정되어 BL 102에서 경로를 알립니다.

경로 제어 내보내기



이 'Export Route Control' 플래그의 결과로 생성된 경로 맵을 보려면 다음 명령을 사용합니다.

```
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
```

'BGP > EIGRP redistribution'을 검색하려면 route-map을 확인합니다. 그러나 경로 맵 자체는 소스 프로토콜이 OSPF, EIGRP 또는 BGP인지에 관계없이 동일해야 합니다. 고정 경로는 다른 경로 맵으로 제어됩니다.

```
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
```

위 출력에서 VRF 태그는 루프 방지를 위해 이 접두사에 설정되고 'Export Route Control'로 구성된 서브넷이 명시적으로 일치됩니다.

BL 수신 및 광고 시 수송 경로

앞에서 설명한 것처럼 수신 BL과 알림 BL이 다른 경우 BGP를 사용하여 패브릭을 통해 경로를 광고해야 합니다. BL들이 동일할 때, 재분배 또는 광고는 리프 상의 프로토콜들 사이에서 직접적으로 수행될 수 있다.

다음은 이 구현 방법에 대한 간략한 설명입니다.

- **동일한 리프에 있는 두 OSPF L3Out 간의 전송 라우팅: 경로 알림**은 OSPF 프로세스 레벨에 적용되는 '영역 필터'를 통해 제어됩니다. 경로가 재배포가 아닌 영역 간에 광고되므로 영역 0의 L3Out은 leaf에 배포해야 합니다. 필터 목록을 보려면 'show ip ospf vrf <name>'을 사용하십시오. 'show route-map <filter name>'을 사용하여 필터의 내용을 표시합니다.
- **동일한 리프에 있는 OSPF와 EIGRP L3Outs 간의 트랜짓 라우팅: 경로 광고**는 'show ip ospf' 및 'show ip eigrp'로 표시될 수 있는 재배포 경로 맵을 통해 제어됩니다. 동일한 BL에 여러 OSPF L3Outs가 있는 경우 이러한 OSPF L3Outs 중 하나에만 재배포할 수 있는 유일한 방법은 다른 OSPF L3Outs가 스텁 또는 NSSA인 경우 외부 LSA를 허용하지 않도록 '재배포된 LSA를 NSSA 영역**으로 보내기'가 비활성화된 경우입니다**.
- **동일한 리프의 OSPF 또는 EIGRP와 BGP 간 전송 라우팅:** IGP로의 경로 알림은 재배포 경로 맵을 통해 제어됩니다. BGP로의 경로 알림은 경로를 전송해야 하는 bgp 인접 디바이스에 직접 적용되는 아웃바운드 경로 맵을 통해 제어됩니다. 이는 'show bgp ipv4 unicast neighbor <neighbor address> vrf <name>으로 확인할 수 있습니다. | grep Outbound'.

- **동일한 리프에 있는 두 BGP l3Out 간의 전송 라우팅:** 모든 알림은 경로를 전송해야 하는 bgp 인접 디바이스에 직접 적용되는 경로 맵을 통해 제어됩니다. 이는 'show bgp ipv4 unicast neighbor <neighbor address> vrf <name>으로 확인할 수 있습니다. | grep Outbound'.

전송 라우팅 문제 해결 시나리오 #1: 전송 경로가 알려지지 않음

이 트러블슈팅 시나리오에서는 한 L3Out을 통해 학습해야 하는 경로가 다른 L3Out으로 전송되지 않도록 합니다.

항상 그렇듯이 ACI와 관련된 사항을 검토하기 전에 기본을 점검하십시오.

- 프로토콜 인접성이 향상되었습니까?
- ACI가 광고해야 하는 경로가 처음부터 외부 프로토콜에서 학습되었습니까?
- BGP의 경우 일부 BGP 특성으로 인해 경로가 삭제됩니까? (as-path 등).
- 수신 L3Out이 OSPF 데이터베이스, EIGRP 토폴로지 테이블 또는 BGP 테이블에 있습니까?
- BGP 경로 리플렉터 정책이 포드 프로필에 적용되는 포드 정책 그룹에 적용됩니까?

모든 기본 프로토콜 확인이 올바르게 구성된 경우, 아래는 트랜짓 경로가 알려지지 않은 다른 일반적인 원인입니다.

가능한 원인: OSPF 영역 없음 0

영향을 받는 토폴로지가 동일한 경계 리프에 있는 두 개의 OSP L3Out과 관련된 경우, 한 영역에서 다른 영역으로 경로를 알릴 수 있는 영역 0이 있어야 합니다. 자세한 내용은 위의 "동일한 리프에 있는 두 OSPF L3Out 간의 전송 라우팅" 글머리 기호를 참조하십시오.

가능한 원인: OSPF 영역이 스텁 또는 NSSA임

이는 OSPF L3Out이 외부 LSA를 광고하도록 구성되지 않은 스텁 또는 NSSA 영역으로 구성된 경우에 표시됩니다. OSPF에서는 외부 LSA가 스텁 영역에 광고되지 않습니다. 'Send Redistributed LSAs into NSSA Area(NSSA 영역으로 재배포된 LSA 보내기)'를 선택한 경우 NSSA 영역으로 광고됩니다.

전송 라우팅 문제 해결 시나리오 #2: 전송 경로를 받지 못했습니다.

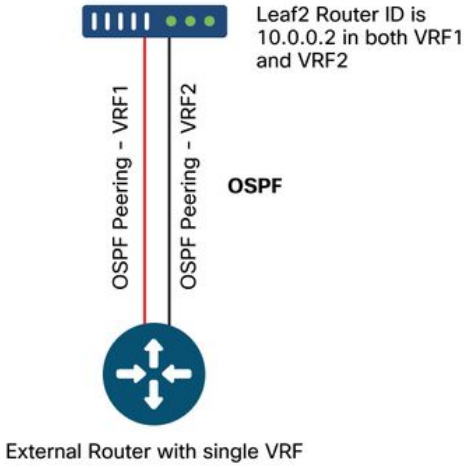
이 시나리오에서 문제는 ACI L3Out에 의해 광고된 일부 경로가 다른 L3Out에서 다시 수신되지 않는다는 것입니다. 이 시나리오는 L3Out이 두 개의 개별 패브릭에 있고 외부 라우터로 연결된 경우 또는 L3Out이 서로 다른 VRF에 있고 경로가 외부 라우터에 의해 VRF 간에 전달되는 경우에 적용할 수 있습니다.

가능한 원인: BL이 여러 VRF에서 동일한 라우터 ID로 구성됨

컨피그레이션 관점에서 라우터 ID는 동일한 VRF 내에서 중복될 수 없습니다. 그러나 두 VRF가 동일한 라우팅 프로토콜 도메인에 연결되어 있지 않으면 일반적으로 서로 다른 VRF에서 동일한 라우터 ID를 사용하는 것이 좋습니다.

다음 토폴로지를 고려하십시오.

단일 VRF를 사용하는 외부 라우터 — 전송 경로를 수신하지 못했습니다.



여기서 문제는 ACI leaf에서 자체 라우터 ID가 수신되는 LSA를 확인하여 OSPF 데이터베이스에 설치되지 않는다는 것입니다.

또한 VPC 쌍에서 동일한 설정이 확인될 경우 일부 라우터에서 LSA가 계속 추가 및 삭제됩니다. 예를 들어 라우터는 VPC 피어에서 LSA가 VRF로 들어오고 LSA가 다른 VRF에서 시작된 동일한 노드(라우터 ID가 동일)에서 오는 것을 볼 수 있습니다.

이 문제를 해결하려면 사용자가 L3Out이 있는 각 VRF 내에서 다른 고유한 라우터 ID를 가져야 합니다.

가능한 원인: 동일한 VRF 태그가 있는 다른 패브릭에서 수신된 하나의 ACI 패브릭의 L3Out에서 경로

ACI의 기본 route-tag는 변경하지 않는 한 항상 동일합니다. 기본 VRF 태그를 변경하지 않고 한 VRF 또는 ACI 패브릭의 한 L3Out에서 다른 VRF 또는 ACI 패브릭의 다른 L3Out으로 경로를 광고하면 수신 BL에 의해 경로가 삭제됩니다.

이 시나리오의 해결책은 ACI의 각 VRF에 대해 고유한 Route-Tag 정책을 사용하는 것입니다.

트랜짓 라우팅 문제 해결 시나리오 #3 - 예기치 않게 트랜짓 경로 알림

이 시나리오는 통과 경로가 L3Out에 알려지면 알려질 의도가 없는 경우에 나타납니다.

가능한 원인: 'Aggregate Export'를 사용하는 0.0.0.0/0 사용

외부 서브넷이 0.0.0.0/0으로 구성되면 'Export Route Control Subnet'(경로 제어 서브넷 내보내기) 및 'Aggregate Export'(집계 내보내기)를 통해 match all redistribution route-map이 설치됩니다. 이 경우 OSPF, EIGRP 또는 BGP를 통해 학습된 BL의 모든 경로는 이(가) 구성된 L3Out으로 광고됩니다.

다음은 집계 내보내기의 결과로 leaf에 배포되는 경로 맵입니다.

```
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
```

이는 ACI 환경과 관련된 라우팅 루프의 가장 큰 원인입니다.

계약 및 L3Out

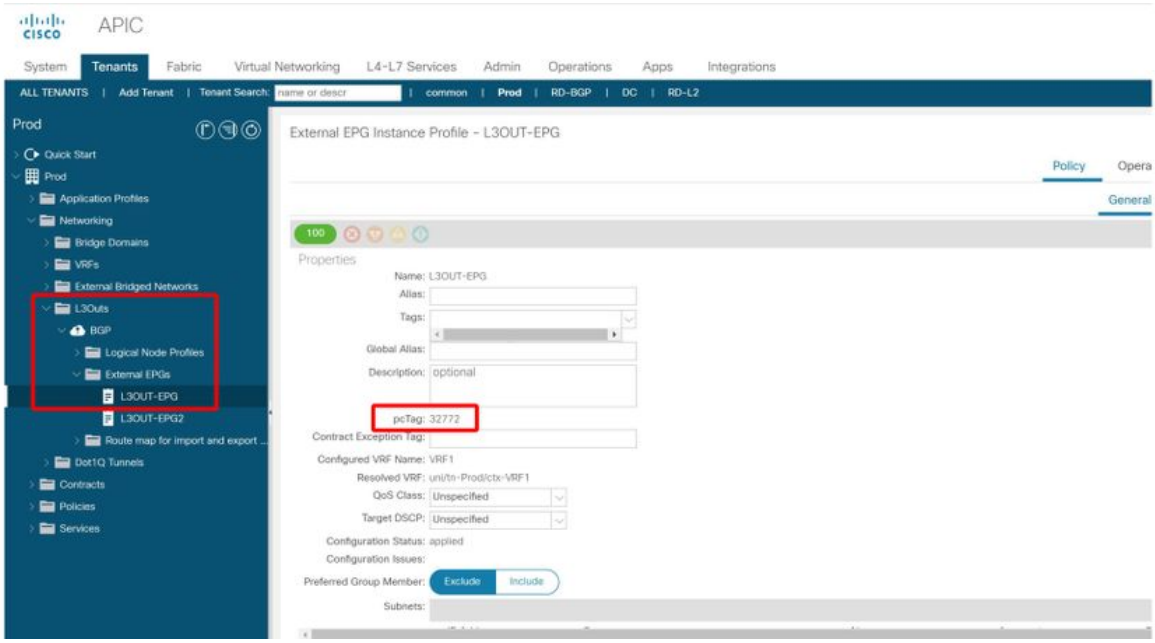
L3Out의 접두사 기반 EPG

내부 EPG(non-L3Out)에서는 소스의 pcTag와 대상 EPG의 pcTag를 파생한 후에 계약이 적용됩니다. 다운링크 포트에서 수신된 패킷의 캡슐화 VLAN/VXLAN은 패킷을 EPG에 분류하여 이 pcTag를 구동하는 데 사용됩니다. MAC 주소 또는 IP 주소를 학습할 때마다 액세스 캡슐화 및 관련 EPG pcTag와 함께 학습됩니다. pcTag 및 계약 시행에 대한 자세한 내용은 "보안 정책" 장을 참조하십시오.

또한 L3Outs는 'Tenant(테넌트) > Networking(네트워킹) > L3OUT > Networks(네트워크) > L3OUT-EPG' 아래에 있는 L3Out EPG(외부 EPG)를 사용하여 pcTag를 구동합니다. 그러나 L3Outs는 VLAN 및 인터페이스를 사용하여 패킷을 분류하지 않습니다. 분류는 'Longest Prefix Match' 방식으로 소스 접두사/서브넷을 기반으로 합니다. 따라서, L3Out EPG는 **프리픽스 기반 EPG**로 지칭될 수 있다. 패킷은 서브넷을 기준으로 L3Out으로 분류된 후 일반 EPG와 유사한 정책 적용 패턴을 따릅니다.

다음 다이어그램은 GUI에서 지정된 L3Out EPG의 pcTag를 찾을 수 있는 위치를 보여줍니다.

L3Out의 pcTag 위치



사용자는 접두사 기반 EPG 테이블을 정의합니다. 이는 '외부 EPG용 외부 서브넷' 서브넷 범위를 사용하여 수행됩니다. 해당 범위의 각 서브넷 집합은 고정 LPM(Longest Prefix Match) 테이블에 항목을 추가합니다. 이 서브넷은 해당 접두사에 속하는 IP 주소에 사용할 pcTag 값을 가리킵니다.

다음 명령을 사용하여 리프 스위치에서 접두사 기반 EPG 서브넷의 LPM 테이블을 확인할 수 있습니다.

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

설명:

- LPM 테이블 항목은 VRF VNID로 범위가 지정됩니다. 조회는 vrf_vnid/src pcTag/dst pcTag에 따라 수행됩니다.
- 각 항목은 단일 pcTag를 가리킵니다. 따라서 두 L3Out EPG는 동일한 VRF 내에서 동일한 마스크 길이를 갖는 동일한 서브넷을 사용할 수 없습니다.
- 서브넷 0.0.0.0/0은 항상 특수 pcTag 15를 사용합니다. 따라서 중복될 수 있지만 정책 시행의 영향을 완전히 이해하고 있어야만 합니다.
- 이 테이블은 양방향으로 쓰인다. L3Out에서 Leaf 로컬 엔드포인트까지 소스 pcTag가 이 테이블을 사용하여 파생됩니다.Leaf 로컬 엔드포인트에서 L3Out까지 대상 pcTag는 이 테이블을 사용하여 파생됩니다.
- VRF에 'Policy Control Enforcement Direction'에 대한 'Ingress' 시행 설정이 있는 경우, LPM 접두사 테이블이 L3Out BLs 및 L3Out과 계약한 VRF의 리프 스위치에 표시됩니다.

예 1: 특정 접두사가 있는 단일 L3Out

시나리오: 하나의 L3Out EPG가 포함된 VRF Prod:VRF1의 단일 BGP L3Out. 접두사 172.16.1.0/24은 외부 소스에서 수신되므로 L3Out EPG로 분류해야 합니다.

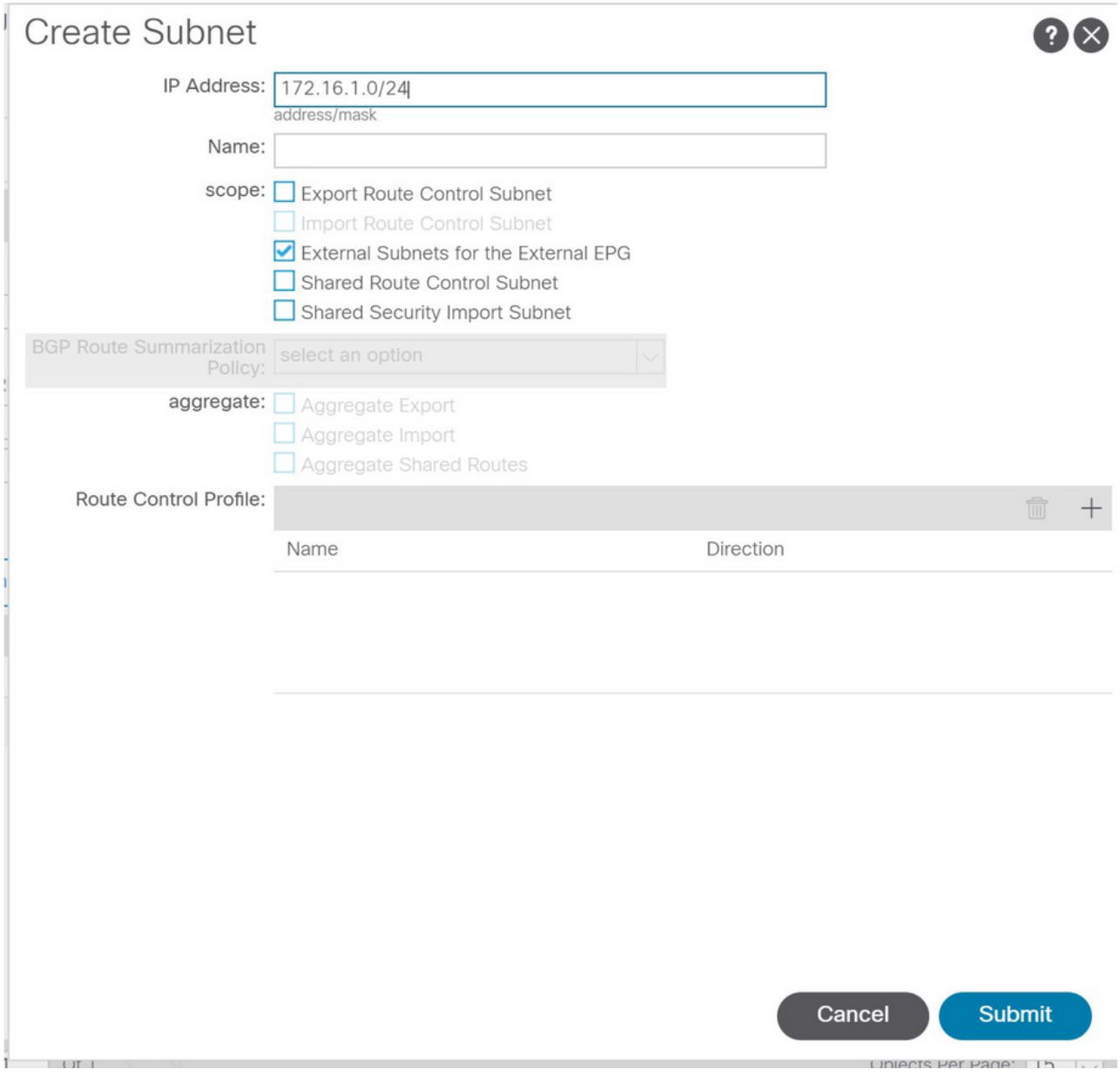
```
bdsol-aci32-leaf3# show ip route 172.16.1.0  vrf Prod:VRF1
```

```
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
```

먼저 접두사 테이블에 서브넷을 추가합니다.

'외부 EPG에 대한 외부 서브넷' 범위가 있는 서브넷



L3Out의 VRF가 있는 리프 스위치에서 접두사 목록의 프로그래밍을 확인합니다.

```
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
```

L3Out EPG의 pcTag는 vrf 범위 32772에 2097154.

예 2: 여러 접두사가 포함된 단일 L3Out

이전 예를 확장하면 이 시나리오에서 L3Out이 여러 접두사를 수신합니다. 각 접두사를 입력하는 것이 기능적으로는 사운드이지만, 다른 옵션(의도한 설계에 따라)은 L3Out에서 수신된 모든 접두사를 허용하는 것입니다.

이는 '0.0.0.0/0' 접두사로 수행할 수 있습니다.

Subnet - 0.0.0.0/0

Policy | Faults | History

Properties

IP Address: 0.0.0.0/0
address/mask

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

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

BGP Route Summarization Policy: select an option

Route Control Profile:

Name	Direction

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

그러면 다음 policy-mgr 접두사 테이블 항목이 생성됩니다.

```
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
```

> 0.0.0.0/0에 할당된 pcTag는 32772이 아닌 값 15를 사용합니다. pcTag 15는 L3Out에서 모든 접두사를 일치시키는 와일드카드 역할을 하는 0.0.0.0/0에서만 사용되는 예약된 시스템 pcTag입니다.

VRF에 0.0.0.0/0을 사용하는 단일 L3Out EPG가 포함된 단일 L3Out이 있는 경우 policy-prefix는 고유한 상태를 유지하며 모두 catch하는 가장 쉬운 방법입니다.

예 3a: VRF에 있는 여러 L3Out EPG

이 시나리오에서는 동일한 VRF에 여러 L3Out EPG가 있습니다.

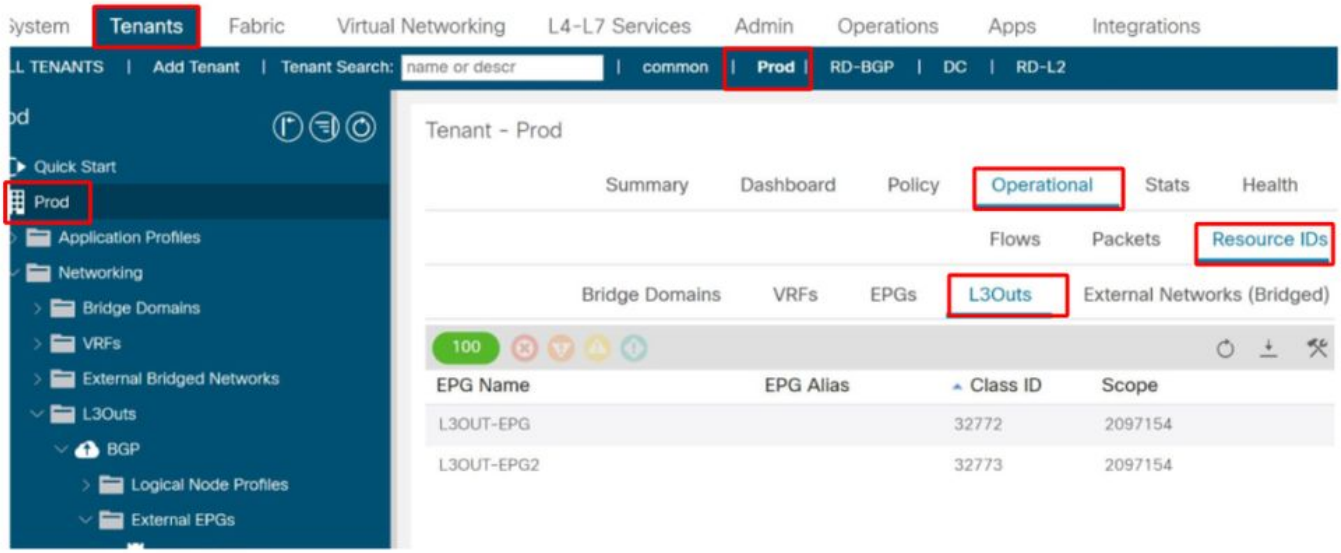
참고: 접두사 기반 EPG 관점에서 다음 두 컨피그레이션은 동일한 LPM policy-mgr 접두사 테이블 엔트리를 생성합니다.

1. L3Out EPG가 각각 1개씩 포함된 L3Out 2개.
2. L3Out EPG 2개가 포함된 L3Out 1개

두 시나리오 모두에서 L3Out EPG의 총 수는 2입니다. 즉, 각 EPG에는 고유한 pcTag 및 연결된 서브넷이 있습니다.

지정된 L3Out EPG의 모든 pcTag는 GUI의 'Tenant(테넌트) > Operational(운영) > Resource ID(리소스 ID) > L3Outs(L3Outs)'에서 볼 수 있습니다.

L3Out pcTag 확인



이 시나리오에서 ACI 패브릭은 외부 라우터에서 여러 접두사를 받으며 L3Out EPG 정의는 다음과 같습니다.

- L3OUT-EPG에 할당된 172.16.1.0/24입니다.
- L3OUT-EPG2에 할당된 172.16.2.0/24입니다.
- 172.16.0.0/16은 L3OUT-EPG에 할당되었습니다(172.16.3.0/24 접두사를 catch하기 위해).

이를 확인하기 위해 다음과 같이 컨피그레이션을 정의합니다.

- L3OUT-EPG에는 '외부 EPG용 외부 서브넷' 범위가 포함된 서브넷 172.16.1.0/24 및 172.16.0.0/16이 있습니다.
- L3OUT-EPG2에는 '외부 EPG의 외부 서브넷' 범위가 포함된 서브넷 172.16.2.0/24이 있습니다.

결과 접두사 테이블 항목은 다음과 같습니다.

```
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
```

172.16.2.0/24은 pcTag 32773(L3OUT-EPG2)에 할당되고 172.16.0.0/16은 32772(L3OUT-EPG)에 할당됩니다.

이 시나리오에서는 /16 수퍼넷이 동일한 EPG에 할당되므로 172.16.1.0/24에 대한 항목이 중복됩니다.

여러 L3Out EPG는 단일 L3Out 내의 접두사 그룹에 서로 다른 계약을 적용하는 것이 목표일 때 유용합니다. 다음 예에서는 여러 L3Out EPG에서 계약이 어떻게 재생되는지 보여줍니다.

예 3b: 계약이 서로 다른 여러 L3Out EPG

이 시나리오에는 다음 설정이 포함됩니다.

- ICMP만 허용하는 ICMP 계약입니다.
- tcp 대상 포트 80만 허용하는 HTTP 계약입니다.
- EPG1(pcTag 32770)은 L3OUT-EPG(pcTag 32772)에서 사용하는 HTTP 계약을 제공합니다.
- EPG2(pcTag 32771)는 L3OUT-EPG2(pcTag 32773)에서 사용하는 ICMP 계약을 제공합니다.

이전 예제의 동일한 policymgr 접두사가 사용됩니다.

- L3OUT-EPG의 172.16.1.0/24은 HTTP를 EPG1에 허용해야 함
- L3OUT-EPG2의 172.16.2.0/24은 EPG2에 대한 ICMP를 허용해야 합니다.

policy-mgr 접두사 및 영역 지정 규칙:

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

Triage를 사용한 데이터 경로 검증 — 정책에서 허용하는 흐름

외부 네트워크의 172.16.2.1과 EPG2의 192.168.3.1 사이의 ICMP 흐름을 통해 추적을 사용하여 흐름을 파악하고 분석할 수 있습니다. 이 경우 트래픽이 다음 중 하나로 들어갈 수 있으므로 리프 스위치 103 및 104 둘 다에서 Triage를 시작합니다.

```
admin@apic1:~> ftriage route -ii LEAF:103,104 -sip 172.16.2.1 -dip 192.168.3.1
fTriage Status: {"dbgFtriage": {"attributes": {"operState": "InProgress", "pid": "14454",
"apicId": "1", "id": "0"}}}
Starting ftriage
Log file name for the current run is: ftlog_2019-10-02-22-30-41-871.txt
2019-10-02 22:30:41,874 INFO     /controller/bin/ftriage route -ii LEAF:103,104 -sip 172.16.2.1
-dip 192.168.3.1
2019-10-02 22:31:28,868 INFO     ftriage:     main:1165 Invoking ftriage with default password
and default username: apic#fallback\\admin
2019-10-02 22:32:15,076 INFO     ftriage:     main:839  L3 packet Seen on bdsol-aci32-leaf3
Ingress: Eth1/12 (Po1) Egress: Eth1/12 (Po1) Vnid: 11365
2019-10-02 22:32:15,295 INFO     ftriage:     main:242  ingress encap string vlan-2551
```

```
2019-10-02 22:32:17,839 INFO     ftriage:     main:271  Building ingress BD(s), Ctx
2019-10-02 22:32:20,583 INFO     ftriage:     main:294  Ingress BD(s) Prod:VRF1:l3out-BGP:vlan-
2551
2019-10-02 22:32:20,584 INFO     ftriage:     main:301  Ingress Ctx: Prod:VRF1
2019-10-02 22:32:20,693 INFO     ftriage:   pktrec:490  bdsol-aci32-leaf3: Collecting transient
losses snapshot for LC module: 1
2019-10-02 22:32:38,933 INFO     ftriage:     nxos:1404 bdsol-aci32-leaf3: nxos matching rule
id:4343 scope:34 filter:5
2019-10-02 22:32:39,931 INFO     ftriage:     main:522  Computed egress encap string vlan-2502
2019-10-02 22:32:39,933 INFO     ftriage:     main:313  Building egress BD(s), Ctx
2019-10-02 22:32:41,796 INFO     ftriage:     main:331  Egress Ctx Prod:VRF1
2019-10-02 22:32:41,796 INFO     ftriage:     main:332  Egress BD(s): Prod:BD2
2019-10-02 22:32:48,636 INFO     ftriage:     main:933  SIP 172.16.2.1 DIP 192.168.3.1
2019-10-02 22:32:48,637 INFO     ftriage:  unicast:973  bdsol-aci32-leaf3: <- is ingress node
2019-10-02 22:32:51,257 INFO     ftriage:  unicast:1202 bdsol-aci32-leaf3: Dst EP is local
2019-10-02 22:32:54,129 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: EP if(Po1) same as
egr if(Po1)
2019-10-02 22:32:55,348 INFO     ftriage:     misc:657  bdsol-aci32-leaf3:
DMAC(00:22:BD:F8:19:FF) same as RMAC(00:22:BD:F8:19:FF)
2019-10-02 22:32:55,349 INFO     ftriage:     misc:659  bdsol-aci32-leaf3: L3 packet getting
routed/bounced in SUG
2019-10-02 22:32:55,596 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: Dst IP is present in
SUG L3 tbl
2019-10-02 22:32:55,896 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: RW seg_id:11365 in
SUG same as EP segid:11365
2019-10-02 22:33:02,150 INFO     ftriage:     main:961  Packet is Exiting fabric with peer-
device: bdsol-aci32-n3k-3 and peer-port: Ethernet1/16
```

Triage는 L3OUT_EPG2에서 EPG로의 ICMP 규칙에 대한 zoning-rule hit을 확인합니다.

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

Triage를 사용한 데이터 경로 검증 — 정책에서 허용되지 않는 흐름

172.16.1.1(L3OUT-EPG)에서 192.168.3.1(EPG2)로 전달되는 ICMP 트래픽의 경우 정책 삭제를 예상합니다.

```
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"}}}
```

분류는 SECURITY_GROUP_DENY(정책 삭제) 이유로 패킷이 삭제되고 파생된 소스 pcTag가 32772 대상 pcTag가 32771 있는지 확인합니다. 영역 지정 규칙에 대해 이 항목을 검사하면 해당 EPG 사이에 항목이 분명히 없습니다.

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

예 4: 여러 L3Out과 여러 접두사

시나리오는 예 3과 유사하게 설정되지만(L3Out 및 L3Out EPG 정의), 두 L3Out EPG에 모두 정의된 네트워크는 0.0.0.0/0입니다.

계약 컨피그레이션은 다음과 같습니다.

- ICMP1을 허용하는 ICMP1 계약입니다.
- ICMP를 허용하는 ICMP2 계약입니다.
- EPG1(pcTag 32770)은 L3OUT-EPG(pcTag 32772)에서 사용하는 ICMP1 계약을 제공합니다.
- EPG2(pcTag 32771)는 L3OUT-EPG2(pcTag 32773)에서 사용하는 ICMP2 계약을 제공합니다.

이 컨피그레이션은 외부 네트워크에서 여러 접두사를 광고하는 경우 이상적으로 보일 수 있지만, 서로 다른 허용 흐름 패턴을 따르는 접두사의 청크가 2개 이상 있습니다. 이 예에서 접두사 하나는 ICMP1만 허용하고 다른 하나는 ICMP2만 허용해야 합니다.

동일한 VRF에서 '0.0.0.0/0'을 두 번 사용하더라도 policy-mgr 접두사 테이블에 하나의 접두사만 프로그래밍됩니다.

```
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
```

아래에서 2개의 플로우를 재검토했습니다. 위의 계약 컨피그레이션에 따라 다음 사항이 예상됩니다.

1. 172.16.2.1(L3OUT-EPG2)에서 192.168.3.1(EPG2)로의 연결은 ICMP2에서 허용해야 **합니다.**
2. EPG1과 L3OUT-EPG2 사이에 contract가 없으므로 172.16.2.1(L3OUT-EPG2)에서 192.168.1.1(EPG1)로의 연결은 허용되지 **않아야** 합니다

Triage를 사용한 데이터 경로 검증 — 정책에서 허용하는 흐름

172.16.2.1(L3OUT-EPG2)에서 192.168.3.1(EPG2 — pcTag 32771)로의 ICMP 플로우로 Triage를 실행합니다.

```
Starting ftriage
Log file name for the current run is: ftlog_2019-10-02-23-11-14-298.txt
2019-10-02 23:11:14,302 INFO     /controller/bin/ftriage route -ii LEAF:103,104 -sip 172.16.2.1
```

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

이 흐름은 zoning-rule 4336에 의해 (예상대로) 허용됩니다.

Triage를 사용한 데이터 경로 검증 — 정책에서 허용되지 않는 흐름

172.16.2.1(L3OUT-EPG2)에서 192.168.1.1(EPG1 — pcTag 32770)로의 ICMP 플로우로 Triage를 실행합니다.

```
admin@apic1:~> ftriage route -ii LEAF:103,104 -sip 172.16.2.1 -dip 192.168.1.1
fTriage Status: {"dbgFtriage": {"attributes": {"operState": "InProgress", "pid": "31500",
"apicId": "1", "id": "0"}}}
Starting ftriage
Log file name for the current run is: ftlog_2019-10-02-23-53-03-478.txt
2019-10-02 23:53:03,482 INFO     /controller/bin/ftriage route -ii LEAF:103,104 -sip 172.16.2.1
-dip 192.168.1.1
2019-10-02 23:53:50,014 INFO     ftriage:     main:1165 Invoking ftriage with default password
and default username: apic#fallback\\admin
2019-10-02 23:54:39,199 INFO     ftriage:     main:839  L3 packet Seen on bdsol-aci32-leaf3
Ingress: Eth1/12 (Po1) Egress: Eth1/12 (Po1) Vnid: 11364
2019-10-02 23:54:39,417 INFO     ftriage:     main:242  ingress encap string vlan-2551
2019-10-02 23:54:41,962 INFO     ftriage:     main:271  Building ingress BD(s), Ctx
2019-10-02 23:54:44,765 INFO     ftriage:     main:294  Ingress BD(s) Prod:VRF1:l3out-BGP:vlan-
2551
2019-10-02 23:54:44,766 INFO     ftriage:     main:301  Ingress Ctx: Prod:VRF1
2019-10-02 23:54:44,875 INFO     ftriage:   pktrec:490  bdsol-aci32-leaf3: Collecting transient
losses snapshot for LC module: 1
2019-10-02 23:55:02,905 INFO     ftriage:     nxos:1404 bdsol-aci32-leaf3: nxos matching rule
```

```
id:4341 scope:34 filter:5
2019-10-02 23:55:04,525 INFO     ftriage:     main:522  Computed egress encap string vlan-2501
2019-10-02 23:55:04,526 INFO     ftriage:     main:313  Building egress BD(s), Ctx
2019-10-02 23:55:06,390 INFO     ftriage:     main:331  Egress Ctx Prod:VRF1
2019-10-02 23:55:06,390 INFO     ftriage:     main:332  Egress BD(s): Prod:BD1
2019-10-02 23:55:13,571 INFO     ftriage:     main:933  SIP 172.16.2.1 DIP 192.168.1.1
2019-10-02 23:55:13,572 INFO     ftriage:  unicast:973  bdsol-aci32-leaf3: <- is ingress node
2019-10-02 23:55:16,159 INFO     ftriage:  unicast:1202 bdsol-aci32-leaf3: Dst EP is local
2019-10-02 23:55:18,949 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: EP if(Po1) same as
egr if(Po1)
2019-10-02 23:55:20,126 INFO     ftriage:     misc:657  bdsol-aci32-leaf3:
DMAC(00:22:BD:F8:19:FF) same as RMAC(00:22:BD:F8:19:FF)
2019-10-02 23:55:20,126 INFO     ftriage:     misc:659  bdsol-aci32-leaf3: L3 packet getting
routed/bounced in SUG
2019-10-02 23:55:20,395 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: Dst IP is present in
SUG L3 tbl
2019-10-02 23:55:20,687 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: RW seg_id:11364 in
SUG same as EP segid:11364
2019-10-02 23:55:26,982 INFO     ftriage:     main:961  Packet is Exiting fabric with peer-
device: bdsol-aci32-n3k-3 and peer-port: Ethernet1/16
```

이 흐름은 zoning-rule 4341에 의해 허용됨(예기치 않음). 이제 zoning-rule을 분석하여 그 이유를 파악해야 합니다.

데이터 경로 검증 — zoning-rules

최근 2번의 테스트에 해당하는 zoning-rule은 다음과 같습니다.

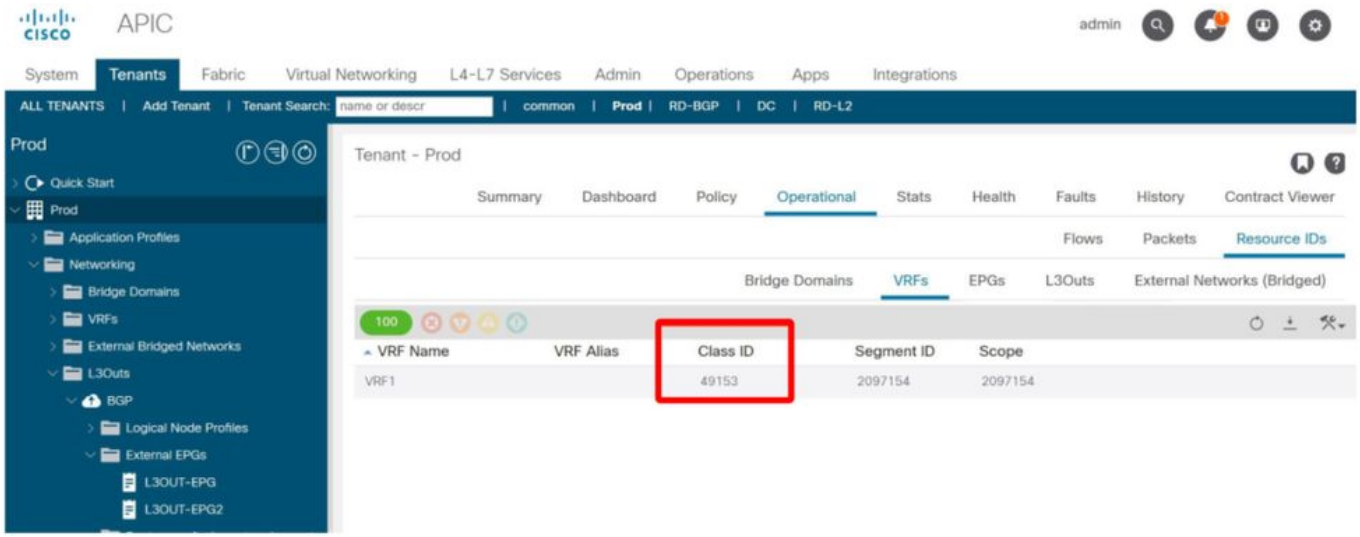
- Expected — 플로우가 zoning-rule line 4336(ICMP2 계약)에 도달합니다.
- 예기치 않은 흐름 발생 - zoning-rule line 4341(ICMP1 계약).

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

두 흐름 모두 VRF의 src pcTag를 49153. 이는 VRF의 pcTag입니다. 이는 UI에서 확인할 수 있습니

다.

VRF의 pcTag 확인



다음은 0.0.0.0/0 접두사가 L3Out과 함께 사용될 때 발생합니다.

- 내부 EPG에서 0.0.0.0/0의 L3Out EPG로의 트래픽은 목적지 pcTag 15를 파생합니다.
- 0.0.0.0/0의 L3Out EPG에서 ACI 내부 EPG로의 트래픽은 VRF의 소스 pcTag를 49153.

contract_parser 스크립트는 zoning-rule에 대한 종합적인 보기를 제공합니다.

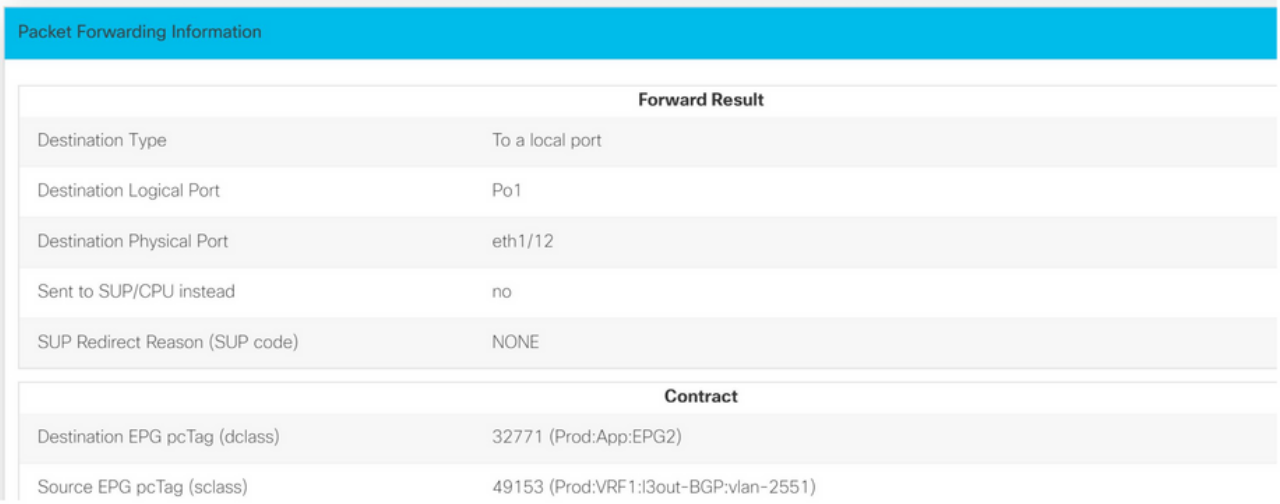
```
bdsol-aci32-leaf3# contract_parser.py --vrf Prod:VRF1
Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4]
[flags][contract:{str}] [hit=count]
[7:4339] [vrf:Prod:VRF1] permit ip icmp tn-Prod/ap-App/epg-EPG1(32770) pfx-0.0.0.0/0(15)
[contract:uni/tn-Prod/brc-ICMP2] [hit=0]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

ELAM Assistant 앱을 사용하여 패킷에서 사용하는 pcTag 확인

ELAM Assistant App은 라이브 트래픽 흐름의 소스 및 목적지 pcTag를 확인하는 또 다른 방법을 제공합니다.

아래 스크린샷은 pcTag 서버에서 pcTag 서버로의 트래픽에 대한 32771 결과를 49153.

ELAM Assistant 앱 출력 - 소스 32771 - dst 49153



Packet Forwarding Information

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

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

결론

서브넷을 사용하는 모든 L3Out이 서브넷을 사용하는 다른 모든 L3Out에 적용되는 계약을 상속하므로 0.0.0.0/0의 사용은 VRF 내에서 신중하게 추적해야 합니다. 계획되지 않은 허용 흐름으로 이어질 수 있습니다.

공유 L3Out

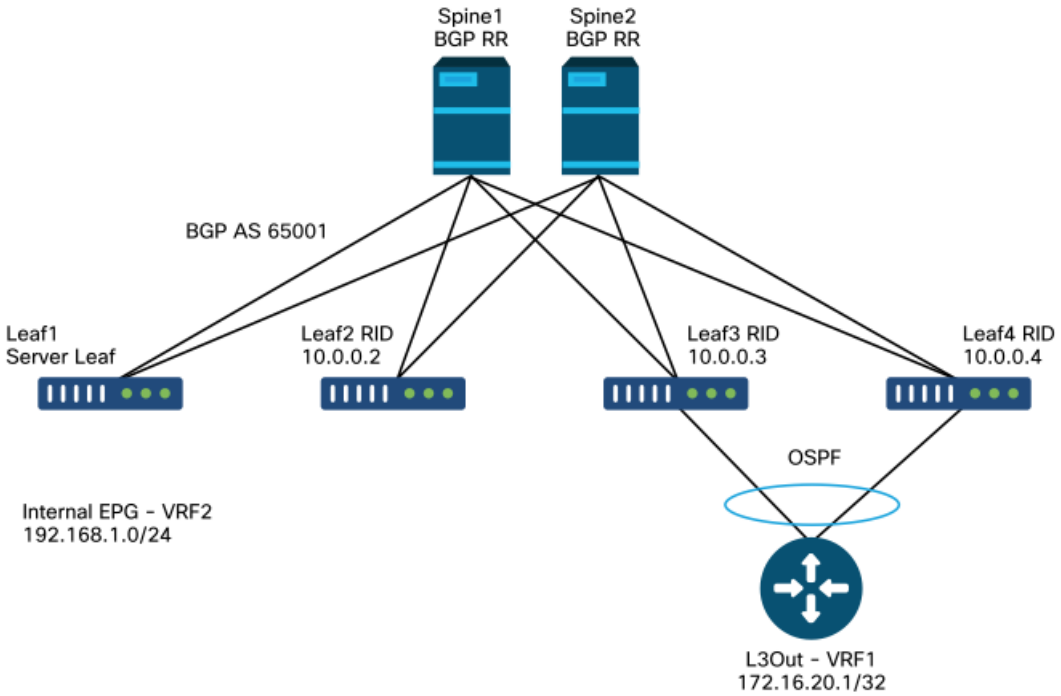
개요

이 섹션에서는 공유 L3Out 컨피그레이션에서 경로 광고 문제를 해결하는 방법에 대해 설명합니다. '공유 L3Out'은 L3Out이 하나의 VRF에 있지만 L3Out과 계약을 체결한 내부 EPG가 다른 VRF에 있는 시나리오를 의미합니다. 공유 L3Out을 사용하면 ACI 패브릭에 대한 내부 경로 유출이 수행됩니다.

이 섹션에서는 보안 정책 트러블슈팅에 대해 자세히 설명하지 않습니다. 자세한 내용은 이 책의 "보안 정책" 장을 참조하십시오. 이 섹션에서는 보안을 위해 외부 정책 접두사 분류에 대해서도 자세히 설명하지 않습니다. "외부 전달" 장의 "계약 및 L3Out" 섹션을 참조하십시오.

이 섹션에서는 예를 위해 다음 토폴로지를 사용합니다.

공유 L3Out 토폴로지



상위 레벨에서 공유 L3Out이 작동하려면 다음 컨피그레이션이 있어야 합니다.

- 외부 경로를 내부 VRF로 유출하려면 L3Out 서브넷을 '공유 경로 제어 서브넷' 범위로 구성해야 합니다. 구성된 서브넷보다 더 구체적인 모든 경로를 유출하도록 'Aggregate Shared' 옵션도 선택할 수 있습니다.
- 이 L3Out을 통한 통신을 허용하는 데 필요한 보안 정책을 프로그래밍하려면 L3Out 서브넷을 '공유 보안 가져오기 서브넷' 범위로 구성해야 합니다.
- 외부 VRF에서 BD 서브넷을 프로그래밍하고 이를 광고하려면 내부 BD 서브넷을 'VRF 간 공유'와 '외부 광고'로 설정해야 합니다.
- 공유 L3Out의 내부 EPG와 외부 EPG 간에 '테넌트' 또는 '전역' 범위 계약을 구성해야 합니다.

다음 섹션에서는 유출된 경로가 ACI에서 어떻게 광고되고 학습되는지에 대해 자세히 설명합니다.

공유 L3Out 워크플로 - 외부 경로 학습

이 섹션에서는 패브릭에 광고되는 학습된 외부 경로의 경로를 간략하게 설명합니다.

경계 리프에 표시된 외부 경로

이 명령은 OSPF에서 학습한 외부 경로를 표시합니다.

```
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
```

그런 다음 경로를 BGP로 가져와야 합니다. 기본적으로 모든 외부 경로를 BGP로 가져와야 합니다.

보더 리프에 대한 BGP 확인

경로는 BGP VPNv4 Address-family에 있어야 하며, 패브릭 전체에 경로 대상이 배포되어 있어야 합니다. 경로 대상은 외부 VRF에서 내보내고 경로를 수신해야 하는 내부 VRF에서 가져온 BGP 확장 커뮤니티입니다.

그런 다음 BL의 외부 VRF에서 내보내는 경로 대상을 확인합니다.

```
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
```

위 출력은 외부 VRF에서 VPNv4로 광고되는 모든 경로에서 65001:2392068의 route-target을 수신해야 함을 보여줍니다.

다음으로 bgp 경로를 확인합니다.

```
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
```

위의 출력은 경로에 올바른 route-target이 있음을 보여줍니다. 'show bgp vpnv4 unicast 172.16.20.1 vrf overlay-1' 명령을 사용하여 VPNv4 경로를 확인할 수도 있습니다.

서버 leaf에 대한 확인

내부 EPG leaf에서 BL 알림 경로를 설치하려면 (위에서 언급한) route-target을 내부 VRF로 가져와야 합니다. 내부 VRF의 BGP 프로세스를 검사하여 다음을 검증할 수 있습니다.

```
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
```

위 출력은 외부 VRF가 내보내는 경로 대상을 가져오는 내부 VRF를 보여줍니다. 또한 참조되는 'Import Route-Map'이 있습니다. 가져오기 경로 맵에는 '공유 경로 제어 서브넷' 플래그가 있는 공유

L3Out에 정의된 특정 접두사가 포함됩니다.

외부 접두사를 포함하도록 경로 맵 내용을 확인할 수 있습니다.

```
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
```

위 출력은 가져올 서브넷을 포함하는 가져오기 경로 맵을 보여줍니다.

최종 확인에는 경로가 BGP 테이블에 있으며 라우팅 테이블에 설치되어 있는지 확인하는 과정이 포함됩니다.

서버 리프의 BGP 테이블:

```
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
```

경로를 내부 VRF BGP 테이블로 가져오고 예상 경로 대상을 포함합니다.

설치된 경로를 확인할 수 있습니다.

```
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
```

위 출력에서는 특정 'vsh -c' 명령을 사용하여 'detail' 출력을 가져옵니다. 'detail' 플래그는 재작성 VXLAN VNID를 포함합니다. 외부 VRF의 VXLAN VNID입니다. BL은 이 VNID로 데이터 플레인 트래픽을 수신하면 외부 VRF에서 포워딩 결정을 내립니다.

rw-vnid 값은 16진수이므로 10진수로 변환하면 VRF VNID가 2392068이 됩니다. 'show system internal epm vrf all'을 사용하여 해당 VRF를 검색합니다. | leaf의 grep 2392068' 'moquery -c fvCtx -f 'fv.Ctx.seg=="2392068"' 명령을 사용하여 APIC에서 전역 검색을 수행할 수 있습니다.

다음 홉의 IP도 BL PTEP를 가리켜야 하며 '%overlay-1'은 다음 홉의 경로 조회가 오버레이 VRF에 있음을 나타냅니다.

공유 L3Out 워크플로 - 내부 경로 알림

이전 섹션에서 설명한 것처럼, 공유 L3Out에서 내부 BD 서브넷을 알리는 작업은 다음에 의해 처리됩니다.

- BD 서브넷(내부 VRF)은 BL(외부 VRF)에 고정 경로로 설치됩니다. 이러한 고정 경로 구축은 내부 EPG와 L3Out 간의 계약 관계의 결과입니다.
- 고정 경로는 BD 서브넷에서 '외부에 보급됨' 범위가 설정되면 외부 프로토콜로 재배포됩니다.

BL에서 BD 고정 경로 확인

```
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
```

위 출력에서 내부 VRF의 VNID가 재작성용으로 설정되어 있습니다. 다음 홉도 proxy-v4-anycast 주소로 설정됩니다.

위의 경로는 "경로 알림" 섹션에 나와 있는 것과 동일한 경로 맵을 통해 외부에 광고됩니다.

BD 서브넷이 'Advertise Externally'로 설정된 경우 내부 EPG가 계약 관계를 갖는 **모든 L3Out**의 **외부 프로토콜**로 재배포됩니다.

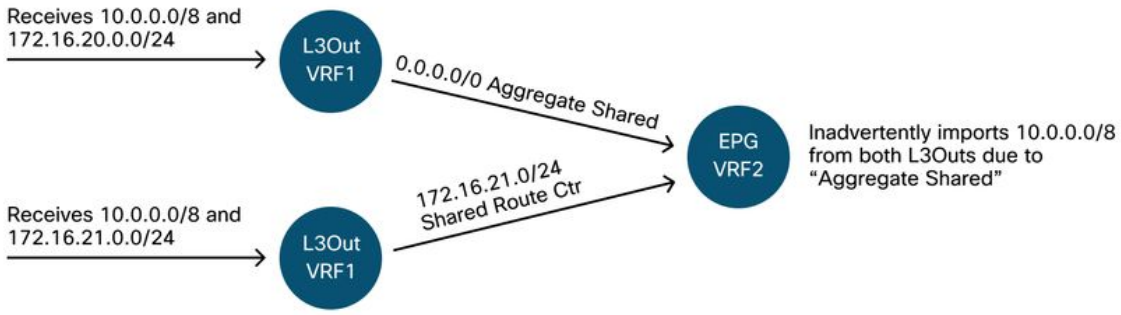
공유 L3Out 문제 해결 시나리오 - 예기치 않은 경로 유출

이 시나리오에는 외부 VRF에 여러 L3Out이 있으며 내부 EPG가 '공유' 범위 옵션으로 네트워크가 정의되지 **않은** L3Out에서 경로를 수신하는 중입니다.

'Aggregate Shared' 사용

다음 그림을 고려하십시오.

예기치 않은 경로 누수



'공유 경로 제어 서브넷' 플래그에서 프로그래밍된 접두사 **목록이 있는 BGP 가져오기** 맵은 VRF 레벨에서 적용됩니다. VRF1의 L3Out 중 하나에 '공유 경로 제어 서브넷'이 있는 서브넷이 있는 경우 VRF1 내의 L3Outs에서 이 공유 경로 제어 서브넷과 일치하는 모든 경로를 VRF2로 가져옵니다.

위의 설계는 예기치 않은 트래픽 흐름을 초래할 수 있습니다. 내부 EPG와 예기치 않은 광고 L3Out EPG 간에 contract가 없는 경우 트래픽이 드롭됩니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.