ACI 패브릭 L3Out

목차

서론

Cisco® Application Centric Infrastructure(Cisco ACI™)의 Layer 3 Out(L3Out)은 라우팅을 통해 ACI 외부로의 연결을 정의하는 일련의 구성입니다. 본 문서는 Cisco ACI 설계 개념 및 ACI L3Out 관련 옵션에 대한 철저한 설명을 목표로 합니다. 본 문서에서는 모든 상황에 대한 단계별 구성 예시를 제공하지는 않으며 핵심 개념을 이해하는 것에 초점을 두고 있습니다. 따라서 ACI 에 대한 기초적인 이해와 더불어 OSPF, EIGRP, BGP, MP-BGP 등 표준 라우팅 프로토콜에 대한 충분한 지식을 갖추고 본 문서를 읽는 것을 추천합니다.

Cisco ACI Layer 3 Out 개요

ACI 패브릭은 여러 가지 구성 요소로 형성됩니다. 일부 구성 요소에는 브리지 도메인(BD)과 엔드포인트 그룹(EPG)이 포함되어 있으며 엔드포인트 집합에 대해 계층(L2) 연결 또는 기본 게이트웨이 기능을 제공합니다. 또 다른 구성 요소로 Layer 3 Out(L3Out 또는 APIC Release 4.2 이전 Cisco APIC GUI 에서 라우팅된 외부 네트워크)이 있는데, 이 Layer 3 Out 은 라우팅 프로토콜 또는 고정 경로를 통해 ACI 및 ACI 패브릭 외부의 기타 네트워크 도메인에 연결된 서버 간에 계층 3(L3) 연결을 제공합니다.

Cisco ACI 는 본래 엔드포인트를 관리할 목적으로 데이터 센터에서 스텁 네트워크로서 기능하기 위해 구축되었습니다. ACI Layer 3 Out(L3Out)은 초기 전송 네트워크가 아닌 ACI 로 형성된 스텁 네트워크, 그리고 인트라넷과 인터넷, WAN 등 나머지 네트워크 간의 보더 네트워크 형태로 설계되었습니다.

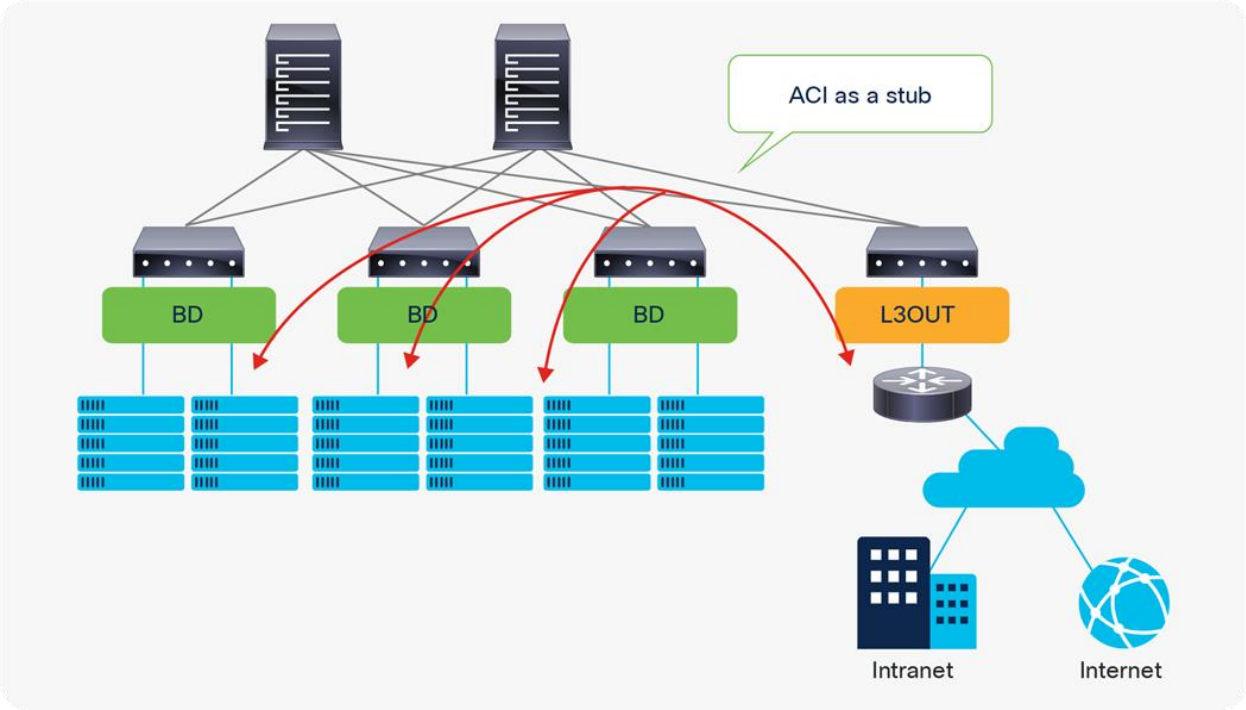

Figure 1.
스텁 네트워크로서의 ACI 패브릭

이러한 스텁 특성으로 인해 ACI 네트워크를 통한 L3Out 간의 트래픽 트래버싱은 본래 지원되지 않았습니다.

그러나 Cisco ACI 에서는 APIC Release 1.1 을 시작으로 전송 라우팅 기능을 도입했습니다. 이는 L3Out 간에 트래픽이 트래버싱될 수 있도록 ACI 패브릭이 전송 네트워크 역할을 할 수 있도록 지원하는 기능입니다. 자세한 내용은 "L3Out 전송 라우팅" 섹션을 참조하시기 바랍니다.

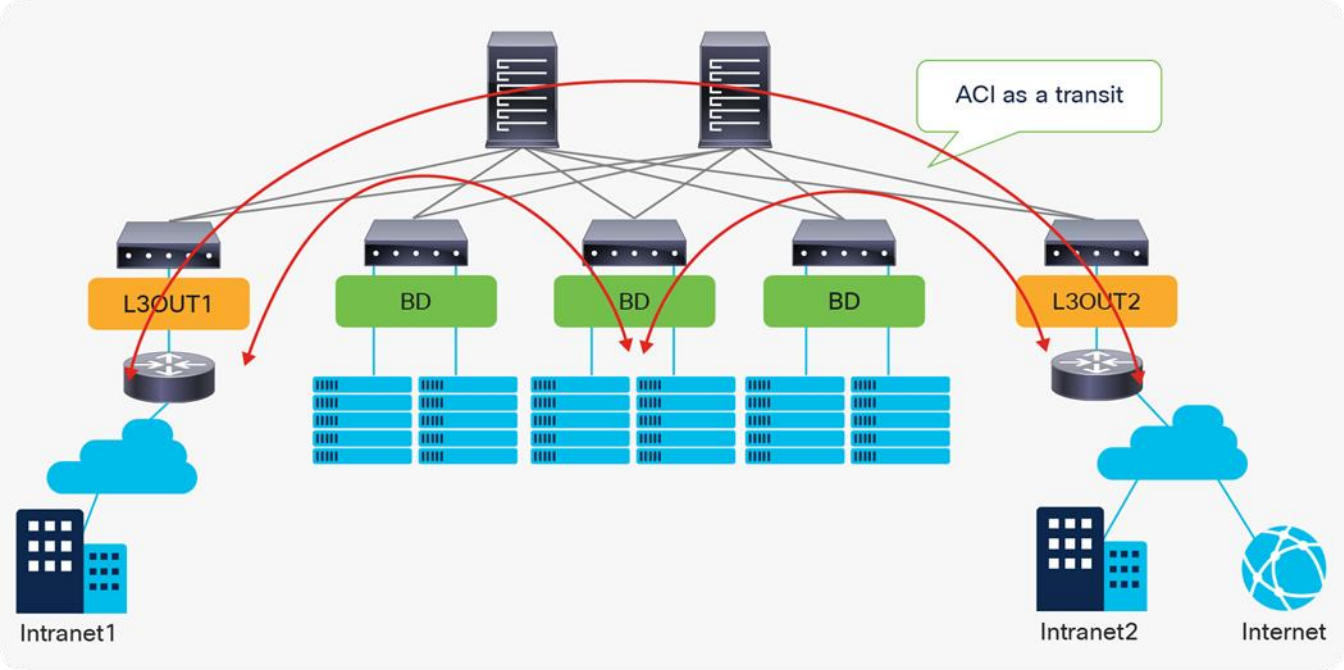

Figure 2.
전송 네트워크로서의 ACI 패브릭

참고:

근본적으로 L3Out 은 이면에 다른 서브넷이 있는 네트워크 장치를 연결합니다. ACI BD/EPG 에서는 모든 IP 주소가 /32(IPv6 에서는 /128) 엔드포인트로서 학습됩니다. 따라서 BD 또는 EPG 를 통해 이면에 여러 개의 서브넷이 포함되어 있는 네트워크 장치를 ACI 에 연결하면 엔드포인트에 /32 IP 주소가 대량으로 발생하는데, 이는 비효율적이기 때문에 확장성이 한계에 도달할 가능성이 높습니다. 본 내용에 관해서는 "ACI 패브릭 엔드포인트 학습" 백서의 L3Out 및 표준 엔드포인트" 섹션을 참고하시기 바랍니다.

L3Out 의 기본 구성 요소

L3Out 에서는 다음과 같은 다섯 가지 핵심 기능에 대해 필수 구성 객체를 제시합니다.

1. 라우팅 프로토콜(또는 고정 경로)을 통한 외부 경로 학습
2. 학습된 외부 경로(또는 고정 경로)를 다른 리프 스위치로 분배
3. ACI 내부 경로(BD 서브넷)를 ACI 외부로 보급
4. 학습된 외부 경로를 기타 L3Out(전송 라우팅)으로 보급
5. Contract 를 이용해 L3Out 을 통해 외부 네트워크에서 트래픽이 도착하거나 또는 네트워크로 전송되도록 지원

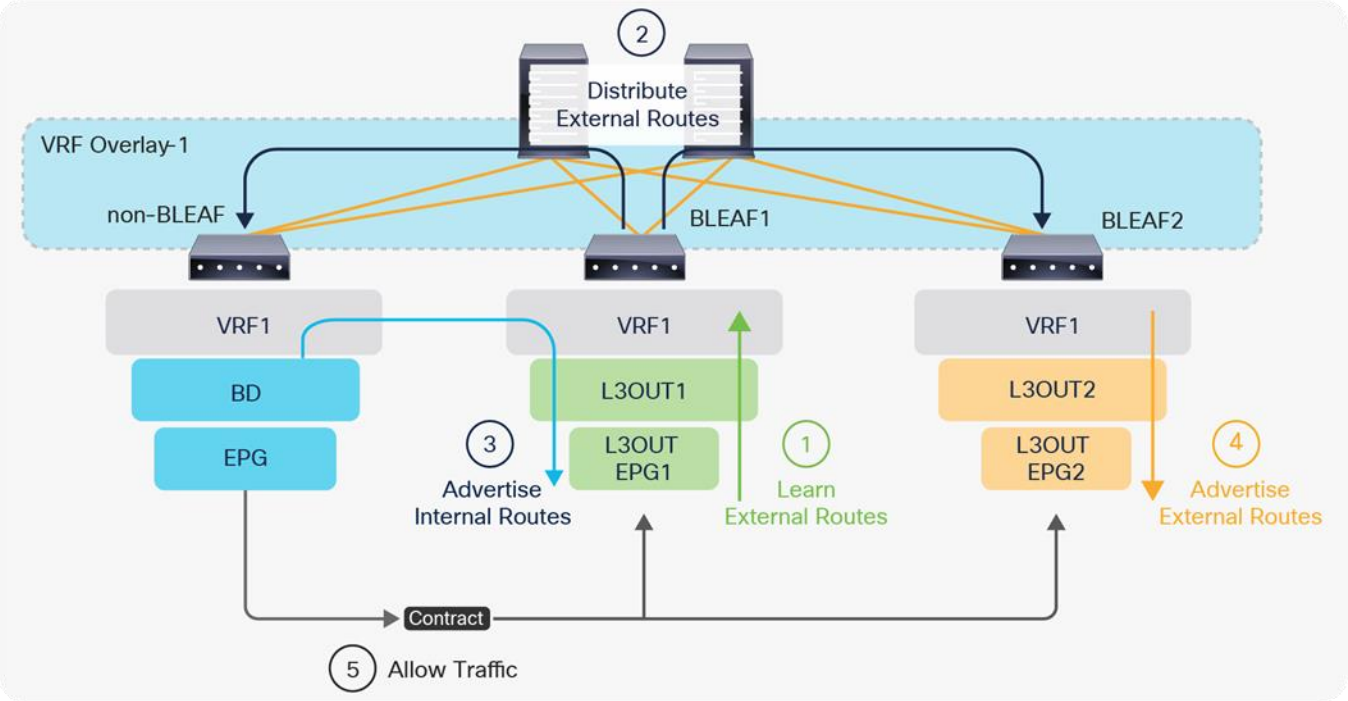

Figure 3.
L3Out 의 다섯 가지 기본 구성 요소

다음 내용에 각 단계가 간략히 설명되어 있습니다. 각 단계에 대한 상세 정보는 후반부 섹션 또는 Cisco APIC 계층 3 네트워킹 구성 가이드을 참조하시기 바랍니다.

1. 보더 리프 스위치에서 외부 경로 학습

아래 Figure 4 에는 테넌트 아래에 있는 L3Out 의 각 구성 요소가 설명되어 있습니다(**Tenant > Networking > External Routed Networks > L3Out**). 볼드체로 표시된 부분은 외부 네트워크 장치에서 외부 경로를 학습하고 라우팅 프로토콜을 구성하기 위한 필수 구성 요소입니다. L3Out EPG 자체가 라우팅 프로토콜 구성이 아니라 EPG 와 같은 보안 구문이지만, 리프 스위치에 있는 관련 인터페이스 매개변수와 라우팅 프로토콜을 배포하기 위해서는 한 개 이상의 L3Out EPG 가 필요합니다.

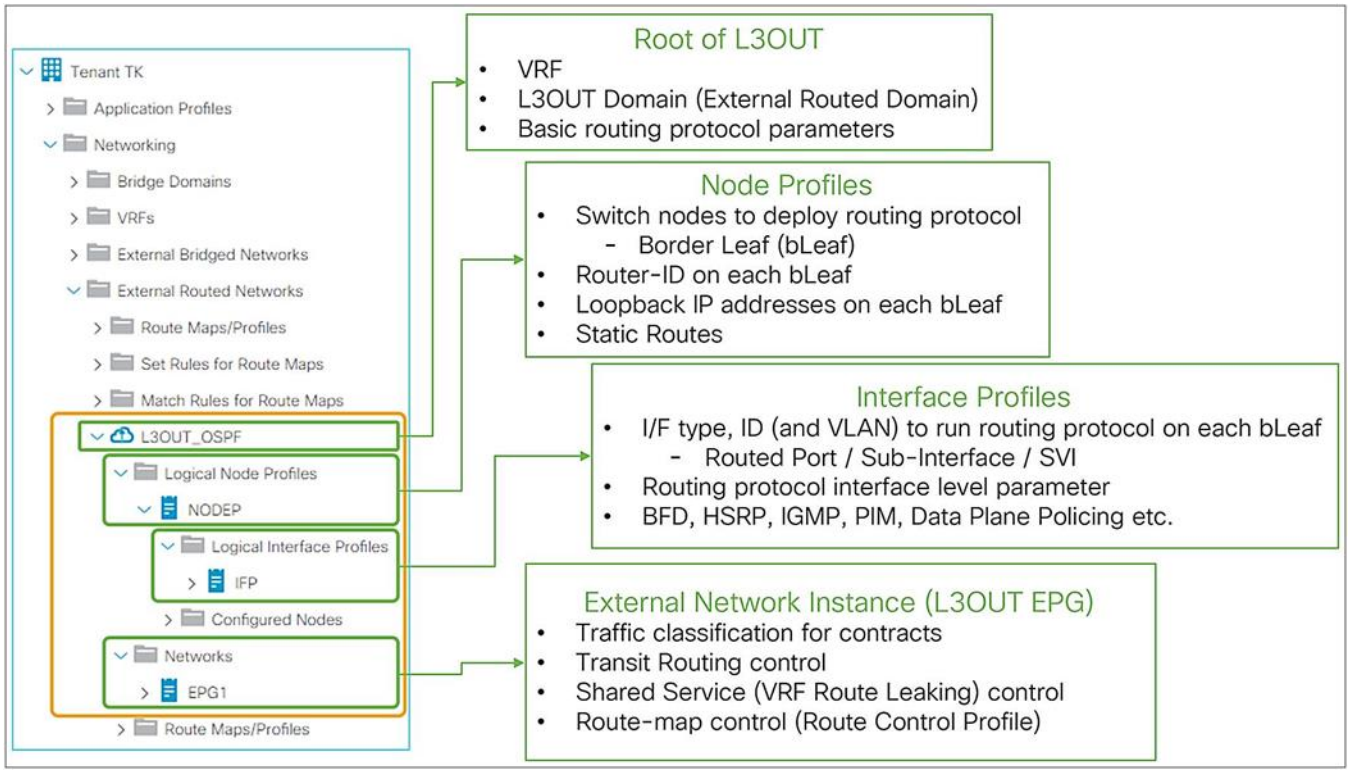

Figure 4.

GUI 내 L3Out 의 기본 구성 요소(APIC 3.2 Release)

다음 단계는 Figure 4 에 나와 있는 구성 요소로 ACI 보더 리프에 라우팅 프로토콜을 배포하는 절차를 요약한 것입니다.

1. L3Out 의 본질
   a. 배포할 라우팅 프로토콜 선택(OSPF, BGP 등)
   b. VRF 를 선택해 라우팅 프로토콜 배포
   c. L3Out 도메인을 선택해 L3Out 구성에서 사용할 수 있는 VLAN 과 인터페이스의 범위를 정의
      해당 도메인 자체는 패브릭 액세스 정책을 통해 구성됨

2. 노드 프로필
   a. 라우팅 프로토콜을 배포할 리프 스위치 선택
      (일명 보더 리프 스위치)
   b. 각 리프에서 라우팅 프로토콜에 대한 라우터 ID 를 구성
      (Cisco ACI 에서는 일반적인 라우터와 다르게 스위치상 IP 주소에 기반해 라우터 ID 를 자동으로 할당하지 않음)
3. 인터페이스 프로필
   a. 라우팅 프로토콜이 실행될 리프 인터페이스를 구성
      본 단계는 인터페이스 유형(SVI, 라우팅된 포트 또는 하위 인터페이스), 인터페이스 ID, IP 주소 등의 구성 요소를 입력하는 과정으로 이루어집니다.
   b. 인터페이스 수준의 라우팅 프로토콜 매개변수(hello 간격 등)에 대한 정책 선택
      대부분의 배포에서 기본 구성(정책)을 사용함
4. 외부 EPG(L3Out EPG)
   a. IP 주소 또는 SVI 자체 등의 인터페이스 매개변수와 라우팅 프로토콜을 배포하고 인접 라우터로 라우팅 프로토콜 피어링을 설정하는 데 비어 있는 외부 EPG 만으로 충분함
      외부 EPG 를 사용하는 자세한 방법은 이후에 설명하겠습니다.

노드 프로필 또는 라우팅 프로토콜 옵션 등의 각 구성 요소에 대한 상세 내용은 "L3Out 노드 및 인터페이스 프로필" 또는 "L3Out BGP" 등의 후반부 섹션에 기술되어 있습니다. 라우팅 프로토콜이 보더 리프 스위치에 배포되고 외부 장치와 인접 관계가 수립되면 해당 보더 리프 스위치에서 외부 경로를 학습할 수 있습니다.

이 시점에서 외부 경로는 해당 보더 리프 스위치에만 존재하며 ACI 패브릭에서는 이들 경로를 타 리프 스위치로 배포하기 전입니다(다음 섹션 "ACI 패브릭 내에서 외부 경로 배포" 참조).

2. ACI 패브릭 내에서 외부 경로 배포

ACI 에서는 ACI 인프라 VRF(오버레이-1 VRF) 내에서 VPNv4 가 포함된 멀티 프로토콜 BGP(MP-BGP)를 사용해 보더 리프에서 타 리프 스위치로 외부 경로를 배포합니다. 각 스위치 간 ISIS 등 ACI 인프라 VRF 에 있는 타 구성 및 구성 요소와 유사하게 이 구성 역시 배경에서 자동화됩니다. 사용자는 다음과 같이 두 가지 구성만 수행하면 됩니다.

- **BGP AS 번호** 선택
  - ACI 패브릭 전체를 나타내는 AS 번호 리프와 스파인 간의 인프라 MP-BGP, 그리고 사용자 L3Out 의 BGP 에 대해 사용되어 외부 장치로 BGP 피어를 설정
- **BGP 경로 리플렉터**로서 스파인 스위치를 선택
  - 각 리프 스위치는 선택된 경로 리플렉터 스파인 스위치에 대한 BGP 클라이언트 역할을 함
  - 해당 MP-BGP 는 포드마다 적용됨 각 포드마다 최소 한 개 이상의 경로 리플렉터 스파인이 있는지 확인. 각 포드마다 두 개의 경로 리플렉터를 권장
  - 내부 MP-BGP(VPNv4)용 **경로 리플렉터**와 멀티 포드 MP-BGP(VPNv4, eVPN)용 포드 간의 **외부 경로 리플렉터**는 구성이 서로 다름

이들 두 구성 요소가 **System > System Settings > BGP Route Reflector** 에서 구성되고 **Fabric > Fabric Policies > Pods** 에서 **패브릭 포드 프로필**에 할당되면 외부 경로의 배포가 MP-BGP 와 함께 발생하고 비보더 리프 스위치에 외부 경로가 보더 리프 스위치 TEP IP 주소를 가리키는 iBGP 경로 형태로 나타납니다(Figure 5 및 Figure 6 참조). 더 자세한 내용은 "인프라 MP-BGP" 섹션에서 확인하시기 바랍니다.

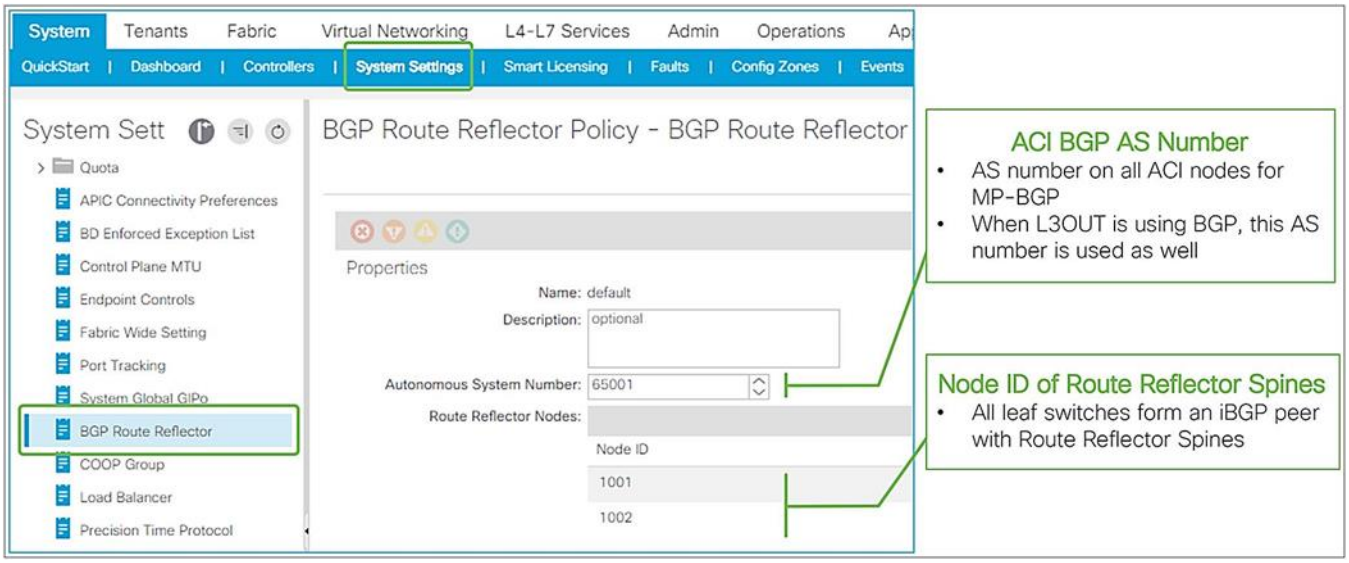

Figure 5.

APIC GUI(Release 3.2) 내 ACI BGP AS 번호 및 MP-BGP 경로 리플렉터 스파인

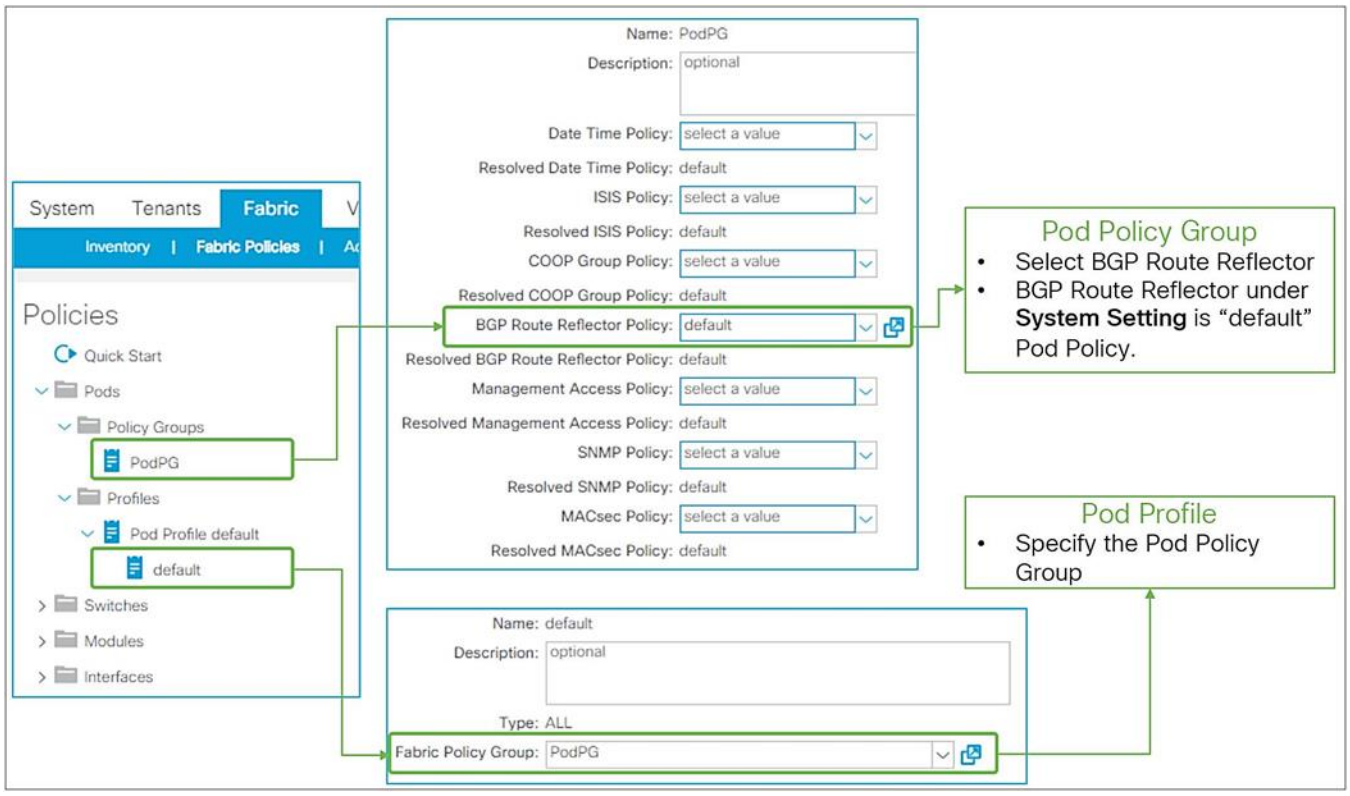

Figure 6.
APIC GUI(Release 3.2) 내 BGP 경로 리플렉터용 포드 프로필 및 정책 그룹

3. 외부 장치에 내부 경로(BD 서브넷) 보급

MP-BGP 경로 리플렉터 정책이 구성되고 포드 프로필에 할당되면 모든 리프 스위치에는 특정 VRF 에 대한 라우팅 테이블에 외부 경로가 포함되어야 합니다. 외부 장치가 ACI 와 연결된 서버에 연결되려면 ACI 가 BD 서브넷을 외부로 보급해야 합니다.

아래 Figure 7 에서는 BD 서브넷을 보급하는 가장 기본적인 방법이 요약되어 있습니다. 이는 **Tenant > Networking > Bridge Domaine > BD > L3 Configurations 탭**에서 L3Out 을 BD 에 연결하는 방법입니다.

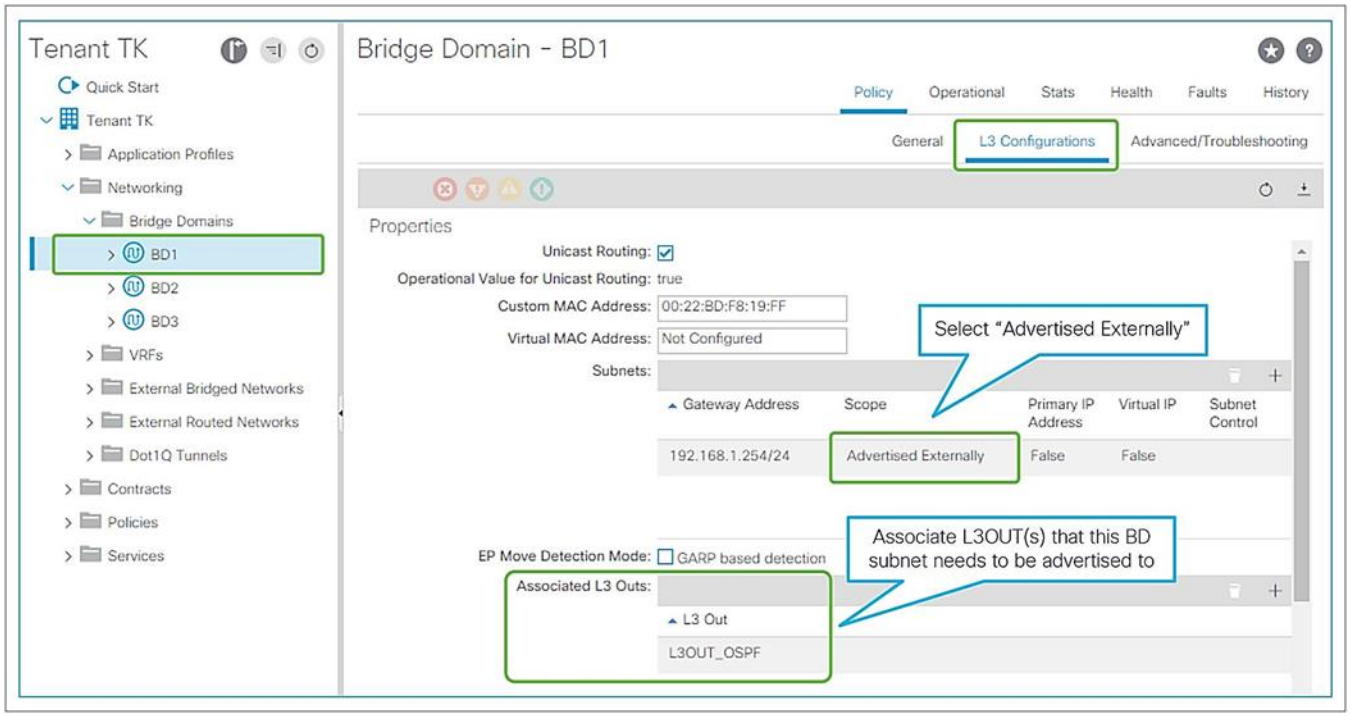

Figure 7.
GUI(APIC Release 3.2) 내 내부 경로(BD 서브넷) 보급

요점은 다음과 같습니다.

- "외부로 보급" 범위로 BD 서브넷 표시
- BD 서브넷을 외부로 보급해야 하는 L3Out 을 BD 에 연결

위 두 가지 구성을 통해 보더 리프 스위치에 경로 맵 규칙이 내부적으로 생성되어 연결된 L3Out 의 라우팅 프로토콜로 BD 서브넷(고정 또는 직접 경로)이 재배포됩니다.

BD 가 동일한 보더 리프에 배포될 경우 경로 맵 규칙을 통해 재배포되어 보급되지만 이것이 일반적인 경우는 아닙니다. BD 서브넷은 외부 경로 전용인 MP-BGP 를 통해 배포되지 않는다는 점에 유의해야 합니다. BD 의 EPG 와 L3Out 간의 Contract 가 필요한데, Contract 가 구성되면 APIC 에서는 L3Out 과 BD 측의 논의가 필요하다는 점을 파악하고 보더 리프 스위치에 BD 서브넷을 설치합니다. 이후 위에서 언급한 경로 맵을 사용해

재배포가 이루어집니다. 트래픽 허용에도 Contract 가 필요하기 때문에 사용자는 일반적으로 이러한 상세 사항에는 주의를 기울일 필요가 없습니다.

자세한 내용은 "ACI BD 서브넷 보급" 섹션을 참조하시기 바랍니다.

4. 타 외부 장치로 외부 경로 보급(전송 라우팅)

일반적인 EPG 대신 두 개의 L3Out 간에 통신이 필요한 경우, L3Out 간의 외부 경로 보급이 필요한데 이를 전송 라우팅이라고 합니다.

L3Out 서브넷(**Tenant > Networking > External Routed Networks > L3Out > Networks > L3Out EPG > Subnets**)의 범위에서 "경로 제어 서브넷 내보내기"의 확인란을 체크하면 외부 경로를 외부로 보급(전송 라우팅)할 수 있습니다.

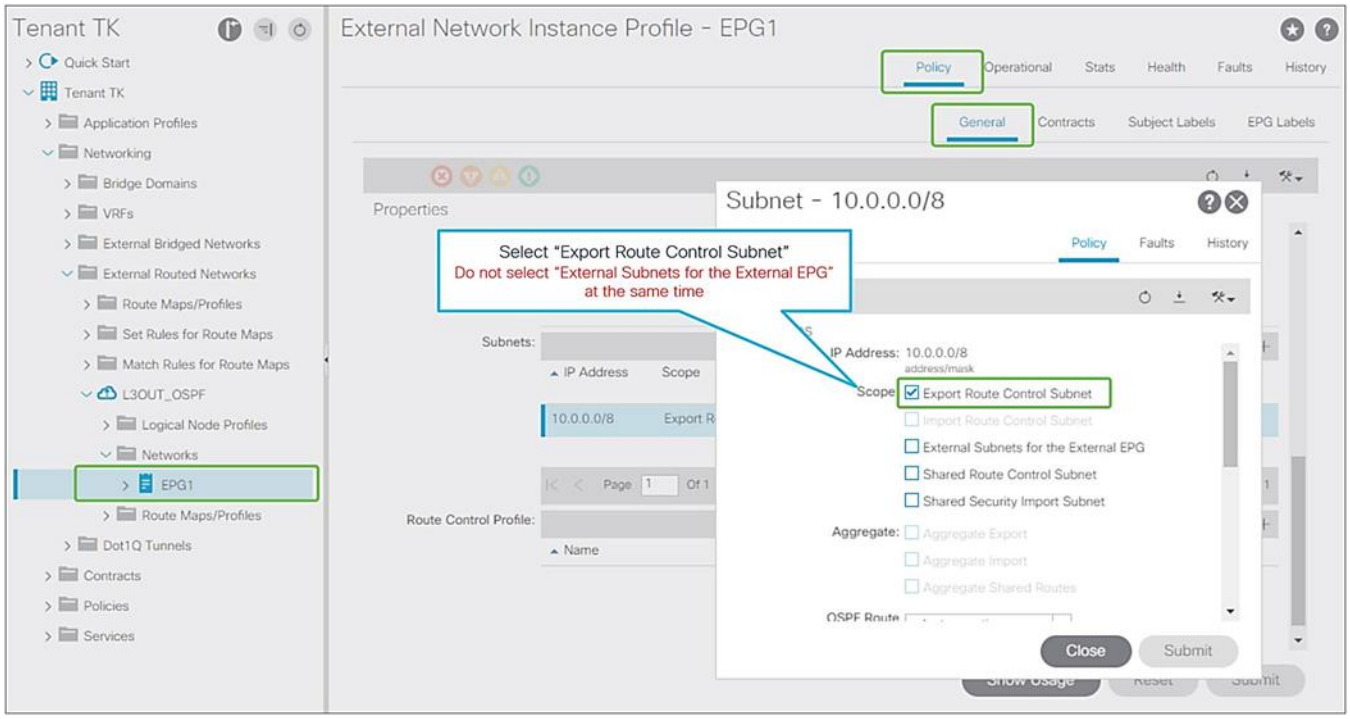

Figure 8.
전송 라우팅 GUI(APIC Release 3.2)용 경로 제어 서브넷 내보내기

"경로 제어 서브넷 내보내기" 범위가 선택되면 보더 리프 스위치에서 경로 맵 규칙이 생성되어 구성된 서브넷(Figure 8 의 10.0.0.0/8)을 타 L3Out(라우팅 프로토콜 또는 고정 경로)에서 해당 L3Out 용 라우팅 프로토콜로 재배포합니다. 두 개의 L3Out 이 서로 다른 보더 리프 스위치에 위치해 있을 때 MP-BGP 에서 재배포가 이루어집니다. 두 개의 L3Out 이 동일한 보더 리프에 위치한 경우 각 L3Out 에 대한 라우팅 프로토콜 사이에서 바로 재배포가 이루어집니다. 두 개의 L3Out 이 동일한 보더 리프에서 동일한 라우팅 프로토콜을 사용하는 경우 재배포가 아닌 다른 방식이 사용됩니다.

경로 맵 규칙에서 IP 식별 번호 목록을 사용하므로 "경로 제어 서브넷 내보내기" 범위가 포함된 서브넷은 라우팅 프로토콜 데이터베이스에 있는 서브넷과 완전히 일치해야 합니다. 예를 들어 "경로 제어 서브넷 내보내기"

범위가 포함된 10.0.0.0/8 에서는 "10.0.0.0/8" 경로만 내보내며, 10.0.0.0/16 은 내보내지 않습니다. 통합 및 요약 내용은 "L3Out 서브넷 범위 선택" 섹션 또는 "L3Out 전송 라우팅" 섹션을 참조하시기 바랍니다.

주의:

"경로 제어 서브넷 내보내기" 범위가 포함된 외부 경로는 구성된 L3Out 에서 보급됩니다. 이 범위는 동일한 경로를 학습하는 L3Out 에서 구성되어서는 안 됩니다. 이는 L3Out 이 학습 출처로 경로를 다시 보급하려고 시도하기 때문입니다. 이로 인해 루프가 발생할 수 있습니다.

그러나 "외부 EPG 용 외부 서브넷" 범위는 경로를 학습하는 L3Out 에서 구성되어야 합니다. 따라서 이 두 가지의 범위를 한 개의 L3Out 에 배치하는 것은 적절한 구성이 아닙니다. "외부 EPG 용 외부 서브넷" 범위에 대한 자세한 사항은 아래 5 번째 단계를 참조하시기 바랍니다.

5. Contract 를 통한 트래픽 허용

이전 섹션에서는 ACI 와 외부 네트워크 간에 경로를 교환하는 데 필요한 라우팅 프로토콜의 필수 구성을 다루었습니다. 그러나 라우팅 테이블의 관점에서 전환이 이론적으로는 가능하더라도 ACI 에서는 트래픽이 Contract 없이 EPG 사이를 지날 수 없으며, 이는 L3Out EPG 도 마찬가지입니다.

여기서 요점은 ACI 가 Contract 를 적용하기 위해 외부 경로를 분류하는 방식입니다. 일반적인 EPG 는 VLAN 과 패킷이 수신된 리프 인터페이스를 토대로 분류되지만, L3Out 의 경우 L3Out EPG 의 트래픽이 식별 번호 매칭에 기반해 분류됩니다. 이를 위해 L3Out 서브넷에 있는 "외부 EPG 를 위한 외부 서브넷" 범위(**Tenant > Networking > External Routed Networks > L3Out > Networks > L3Out EPG > Subnets**)가 사용됩니다.

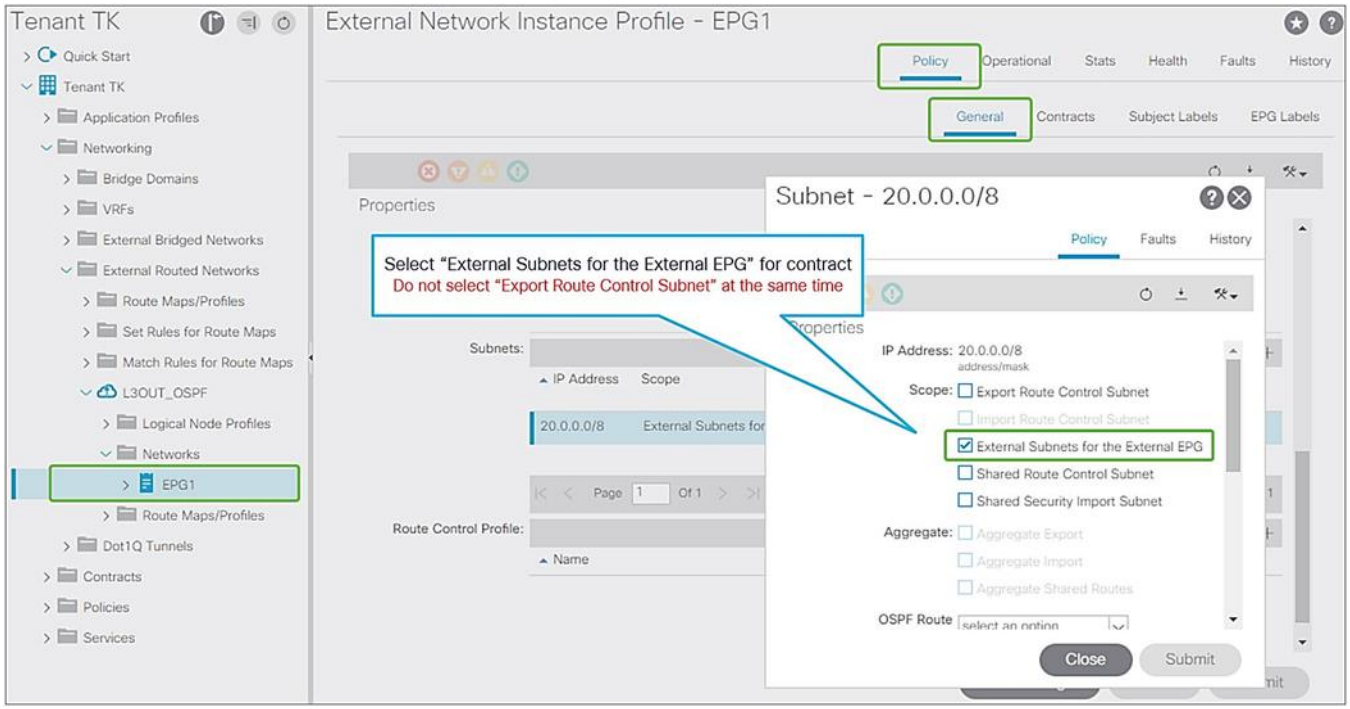

Figure 9.

GUI(APIC Release 3.2) 내 Contract 용 외부 EPG 에 대한 외부 서브넷

"경로 제어 서브넷 내보내기" 범위와 달리 "외부 EPG 용 외부 서브넷" 범위는 라우팅 테이블에 전혀 영향을 주지 않으며 Contract 를 적용하기 위해 출처 또는 목표 IP 주소를 토대로 트래픽 분류 방식을 정의할 뿐입니다. 라우팅 테이블에 오직 기본 경로 0.0.0.0/0 만 있을 때도 사용자는 L3Out EPG(Figure 9 아래의 **Tenant > Networking > External Routed Networks > L3Out > Networks** 의 EPG1)에서 "외부 EPG 용 외부 서브넷"으로 20.0.0.0/8 과 같은 특정 서브넷을 구성할 수 있습니다. 또한 다른 L3Out EPG 에서 "외부 EPG 용 외부 서브넷"을 사용해 30.0.0.0/8 을 구성하고 또 다른 일련의 Contract 를 적용할 수 있습니다. 이 범위는 "경로 제어 서브넷 내보내기"와 같은 IP 식별 번호 목록을 통해 실행되지 않습니다. 따라서 가장 긴 식별 번호 매치(LPM)를 토대로 매칭이 이루어집니다. 예를 들어 원본 IP 20.1.1.1 이 포함된 패킷의 소스는 "외부 EPG 용 외부 서브넷" 범위가 포함된 20.0.0.0/8 로 인해 Figure 9 에서 L3Out EPG1 로 분류됩니다.

트래픽 IP 가 "VRF" 내 "외부 EPG 용 외부 서브넷"에서 어느 서브넷과도 일치하지 않을 경우(해당 범위는 L3Out 이 아닌 각 VRF 마다 적용된다는 점에 유의. 자세한 내용은 아래 "주의" 참조), VRF 내에 해당 IP 에 대한 Contract 가 포함된 L3Out EPG 가 없기 때문에 트래픽이 손실될 가능성이 높습니다. 동일한 VRF 내에 "외부 EPG 용 외부 하위넷" 범위가 포함된 0.0.0.0/0 이 있을 경우, Contract 의 관점에서 0.0.0.0/0 가 포함된 해당 L3Out EPG 는 VRF 내 모든 트래픽을 대체하게 됩니다.

트래픽 분류가 "외부 EPG 용 외부 서브넷" 범위로 구성되면 사용자는 해당 L3Out 과 통신해야 하는 모든 구성 요소와 L3Out EPG 간의 Contract 만 구성하면 됩니다.

자세한 내용은 "L3Out 서브넷 범위 옵션" 섹션 또는 "L3Out Contract" 섹션을 참조하시기 바랍니다.

주의:

이들 L3Out 서브넷 범위는 각 VRF 마다 적용됩니다. 따라서 10.0.0.0/8 서브넷이 L3Out A 에서 학습되고 원본 IP 10.0.0.1 이 포함된 트래픽이 L3Out A 에서 수신되더라도, L3Out EPG B 에 어떤 이유로 L3Out EPG A 대신 "외부 EPG 용 외부 서브넷" 범위가 포함된 10.0.0.0/8 이 있다면 트래픽은 L3Out B(여기서는 L3Out EPG B 로 지칭)에서 L3Out EPG 로 분류될 수 있습니다. 이는 Contract 규칙이 적용되는 리프에 따라 달라질 수 있습니다. Contract 가 적용될 리프를 결정하는 요인 중 하나로 "L3Out Contract" 섹션의 정책 제어 적용 지침이 있습니다.

동일한 서브넷이 동일한 VRF 의 여러 L3Out EPG 에서 "외부 EPG 용 외부 서브넷" 범위를 통해 구성되면 해당 구성은 거부되지만 0.0.0.0/0 는 예외입니다. 이는 "외부 EPG 용 외부 서브넷" 범위가 포함된 0.0.0.0/0 를 여러 L3Out EPG 에서 구성해야 한다는 의미가 아니며, 예기치 못한 트래픽 허용을 방지하기 위한 권장 사항에 반합니다. 자세한 내용은 "L3Out Contract" 섹션을 참조하시기 바랍니다.

인프라 MP-BGP

이 섹션에서는 멀티 프로토콜 BGP(MP-BFP)가 L3Out 에서 학습된 외부 경로를 ACI 패브릭 인프라에서 모든 리프 스위치로 배포하는 방식을 상세히 설명합니다.

이전 섹션의 Figure 5 와 Figure 6 에는 인프라 MP-BGP 에 대한 APIC GUI 내 구성(BGP AS 및 BGP 경로 리플렉터 스파인)이 표시되어 있습니다. 구성이 완료되면 MP-BGP(Figure 10 내 청색 부분)가 리프와 스파인 스위치에 배포됩니다.

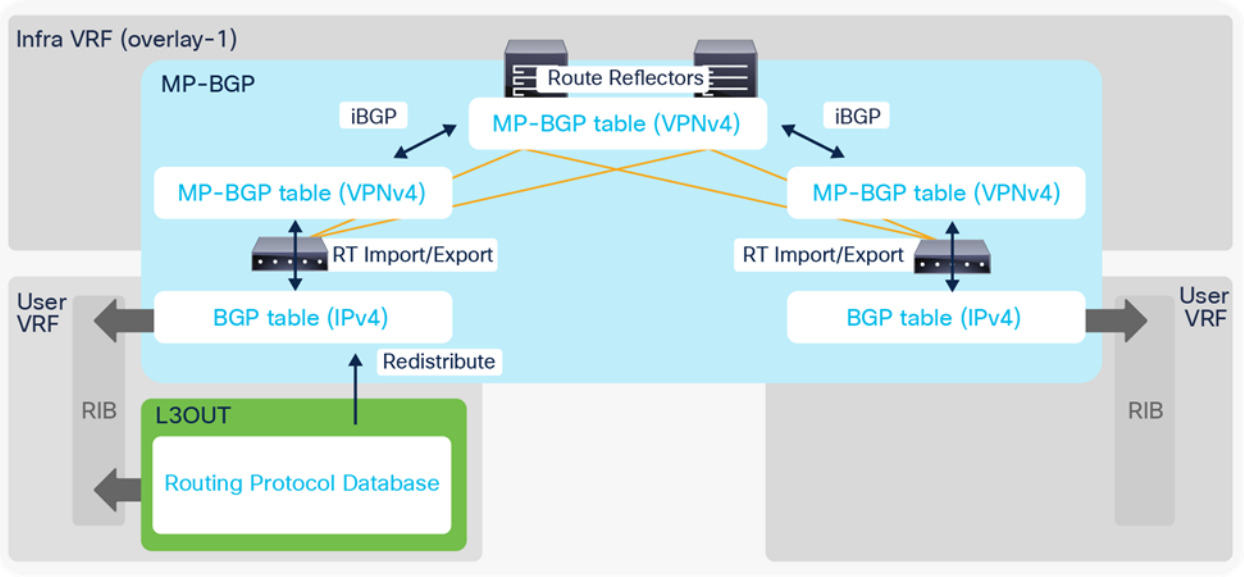

Figure 10.

인프라 MP-BGP 아키텍처

다음 내용은 Figure 10 에 나와 있는 각 구성 요소에 대한 설명입니다.

1. BGP IPv4/v6 주소 패밀리(AF)는 모든 사용자 VRF 내 모든 리프 스위치(보더 및 비보더 리프 스위치 모두)에 배포됨
2. BGP VPNv4/v6 주소 패밀리 또한 인프라 VRF(오버레이-1 VRF) 내 모든 리프 및 경로 리플렉터 스파인 스위치에 배포됨
   a. 모든 리프 스위치에서 인프라 VRF 내 경로 리플렉터 스파인 스위치로 iBGP 세션을 설정합니다.
   b. 모든 리프 스위치에서 인프라 VRF 내 경로 리플렉터 스파인을 통해 VPNv4/v6 경로를 교환합니다.
3. L3Out 이 리프에 배포되면 동일한 보더 리프에 있는 BGP IPv4/v6 AF 가 동일한 사용자 VRF 내 L3Out 의 라우팅 프로토콜에서 모든 경로에 대해 재배포 규칙을 자동으로 생성함
   a. 이러한 재배포를 "**Interleak**"라고 합니다. L3Out 에서 BGP 를 사용할 경우 L3Out 과 인프라 MP-BGP 에 대한 BGP 프로세스는 동일하므로 BGP 를 통해 학습된 경로에 재배포(Interleak)할 필요가 없습니다.

4. 재배포된 IPv4/v6 경로는 VPNv4/v6 로서 사용자 VRF 에서 인프라 VRF 로 내보내짐
5. 다른 리프 스위치에서 경로 리플렉터 스파인을 통해 배포된 VPNv4/v6 경로는 IPv4/v6 로서 인프라 VRF 에서 사용자 VRF 로 가져오기 됨
    a. 각 리프에서 BGP IPv4/v6 AF 에는 VPNv4/v6 AF 로 경로를 교환하기 위해 경로 대상(RT)이 포함된 내보내기 및 가져오기 규칙이 존재합니다. RT 의 형식은 "<ACI BGP AS>:<VRF VNID>"입니다. 따라서 모든 리프 스위치에서 각 VRF 에 동일한 RT 가 포함되며 동일한 VRF 내 모든 VPNv4/v6 경로는 동일한 RT 를 공유합니다. 보더 리프는 RT 를 사용해 IPv4/v6 외부 경로를 VPNv4/v6 AF 로 내보내며, 타 리프 스위치의 각 사용자 VRF 는 RT 에 기반해 다른 VRF 의 VPNv4/v6 경로를 잘못 가져오는 일 없이 자체 VRF 에서 IPv4/v6 AF 로 VPNv4/v6 경로를 가져올 수 있습니다.

참고:

규칙 집합은 L3Out 에서 BGP IPv4/v6 AF 로 Interleak Route Profile 을 통해 재배포(Interleak) 경로 맵에 적용될 수 있습니다. 자세한 내용은 ""L3Out 경로 프로필 / 경로 맵" 섹션의 Interleak 의 경로 프로필"을 참조하시기 바랍니다.

L3Out 의 루트(Root) 구성 요소

이전 "L3Out 의 기본 구성 요소" 섹션에서 설명한 바와 같이 L3Out 에는 논리 노드 또는 인터페이스 프로필이라는 구성 요소와 그 하위 객체인 네트워크가 포함됩니다. 각 하위 구성 요소에 대한 상세 내용은 각 섹션 후반부에서 다루며 본 섹션에서는 L3Out 의 루트 구성 요소를 살펴보겠습니다.

L3Out 의 루트 구성 요소에서 가장 중요한 구성은 **VRF, 라우팅된 외부 도메인, 그리고 라우팅 프로토콜**입니다.

- **VRF**
  L3Out 과 그 라우팅 프로토콜이 배포되는 VRF 입니다. 이는 동일한 테넌트의 VRF 이거나 공통 테넌트의 VRF 일 수 있습니다.
- **라우팅된 외부 도메인**
  L3Out 에서 인터페이스와 VLAN 의 집합을 사용할 수 있도록 허용하는 도메인입니다. 도메인 자체는 "**Fabric > Access Policies > Physical and External Domains > External Routed Domains**"에서 VLAN 풀 및 연결 가능한 액세스 엔티티 프로필(AEP)과 함께 구성됩니다.
- **라우팅 프로토콜**
  논리 노드 또는 인터페이스 프로필로 지정된 노드와 인터페이스에서 L3Out 으로 배포되는 라우팅 프로토콜입니다. Cisco ACI 에서는 한 가지를 제외하고 L3Out 당 한 개의 라우팅 프로토콜만 허용합니다. OSPF 를 BGP 용 IGP 로서 사용하기 위해 BGP 와 OSPF 는 예외적으로 동일한 L3Out 에서 구성될 수 있습니다. 라우팅 프로토콜이 선택되면 OSPF 영역 번호 또는 EIGRP AS 번호 구성 등의 매개변수가 동일한 창에 나타납니다. 각 라우팅 프로토콜 매개변수에 대한 자세한 내용은 각 라우팅 프로토콜 섹션 후반부에 기술되어 있습니다(BGP, OSPF, EIGRP).

위 세 가지를 제외한 구성은 선택 사항이지만 Figure 11 에서는 L3Out 루트 구성 요소의 GUI 예시와 각 L3Out 별 옵션에 대한 간략한 설명이 나와 있습니다.

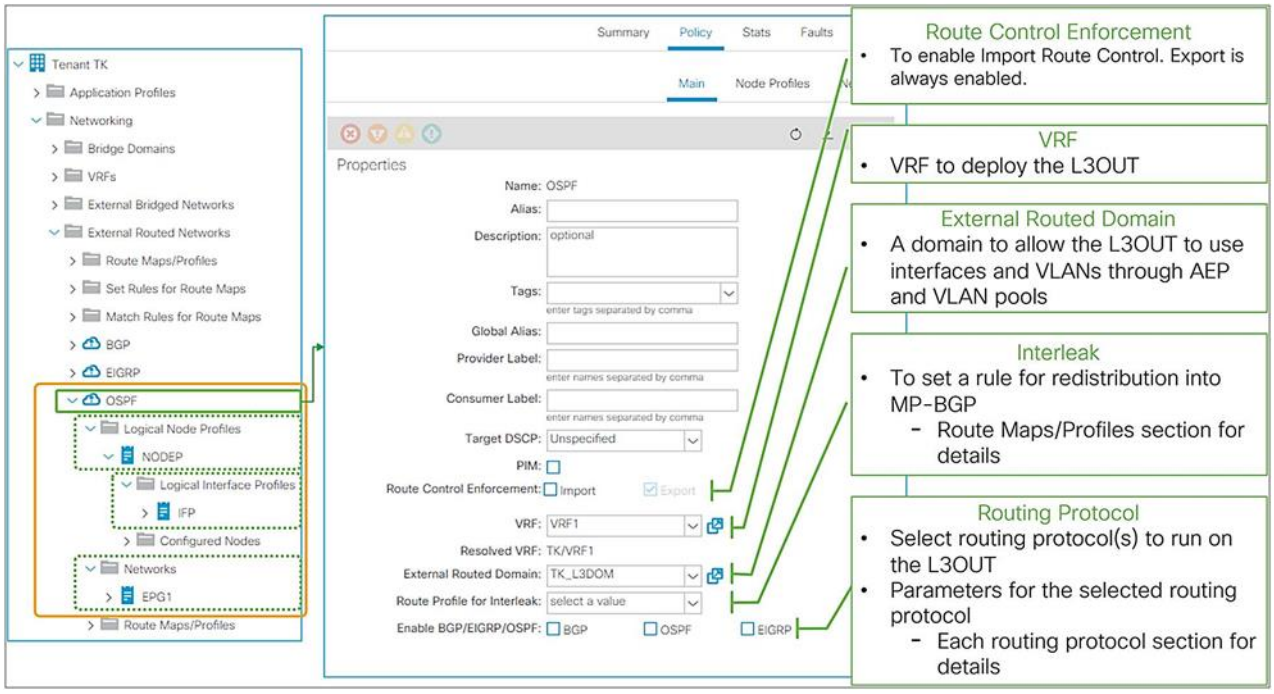

Figure 11.
APIC GUI(Release 3.2) 내 L3Out 루트 구성 요소

- **공급자 레이블**
  GOLF(거대 오버레이 전환) 기능에 대한 사항입니다. 이 레이블은 인프라 테넌트 내 GOLF L3Out 에서 구성됩니다. Cisco APIC 계층 3 네트워킹 구성 가이드의 "GOLF" 섹션을 참조하시기 바랍니다.
- **소비자 레이블**
  GOLF 기능에 대한 사항입니다. 이 레이블은 GOLF 뒤에서 외부 장치와 통신해야 하는 사용자 테넌트 또는 VRF 내 L3Out 에서 구성됩니다. 이 레이블은 인프라 테넌트 내 GOLF L3Out 의 공급자 레이블과 반드시 일치해야 합니다. 사용자 테넌트 또는 VRF 내 L3Out 이 L3Out EPG(GUI 내 L3Out 네트워크)를 GOLF L3Out 에 적용하도록 허용합니다. Cisco APIC 계층 3 네트워킹 구성 가이드의 "GOLF" 섹션을 참조하시기 바랍니다.
- **PIM**
  프로토콜 독립 멀티캐스트(Protocol Independent Multicast)의 약자입니다. 일반적으로 VRF 구성 요소에 구성되며 필요한 경우 해당 확인란은 자동으로 선택되므로 사용자가 이 옵션을 직접 선택하거나 해제할 필요가 없습니다. 자세한 내용은 Cisco APIC 계층 3 네트워킹 구성 가이드의 "IP 멀티캐스트" 섹션을 참조하시기 바랍니다.
- **경로 제어 적용**
  L3Out EPG(GUI 내 L3Out 네트워크)에서 서브넷에 대해 사용자가 **경로 제어 서브넷 가져오기** 범위를 구성할 수 있도록 허용합니다. 자세한 내용은 L3Out 서브넷 범위 옵션을 참조하시기 바랍니다.

- **Interleak 용 경로 프로필**
  인프라 MP-BGP 로 외부 경로를 재배포하기 위해 사용하는 경로 맵을 사용자 지정합니다. "L3Out 경로 프로필 / 경로 맵" 섹션의 "Interleak 의 경로 프로필" 섹션을 참조하시기 바랍니다.

L3Out 노드 및 인터페이스 프로필

L3Out 노드와 인터페이스 프로필의 주요 기능은 보더 리프 스위치가 될 스위치 노드, 그리고 라우팅 프로토콜을 지원해야 하는 인터페이스를 지정하는 것입니다. 이들 두 프로필의 또 다른 기능은 Figure 12 에 나와 있는 것처럼 고정 경로와 인터페이스 수준 라우팅 매개변수 등입니다.

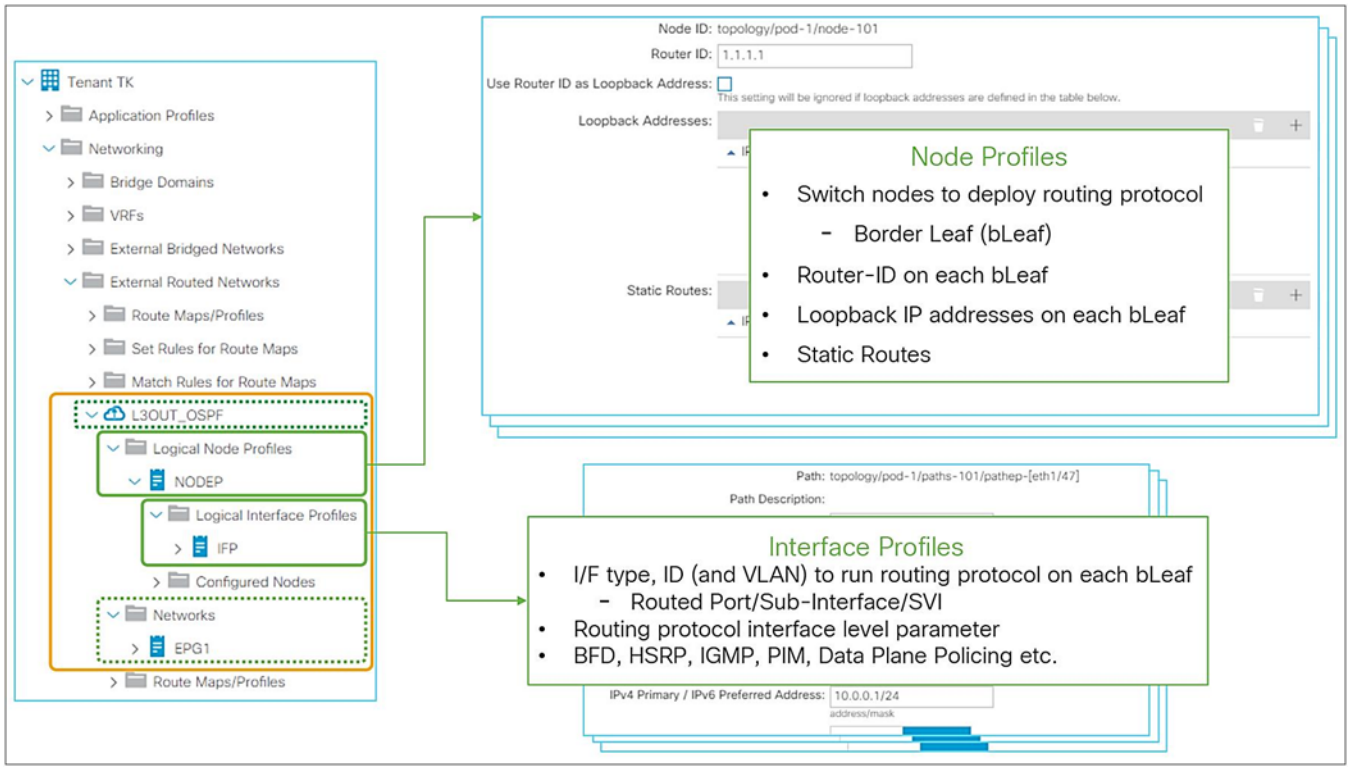

Figure 12.
논리 노드 프로필 또는 논리 인터페이스 프로필 GUI(APIC Release 3.2)

노드 및 인터페이스 프로필 설계

노드 프로필과 인터페이스 프로필 내 노드 ID 가 일치하기만 하면 노드와 인터페이스 프로필을 사용해 다양한 방법으로 동일한 구성을 얻을 수 있습니다.

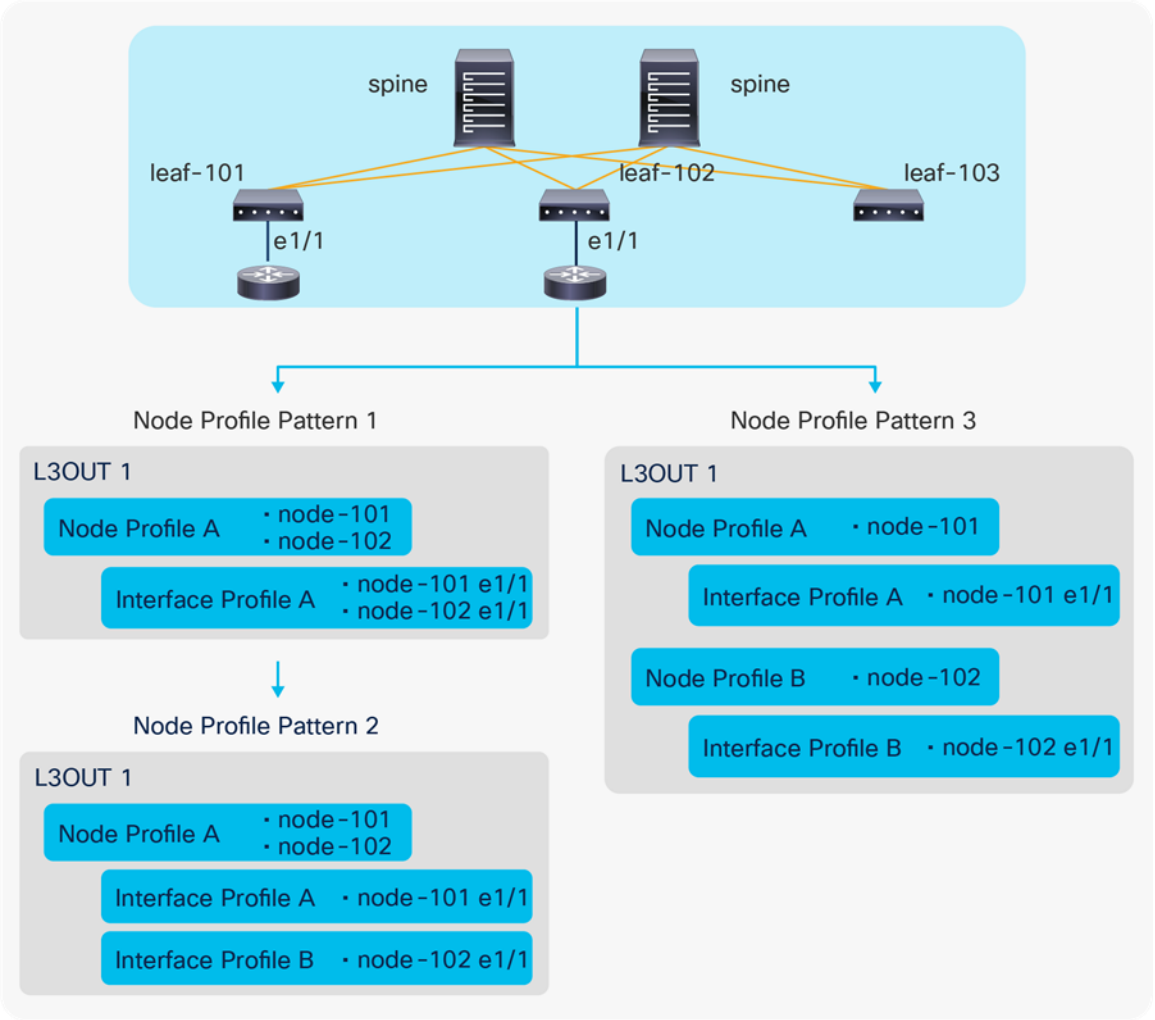

Figure 13.

L3Out 노드 프로필 구성 패턴

Figure 13 에는 노드-101 e1/1 과 노드-102 e1/1 이 L3Out1 의 일부가 되고 L3Out1 에서 정의된 라우팅 프로토콜을 지원하도록 구성하는 세가지 방식("방식"으로 지칭)이 나와 있습니다.

- 패턴 1: 두 인터페이스 모두 논리 노드 프로필 A 의 동일한 논리 인터페이스 프로필 A 에 위치함
- 패턴 2: 각 인터페이스가 동일한 논리 노드 프로필 A 의 논리 인터페이스 프로필 A 와 B 에 각각 위치함
- 패턴 3: 각 인터페이스가 각 논리 노드 프로필 A 와 B 의 논리 인터페이스 프로필 A 와 B 에 각각 위치함

모든 구성 패턴은 올바르며 ACI 보더 리프를 동일하게 프로그래밍합니다.

참고:

IPv4 와 IPv6 주소가 동일한 인터페이스에서 구성되어야 할 경우, IPv4 와 IPv6 에 대한 논리 인터페이스 프로필은 상이해야 하지만 논리 노드 프로필은 계속 공유할 수 있습니다.

논리 노드 프로필 상세 사항

이 섹션에서는 논리 노드 프로필의 각 옵션을 살펴봅니다.

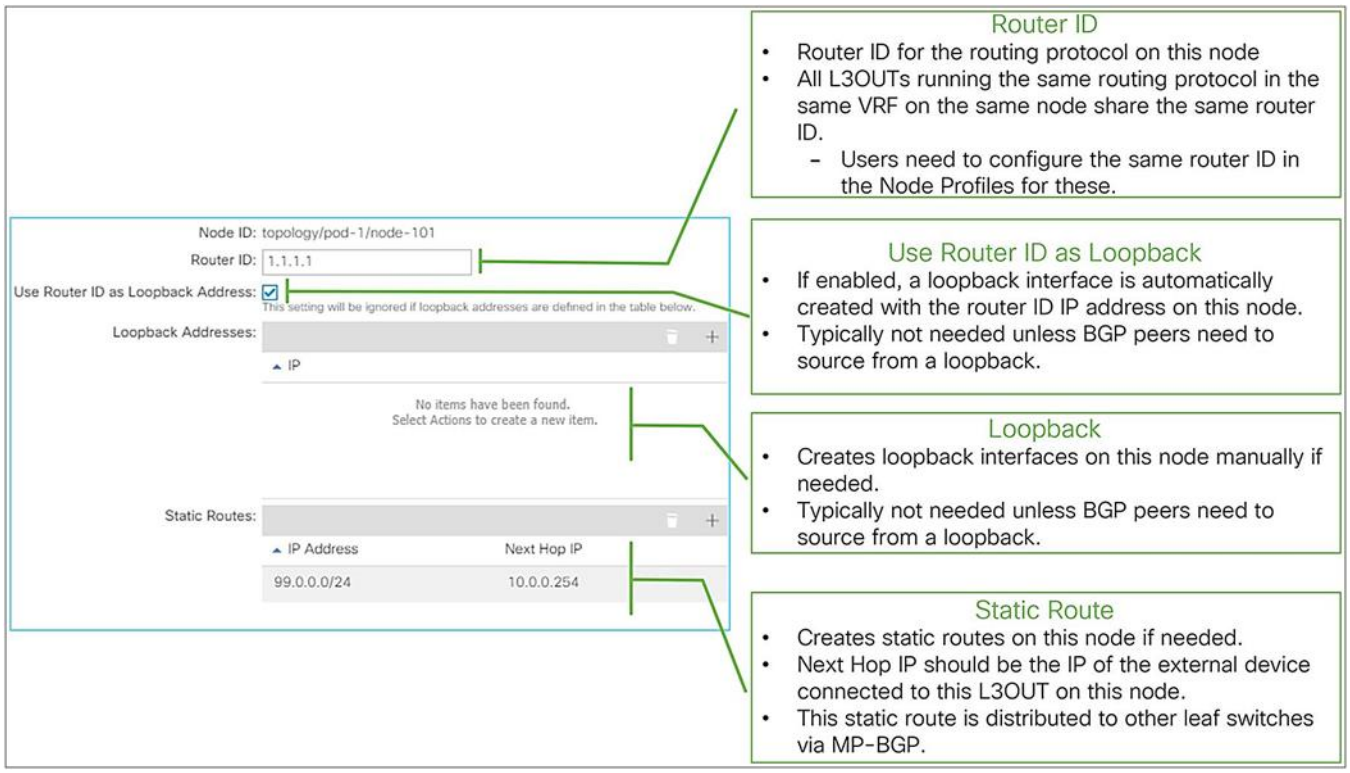

Figure 14.

GUI(APIC Release 3.2) 내 논리 노드 프로필 옵션

- **노드 ID**

  L3Out 의 라우팅 프로토콜이 배포되어야 하는 노드 ID 입니다. 이 노드를 보더 리프라고 합니다.

- **라우터 ID**

  이 노드의 L3Out 에 정의된 라우팅 프로토콜에 대한 각 VRF 별 라우터 ID 입니다. 일반적인 라우터의 라우터 ID 에 대한 동일한 보안 주체가 Cisco ACI 에도 적용됩니다.

  이는 독립 실행형 Cisco NX-OS 장치에 있을 경우 다음 CLI 와 같습니다. 이는 단순히 비교를 위한 것으로, APIC 에서 구성하기 위한 실제 NX-OS–style CLI 가 아닙니다.

```
router ospf default
  vrf VRF1
    router-id 1.1.1.1
```

- **라우터 ID 를 루프백 주소로 사용**
  이 노드에서 IP 주소로 라우터 ID 를 사용해 루프백 인터페이스를 생성하려면 이 옵션을 활성화합니다. 일반적으로는 IP 주소로 라우터 ID 를 사용해 루프백에서 BGP 피어를 공급하려는 경우가 아닌 한 필요하지 않습니다.

  이는 독립 실행형 NX-OS 장치에 있을 경우 다음 CLI 와 같습니다. 이는 단순히 비교를 위한 것으로, APIC 에서 구성하기 위한 실제 NX-OS–style CLI 가 아닙니다.

```
router ospf default
  vrf VRF1
    router-id 1.1.1.1
interface loopback10
  vrf member VRF1
  ip address 1.1.1.1/32
```

  아래 다음 옵션에서 루프백 인터페이스가 수동으로 구성되는 경우 이 옵션은 무시됩니다.

- **루프백 주소**
  임의의 IP 주소를 사용해 이 노드에서 루프백 인터페이스를 수동으로 생성합니다. 일반적으로는 루프백 IP 주소에서 BGP 피어를 공급하려는 경우가 아닌 한 필요하지 않습니다.

- **고정 경로**
  이 노드에서 고정 경로를 생성합니다. 고정 경로에 대한 다음 홉 IP 는 L3Out 에 연결되어야 합니다. 다음 홉 IP 가 구성되지 않을 경우 다음 홉이 없는 고정 경로가 노드에서 생성됩니다.
  여기에서 구성된 고정 경로는 라우팅 프로토콜에서 학습된 외부 경로와 같이 인프라 MP-BGP 를 통해 다른 리프 스위치로 배포됩니다.
  자세한 내용은 "L3Out 고정 경로" 섹션을 참조하시기 바랍니다.

참고:

동일한 VRF 에서 노드와 라우팅 프로토콜이 동일한 L3Out 이 2 개일 경우, 두 L3Out 의 노드 프로필에 있는 라우터 ID 가 일치해야 합니다. 노드와 라우팅 프로토콜이 동일한 여러 개의 L3Out 에서 상이한 라우터 ID 를 사용하는 것은 한 개의 독립 실행형 NX-OS 장치에서 다음 두 가지 구성을 입력하는 것과 같기 때문입니다.

```
router ospf default                 router ospf default
  vrf VRF1                  또한      vrf VRF1
    router-id 1.1.1.1                   router-id 2.2.2.2
```

CLI 는 단순히 비교를 위한 것으로, APIC 에서 구성하기 위한 실제 NX-OS–style CLI 가 아닙니다.

논리 인터페이스 프로필 상세 사항

여기서는 논리 인터페이스 프로필의 주요 구성 옵션을 살펴보겠습니다.

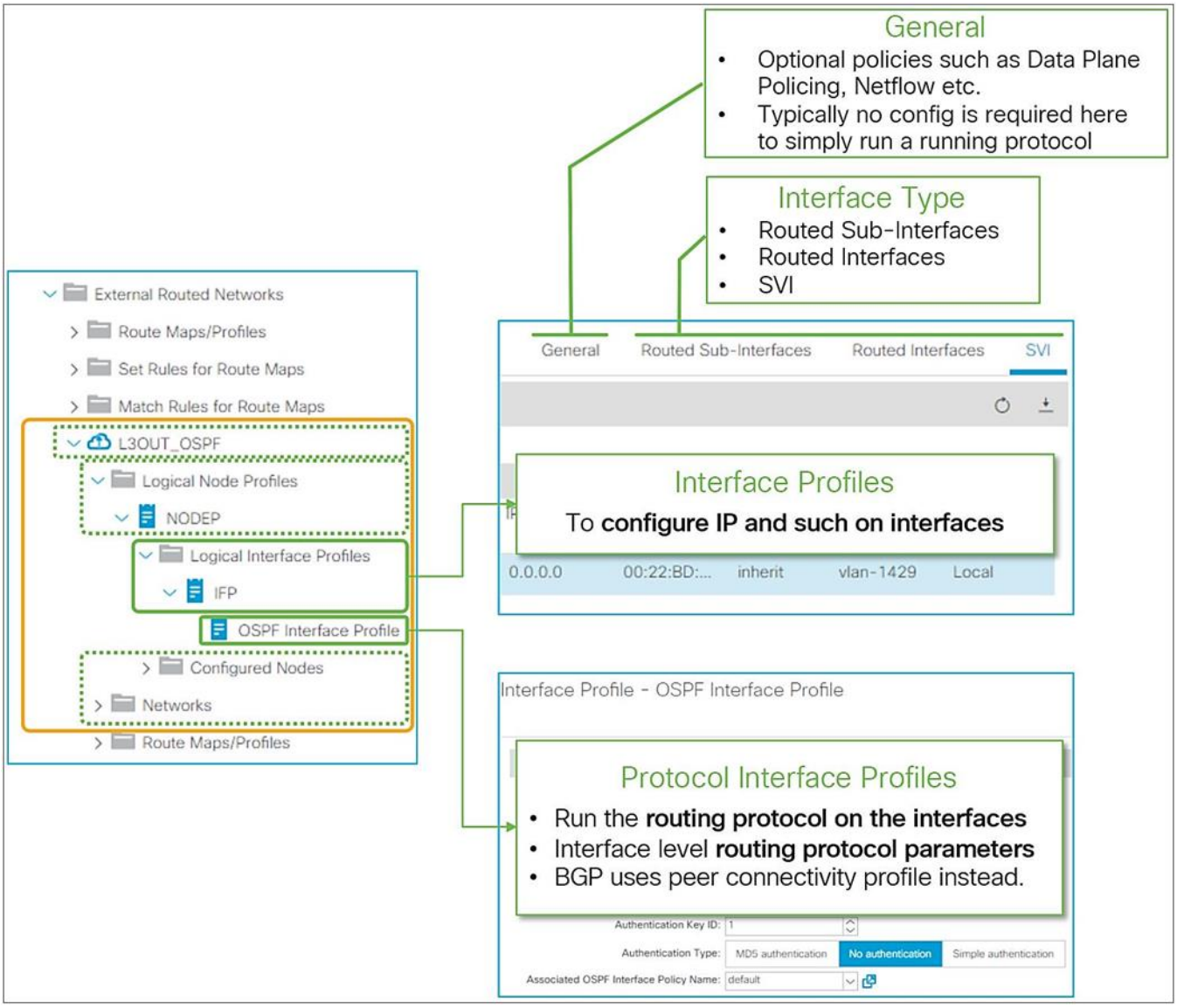

Figure 15.

GUI(APIC Release 3.2) 내 논리 인터페이스 프로필 및 프로토콜 인터페이스 프로필

Figure 15 에서는 논리 인터페이스 프로필에서 사용 가능한 옵션의 개요가 제시되어 있습니다. 인터페이스 프로필의 주요 목적은 보더 리프 스위치에서 라우팅 프로토콜을 실행하도록 인터페이스를 생성 및 구성하는 데 있습니다. 이는 독립 실행형 NX-OS 장치에서 'ip router ospf 1 area 0' 등의 라우팅 프로토콜 명령어와 IP 주소를 구성하는 것과 유사합니다. 이는 **인터페이스 유형**(Figure 15 참조)과 **프로토콜 인터페이스 프로필을** 구성함으로써 수행됩니다. 프로토콜 프로필이 없으면 인터페이스는 라우팅 프로토콜에 연결되지 않습니다(자세한 내용은 각 라우팅 프로토콜 섹션 BGP, OSPF, EIGRP 참조). **인터페이스 유형**과 **프로토콜 인터페이스 프로필** 외에도 Data Plane Policing, NetFlow, PIM Interface Policy, Internet Group Management Protocol(IGMP)처럼 옵션으로 제공되는 인터페이스 수준의 기능에 대해 논리 인터페이스 프로필에서 일반 탭을 구성해야 할 수도 있습니다. 양방향 전환 탐지(BFD) 역시 논리 인터페이스 프로필에서 구성할 수 있습니다. BFD 에 대한 자세한 내용은 "L3Out BFD" 섹션을 참조하시기 바랍니다.

다음 항에서는 각 **인터페이스 유형**과 그 매개변수를 살펴봅니다. 프로토콜 인터페이스 프로필과 기타 옵션에 대한 자세한 내용은 각 라우팅 프로토콜에 대한 해당 섹션을 참고하시기 바랍니다.

L3Out 을 통해 다음과 같은 유형의 인터페이스를 구성할 수 있습니다.

1. 라우팅된 하위 인터페이스
2. 라우팅된 인터페이스
3. SVI
4. 부동 SVI(APIC Release 4.2 에서 도입됨)

L3Out 의 인터페이스와 관련된 설계 고려 사항은 표준 라우터 또는 계층 3 스위치와 거의 동일합니다.

실제 포트가 EPG 에서 트렁크 포트로 이미 사용되는 경우, 동일한 포트는 L3Out 에서 라우팅된 하위 인터페이스 또는 라우팅된 인터페이스(L3 포트)로서 사용될 수 없는데, 이는 인터페이스가 EPG 에서 스위치 포트(L2 포트)로서 이미 구성되었기 때문입니다.

Figure 16 에는 라우팅된 하위 인터페이스에 대한 공통 매개변수의 의미가 설명되어 있습니다. 이들 매개변수 중 대부분은 다른 인터페이스 유형에서도 찾아볼 수 있으나 VLAN 매개변수는 예외적으로, 라우팅된 하위 인터페이스와 SVI 에는 구성될 수 있지만 라우팅된 인터페이스에는 구성될 수 없습니다.

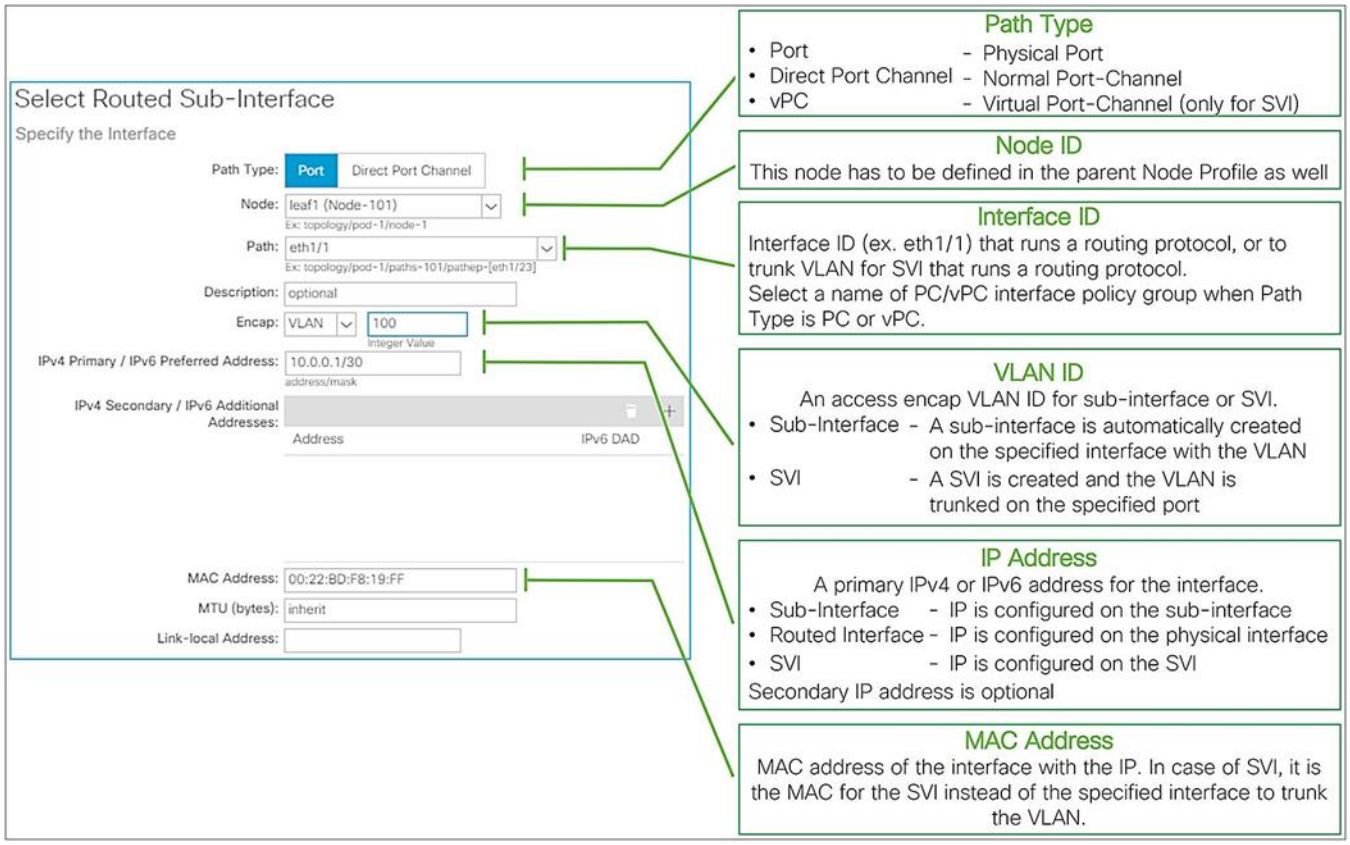

Figure 16.
논리 인터페이스 프로필 공통 매개변수

다음 목록에는 각 매개변수 유형에 대한 추가적인 정보가 자세히 설명되어 있습니다.

- **경로 유형**
  다음 표에서와 같이, L3Out 에서 사용 가능한 경로 유형에는 세 가지가 있습니다.

경로 유형	설명	지원되는 I/F 유형
포트	단일 리프 스위치에 있는 실제 포트(예: eth1/1)	라우팅된 인터페이스 하위 인터페이스 SVI
직접 포트 채널	단일 리프 스위치에 있는 일반 포트 채널	라우팅된 인터페이스* 하위 인터페이스* SVI
가상 포트 채널	두 개의 리프 스위치를 아우르는 vPC	SVI

* APIC Release 3.2(1)부터 지원되며 2 세대 이상의 리프 스위치에서만 지원

- **노드**
  인터페이스에 대한 보더 리프를 지정합니다. PC 또는 vPC 를 경로 유형으로서 선택할 때는 이 옵션을 사용할 수 없으며 필요하지도 않습니다. 그 이유는 사용자가 **경로**로 PC/vPC 인터페이스 정책 그룹의 이름을 선택해야 하는데 이 구성에는 노드 정보가 이미 포함되어 있기 때문입니다.
  이 노드 ID 는 상위 논리 노드 프로필의 노드 ID 와 일치해야 합니다.

- **경로**
  eth1/1 등 **경로 유형 포트**에 대한 인터페이스 ID, 또는 **경로 유형 PC 또는 vPC** 에 대한 PC/vPC 인터페이스 정책 그룹의 이름입니다.

- **캡슐화**
  경로 필드에서 구성된 인터페이스에 대한 VLAN ID 입니다. 이 VLAN ID 는 PI-VLAN(플랫폼 독립형 VLAN) 등의 일부 내부 ID 와는 다르게 캡슐화 또는 액세스 캡슐화 VLAN 이라고도 불립니다. SVI 가 사용될 때 이 VLAN ID 는 L3Out 과 연관된 라우팅된 외부 도메인(L3 Domain)의 VLAN 풀에 포함되어야 합니다. 라우팅된 인터페이스나 하위 인터페이스가 사용될 때는 L3 Domain 의 VLAN 풀은 필요하지 않습니다.

  - 라우팅된 인터페이스가 사용될 때는 이 필드가 필요하지 않으므로 표시되지 않습니다.
  - 하위 인터페이스가 사용될 때 이 캡슐화 VLAN 을 통해 하위 인터페이스가 생성됩니다.
  - SVI 가 사용될 때 이 캡슐화 VLAN 이 인터페이스에서 트렁크되며 지정된 리프에서 VLAN 에 대한 SVI 가 생성됩니다. 여러 트렁크 인터페이스가 포함된 한 개의 SVI 등 다양한 유형의 SVI 구성이 지원되지만(Figure 17), 동일한 인터페이스가 각기 다른 두 개의 SVI 에 각기 다른 두 개의 VLAN 을 트렁크해야 할 경우, 각 SVI 는 각기 다른 논리 인터페이스 프로필에서 구성되어야 합니다.

- **IPv4 기본 또는 IPv6 선호 주소**
  하위 인터페이스, 라우팅된 인터페이스 또는 SVI 상의 주요 IP 주소입니다. 이 IP 주소는 다른 라우팅 프로토콜 스피커로 피어링하는 데 사용됩니다.

- **IPv4 보조 또는 IPv6 추가 주소(선택 사항)**
  외부 장치가 고정 경로를 포함하는 한 개의 IP 를 가리킬 수 있도록 두 개의 보더 리프 스위치에서 공통의 IP 가 필요할 때, 별도의 IP 주소를 정의하는 데 유용합니다.

- **MAC 주소(선택 사항)**
  하위 인터페이스, 라우팅된 인터페이스 또는 SVI 에 대한 MAC 주소입니다. 대부분의 경우 이 필드는 기본값으로 둘 수 있습니다. SVI 또는 하위 인터페이스에 대한 기본 MAC 주소 변경은 외부 장치에서 MAC 플랩을 방지하기 위해 필요할 수도 있습니다. 그 이유는 ACI 에서 모든 인터페이스에 대해 기본적으로 동일한 MAC 주소를 사용하기 때문입니다. 예를 들어 두 개의 보더 리프 스위치가 vPC 가 없이 동일 VLAN 의 동일한 외부 장치에 연결될 경우, 해당 외부 장치에서는 두 개의 보더 리프 스위치 간에 MAC 플래핑 현상이 발생하게 됩니다. 이 문제는 각기 다른 보더 리프 스위치의 SVI 에 고유의 MAC 주소를 지정하여 해결할 수 있습니다.

- **MTU(바이트)(선택 사항)**
  하위 인터페이스, 라우팅된 인터페이스 또는 SVI 에 대한 MTU(최대 전송 유닛) 값을 바이트로 나타낸 것입니다. 기본 "상속"은 APIC 가 9,000 바이트의 ACI 기본 MTU 로 인터페이스를 구성한다는 의미이므로, 라우팅 프로토콜에 따라 조정이 필요할 수 있습니다. 대부분의 라우터 인터페이스에서는 점보 프레임을 기본값으로 사용하지 않으며, OSPF 나 EIGRP 와 같은 라우팅 프로토콜은 라우터 인터페이스 간의 MTU 가 일치하지 않는 한 피어링을 올바르게 설정하지 않습니다.

- **링크 로컬 주소(선택 사항)**
  하위 인터페이스, 라우팅된 인터페이스 또는 SVI 에 대한 IPv6 링크 로컬 주소입니다. ACI 에서는 기본적으로 각 리프의 시스템 MAC 주소의 IPv6 링크 로컬 주소를 EUI-64 형식으로 생성합니다.

참고:

다음 명령어는 필요한 경우 리프 스위치의 시스템 MAC 주소를 확인하여 IPv6 링크 로컬 주소를 계산하는 방법을 나타낸 것입니다.

```
leaf1# show sprom backplane | grep 'MAC Address'
 MAC Addresses    : 01-23-45-67-89-ab
```

참고:

SVI 의 경우, IP 주소가 **경로**마다 구성되더라도 SVI IP 주소는 L2 인터페이스마다 구성될 필요가 없습니다. 동일한 SVI 와 그 IP 주소를 여러 L2 인터페이스에 배포해야 할 경우, Figure 17 에 나와 있는 구성을 적용하여 이를 달성할 수 있습니다.

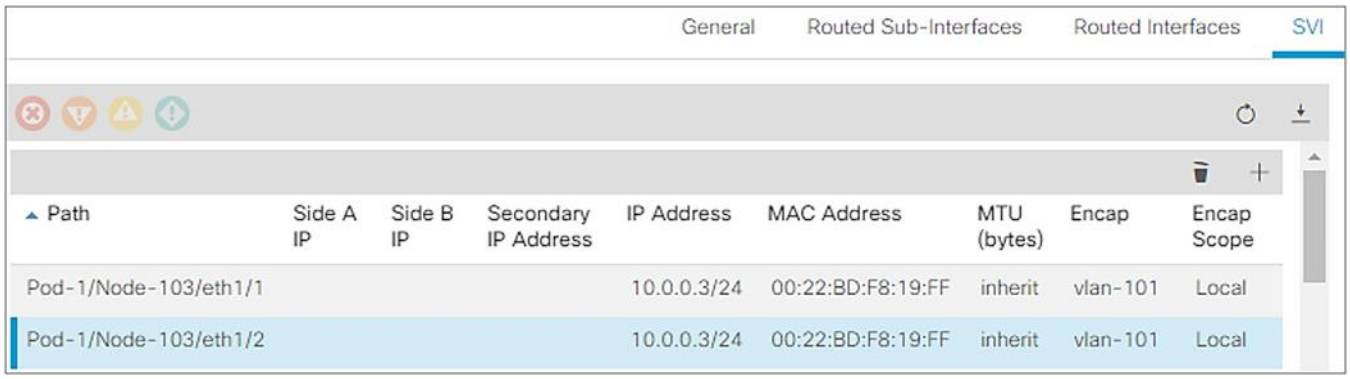

Figure 17.
SVI 로서 서로 다른 두 개의 경로에 동일한 VLAN 을 구성하는 방법

L3Out 브리지 도메인

L3Out SVI 가 인스턴트화되면 Cisco ACI 에서는 SVI 가 계층 2 초과 도메인을 제공할 수 있도록 내부에서 브리지 도메인(BD)을 생성합니다. 이 BD 를 일컬어 L3Out BD 또는 외부 BD 라고하며, APIC 에서 사용자에게 일반적인 BD 로 표시되지 않습니다. L3Out BD 는 L3Out SVI 의 각 액세스 캡슐화 VLAN 에 대해 내부적으로 생성되나, 일반적인 BD 에는 동일한 초과 도메인에 매핑된 여러 액세스 캡슐화 VLAN 이 포함될 수 있습니다. 이 L3Out BD 에는 다른 보더 리프 스위치도 동일한 L3Out 에서 L3Out SVI 의 동일한 액세스 캡슐화 VLAN 을 사용하는 경우, 여러 개의 보더 리프 스위치가 포함될 수 있습니다.

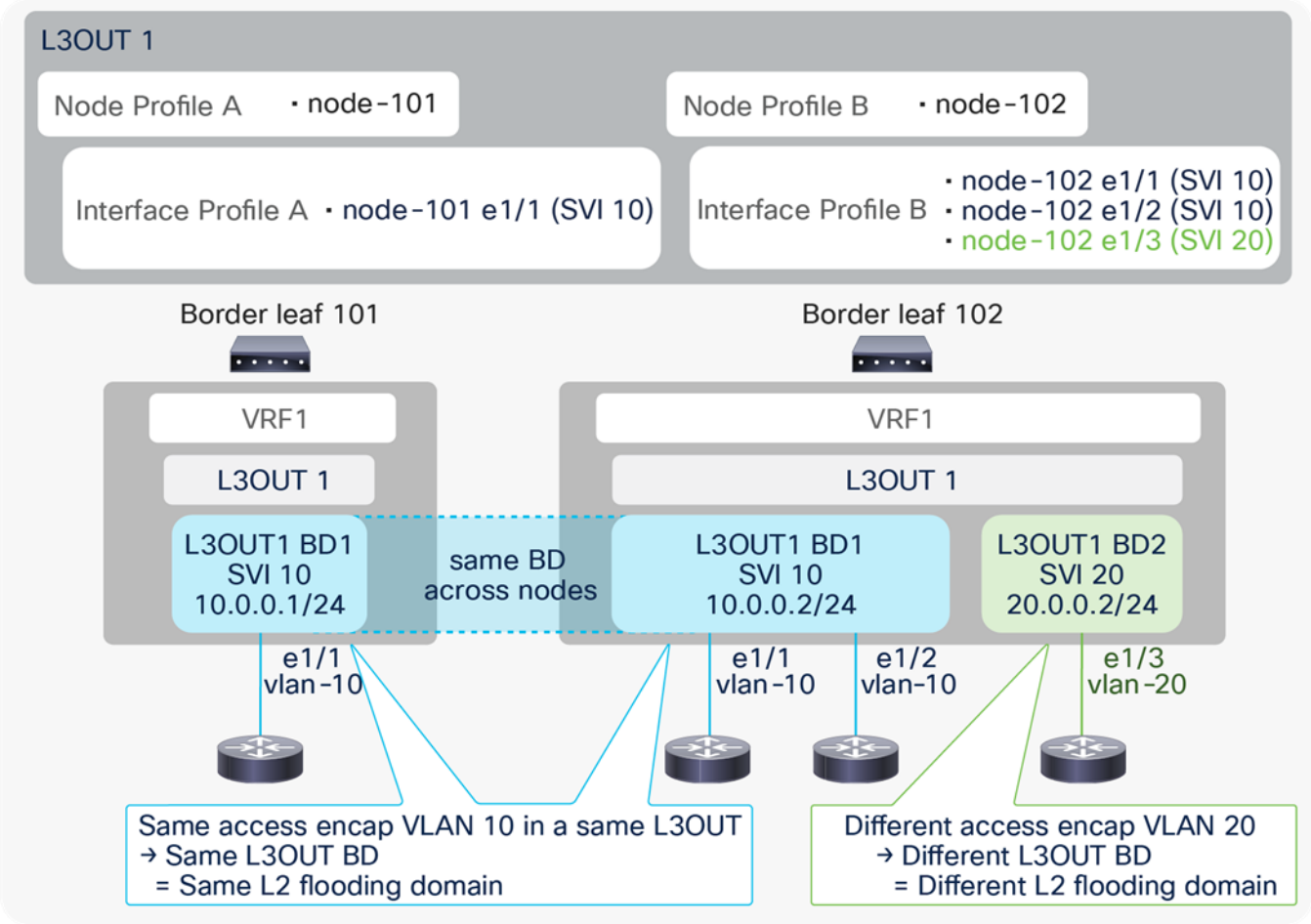

Figure 18.

L3Out BD 및 액세스 캡슐화 VLAN(동일한 L3Out 내)

Figure 18 에서 한 개의 L3Out 에는 여러 개의 노드와 인터페이스 프로필이 포함된 서로 다른 두 개의 액세스 캡슐화 VLAN 인 10 과 20 이 있습니다. 이 Figure 에서 동일한 액세스 캡슐화 VLAN 10 이 포함된 세 개의 라우터 모두 동일한 L3Out BD1 에 속합니다. 이는 L3Out BD 가 노드 프로필 및 인터페이스 프로필과는 별개라는 점을 나타냅니다. L3Out BD 의 인스턴트화는 캡슐화 VLAN ID 에만 의존합니다.

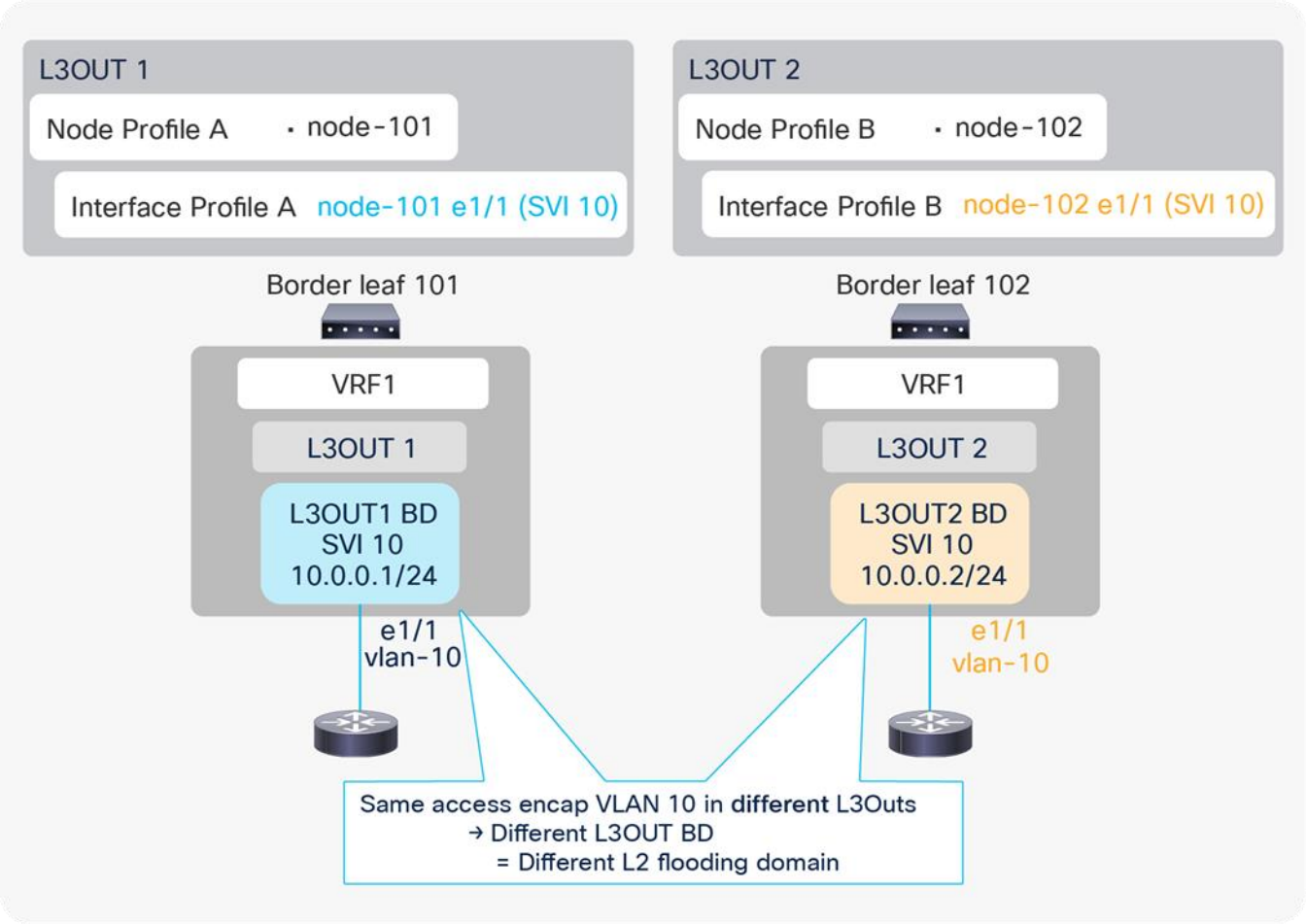

Figure 19.

L3Out BD 및 액세스 캡슐화 VLAN(서로 다른 L3Out 내)

Figure 19 에서 L3Out BD 는 **L3Out 내에서** 액세스 캡슐화 VLAN 마다 생성됩니다. 두 개의 L3Out 이 동일한 액세스 캡슐화 VLAN 을 사용하더라도, 각 L3Out 에서는 고유의 L3Out BD 가 생성됩니다. 따라서 동일한 액세스 캡슐화 VLAN ID 를 사용하는 여러 개의 L3Out 은 동일한 보더 리프에서 공존할 수 없습니다. 이 방식은 L3Out SVI 의 SVI 캡슐화 범위 옵션을 통해 변경할 수 있습니다.

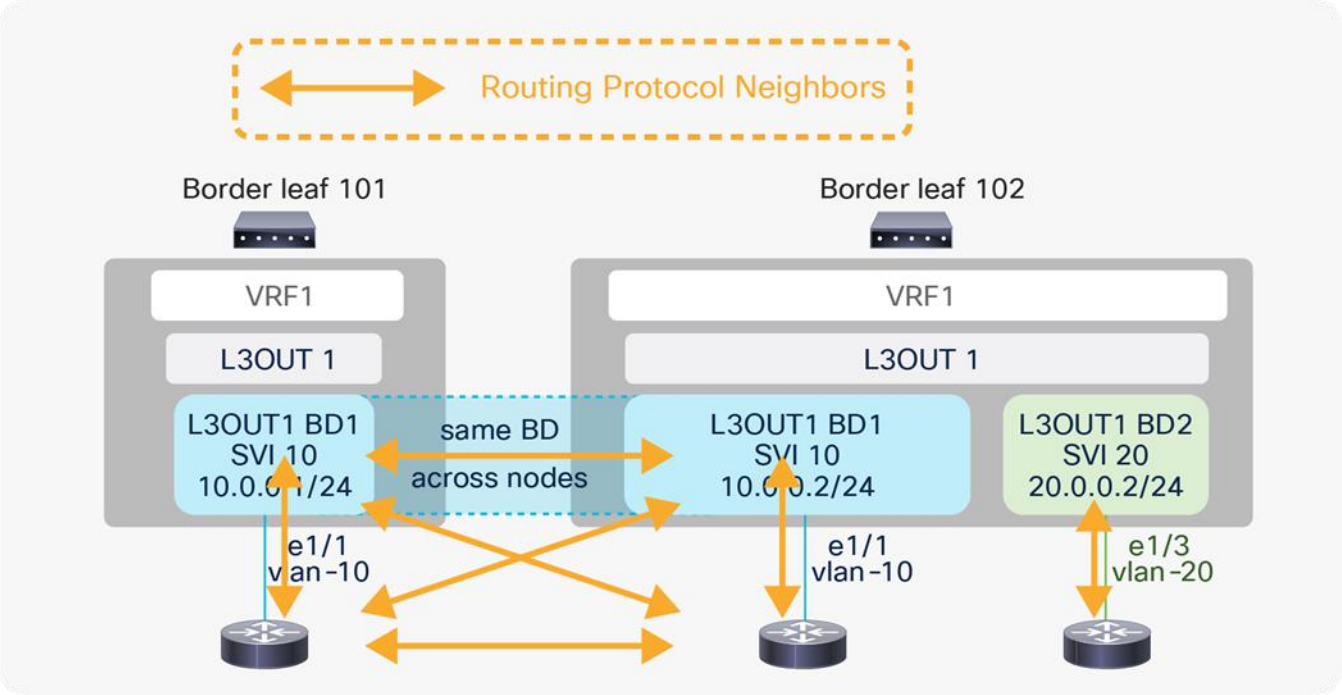

Figure 20.
L3Out BD 및 라우팅 프로토콜 인접 라우터

Figure 20 에서 동일한 L3Out BD 에 연결된 외부 라우터는 ACI 를 통해 프로토콜 Hello 를 교환하고, ACI 보더 리프 스위치에서 서로 간에 인접 라우터가 됩니다. 그러나 라우팅 프로토콜이 BGP 인 경우에는 BGP 피어가 계층 2 도메인 내로 제한되지 않기 때문에 이는 중요하지 않습니다.

SVI 캡슐화 범위

SVI 캡슐화 범위 옵션은 APIC Release 2.3(1)에서 도입되었습니다. 이 옵션은 **Tenant > Networking > External Routed Networks > L3Out > Logical Node Profiles > Logical Interface Profiles > SVI 탭**에서 찾을 수 있습니다. 구성 가능한 옵션은 "VRF"와 "로컬"입니다. 기본값은 "로컬"로 설정되어 있습니다. 이전 "L3Out 브리지 도메인" 서브섹션에서 설명한 바와 같이 이 설정에서는 이전 ACI 버전과 동일한 방식이 제공됩니다.

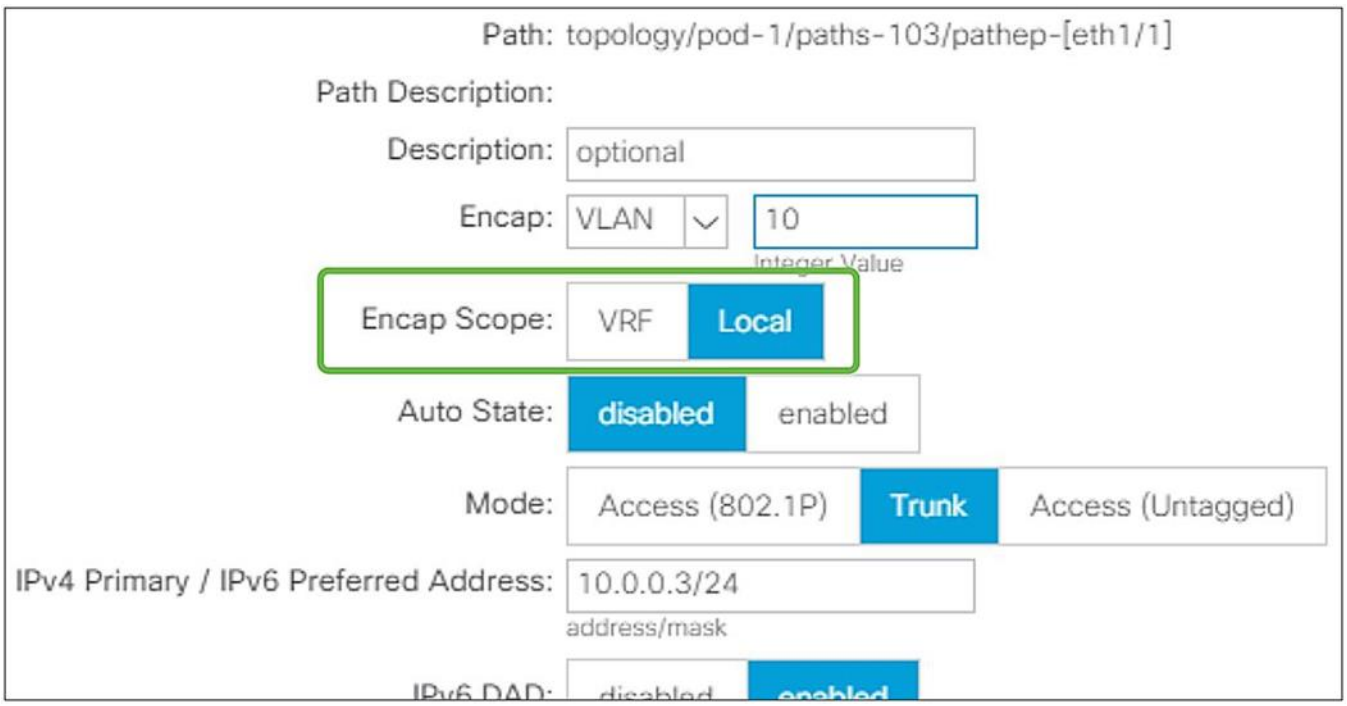

Figure 21.

GUI(APIC Release 3.2) 내 L3Out SVI 캡슐화 범위

SVI 캡슐화 범위 "VRF"에서는 동일한 VRF 에서 여러 개의 L3Out 이 L3Out BD 를 공유할 수 있는데, 이로써 동일한 리프에서도 동일한 액세스 캡슐화 VLAN 이 공유됩니다. 이 기능의 주요 시나리오는 다음과 같습니다.

- 시나리오 1: 동일한 리프에 있는 동일한 SVI 의 여러 라우팅 프로토콜
- 시나리오 2: 동일한 리프에 있는 각 BGP 피어에 대한 세부 경로 제어(각 BGP 피어에 대해 전용 L3Out 을 사용)

각 시나리오의 자세한 내용은 아래에 기술되어 있습니다.

시나리오 1: 동일한 리프에 있는 동일한 SVI 의 여러 라우팅 프로토콜

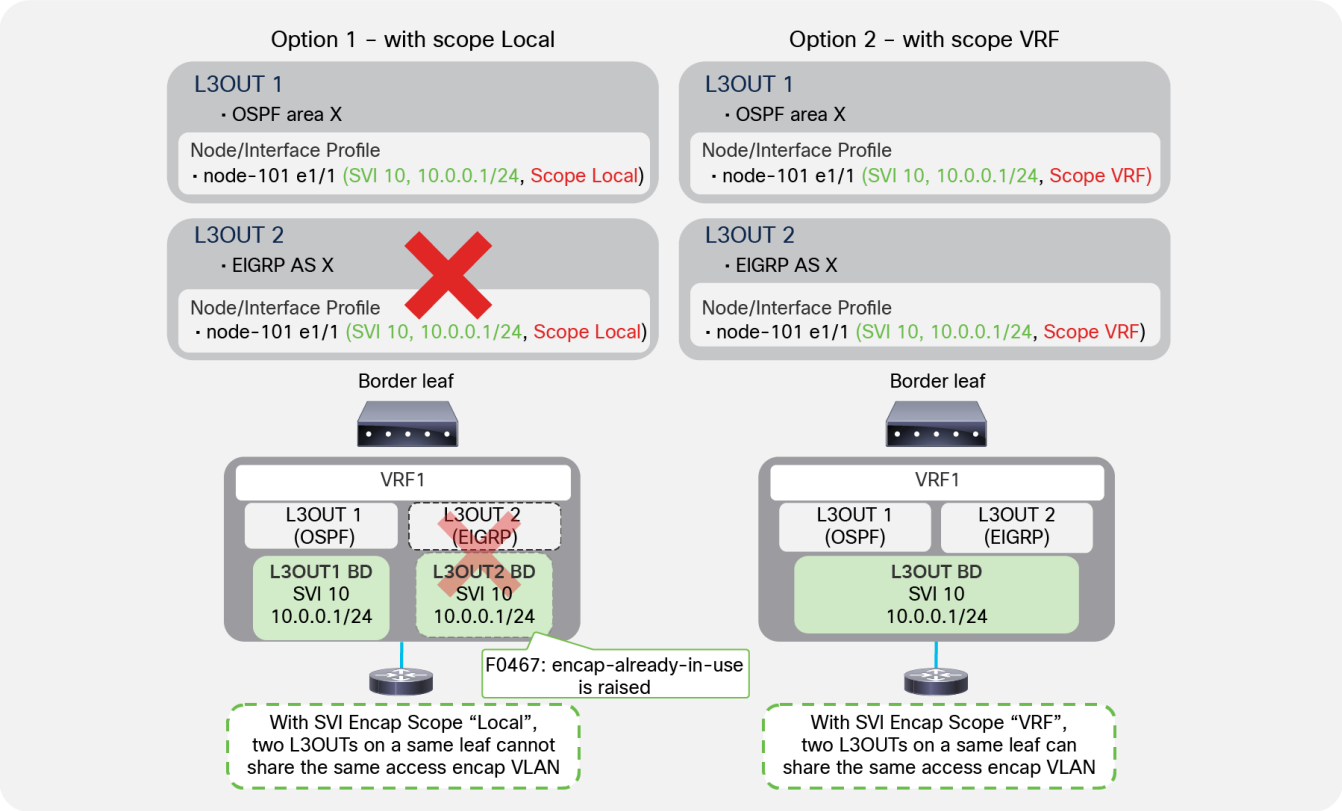

Figure 22.

SVI 캡슐화 범위가 포함된 동일한 SVI 에 있는 여러 라우팅 프로토콜

"L3Out 브리지 도메인" 서브섹션에서 기술한 바와 같이 기본값 또는 SVI 캡슐화 범위 "로컬"로, 각 L3Out 에서 액세스 캡슐화 VLAN 마다 L3Out BD/SVI 를 배치합니다. 따라서 동일한 액세스 캡슐화 VLAN 을 사용하는 두 개의 L3Out 은 동일한 보더 리프에서 공존할 수 없습니다. ACI 에서는 각 L3Out 이 한 개의 라우팅 프로토콜에 대해서만 구성될 수 있습니다. 즉, 기본적으로 특정 리프에 있는 한 개의 L3Out SVI 는 여러 개의 라우팅 프로토콜을 실행할 수 없습니다. BGP 와 OSPF 는 예외인데, 이는 ACI 가 동일한 L3Out 에서 OSPF 와 BGP 의 구성으로 BGP 에 대한 IGP 연결성을 제공하도록 허용하기 때문입니다.

Figure 22 에서와 같이, 두 개의 L3Out 에 있는 IP 주소처럼 동일한 SVI 매개변수를 구성함으로써 SVI 캡슐화 범위 "VRF"를 통해 동일한 VLAN 캡슐화에 동일한 인터페이스의 동일한 리프로 두 개의 라우팅 프로토콜을 구성할 수 있습니다.

참고:

캡슐화 범위 "VRF" 옵션은 서로 다른 두 개의 OSPF 영역이 동일한 리프 스위치의 동일한 SVI 에 배포되어야 할 때도 유용한데, 이는 동일한 리프와 SVI 에서 OSPF 영역마다 한 개씩 두 개의 L3Out 을 구성할 수 있기 때문입니다.

시나리오 2: 동일한 리프의 각 BGP 피어에 대한 세부 경로 제어

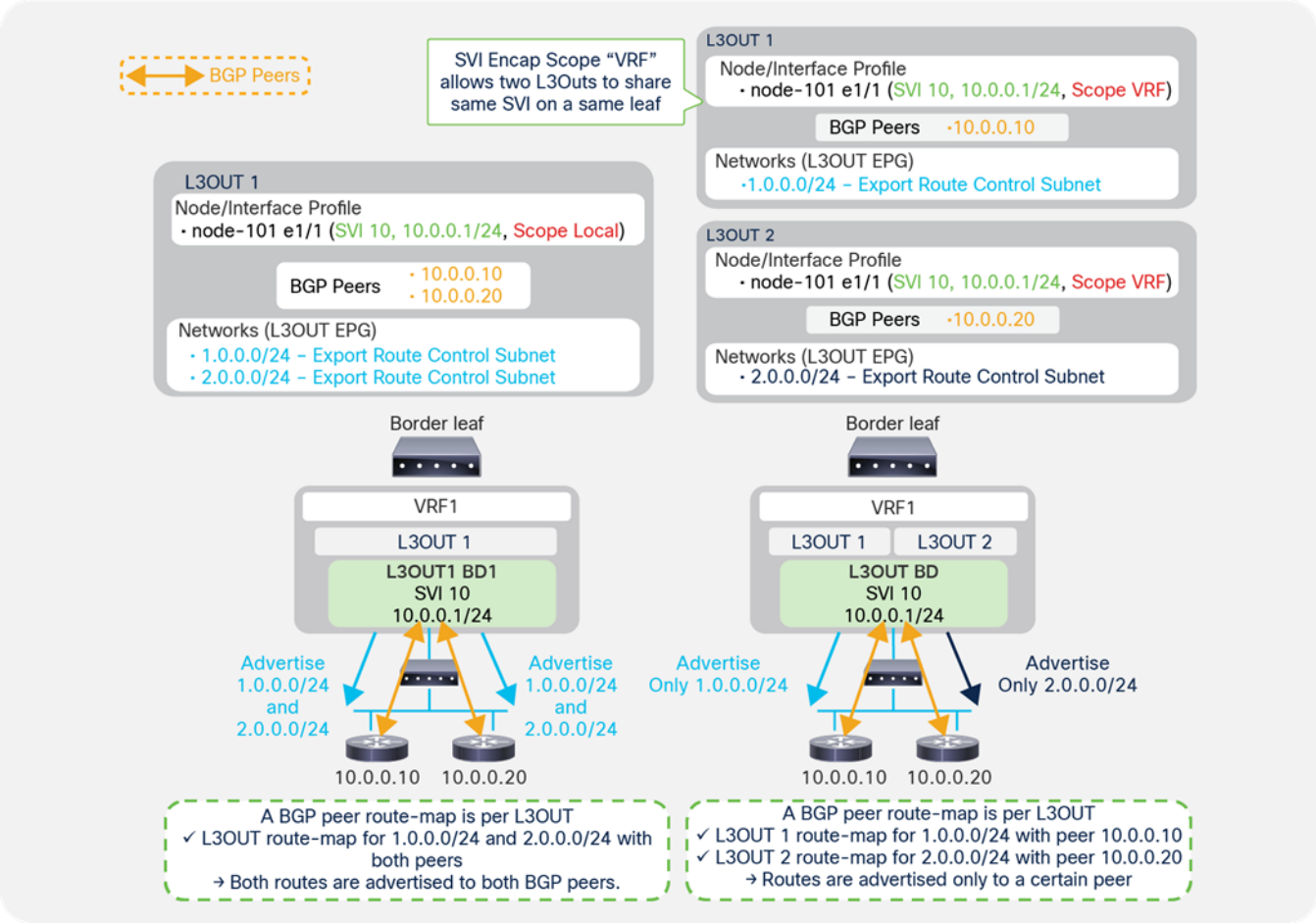

Figure 23.

일반적인 BGP 경로 제어(좌) 및 SVI 캡슐화 범위 VRF 가 포함된 세부 BGP 경로 제어(우)

경로 제어를 BGP 로 구성하고자 할 경우 "경로 제어 서브넷 내보내기"라는 이름의 구성을 사용해야 합니다. 이는 각 L3Out 별 구성입니다. BGP 의 경우 ACI 에서는 각 L3Out 와 각 리프별 경로 맵을 내부적으로 생성해 APIC 에서 구성된 경로 제어 정책을 적용합니다. 자세한 내용은 "L3Out 전송 라우팅" 섹션을 참조하시기 바랍니다.

이에 따라 여러 BGP 피어와 서로 다른 경로 제어 정책이 각 피어에 적용되어야 할 경우, 각 BGP 피어에 별도의 L3Out 이 필요합니다. 각 BGP 피어가 서로 다른 보더 리프 스위치에 연결되어 있는 경우 각 피어에 대해 L3Out 을 생성해도 무방합니다. 그러나 모든 BGP 피어가 동일한 보더 리프에 연결되어 있는 경우에는 기본적으로 각 BGP 피어에 대해 상이한 VLAN 또는 SVI 를 사용해야만 가능합니다. 그 이유는 서로 다른 두 개의 L3Out 에서 동일한 리프의 동일한 액세스 캡슐화 VLAN 을 사용할 수 없기 때문입니다.

Figure 23 에서와 같이 각 BGP 피어에 대해 서로 다른 두 개의 VLAN 을 보유할 수는 있지만, 다중 홉 L3 인접 라우터가 될 수 있는 BGP 피어의 특성으로 인해 보더 리프에 연결된 단일 라우터 또는 스위치 뒤에는 보통 여러 개의 BGP 피어가 존재합니다. 이러한 상황에서는 각 BGP 피어에 대해 서로 다른 두 개의 VLAN 을 보유하기가 어렵습니다.

SVI 캡슐화 범위 "VRF" 옵션이 포함된 APIC Release 2.3(1)부터는 동일한 VRF 에 있는 여러 개의 L3Outs 에서 동일한 액세스 캡슐화 VLAN/SVI 를 공유할 수 있는데, 그 이유는 액세스 캡슐화 VLAN 마다 적용되는 L3Out BD 이 여러 개의 L3Out 을 포함할 수 있기 때문입니다. 결과적으로 다양한 경로 제어 규칙이 동일한 VLAN/SVI 뒤에 있는 각 BGP 피어에 사용될 수 있도록 여러 개의 BGP L3Out 을 동일한 보더 리프에 동일한 VLAN/SVI 로 배포할 수 있습니다(Figure 23 의 우측 참조).

참고:

SVI 캡슐화 범위 "VRF" 옵션이 포함된 이 피어별 경로 제어는 BGP 에만 적용되는데, 그 이유는 ACI 가 BGP 와는 달리 L3Out 이 아닌 VRF 마다, 그리고 OSPF 와 EIGRP 에 대한 리프마다 경로 맵을 생성하기 때문입니다. "경로 제어 서브넷 내보내기" 등의 경로 제어 정책에 대한 자세한 내용은 "L3Out 서브넷 범위 옵션" 또는 "L3Out 전송 라우팅" 섹션을 참조하시기 바랍니다.

참고:

시나리오 1 과 2 모두 IP, MTU 등 동일한 리프에 대한 SVI 매개변수가 두 L3Out 에서 모두 동일해야 합니다. 이는 보더 리프에서 동일한 SVI 에 매개변수가 반드시 적용되어야 하며 충돌이 없어야 하기 때문입니다.

참고:

APIC Release 4.2(1)에 도입된 "BGP 피어별 경로 맵" 기능을 사용하면 시나리오 2(BGP 피어별 경로 제어)도 실현할 수 있습니다.

SVI 자동 상태

SVI 자동 상태 옵션은 APIC Release 2.2(3) 및 3.1(1)에서 도입되었으며 3.0(x)에서는 제공되지 않습니다. 이 옵션은 **Tenant > Networking > External Routed Networks > L3Out > Logical Node Profiles > Logical Interface Profiles > SVI 탭**에서 찾을 수 있습니다. 기본값으로 비활성화되어 있어 이전 ACI 버전과 동일한 기능을 제공합니다.

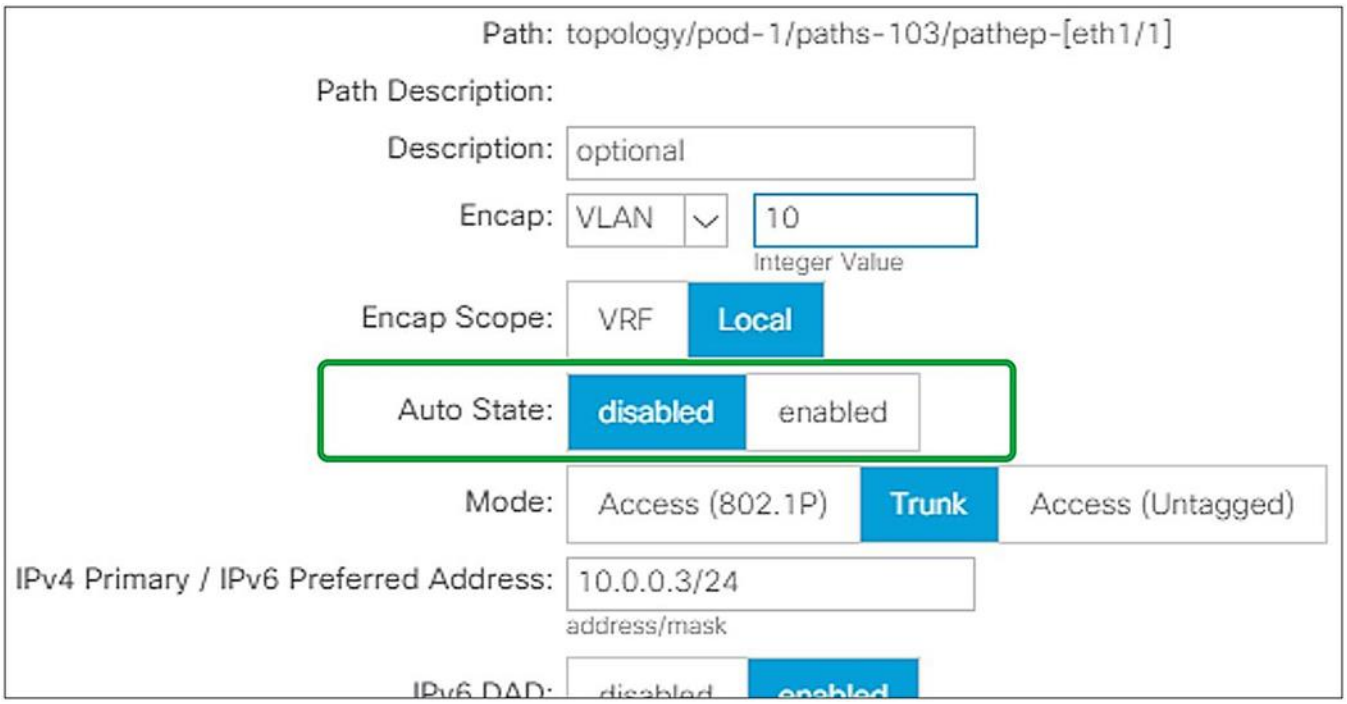

Figure 24.
GUI(APIC Release 3.2) 내 L3Out SVI 자동 상태

ACI 에서는 VLAN 멤버 포트의 상태에 관계없이 리프의 SVI 가 항상 작동합니다. 이는 일반적으로는 문제가 되지 않지만 고정 경로를 사용할 때는 문제가 발생할 수 있습니다. SVI 자동 상태를 활성화하면 VLAN 멤버 포트가 모두 작동하지 않을 때 보더 리프로 L3Out SVI 의 작동을 해제할 수 있습니다. 다음은 SVI 자동 상태의 사용 사례입니다.

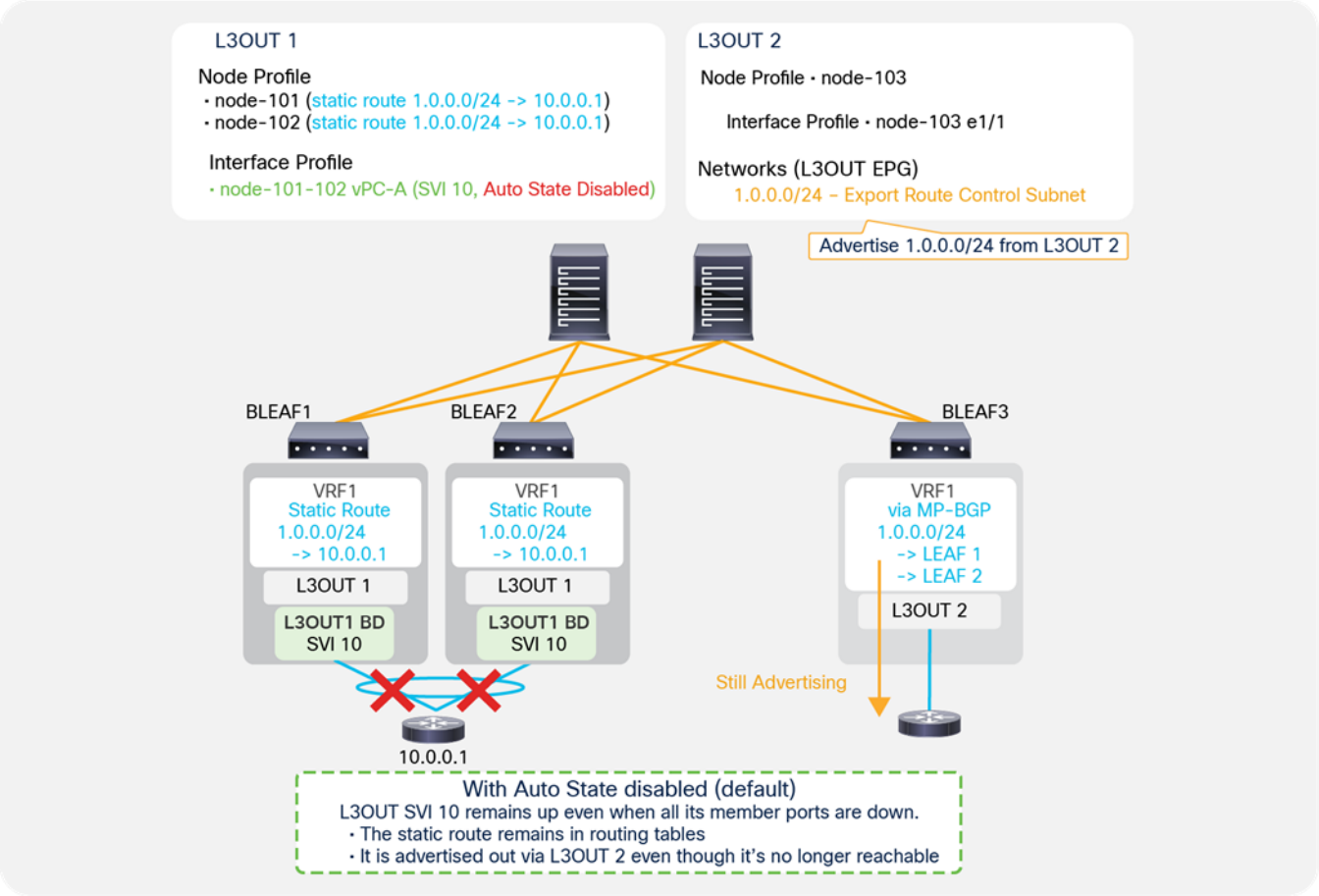

Figure 25.

고정 경로가 포함되고 비활성화된 SVI 자동 상태

Figure 25 에서는 SVI 자동 상태가 비활성화되었을 때 고정 경로 관련 문제점을 나타냅니다. Figure 25 의 L3Out 에는 vPC 가 포함되고 SVI 자동 상태가 비활성화된 보더 리프 스위치 1 과 2 에서 구성된 SVI 10 이 있습니다. 이 외에도 L3Out 1 에는 리프 1 과 리프 2 에서 구성된 고정 경로 1.0.0.0/24 가 포함되어 있습니다. 반면 Figure 25 의 L3Out 2 는 1.0.0.0/24 에 대해 리프 3 의 라우팅 테이블에 있을 경우 1.0.0.0/24 의 재배포 시도하는 "경로 제어 서브넷 내보내기"를 통해 리프 3 에 배포됩니다. 이 경우 리프 1 과 리프 2 의 외부 라우터 10.0.0.1 에 연결된 vPC 인터페이스가 중단되고 VLAN10 의 멤버 포트가 없더라도 SVI 자동 상태가 비활성화되어 있으므로 리프 1 과 리프 2 의 L3Out 10 은 작동이 유지됩니다. 따라서 SVI 10 서브넷의 다음 홉을 보유한 고정 경로가 각 라우팅 테이블에서 유지됩니다. ACI 패브릭에는 이제 해당 경로에 대한 연결 가능성이 없지만 리프 3 에서는 MP-BGP 를 통해 수신한 경로를 열람할 수 있고, 재배포와 보급이 실행됩니다. 이를 방지하기 위한 방법 중 하나로 L3Out SVI 10 에서 SVI 자동 상태를 활성화하는 것이 있습니다.

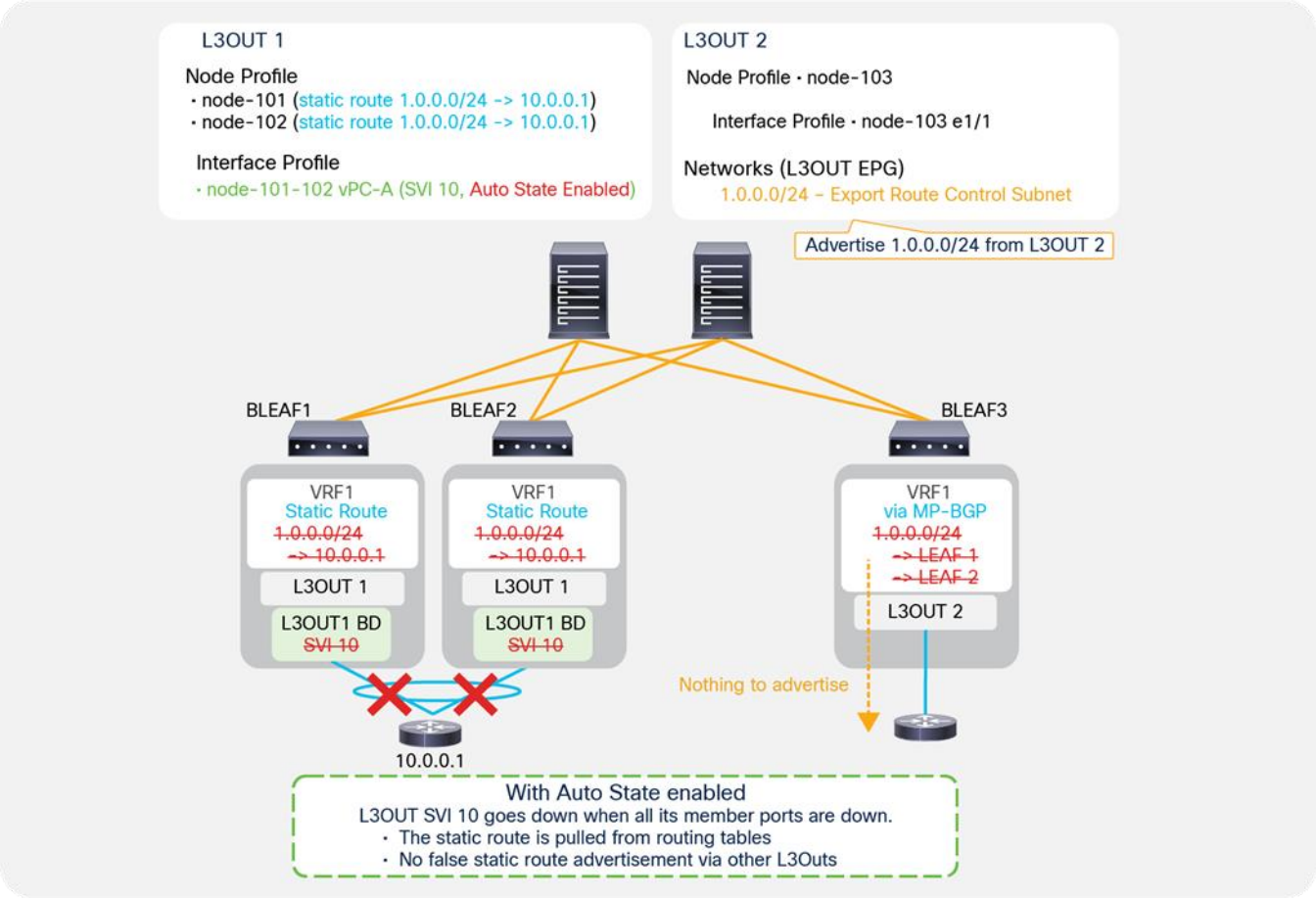

Figure 26.
고정 경로가 포함되고 활성화된 SVI 자동 상태

Figure 26 에서는 Figure 25 에서 거론된 문제를 해결할 수 있는 SVI 자동 상태를 활성화하는 방법을 설명합니다. SVI 자동 상태가 활성화되고 모든 VLAN 멤버 인터페이스(Figure 26 내 vPC 인터페이스)가 중지되면 리프 1 과 리프 2 의 L3Out SVI 10 역시 중지됩니다. 이에 따라 리프 1 과 2 에서는 SVI 10 서브넷의 다음 홉이 포함된 고정 경로를 제거합니다. 따라서 리프 3 에서는 MP-BGP 를 통해 1.0.0.0/24 를 더는 열람할 수 없으며 연결 불가능한 경로에 대한 재배포와 보급이 중지됩니다.

참고:

Figure 25 에서 언급된 문제는 SVI 자동 상태를 활성화하는 대안 선택으로서 고정 경로에 대한 BFD 를 사용하여 방지할 수 있습니다.

참고:

vPC 가 포함된 L3Out SVI 에서 자동 상태가 활성화될 경우, 두 개의 vPC 리프 스위치에서 모두 VLAN 멤버 포트가 중지될 때만 SVI 의 작동이 중지됩니다.

L3Out 고정 경로

Cisco ACI 에서 고정 경로는 L3Out 의 한 부분으로 구성됩니다. 고정 경로는 **"Tenant > Networking > External Routed Networks > L3Out > Logical Node Profiles > Node > Static Routes"**의 각 논리 노드 프로필에서 구성됩니다. 동적 라우팅 프로토콜 없이 오직 고정 경로만 필요할 경우, 사용자는 루트 L3Out 구성 요소의 동적 라우팅 프로토콜 확인란은 빈 칸으로 두고 고정 경로가 포함된 논리 노드 프로필과 논리 인터페이스 프로필만 구성하면 됩니다. 그러나 이 경우에도 루트 L3Out 구성 요소에서 VRF 와 라우팅된 외부 도메인은 연결해야 합니다.

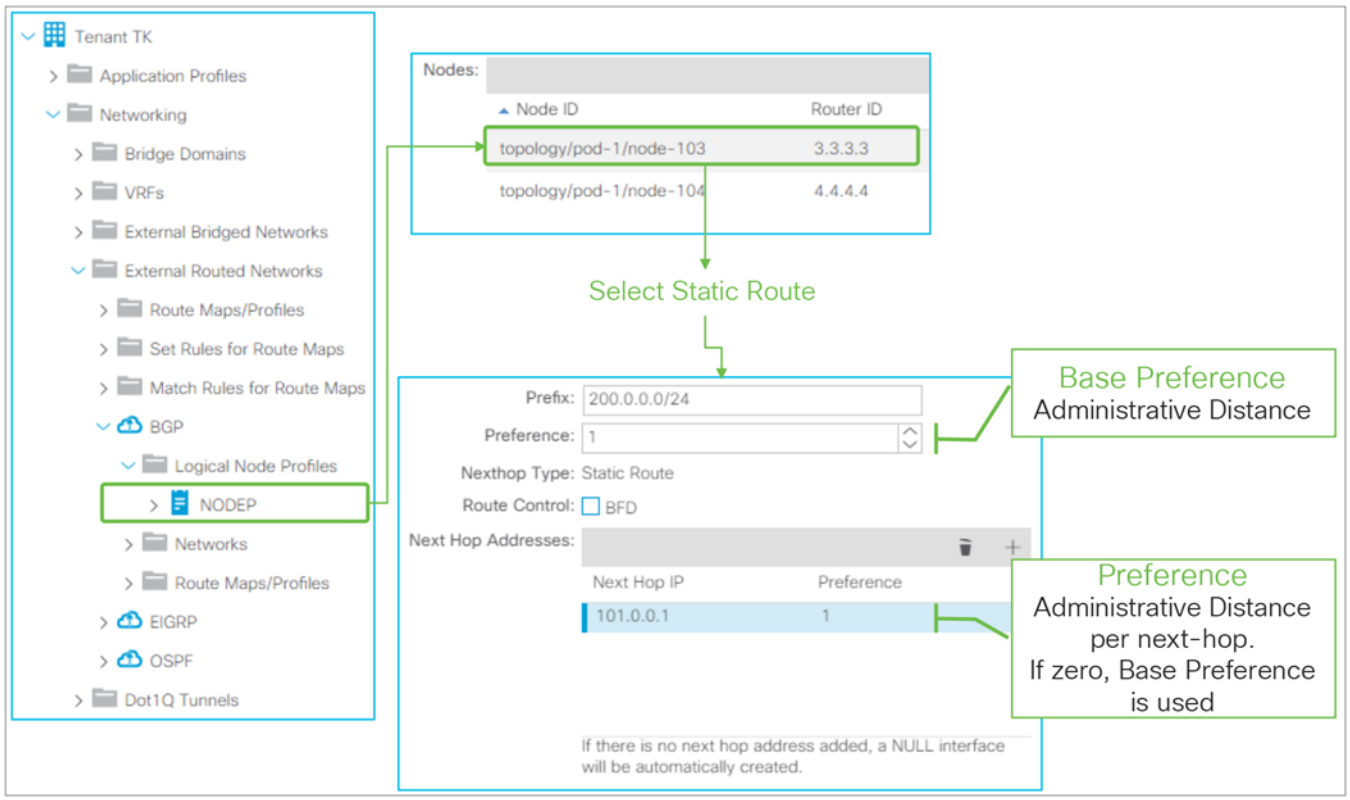

Figure 27.
GUI(APIC Release 3.2) 내 L3Out 고정 경로 구성

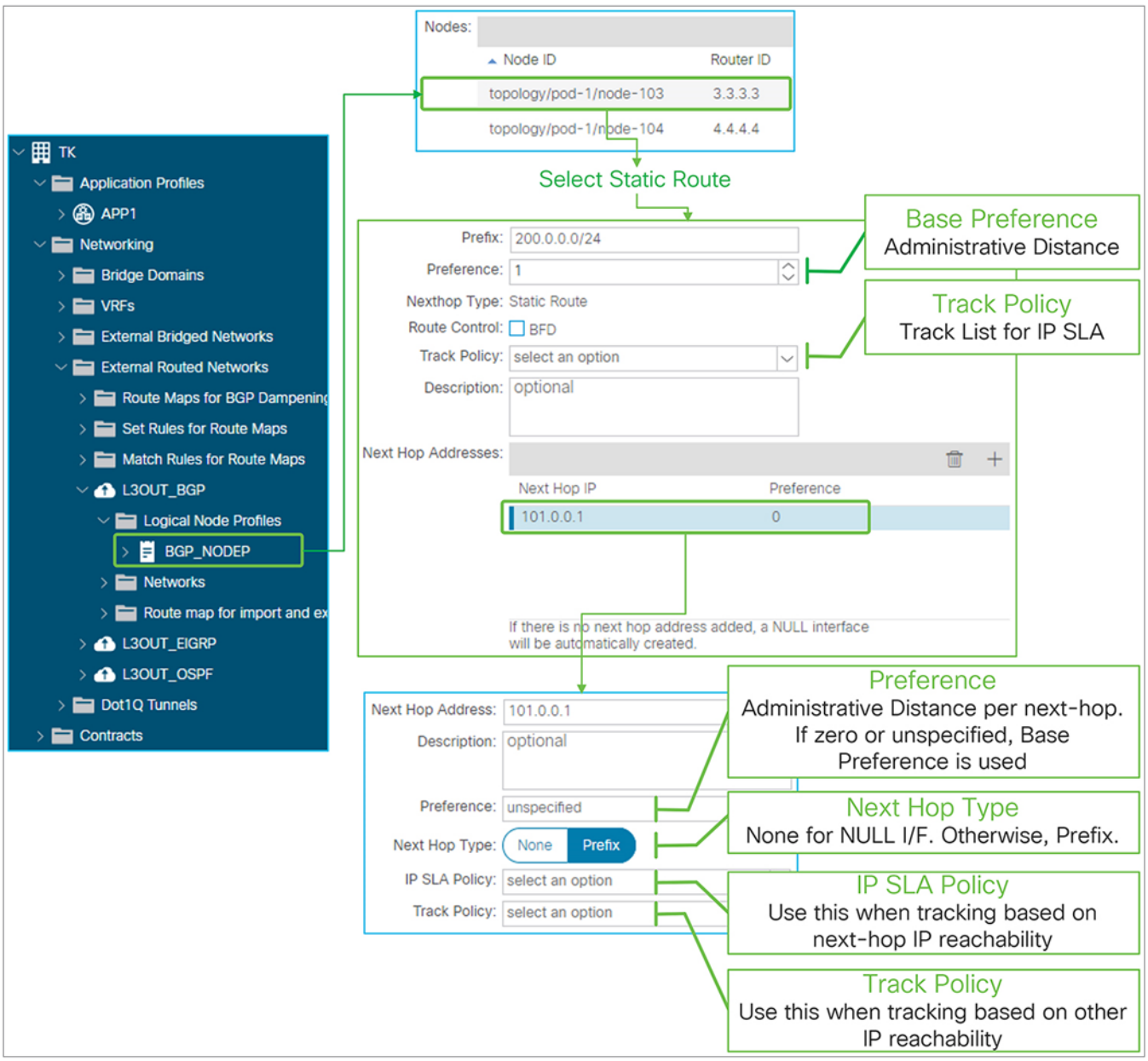

Figure 28.

GUI(APIC Release 4.1) 내 L3Out 고정 경로

- **식별 번호**

  고정 경로에 대한 식별 번호를 구성합니다.

- **선호 설정(기본 선호 설정)**

  고정 경로에 대한 관리 거리(AD)를 구성합니다. AD 는 각 고정 경로 또는 다음 홉마다 설정할 수 있습니다. 다음 홉 IP 주소에 대한 **선호 설정**이 지정되지 않거나 0 일 경우 AD 가 대안으로 사용되도록 본 선호 설정 옵션(**식별 번호** 필드 바로 아래)에서 구성할 수 있습니다.

- **경로 제어**

  고정 경로에서 양방향 전환 탐지(BFD)를 활성화합니다. 자세한 내용은 "L3Out BFD" 섹션을 참조하시기 바랍니다.

- **트랙 정책**

  APIC Release 4.1(1)에서 도입된 IP SLA 기능에 대한 사항입니다. 고정 경로의 유효성에 대한 지표로서 IP 주소 집합의 연결 가능성을 모니터링하는 트랙 정책을 설정합니다. 트래킹 구성은 고정 경로의 일환, 또는 다음 각 홉 주소로서 여러 가지 방법이나 세부 수준으로 수행할 수 있습니다. 고정 경로 수준의 트랙 정책(해당 필드)은 IP 주소 집합의 연결 가능성에 대한 정보를 라우팅 테이블에서 수집하고, 연결 가능성 조건이 충족되면 라우팅 테이블에서 고정 경로가 보존됩니다.

  개별 다음 홉의 유효성 역시 각 다음 홉 주소에 있는 트랙 정책 또는 IP SLA 정책의 두 가지 구성을 통해 별도로 모니터링할 수 있습니다. 다음 홉 주소에 대한 IP SLA 정책에서는 다음 홉 자체의 연결 가능성을 확인하는 방식(사용할 프로토콜)을 정의합니다. 반면 다음 홉 주소에 대한 트랙 정책에서는 다음 홉이 유효해지도록 다음 홉 주소 자체가 아닌, 확인할 IP 주소를 정의합니다.

  고정 경로과 각 다음 홉이 모두 트랙 정책이나 IP SLA 정책을 보유하고 있을 때는 고정 경로의 트랙 정책이 우선합니다. 자세한 내용은 아래의 "L3Out 고정 경로에 대한 IP SLA 트래킹" 섹션을 참조하시기 바랍니다.

- **다음 홉 주소**

  고정 경로에 대한 다음 홉 IP 주소를 구성할 목적으로, 동일한 고정 경로 식별 번호에 대해 한 개 이상의 다음 홉을 구성할 수 있습니다. APIC Release 1.2(2)부터 구성된 **다음 홉 주소** 항목이 없을 경우 Null-0 다음 홉이 자동으로 생성됩니다.

  - 다음 홉 IP

    고정 경로에 대해 다음 홉으로 사용될 IP 주소

  - 선호 설정

    해당 다음 홉 IP 에 대한 관리 거리 0 이거나 지정되지 않았을 경우 ACI 에서는 하드웨어를 프로그래밍하기 위해 **기본 선호 설정**을 사용합니다.

  - 다음 홉 유형

    없음 또는 식별 번호로 처리 가능 '없음'은 NULL 인터페이스에 대한 사항입니다. '없음'에서는 다음 홉 IP 가 반드시 0.0.0.0/0 여야 합니다. 식별 번호는 NULL(0.0.0.0/0) 대신 실제 다음 홉 IP 를 지정합니다.

    해당 옵션은 고정 경로에 대한 NULL 다음 홉과 NULL 이 아닌 다음 홉을 동시에 보유하기 위해 APIC Release 4.1(1)에서 도입되었습니다. Release 4.1(1) 이전에 고정 경로는 NULL 다음 홉 또는 NULL 이 아닌 다음 홉 중 하나만 보유할 수 있었습니다.

  - IP SLA 정책

    이 옵션은 트랙 정책을 사용하는 방식 대신 다음 홉 IP 에서 바로 IP SLA 정책을 설정합니다. 트랙 정책으로 그룹화 및 모니터링되는 기타 IP 주소 대신 다음 홉 IP 자체를 프로빙해 다음 홉 사용 가능성을 추적하는 것이 목적입니다. SLA 조건이 충족되지 않으면 라우팅 테이블에서 다음 홉이 제거됩니다.

    다음 홉 주소 항목에는 IP SLA 정책 또는 트랙 정책 중 한 가지를 보유할 수 있으며 두 가지를 모두 보유할 수는 없습니다.

    IP SLA 정책과 트랙 정책은 APIC Release 4.1(1)부터 도입되었습니다. 자세한 내용은 "L3Out 고정 경로에 대한 IP SLA 트래킹" 서브섹션을 참조하시기 바랍니다.

- 트랙 정책

  본 구성에서는 ACI 에서 다음 홉 IP 를 직접 모니터링하지 않고, 고정 경로에 대한 해당 다음 홉 항목이 라우팅 테이블에서 유지되어야 할지 여부를 결정하기 위해 연결 가능성을 사용하는 IP 집합 주소를 정의합니다. 해당 트랙 정책에 중첩된 IP SLA 정책에서 정의되는 프로토콜을 사용해 트랙 정책에서 정의되는 IP 주소의 모니터링이 수행됩니다. 트랙 정책의 연결 가능성 조건이 충족되면 라우팅 테이블에서 다음 홉이 보존됩니다.

  다음 홉 주소 항목에는 IP SLA 정책 또는 트랙 정책 중 한 가지를 보유할 수 있으며 두 가지를 모두 보유할 수는 없습니다.

  IP SLA 정책과 트랙 정책은 APIC Release 4.1(1)부터 도입되었습니다. 자세한 내용은 "L3Out 고정 경로에 대한 IP SLA 트래킹" 서브섹션을 참조하시기 바랍니다.

L3Out 고정 경로에 대한 IP SLA 트래킹

APIC Release 4.1(1)에서 도입된 기능으로, IP 주소 집합을 프로빙해 L3Out 고정 경로의 유효성을 확인합니다. 트랙 목록에서는 모니터링할 IP 주소를 정의합니다. 본 목록에는 프로브 IP 주소와 IP SLA 방식, 각 트랙 멤버의 상태에 따라 계산된 값의 임곗값으로 구성된 트랙 멤버가 포함됩니다. 트랙 목록은 임곗값에 기반해 구성이 연결된 위치에 따라 고정 경로 자체 또는 다음 홉을 작동시키거나 중지합니다. 트랙 목록은 고정 경로 및/또는 다음 홉에 연결될 수 있습니다. 트랙 목록에서 구성된 임계점 조건에 기반해 연결 가능성이 충분하다는 점이 트랙 목록에서 나타날 경우 해당 고정 경로 및/또는 다음 홉은 라우팅 테이블 내에 보존됩니다. 트랙 목록이 고정 경로과 다음 홉에서 구성되고 해당 고정 경로에 대한 트랙 목록 자체가 중지 조건의 임계점을 충족할 경우, 고정 경로에 대한 다음 홉의 트랙 목록 상태에 관계없이 라우팅 테이블에서 전체 고정 경로가 제거됩니다.

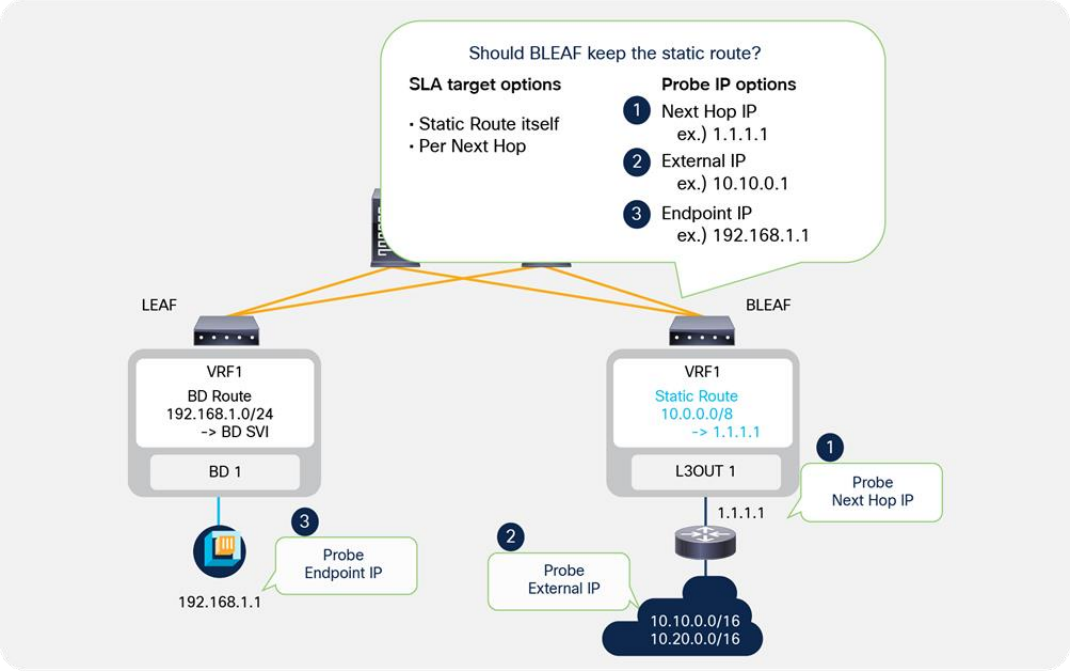

Figure 29.

L3Out 고정 경로에 대한 IP SLA

Figure 29 에 나타난 바와 같이 ACI 에서는 다음 홉 IP 자체와 외부 IP, 그리고 고정 경로와 연관이 있을 수 있는 엔드포인트 IP 를 프로빙할 수 있습니다.

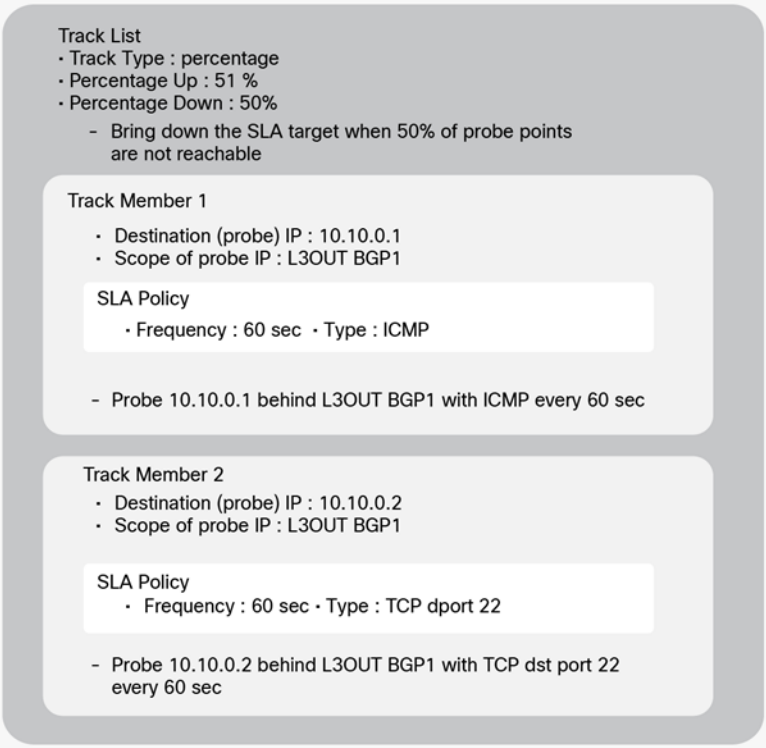

Figure 30.

L3Out 고정 경로에 대한 트랙 목록(IP SLA) 예시

Figure 30 은 트랙 목록 구성 요소와 구성에 대한 예시입니다. 이 트랙 목록에는 두 개의 트랙 멤버(프로브 IP)가 포함됩니다. 한 개는 60 초에 한 번씩 송신되는 프로빙 트래픽에서 사용되는 프로토콜인 ICMP 가 포함된 L3Out BGP1 뒤의 외부 IP 10.10.0.1(APIC GUI 내 트랙 멤버의 범위로 구성)에 대한 것이고, 또 한 개는 60 초에 한 번씩 송신되는 프로빙 트래픽인 TCP 대상 포트 22 가 포함된 L3Out BGP 1 뒤의 외부 IP 10.10.0.2 에 대한 것입니다. 이 트랙 목록에서는 임곗값 조건에 대해 퍼센트값을 사용하며 작동은 51%, 중지는 50%입니다. 따라서 트랙 멤버의 단 50%만 작동 중일 때는 트랙 목록이 중지로 표시됩니다. 본 예시에서는 트랙 멤버 중 한 개가 연결할 수 없는 상태가 되면 퍼센트값이 50%로 하락하고 트랙 목록이 중지로 표시됩니다. 작동 중인 트랙 멤버의 비율이 51%에 도달하면 트랙 목록은 다시 작동으로 표시됩니다. 본 예시에서는 두 개의 트랙 멤버 모두 다시 연결할 수 있는 상태가 되면 퍼센트값이 100%로 상승하고 트랙 목록은 다시 작동으로 표시됩니다.

이 트랙 목록은 고정 경로 또는 다음 홉 구성에 연결되어야 영향을 발휘합니다. 트랙 목록을 고정 경로 또는 다음 홉에 연결하려면 고정 경로 또는 다음 홉 구성에서 트랙 정책 입력란이 사용되어야 합니다.

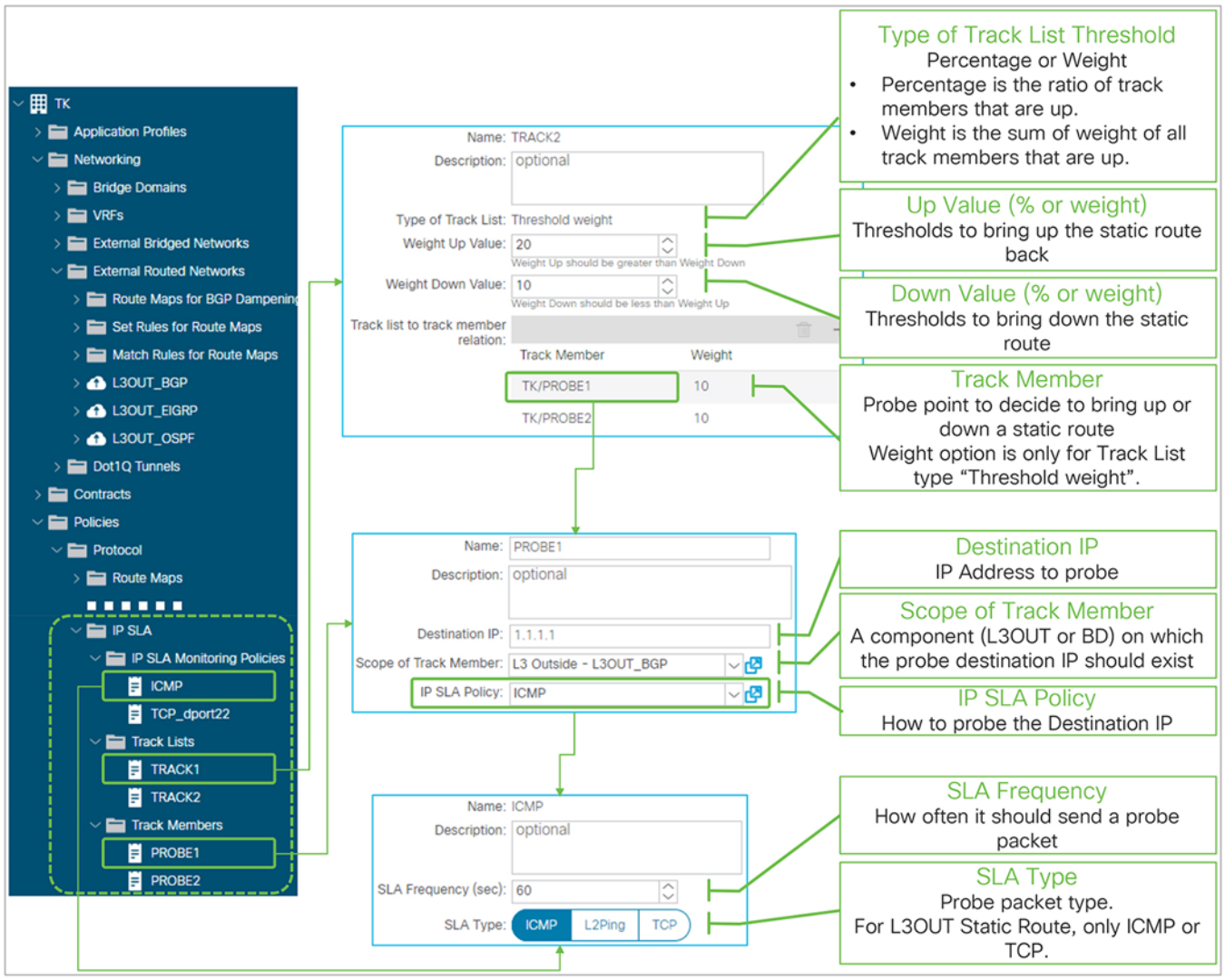

Figure 31.

GUI(APIC release 4.1) 내 L3Out 고정 경로에 대한 IP SLA(트랙 목록)

트랙 목록

- **트랙 목록 임곗값의 유형**

  퍼센트값 또는 중량값으로 표시됩니다. 트랙 목록이 생성되면 매개변수는 변경할 수 없습니다.

  퍼센트값 전체 멤버 수 대비 연결 가능한 트랙 멤버의 비율입니다.

  중량값 연결 가능한 트랙 멤버의 중량 합계입니다.

- **작동 값(퍼센트값 또는 중량값)**

  퍼센트값 또는 중량값이 이 값에 도달하면 이전에 중지로 표시되었을 경우 트랙 목록이 작동으로 표시됩니다. 이에 따라 해당 트랙 목록을 사용하는 고정 경로 또는 다음 홉이 라우팅 테이블에 작동 가능하도록 나타납니다.

- **중지 값(퍼센트값 또는 중량값)**

  퍼센트값 또는 중량값이 이 값에 도달하면 이전에 작동으로 표시되었을 경우 트랙 목록이 중지로 표시됩니다. 이에 따라 해당 트랙 목록을 사용하는 고정 경로 또는 다음 홉이 라우팅 테이블에 중지로 나타납니다.

트랙 멤버(프로브 IP)

트랙 멤버는 ACI 에서 프로브를 송신하는 IP, 해당 IP 의 연결 가능성을 검증하는 데 사용해야 하는 프로토콜, 사용 위치(L3Out, BD 등)를 정의하는 구성입니다. ACI 는 트랙 멤버에 대한 연결을 시도해야 합니다.

- **대상 IP**
  프로빙할 대상 IP 주소로, 고정 경로 및 외부 IP, 또는 엔드포인트 IP 의 다음 홉 IP 일 수 있습니다.
- **트랙 멤버의 범위**
  대상 IP 가 위치해야 하는 구성 요소(L3Out 또는 BD)입니다.
- **IP SLA 정책**
  사용할 프로토콜 및/또는 L4 포트와 관련해 대상 IP 의 프로빙 방법을 정의하는 IP SLA 모니터링 정책입니다.

IP SLA 모니터링 정책

- **SLA 주파수(초)**
  트랙 멤버 IP 를 프로빙하는 초 단위 주파수로, 기본값은 60 초입니다.
- **SLA 유형**
  프로빙 패킷에 사용될 프로토콜을 정의하는 유형입니다. L3Out 고정 경로 SLA 의 경우 대상 포트가 포함된 TCP 또는 ICMP 옵션이 지원됩니다.

참고:

L3Out 고정 경로에서 다음 홉의 트랙 목록 또는 IP SLA 정책을 구성하는 것은 기능적으로 동일합니다. 다음 홉의 IP SLA 정책은 APIC 가 프로브 IP(대상 IP) 및 IP SLA 정책으로서 다음 홉 IP 를 사용해 한 개의 트랙 멤버가 포함된 트랙 목록을 내부적으로 간단하게 생성하는 방법입니다. 이는 트랙 목록을 수동으로 구성하여 이를 트랙 정책에 연결하는 것에 해당합니다.

L3Out BGP

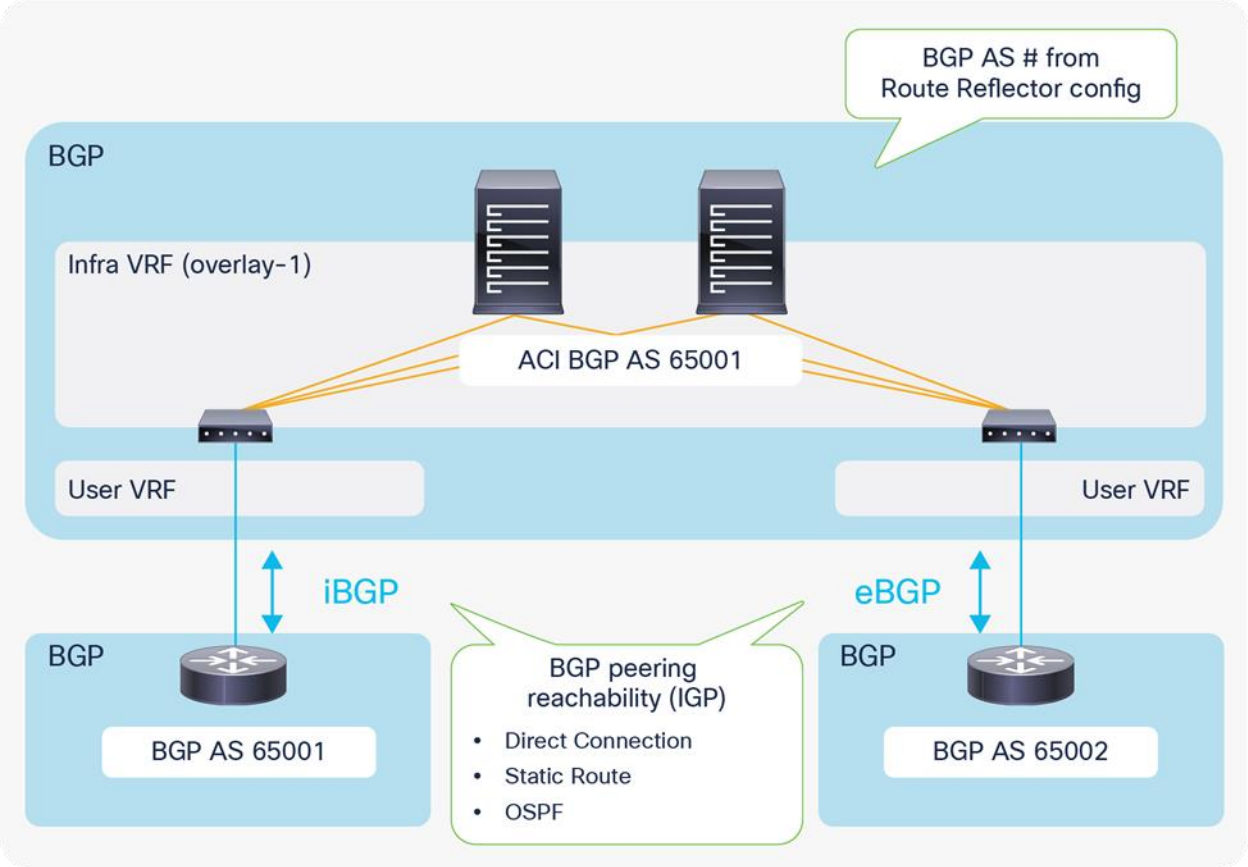

Figure 32.
ACI 및 BGP AS

L3Out 에는 사용자가 구성 리플렉터와 BGP AS 번호를 구성하는 인프라 MP-BGP 가 필요합니다. 인프라 MP-BGP 를 위한 해당 BGP AS 번호는 ACI BGP AS 이며, BGP 가 포함된 L3Out 은 동일한 BGP AS 에 자동으로 속하게 됩니다. 따라서 Figure 32 에 나타난 바와 같이 피어에서 BGP AS 가 다른 객체로 인식되도록 ACI 가 BGP 피어 연결성 프로필의 local-AS 구성을 사용하지 않는 한 외부 장치는 ACI BGP AS 로 피어링해야 합니다. APIC Release 1.1(1)부터 EBGP 연결성 지원이 추가되었습니다.

iBGP 와 eBGP 모두에 대한 BGP 피어링 IP 연결 가능성을 지원하는 방법 또는 IGP 는 다음과 같습니다.

- 직접 연결
- 고정 경로
- OSPF

iBGP 와 eBGP 모두에 대한 BGP 피어링을 지원하는 소스 인터페이스는 다음과 같습니다.

- 논리 노드 프로필의 루프백 인터페이스
- 라우팅된 인터페이스, 라우팅된 하위 인터페이스, 논리 인터페이스 프로필의 SVI

참고:

2 차 IP 주소가 인터페이스에서 구성되더라도 BGP 세션은 각 인터페이스의 기본 IP 주소에서만 공급됩니다.

기본 구성 예시

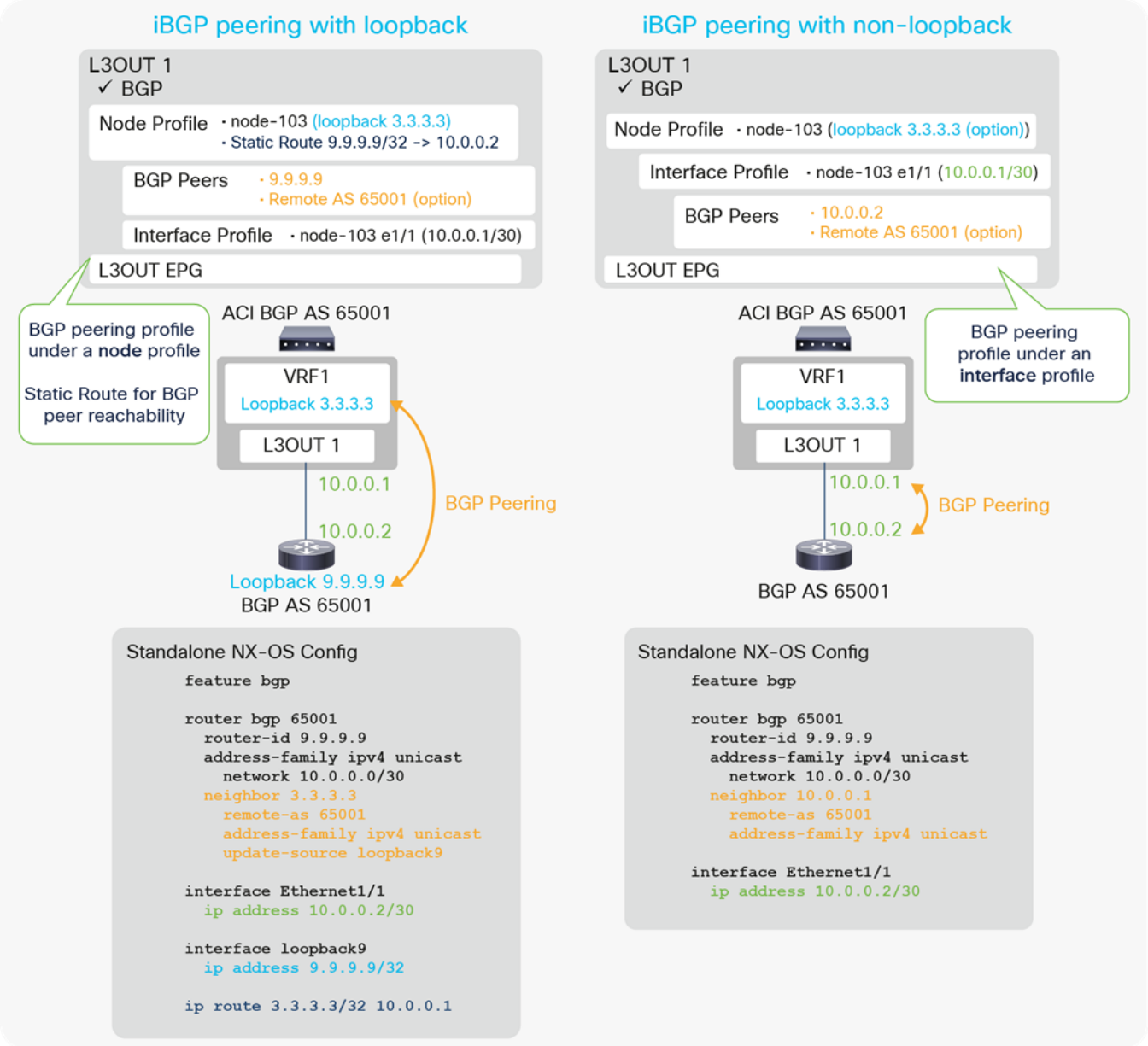

Figure 33.

iBGP 구성 도표

Figure 33 에서는 루프백 및 비 루프백 인터페이스에서 피어링을 사용하는 iBGP 의 구성을 나타낸 것입니다. ACI L3Out 에서 BGP 를 구성하는 주요 구성 요소는 다음과 같습니다.

- L3Out 의 루트에서 BGP 활성화
- BGP 피어 연결성 프로필 구성
  - 소스가 루프백일 경우: 노드 프로필에서 구성
  - 소스가 루프백이 아닐 경우: 인터페이스 프로필에서 구성
- BGP 피어 연결 가능성에 대한 고정 경로(또는 OSPF) 구성
  - 루프백 피어링과 같이 피어에 다중 홉이 부족한 경우로 한정됩니다.

기타 모든 L3Out 구성과 마찬 가지로 사용자는 L3Out 루트에서도 VRF 와 라우팅된 외부 도메인을 연결해야 합니다.

참고:

BGP 피어 연결성 프로필에서는 여러 가지 옵션을 선택할 수 있지만 iBGP 최소 구성에는 인접 라우터의 IP 주소만 있으면 됩니다. 기타 옵션에 대한 자세한 내용은 본 섹션의 "BGP 프로토콜 옵션"을 참조하시기 바랍니다.

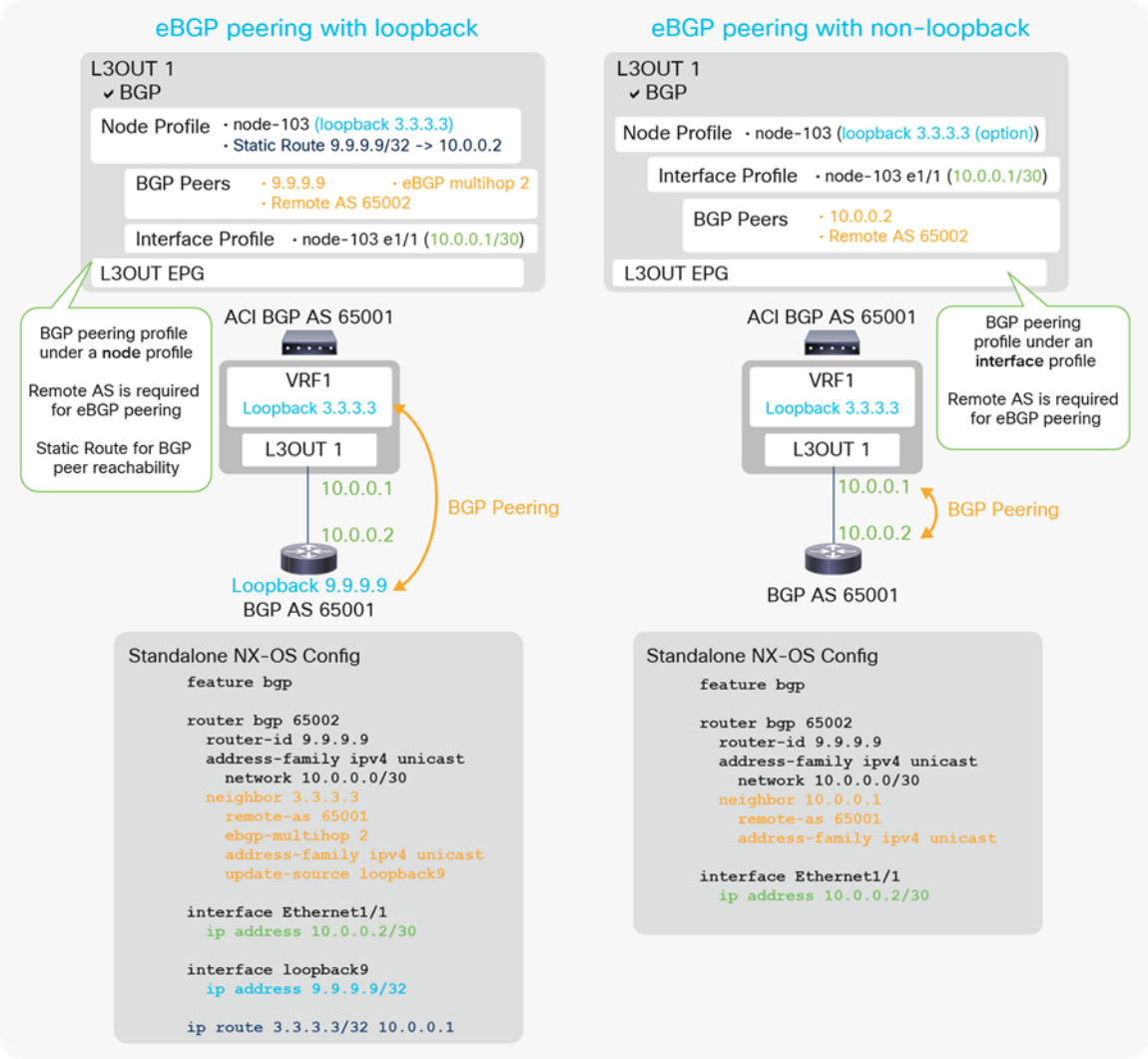

Figure 34.

EBGP 구성 도표

Figure 34 에는 루프백 및 비 루프백 인터페이스에서 피어링을 사용하는 eBGP 의 구성을 나타낸 것입니다. 대부분의 구성은 Figure 33 의 iBGP 구성과 동일하며, BGP 피어 연결성 프로필의 eBGP 피어링에 대한 두 가지 이상의 요구 사항이 있습니다.

- 원격 AS(eBGP 에서는 선택 불가)
- EBGP 다중 홉(루프백 피어링과 같이 피어에 다중 홉이 부족한 경우로 한정)

참고:

BGP 피어 연결성 프로필에서는 여러 가지 옵션을 선택할 수 있지만 eBGP 최소 구성에서는 인접 라우터 IP 주소, 원격 AS 번호, eBGP 다중 홉만 있으면 됩니다. 기타 옵션에 대한 자세한 내용은 본 섹션의 "BGP 프로토콜 옵션"을 참조하시기 바랍니다.

Figure 35 와 Figure 36 에서는 Figure 34 의 구성 예시에 기반해 루프백으로 피어링한 eBGP 용 APIC GUI 구성이 나와 있습니다(루프백이 포함된 eBGP 피어링). 사용자가 IGP 로서 고정 경로 대신 OSPF 를 사용해야 하는 경우, 동일한 L3Out 또는 동일 보더 리프의 다른 L3Out 에서 OSPF 를 활성화 및 구성할 수 있습니다. 동일한 L3Out 에서 OSPF 와 BGP 가 활성화된 경우, OSPF 는 L3Out 루프백과 인터페이스를 보급할 목적으로만 프로그래밍됩니다. BGP 의 포함 여부와 관계없이 동일하므로 OSPF 구성에 대한 자세한 내용은 "L3Out OSPF" 섹션을 참조하시기 바랍니다.

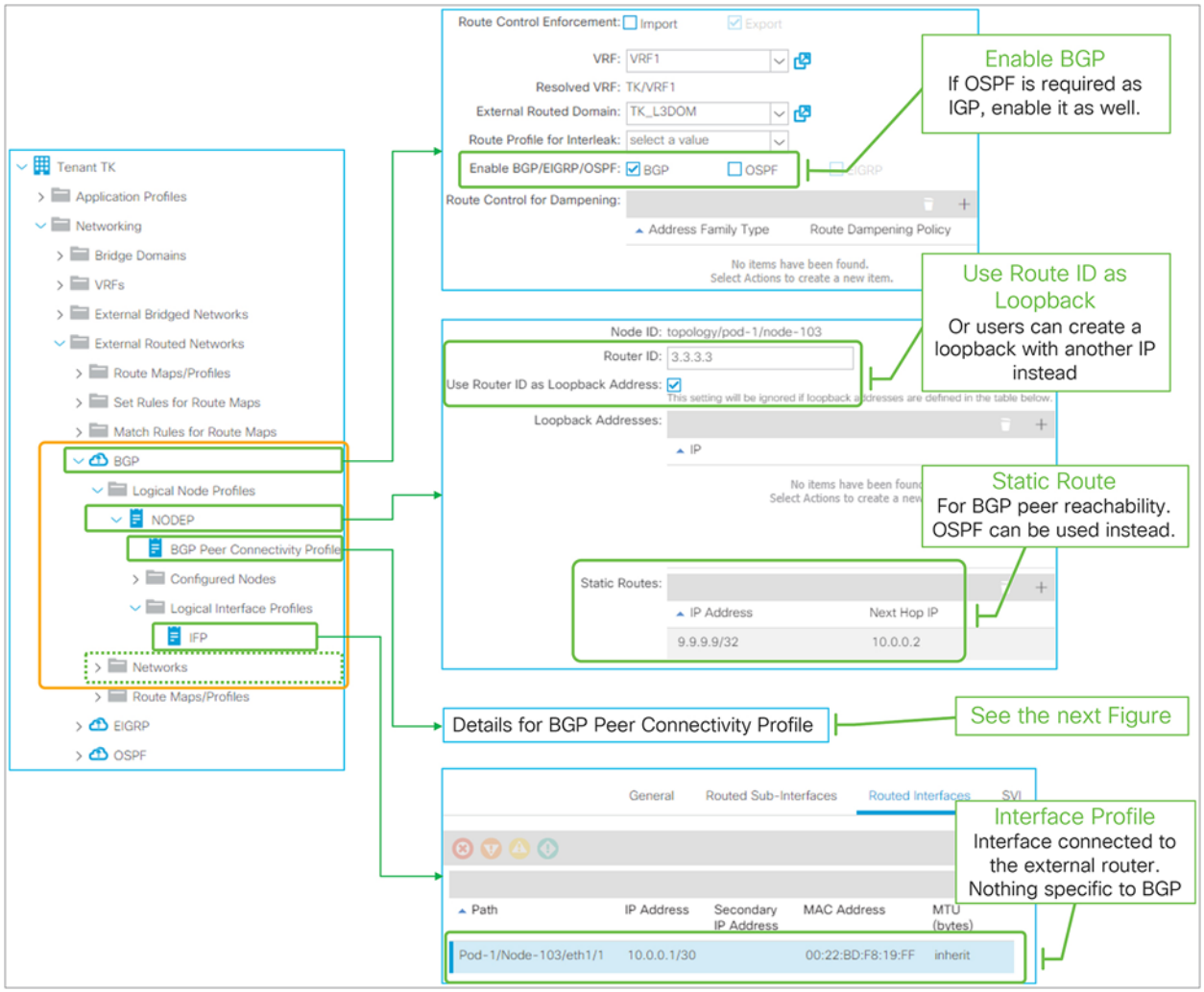

Figure 35.

GUI(APIC Release 3.2) 내 루프백이 포함된 EBGP 피어링

Figure 36.

GUI(APIC Release 3.2) 내 eBGP 피어링에 대한 BGP 피어 연결성 프로필

제한 및 지침

- 인프라 MP-BGP 및 경로 리플렉터용 BGP AS 번호가 전체 패브릭에서 BGP L3Out 에 대해 사용됩니다.
- APIC Release 1.1(1)부터 EBGP 피어링 지원이 추가되었습니다.
- OSPF 또는 고정 경로는 BGP 피어 연결 가능성에 대한 IGP 로서 지원됩니다. BGP L3Out 에서 OSPF 가 활성화된 경우, OSPF 는 L3Out 루프백과 인터페이스 서브넷을 보급할 목적으로만 프로그래밍됩니다.
- 2 차 IP 를 통한 BGP 세션 공급은 지원되지 않습니다.
- L3Out BGP 에는 독립 실행형 Cisco NX-OS 의 "network <subnet>" 명령어에 대응하는 구성이 없습니다. 다만 서브넷 외부 보급에 대한 모든 구성은 재배포를 통해 구현됩니다.
- 모든 라우팅 프로토콜과 고정 경로, 그리고 L3Out 인터페이스 서브넷은 기본값으로 BGP 에 재배포됩니다. 이 기본 재배포는 인프라 MP-BGP 에 필요합니다.
- 거의 모든 유형의 경로가 L3Out BGP 에 재배포되더라도 ACI 에서는 기본적으로 경로를 외부에 보급하지 않습니다. 서브넷을 보급하려면 BD 서브넷 보급 또는 전송 라우팅과 같이 적절한 구성이 필요합니다. 이는 BGP 피어에 대한 아웃바운드 경로 맵을 내부적으로 활용함으로써 구현됩니다.
- 아웃바운드 BGP 피어 경로 맵은 BGP 피어가 아닌 L3Out 마다 적용되므로 한 개의 L3Out 의 서브넷 보급 구성이 동일한 L3Out 의 모든 BGP 피어에도 적용됩니다. 내부 경로 맵 구현에 대한 자세한 내용은 "BD 서브넷 보급"섹션 또는 "전송 라우팅에 대한 내부 경로 맵" 섹션을 참조하시기 바랍니다. 이는 BGP 별 피어 경로 맵을 지원하는 APIC Release 4.2 에서 기능이 향상되었습니다.
- 이 외에도 경로 제어 적용 가져오기를 위한 L3Out 별 인바운드 BGP 피어 경로 맵이 있습니다. 아웃바운드 경로 맵과 동일한 제한이 적용됩니다. 이는 BGP 별 피어 경로 맵을 지원하는 APIC Release 4.2 에서 기능이 향상되었습니다.
- 다음 명령어를 사용하면 BGP 피어에 대한 아웃바운드 또는 인바운드 경로 맵을 확인할 수 있습니다.

```
Leaf1# show bgp ipv4 unicast neighbors vrf TK:VRF1 | egrep 'BGP nei|Inb|Outb'
BGP neighbor is 9.9.9.9,  remote AS 65009, ebgp link,  Peer index 1
  Inbound route-map configured is imp-L3Out-BGP-peer-2916353, handle obtained
  Outbound route-map configured is exp-L3Out-BGP-peer-2916353, handle obtained
```

The route-map name is in a form of "imp-L3Out-<L3Out name>-peer-<VRF VNID>" or "exp-L3Out-<L3Out name>-peer-<VRF VNID>".

BGP 프로토콜 옵션(인접 라우터 수준)

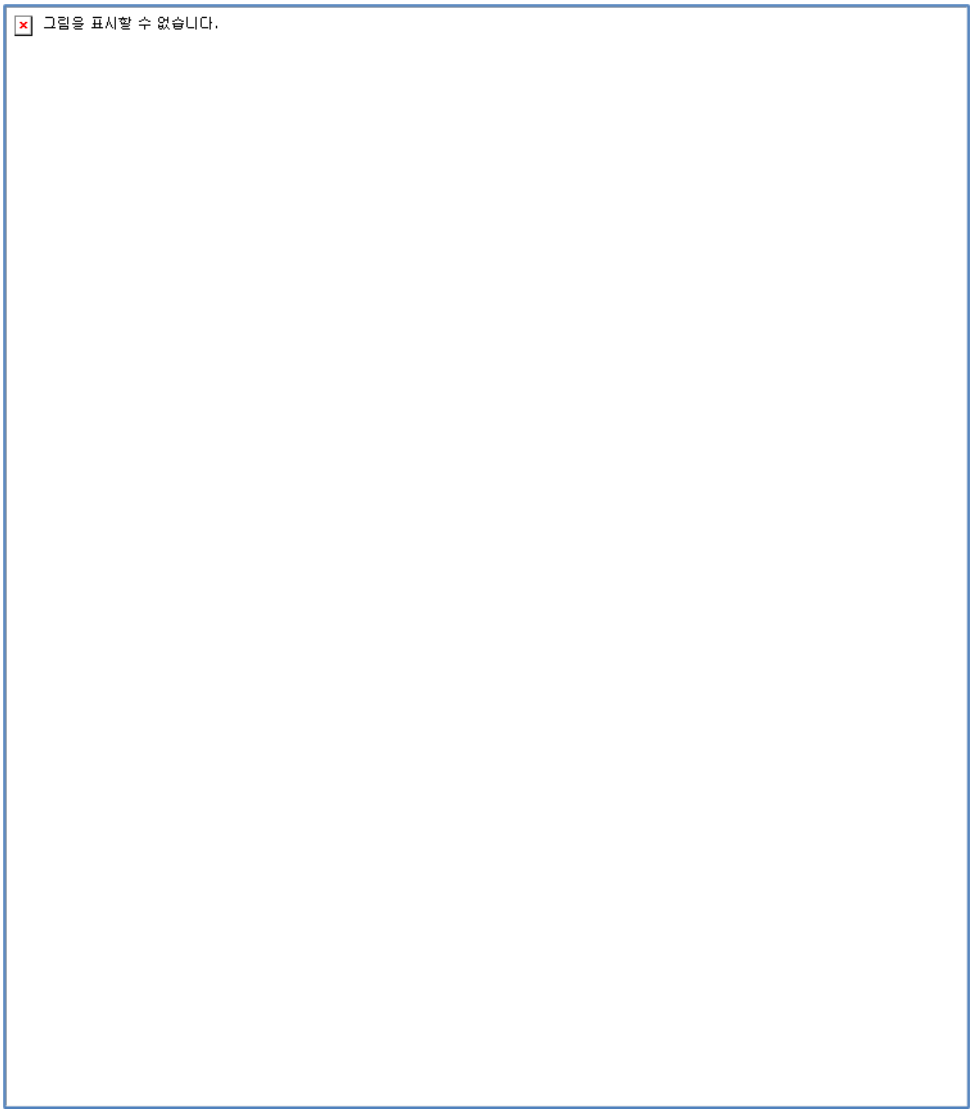

Figure 37.
GUI(APIC Release 3.2) 내 BGP 피어 연결성 프로필

본 서브섹션에서는 **"Tenant > Networking > External Routed Networks > L3Out"**에 위치한 논리 노드 프로필 또는 논리적 인터페이스 프로필의 BGP 피어 연결성 프로필에서 구성할 수 있는 각 인접 라우터별 모든 BGP 프로토콜 옵션을 살펴봅니다. 각종 BGP 집합 규칙은 "L3Out 경로 프로필 또는 경로 맵" 섹션을 참조하시기 바랍니다.

- **동적 인접 라우터(식별 번호 피어)**
  APIC Release 1.2(2)부터 도입된 기능으로, 개별 IP 주소가 아닌 서브넷을 구성(Figure 38 의 10.0.0.0/30)하여 여러 인접 라우터가 포함된 BGP 피어링을 동적으로 설정하는 것이 목적입니다. 이를 통해 L3Out 은 서브넷의 모든 IP 로 BGP 피어링을 동적으로 설정할 수 있습니다. 그러나 동적 인접 라우터 구성이 포함된 BGP 에서는 BGP 세션을 자체적으로 시작하지는 않으므로 BGP 세션을 시작하려면 다른 면에서 ACI 보더 리프 IP 를 명시적으로 구성해야 합니다.

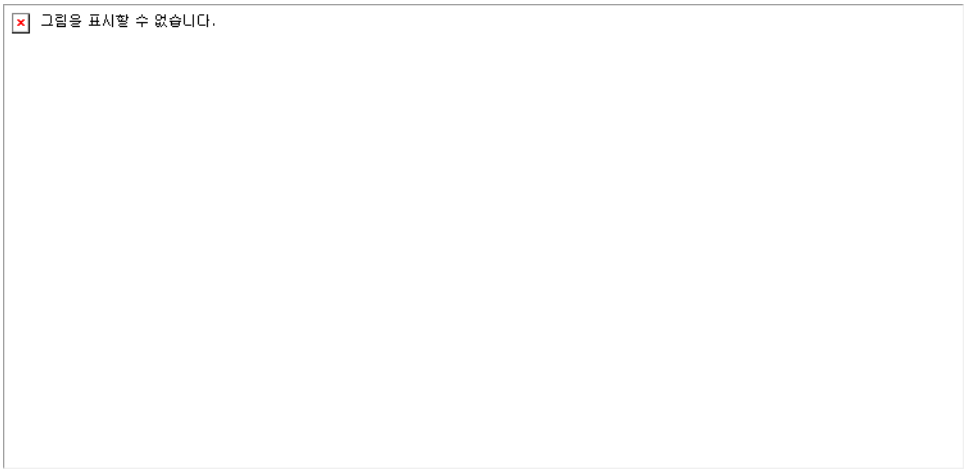

Figure 38.
BGP 동적 인접 라우터

독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  vrf TK:VRF1
    neighbor 10.0.0.0/30
```

이 기능의 명칭은 독립 실행형 NX-OS 의 식별 번호 피어입니다.

- **BGP 제어**
  커뮤니티 송신 및 확장된 커뮤니티 송신은 첫 APIC release 1.0 부터 지원되었습니다. 이외 옵션은 이후 APIC 버전에서 도입되었습니다.
  - 자체 AS 허용
    이 기능은 eBGP 피어링 지원의 일환으로 APIC Release 1.1(1)에서 도입되었습니다. 이 옵션을 통해 경로의 AS_PATH 에 ACI BGP AS 번호가 있더라도 ACI 가 eBGP 인접 라우터에서 경로를 수신할 수 있습니다. 이 옵션은 eBGP 피어에서만 유효합니다.

    독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

    ```
    router bgp 65001
      neighbor 9.9.9.9
        address-family ipv4 unicast
          allowas-in <number>
    ```

    위 동등 명령어의 <number>는 AS_PATH 에서 자체 AS 발생의 최대 수를 나타냅니다. 이 <number> 옵션은 아래의 **허용된 자체 AS 수** 옵션에 설명되어 있습니다.
  - AS 재정의
    APIC Release 3.1(2)에서 도입된 기능입니다. 이 기능을 통해 ACI 가 AS_PATH 에서 ACI BGP AS 로 원격 AS 를 재정의할 수 있습니다. ACI 에서는 일반적으로 동일한 AS 번호로 eBGP L3Out 간의 전송 라우팅을

수행할 때 사용됩니다. 그렇지 않으면 AS_PATH 루프 방지로 인해 eBGP 피어 장치가 ACI 의 경로를 수락하지 않을 수도 있습니다. 이 옵션을 활성화하면 **피어 AS 확인 비활성화** 옵션도 활성화해야 합니다. 이 옵션은 eBGP 피어에서만 유효합니다.

독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  neighbor 9.9.9.9
    address-family ipv4 unicast
      as-override
```

- 피어 AS 확인 비활성화

이 기능은 eBGP 피어링 지원의 일환으로 APIC Release 1.1(1)에서 도입되었습니다. 이 기능을 통해 ACI 는 경로의 AS_PATH 내 최신 AS 가 eBGP 피어에 대한 원격 AS 와 동일하더라도 해당 경로를 eBGP 피어로 보급할 수 있습니다. 이 옵션을 사용하지 않으면 독립 실행형 NX-OS 와 마찬가지로 ACI 도 경로를 보급하지 않습니다. AS_PATH 의 원격 AS 가 최신이 아닐 경우 경로 보급은 이 옵션의 영향을 받지 않으며 해당 경로는 추가 구성 없이 보급됩니다. 이 옵션은 eBGP 피어에서만 유효합니다.

독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  neighbor 9.9.9.9
    address-family ipv4 unicast
      disable-peer-as-check
```

- 다음 홉 자체

이 기능을 통해 eBGP 피어에서 iBGP 피어로 경로를 보급할 때 ACI 가 다음 홉을 업데이트할 수 있습니다. iBGP 피어 간의 경로 보급에서는 경로의 원본 다음 홉이 기본적으로 보관되지만, eBGP 피어 간의 경로 보급에서는 다음 홉이 자체 IP 로 항상 업데이트됩니다.

독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  neighbor 9.9.9.9
    address-family ipv4 unicast
      next-hop-self
```

- 커뮤니티 송신

첫 APIC release 1.0 부터 지원된 기능입니다. ACI L3Out 이 AS2:NN 형식 등 BGP 커뮤니티 특성을 이용해 경로를 보급하려면 이 옵션을 활성화해야 합니다. 그렇지 않으면 경로가 외부로 보급될 때 BGP 커뮤니티 특성이 제거됩니다. L3Out 에서 커뮤니티를 설정하거나 매칭하는 방법에 대한 자세한 내용은 "L3Out 경로 프로필 또는 경로 맵" 섹션을 참조하시기 바랍니다.

독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  neighbor 9.9.9.9
    address-family ipv4 unicast
      send-community {standard}
```

- 확장된 커뮤니티 송신

  첫 APIC release 1.0 부터 지원된 기능입니다. ACI L3Out 이 RT:AS2:NN, RT:AS4:NN 등의 확장된 BGP 커뮤니티 특성과 함께 경로를 보급하려면 이 옵션을 활성화해야 합니다. 그렇지 않으면 경로가 외부로 보급될 때 확장된 BGP 커뮤니티 특성이 제거됩니다. L3Out 에서 확장된 커뮤니티를 설정하거나 매칭하는 방법에 대한 자세한 내용은 "L3Out 경로 프로필 또는 경로 맵" 섹션을 참조하시기 바랍니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  neighbor 9.9.9.9
    address-family ipv4 unicast
      send-community extended
```

- **암호 및 암호 확인**

  첫 APIC release 1.0 부터 지원된 기능입니다. 구성이 이루어지면 L3Out BGP 는 BGP TCP 세션의 MD5 인증을 사용합니다. Figure 39 에서와 같이, 편집 또는 작업 드롭다운을 사용하거나 BGP 피어 연결성 프로필을 우클릭하여 "암호 재설정"을 통해 암호 구성을 재설정할 수 있습니다.

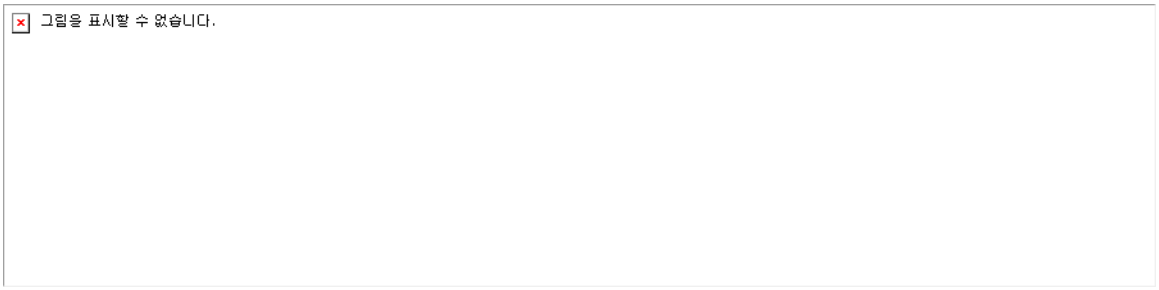

Figure 39.

BGP 피어 연결성 프로필(암호 재설정)

독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  neighbor 9.9.9.9
    password <your password>
```

- **허용된 자체 AS 수**

  이 기능은 eBGP 피어링 지원의 일환으로 APIC Release 1.1(1)에서 도입되었습니다. 이 기능은 **BGP 제어**에서 **자체 AS 허용** 옵션에 대한 최대 수를 설정하는 것이 목적입니다. **자체 AS 허용** 옵션에 대한 자세한 내용은 위 내용을 참조하시기 바랍니다.

- **피어 제어**
  - 양방향 전환 탐지(BFD)

    APIC Release 1.2(2)에서 도입된 기능으로, BGP 인접 라우터에서 BFD 를 활성화하는 데 사용됩니다. 자세한 내용은 "L3Out BFD" 섹션을 참조하시기 바랍니다.

    독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  vrf TK:VRF1
    neighbor 9.9.9.9
      bfd
```

  - 연결된 확인 비활성화

    이 기능은 eBGP 피어링 지원의 일환으로 APIC Release 1.1(1)에서 도입되었습니다. eBGP 피어링의 경우 BGP 프로세스는 로컬 인터페이스의 인접 라우터 IP 가 동일 서브넷에 있는지, 인접 라우터 IP 가 직접 연결되어 있는지 확인합니다. 그렇지 않은 것으로 확인될 경우 TTL 이 1 보다 커야 한다고 자동으로 가정합니다. 따라서 BGP 가 직접 연결된 라우터가 포함된 루프백을 통해 피어링할 때, TTL1 도 기술적으로는 충분하지만 eBGP 다중 홉 TTL 이 2 보다 크지 않은 경우에는 BGP 피어링이 거부됩니다. **연결된 확인 비활성화**는 이러한 시나리오에서 TTL 의 불필요한 증가와 관련해 보안 문제가 있을 경우 eBGP 다중 홉 TTL 을 증가시키는 대안으로 사용할 수 있습니다.

    독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  neighbor 9.9.9.9
    disable-connected-check
```

- **EBGP 다중 홉 TTL**

  이 기능은 eBGP 피어링 지원의 일환으로 APIC release 1.1(1)에서 도입되었습니다. BGP 제어 패킷의 경우 eBGP 피어링 시 기본적으로 1 TTL 을 사용합니다. 인접 라우터 IP 에 다중 홉이 부족할 경우 이 옵션을 통해 TTL 을 증가시켜야 합니다. 필요한 TTL 이 1 이지만 인접 라우터 IP 가 직접 연결된 서브넷에 위치하지 않을 경우(예: 인접 라우터 IP 가 직접 연결된 라우터의 루프백 IP 인 경우), **피어 제어**의 **연결된 확인 비활성화**를 대신 사용할 수 있습니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  neighbor 9.9.9.9
    ebgp-multihop <number>
```

- **가중치**

  APIC Release 1.2(2)에서 도입된 기능으로, 이 인접 라우터에 보급된 모든 경로에서 Cisco 독점 BGP 경로 특성 **가중치**의 기본값을 설정합니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  neighbor 9.9.9.9
    address-family ipv4 unicast
      weight <number>
```

- **비공개 AS 제어**

  APIC Release 1.2(2)에서 도입된 기능으로, ACI BGP AS 가 공개적인 AS 번호일 경우에만 유효한 옵션입니다.

  - 비공개 AS 제거

    이 인접 라우터로 발신되는 eBGP 경로 업데이트 시 AS_PATH 에 비공개 AS 번호만 있는 경우에는 AS_PATH 에서 모든 비공개 AS 번호가 제거됩니다.
    인접 라우터 원격 AS 가 AS_PATH 에 있는 경우에는 이 옵션이 적용되지 않습니다.

  - 모든 비공개 AS 제거

    이 인접 라우터로 발신되는 eBGP 경로 업데이트 시 AS_PATH 에 공개 AS 번호가 포함되는지 여부에 관계없이 AS_PATH 에서 모든 비공개 AS 번호가 제거됩니다.
    인접 라우터 원격 AS 가 AS_PATH 에 있는 경우에는 이 옵션이 적용되지 않습니다.
    이 옵션을 활성화하려면 **비공개 AS 제거**를 활성화해야 합니다.

  - 비공개 AS 를 로컬 AS 로 교체

    이 인접 라우터로 발신되는 eBGP 경로 업데이트 시 AS_PATH 에 공개 AS 또는 인접 라우터 원격 AS 가 포함되는지 여부에 관계없이 AS_PATH 의 모든 비공개 AS 번호가 ACI 로컬 AS 로 교체됩니다.
    이 옵션을 활성화하려면 **모든 비공개 AS 제거**를 활성화해야 합니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  neighbor 9.9.9.9
    address-family ipv4 unicast
      remove-private-as
      remove-private-as all
      remove-private-as replace-as
```

- **BGP 피어 식별 번호 정책(최대 식별 번호)**

  APIC Release 1.2(1)에서 도입된 기능으로, 이 인접 라우터에서 수신된 식별 번호의 수가 구성된 최대 수를 초과할 때 취할 조치를 설정하기 위한 옵션입니다. 이 옵션은 BGP 피어 식별 번호 정책(Figure 40)을 BGP 피어 연결성 프로필에 연결하여 활성화할 수 있습니다.

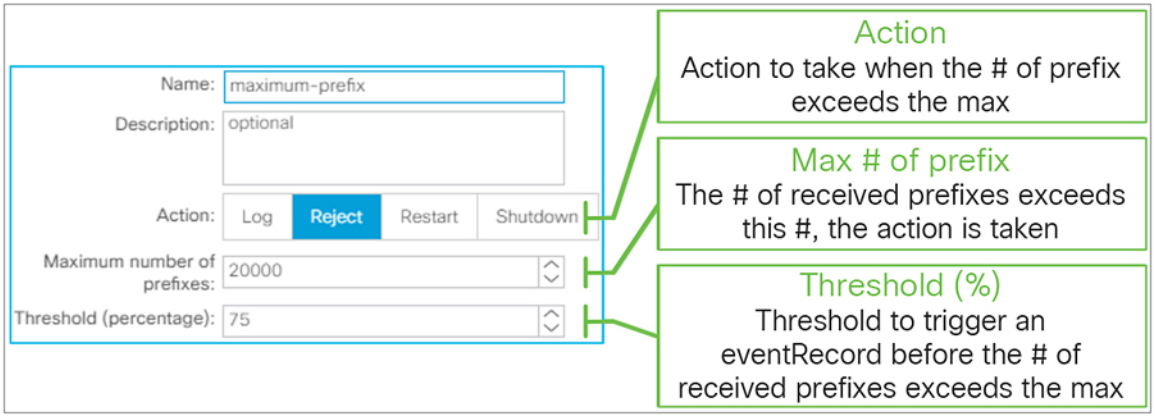

Figure 40.

GUI(APIC Release 3.2) 내 BGP 피어 식별 번호 정책

◦ 작업

이 인접 라우터에서 수신된 식별 번호의 수가 구성된 값을 초과할 때 취해질 조치입니다.

- **로그:** 수신된 식별 번호의 수가 최대치를 초과한다는 F1215 오류 메시지가 사용자에게 표시됩니다. 식별 번호의 최대 수가 10 으로 설정되어 있는 경우 11 개의 식별 번호가 학습될 때 오류 메시지가 표시됩니다.
- **거부:** 수신된 식별 번호의 수가 최대치를 초과한다는 F1215 오류 메시지가 사용자에게 표시됩니다. 수신된 식별 번호의 수가 감소할 때까지 이 인접 라우터에서 식별 번호가 더는 학습되지 않습니다. 식별 번호의 최대 수가 10 으로 설정되어 있는 경우 11 개의 식별 번호가 학습될 때 오류 메시지가 표시되고 12 번째 식별 번호는 거부됩니다.
- **재시작:** 최대 식별 번호 위반으로 인해 BGP 피어가 종료되고 F1214 오류 메시지가 표시됩니다. 수신된 식별 번호의 수가 최대치 미만으로 감소하면 구성된 간격 후에 BGP 피어가 재설정됩니다. 이 작업을 선택하면 "재시작 시간(분)" 구성을 사용할 수 있습니다. 식별 번호의 최대 수가 10 으로 설정되어 있는 경우 11 개의 식별 번호가 학습될 때 BGP 피어가 종료됩니다.
- **종료:** 최대 식별 번호 위반으로 인해 BGP 피어가 종료되고 F1214 오류 메시지가 표시됩니다. 식별 번호의 최대 수가 10 으로 설정되어 있는 경우 11 개의 식별 번호가 학습될 때 BGP 피어가 종료됩니다.

◦ 식별 번호 최대 수

수신된 식별 번호 수가 이 수를 초과하면 구성된 작업이 실행됩니다. 기본값은 식별 번호 20,000 개입니다.

◦ 임곗값(퍼센트)

수신된 식별 번호의 수가 임곗값을 초과할 경우 예방 수단으로 경고(eventRecord) 메시지가 표시됩니다. 식별 번호의 최대 수가 10, 임곗값이 70 퍼센트로 설정되어 있는 경우 8 개의 식별 번호가 학습될 때 경고 메시지가 표시됩니다. 기본값은 75 퍼센트입니다.

독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  vrf TK:VRF1
    neighbor 9.9.9.9
      address-family ipv4 unicast
        maximum-prefix <prefix number> <threshold %>
        maximum-prefix <prefix number> <threshold %> restart <min>
        maximum-prefix <prefix number> <threshold %> warning-only
```

- **원격 AS**

  이 기능은 eBGP 피어링 지원의 일환으로 APIC release 1.1(1)에서 도입된 것으로, 인접 라우터의 AS 번호를 지정하기 위해 eBGP 피어링에 필요합니다. 빈 칸일 때는 ACI BGP AS 번호를 자동으로 사용하므로 이 필드는 iBGP 피어링 시 선택 사항입니다.
  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  vrf TK:VRF1
    neighbor 9.9.9.9
      remote-as <AS #>
```

- **로컬 AS 또는 로컬 AS 구성**

  eBGP 피어링 지원의 일환으로 APIC Release 1.1(1)에서 도입된 것으로, L3Out 이 이 인접 라우터와 피어링하기 위해 구성된 로컬 AS 로 자체 BGP AS 를 가장해야 할 때 사용됩니다. 이 기능이 사용될 때 이 인접 라우터에서는 인접 라우터 및 ACI BGP AS 간에 AS(로컬 AS)가 한 개 더 있는 것으로 보이게 됩니다. 따라서 인접 라우터는 실제 ACI BGP AS 가 아닌 구성된 로컬 AS 로 피어링하게 됩니다. 이러한 상황에서는 로컬 AS 및 실제 AC BGP AS 모두 인접 라우터에 보급된 경로의 AS_PATH 에 추가되며, 로컬 AS 역시 이 인접 라우터에서 학습된 경로 앞에 추가됩니다.

  독립 실행형 NX-OS 와 마찬가지로 다음과 같은 추가 옵션을 사용할 수 있습니다.

  - 앞에 추가 금지,
    이 인접 라우터에서 학습된 경로의 AS_PATH 내 로컬 AS 앞에 ACI 가 추가되지 않도록 방지하는 옵션입니다.
  - 앞에 추가 금지, 교체
    이 옵션을 사용하면 **앞에 추가 금지**의 효과에 더해 ACI 가 이 인접 라우터에 보급된 경로의 AS_PATH 에 로컬 AS 와 실제 ACI BGP AS 대신, 로컬 AS 만 추가할 수 있습니다.
  - 앞에 추가 금지, 교체, 복제
    이 옵션을 사용하면 **앞에 추가 금지** 및 **교체**의 효과에 더해 인접 라우터가 로컬 AS 와 실제 ACI BGP AS 를 모두 사용해 피어링할 수 있습니다.

독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
```

```
vrf TK:VRF1
  neighbor 9.9.9.9
    local-as <AS #>
    local-as <AS #> no-prepend
    local-as <AS #> no-prepend replace-as
    local-as <AS #> no-prepend replace-as dual-as
```

BGP 프로토콜 옵션(L3Out 또는 노드 수준)

- **BGP 프로토콜 프로필**
  논리 노드 인터페이스 프로필을 통해 노드별 BGP 최적 경로 제어 정책과 BGP 타이머 정책을 적용하는 프로필입니다.

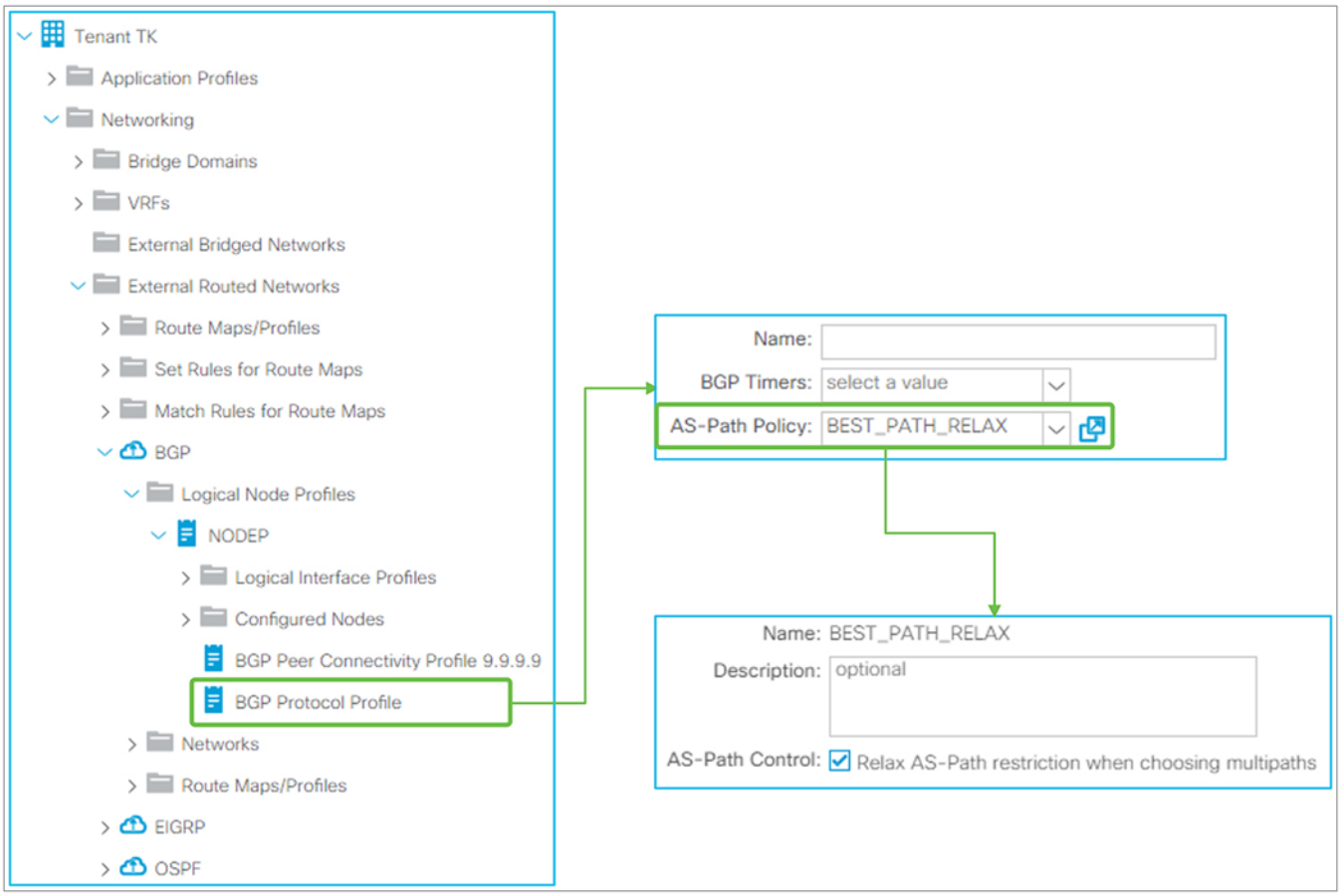

Figure 41.
GUI(APIC Release 3.2) 내 BGP 프로토콜 프로필

  - **BGP 타이머**
    각 노드와 각 VRF 마다 적용할 수 있습니다. 자세한 내용은 아래의 "BGP 프로토콜 옵션(VRF 수준)" 서브섹션 을 참조하시기 바랍니다.

  - **AS-경로 정책**
    노드마다 AS 경로 정책(BGP 최적 경로 제어 정책)을 적용합니다. APIC Release 3.2(7)에서 도입된 옵션으로, APIC Release 4.0, 4.1, 4.2(1)에서는 지원되지 않습니다. "AS 경로 제어"가 활성화되어 있으면 여러 eBGP 피어(다양한 AS 경로) 전체에서 ECMP 를 허용합니다.
    독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  vrf TK:VRF1
    bestpath as-path multipath-relax
```

- **BGP 경로 댐프닝**

  APIC Release 1.2(2)에서 도입된 기능으로, 플래핑 경로 보급을 중단하는 데 사용됩니다. BGP 경로 상태가 사용 가능에서 사용 불가능, 또는 그 반대로 바뀔 경우 1000 의 패널티가 경로에 추가됩니다. 페널티가 저지 제한을 초과할 경우 경로는 '댐프닝됨'으로 표시되고 라우터의 경로 보급이 중단됩니다. **반감기** 시간이 지나면 각 경로의 패널티가 절반으로 감소합니다. 패널티가 재사용 제한의 절반 미만으로 감소하면 경로에서 완전히 제거됩니다.

  ACI 에서는 이러한 경로 댐프닝 매개변수가 매치 정책 없이 경로 프로필에서 정책 설정을 통해 구성됩니다. BGP 경로 댐프닝에 대한 경로 프로필은 개별적인 L3Out 의 수준이 아닌 테넌트 수준입니다. 경로 프로필에 대한 자세한 내용은 "L3Out 경로 프로필 및 경로 맵" 섹션을 참조하시기 바랍니다.

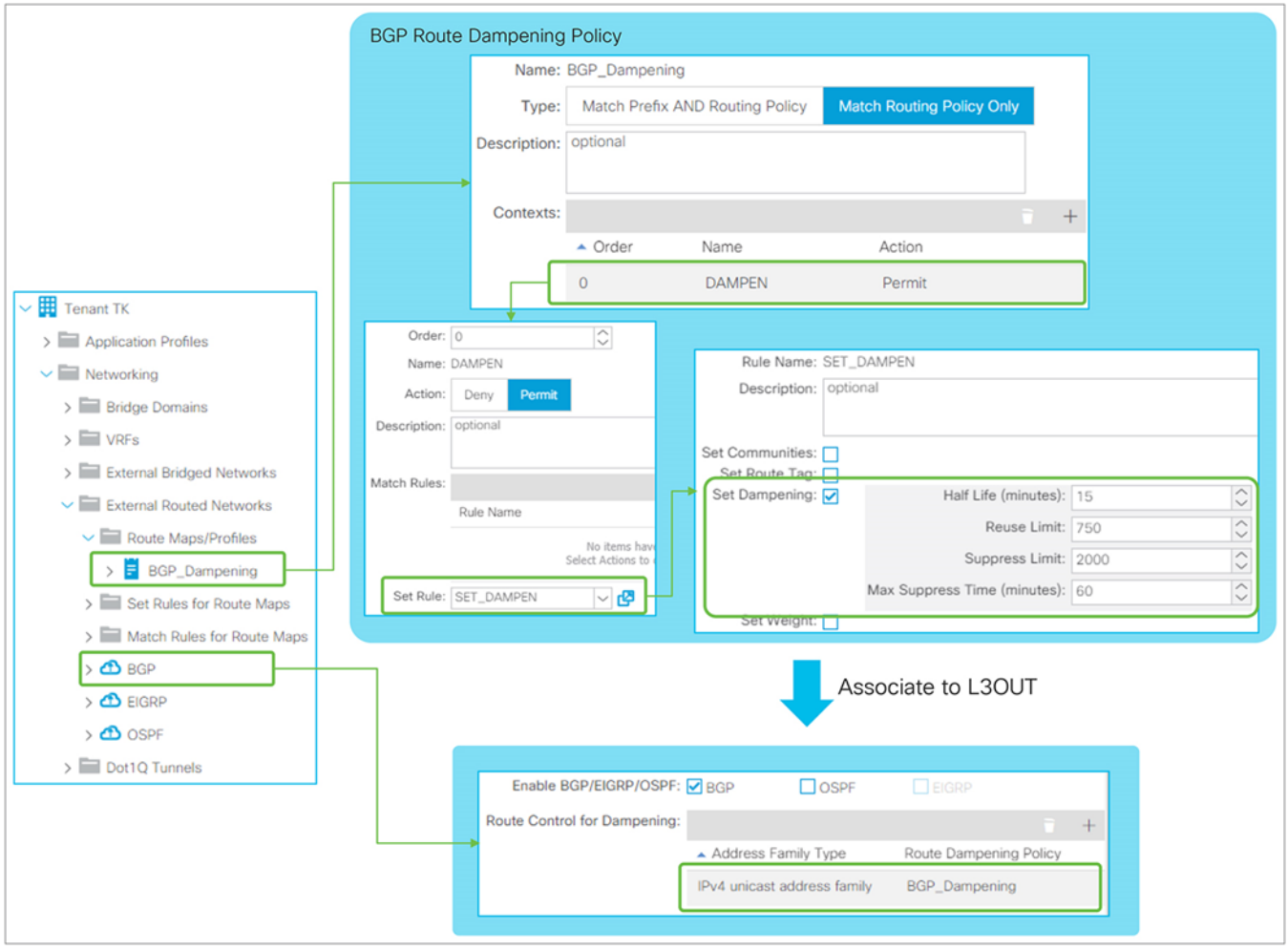

Figure 42.

GUI(APIC Release 3.2) 내 BGP 경로 댐프닝 정책

- 반감기(분)

  빈감기 시간이 지나면 각 경로의 패널티가 절반으로 감소합니다.

- 재사용 제한
  경로의 패널티가 **재사용 제한** 미만으로 감소하면 경로가 다시 사용 및 보급됩니다.
- 저지 제한
  경로의 패널티가 **저지 제한**을 초과하면 경로가 저지되어 보급되지 않습니다.
- 최대 저지 시간(분)
  최대 저지 시간이 지나면 패널티에 관계없이 경로의 저지가 해지되어 다시 보급됩니다. 이는 식별 번호가 무기한으로 댐프닝되는 것을 방지하기 위한 목적입니다.

독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
route-map BGP_dampening
  set dampening <Half Life> <Reuse Limit> <Suppress Limit> <Max Suppress>
router bgp 65001
  vrf TK:VRF1
    address-family ipv4 unicast
      dampening route-map BGP_dampening
```

BGP 프로토콜 옵션(VRF 수준)

- **BGP 타이머 정책**

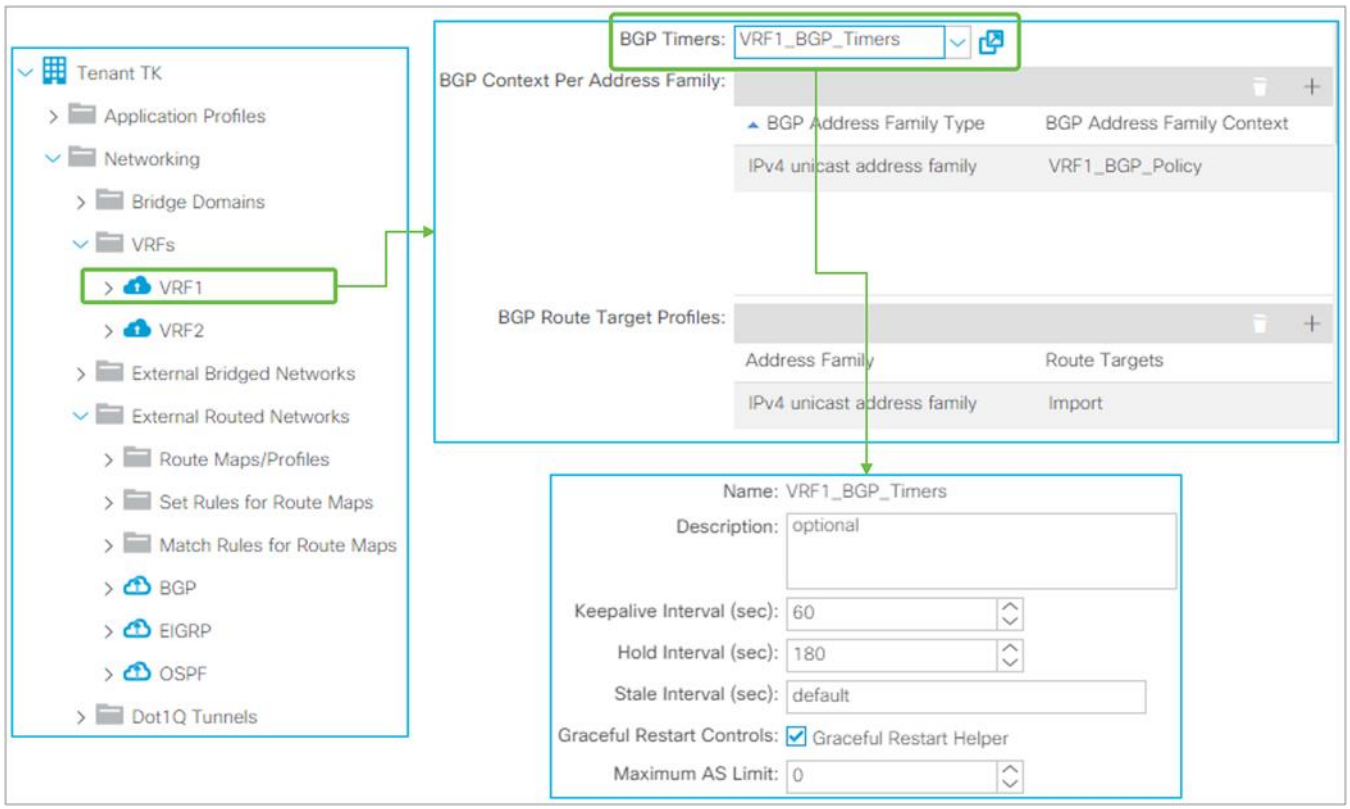

Figure 43.
GUI(APIC Release 3.2) 내 BGP 타이머 정책

BGP 타이머 정책은 **"Tenant > Policies > BGP > BGP Timers"**에 위치하며, **"Tenant > Networking > VRFs"**아래의 VRF 와 연관되어 있습니다. APIC Release 2.2(2)부터 BGP 타이머 정책은 논리 노드 프로필을 우클릭해 구성하여 VRF 가 아닌 각 노드와 각 VRF 별로 BGP 타이머 정책의 범위를 설정할 수 있습니다.

- **Keepalive 간격(초) 및 보류 간격(초)**

  BGP 피어가 설정되면 Keepalive 간격마다 인접 라우터로 Keepalive 메시지가 송신됩니다. 보류 간격 동안 Keepalive 메시지가 수신되지 않으면 BGP 피어는 중지된 것으로 간주합니다. Keepalive 간격의 기본값은 60 초, 보류 간격의 기본값은 180 초(= 3 x Keepalive 간격)입니다. 보류 간격은 BGP OPEN 메시지를 통해 교환되고 더 낮은 값으로 협상되므로 구성된 간격은 새 BGP 세션이 설정되어야만 효력을 발휘합니다. 논리적으로 구성된 Keepalive 간격이 협상된 보류 간격의 1/3(33%)보다 큰 경우, 구성된 값이 아닌 협상된 보류 간격의 1/3 이 Keepalive 간격으로 사용됩니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  vrf TK:VRF1
    timers bgp <keepalive interval> <hold interval>
```

- **오래된 간격(초)**

  정상 재시작이 진행 중일 때는 이전 피어에서 수신된 경로가 전환에 사용되지만 오래된 것으로 표시됩니다. 두 라우터 간의 세션이 재설정되고 경로 정보가 다시 동기화되면 오래된 경로가 모두 삭제되고 최신 교환의 최신 경로가 사용됩니다. **오래된 간격**은 이 간격 내에 세션이 재설정되지 않는 경우 오래된 경로를 삭제하는 타이머 역할을 합니다. 이 간격은 로컬로 적용되며, 기본값은 300 초입니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  vrf TK:VRF1
    graceful-restart stalepath-time <stale interval>
```

- **정상 재시작 제어**

  정상 재시작이 진행 중일 때는 한 개의 라우터에서 라우팅 프로세스를 재시작해 정상 재시작을 유도 중일 수도 있습니다. 또한 피어는 오래된 상태일 수 있지만 재시작 라우터를 통해 정상 재시작 작업을 단순히 지원 중일 가능성도 있습니다. 후자의 경우를 정상 재시작 수신 장치 또는 정상 재시작 도우미라고 부릅니다. ACI 에서는 개별 스위치 노드 내의 상태 저장 감독자 전환이 지원되지 않으므로 Cisco ACI 에서는 정상 재시작 도우미 기능만 제공됩니다. 콜드 재부팅만 사용할 수 있지만 여러 스위치 노드를 활용하는 방법으로 라우팅 프로토콜 고가용성(HA)을 확보할 수 있습니다. 이에 따라,

  - **정상 재시작 도우미**

    VRF 내에서 정상 재시작 도우미 기능을 활성화하며 기본으로 활성화되어 있습니다.

    독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  vrf TK:VRF1
    no graceful-restart
    graceful-restart-helper
```

정상 재시작에는 두 개의 주요 타이머가 있습니다. 하나는 재시작 타이머로, 라우터를 재시작하고 재시작되는 라우터가 라우팅 프로토콜 재시작을 마치는 데 필요한 최대 시간을 피어에게 알림으로써 구성 및 보급됩니다. 이 타이머가 만료되면 정상 재시작 도우미 장치에서 재시작 장치가 라우팅 프로토콜을 재시작하는 데 실패했다고 가정해 오래된 경로를 모두 삭제합니다. 따라서 이 타이머는 ACI 에서 구성되지 않습니다(정상 재시작 도우미). 또 하나는 정상 재시작 도우미 장치에서 구성 및 사용되는 오래된 타이머입니다. 위 **오래된 간격** 옵션을 참조하시기 바랍니다.

- **최대 AS 제한**

APIC Release 2.0(1)에서 도입된 기능으로, 지정된 제한을 초과하는 AS 경로 세그먼트를 다수 보유한 eBGP 경로를 삭제합니다. 기본값은 0 이며 최대치를 한계값으로 나타내지 않습니다.

독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  vrf TK:VRF1
    maxas-limit <number>
```

- **주소 패밀리 컨텍스트**

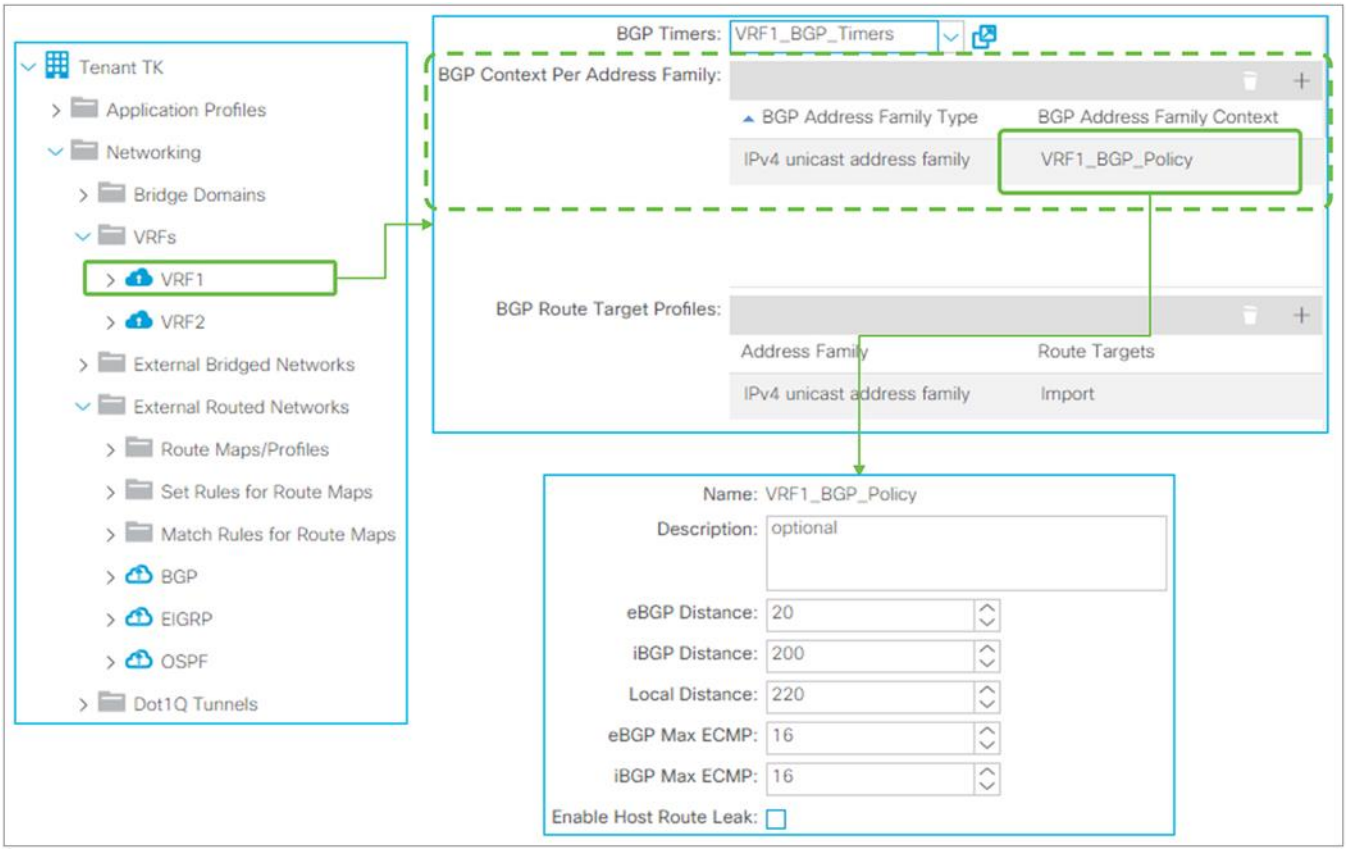

Figure 44.

GUI(APIC Release 3.2) 내 BGP 주소 패밀리 컨텍스트

BGP 주소 패밀리 컨텍스트 정책은 **"Tenant > Policies > BGP > BGP Address Family Context"**에 위치하며, **"Tenant > Networking > VRFs"** 아래의 VRF 와 연관되어 있습니다.

- **eBGP, iBGP, 로컬 거리**

  APIC Release 1.2(1)에서 도입된 기능으로, BGP 에 대한 관리 거리(AD)입니다. 기본값은 다음과 같습니다.

  - eBGP: 20
  - iBGP: 200
  - 로컬: 220(로컬 AD 는 RIB 에 설치 시 삭제 경로 총합에 사용됨)

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
 vrf TK:VRF1
   address-family ipv4 unicast
     distance <eBGP AD> <iBGP AD> <Local AD>
```

- **eBGP, iBGP 최대 ECMP**

  APIC Release 3.0(1)에서 도입된 기능으로, BGP 가 ECMP 용 경로 테이블에 추가하는 경로의 최대 수를 구성합니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  vrf TK:VRF1
    address-family ipv4 unicast
      maximum-paths <eBGP ECMP number>
      maximum-paths ibgp <iBGP ECMP number>
```

- **호스트 경로 유출 활성화**

  APIC Release 2.1(1)에서 도입된 기능으로, GOLF 기능에 대한 사항입니다. 사용자가 eVPN 유형 5 경로(BD 서브넷) 외에도 GOLF 를 통해 eVPN 유형 2(호스트 MAC/IP) 경로를 보급해야 할 때 활성화됩니다. Cisco APIC 계층 3 네트워킹 구성 가이드의 "GOLF" 섹션을 참조하시기 바랍니다.

BGP 경로 요약

APIC Release 1.2(2)에서 도입된 기능으로, ACI BGP L3Out 에서 전송 경로 또는 BD 서브넷에 대해 요약된 식별 번호만 외부로 보급합니다. 이 동작은 NX-OS 명령어의 "**aggregate-address <prefix> summary-only**"에 해당합니다.

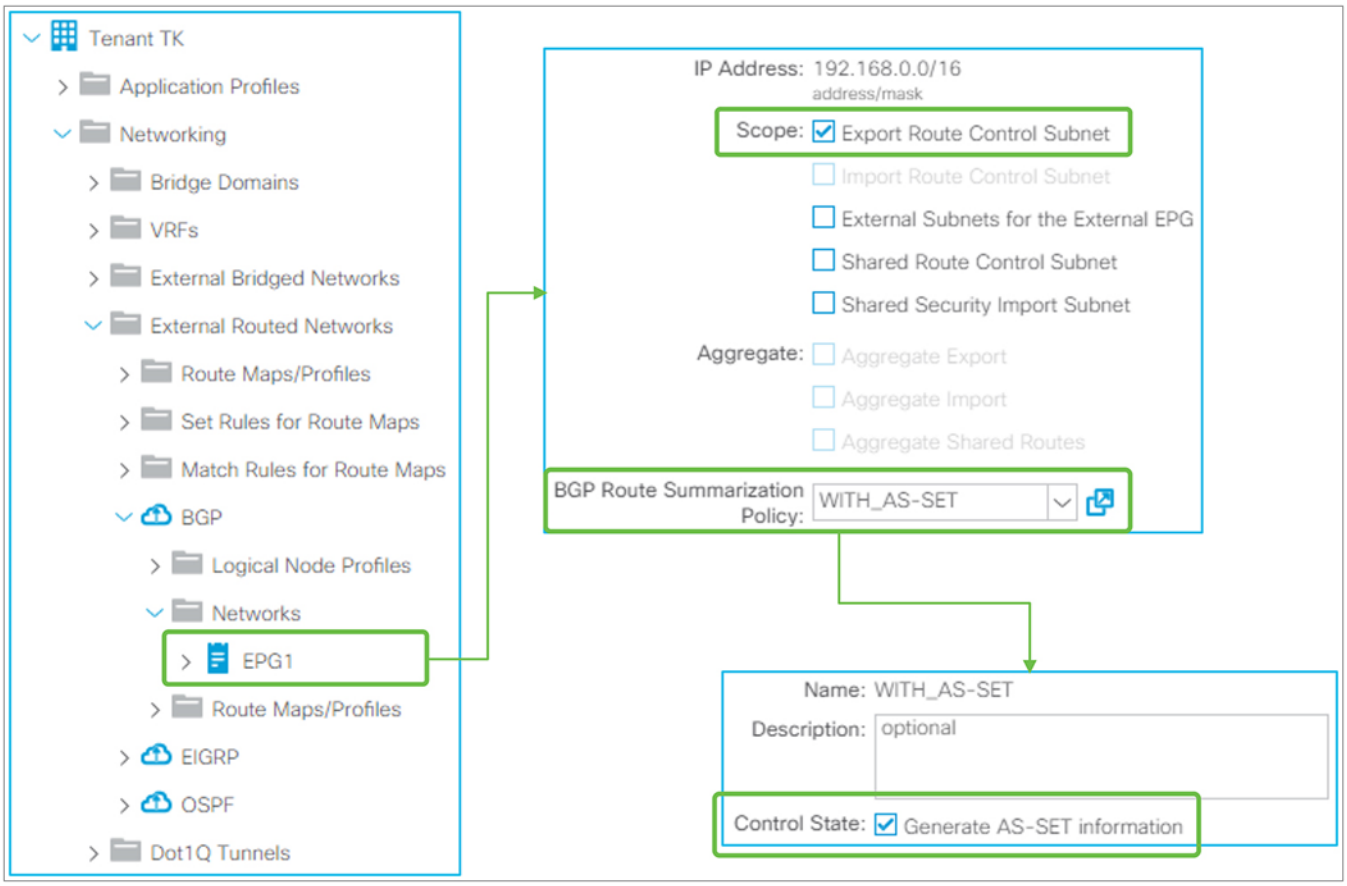

Figure 45.
GUI(APIC Release 3.2) 내 BGP 경로 요약

ACI 내 BGP 라우팅 요약은 "경로 제어 서브넷 내보내기" 범위를 사용해 경로 요약 정책을 L3Out 서브넷에 추가함으로써 구성됩니다. 이는 ACI 에서 외부로 경로를 보급하는(내보내는) 데 사용되기 때문입니다. "경로 제어 서브넷 내보내기" 범위에 대한 자세한 내용은 "L3Out 전송 라우팅" 섹션을 참조하시기 바랍니다.

Figure 45 에서와 같이, 경로 요약 정책을 L3Out 서브넷에 추가하면 보더 리프에서 요약된 경로(Figure 45 의 192.168.0.0/16)에 대한 Null-0 항목을 생성하고 이것은 BGP 피어로 보급됩니다. 일반적인 BGP 라우터와 마찬가지로 보더 리프의 사용자 VRF 에 대한 IPv4/IPv6 BGP 테이블에 기여 경로가 존재하지 않는 경우에는 요약이 발생하지 않는 다는 점에 유의해야 합니다.

지원되는 구성 가능 옵션은 다음과 같습니다.

- **AS-SET 정보 생성**
  이 옵션을 통해 요약된 경로는 기여 경로의 커뮤니티 정보와 AS-PATH 특성을 갖게 됩니다.

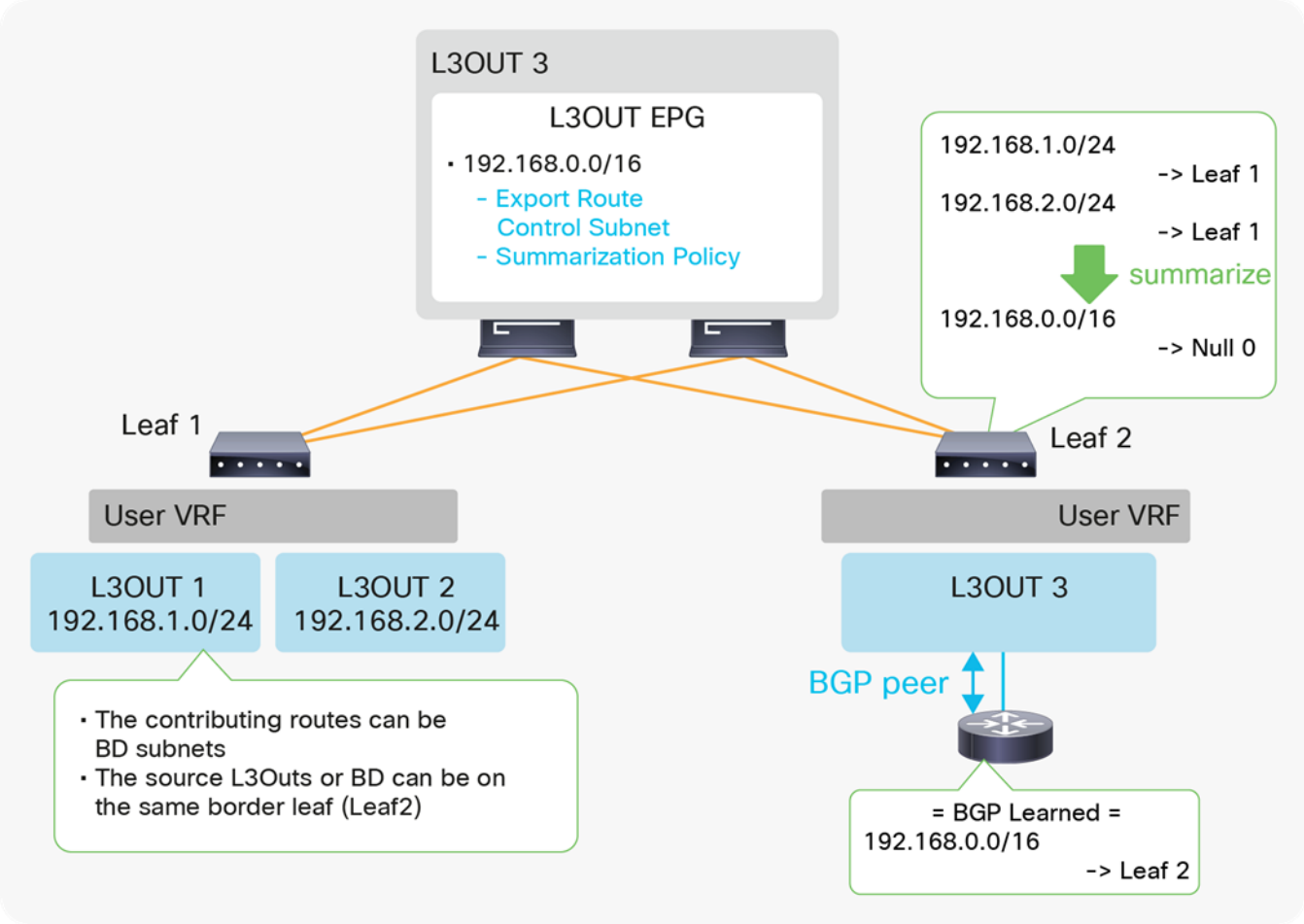

Figure 46.
BGP 경로 요약 토폴로지의 예시

Figure 46 은 L3Out 3 에서 각 서브넷(192.168.1.0/24 및 192.168.2.0/24)이 아닌 요약된 전송 서브넷(192.168.0.0/16) 정보만 공급하는 경우를 나타냅니다. Null-0 다음 홉이 있는 요약된 경로는 외부에만 보급되는 것으로, 인프라 MP-BGP 를 통해 다른 리프 스위치로 보급되지 않습니다. BGP 가 BD 서브넷을 요약할 경우, 요약 구성 외에도 한 개 이상의 기여 BD 서브넷에 대해 올바른 BD 서브넷 보급 구성이 필요합니다("ACI BD 서브넷 보급" 섹션 참조).

독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  vrf TK:VRF1
    address-family ipv4 unicast
      aggregate-address <prefix> summary-only {as-set}
```

BGP 기본 경로 보급

기본 경로(0.0.0.0/0)를 BGP L3Out 에서 외부로 보급하는 데는 두 가지 방법이 있습니다.

1. 전송 라우팅
2. 기본 경로 유출 정책

전송 라우팅은 다른 L3Out 또는 다른 L3Out 에서 구성된 고정 경로에서 학습된 기본 경로를 보급합니다. 전송 라우팅에 대한 자세한 내용은 "L3Out 전송 라우팅" 섹션을 참조하시기 바랍니다.

기본 경로 유출 정책은 독립 실행형 NX-OS 의 "default-originate"에 해당합니다.

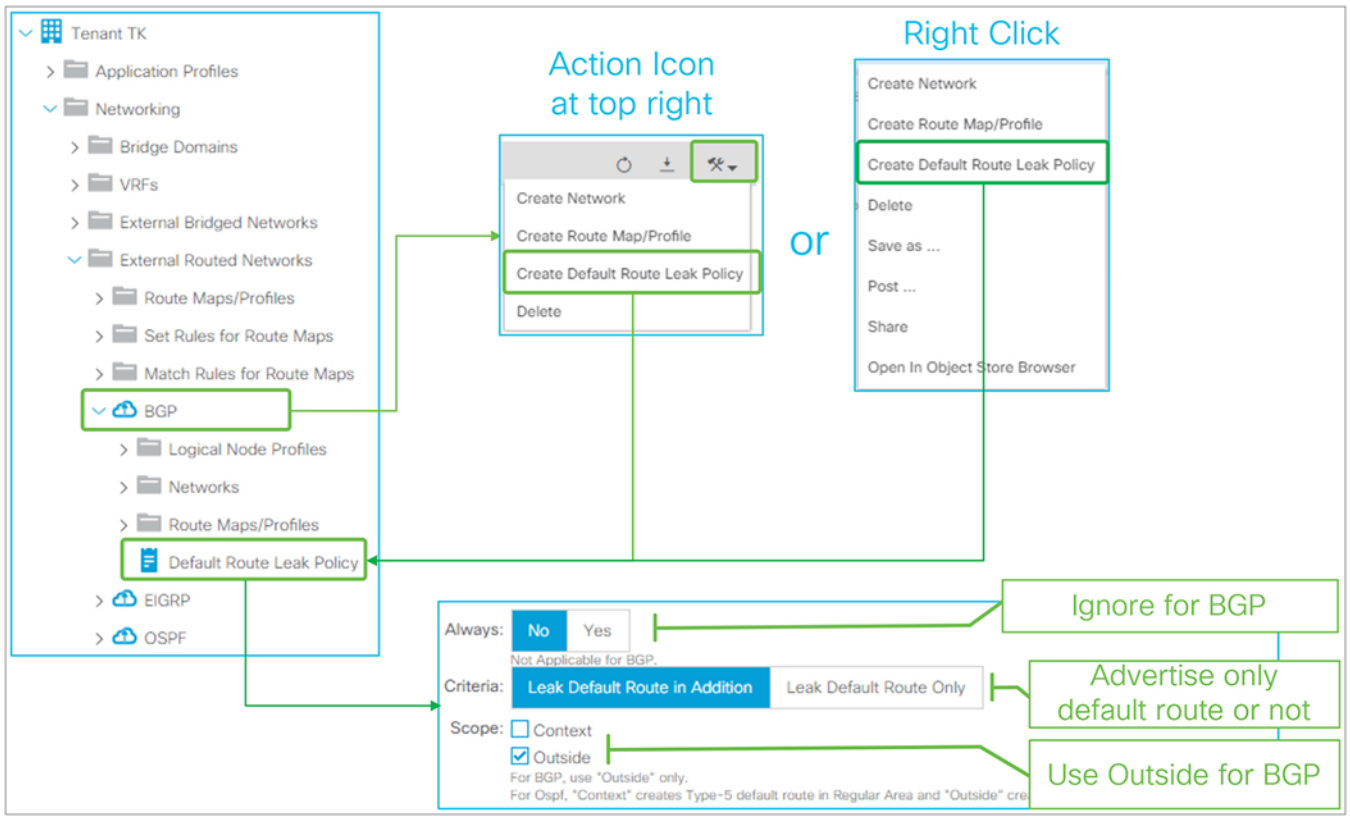

Figure 47.

GUI(APIC Release 3.2) 내 BGP 에 대한 기본 경로 유출 정책

기본 경로 유출 정책은 APIC Release 1.1(1)에서 도입되었으며 다음 수단 중 한 가지를 사용해 L3Out 에서 생성될 수 있습니다.

- L3Out 의 우측 상단에서 드롭다운 메뉴의 "기본 경로 유출 정책 생성"
- L3Out 자체의 우클릭 메뉴에서 "기본 경로 유출 정책 생성"

기본 경로 유출 정책에는 다음과 같은 매개변수가 포함됩니다.

- **항상**
  BGP 의 경우 이 옵션을 무시합니다.
- **기준**
  다른 경로 외에 기본 경로도 보급해야 하는 경우 "**기본 경로 추가로 유출**"을 사용합니다. 기본 경로만 보급해야 하는 경우 "**기본 경로만 유출**"을 사용합니다.

  "**기본 경로만 유출**"이 선택되면 이 L3Out 내 각 BGP 피어의 아웃바운드 경로 맵에 모두 거부가 적용됩니다.
- **범위**
  BGP 의 경우 "**외부**"를 사용합니다.

독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router bgp 65001
  vrf TK:VRF1
    neighbor 9.9.9.9
      address-family ipv4 unicast
        default-originate
```

L3Out OSPF

기본 OSPF 구성은 인프라 MP-BGP 의 ACI BGP AS 를 고려할 필요가 없으므로 ACI 의 BGP 보다 훨씬 더 단순합니다.

기본 구성 예시

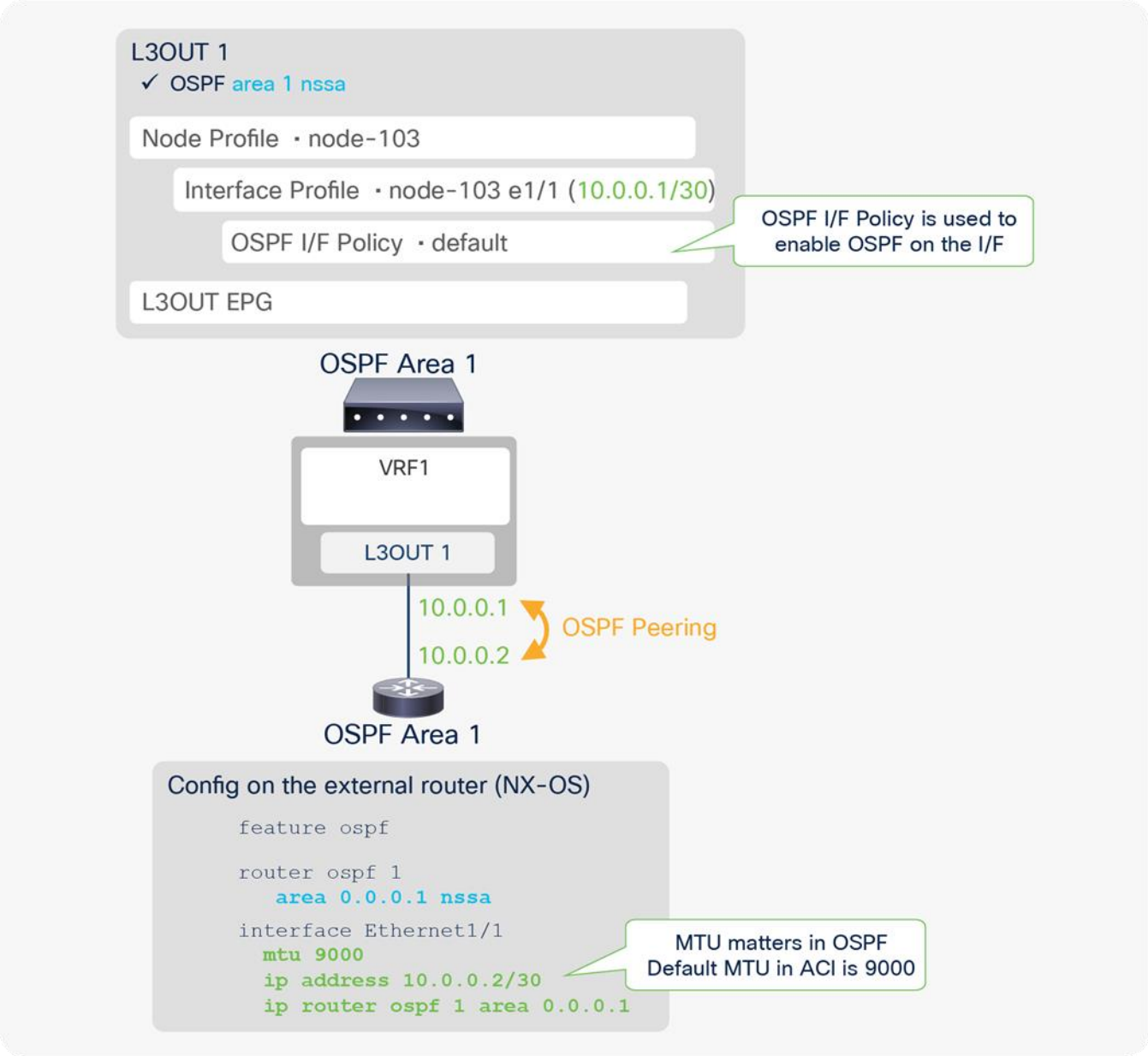

Figure 48.

OSPF 구성 도표

Figure 48 은 ACI 와 외부 라우터(이 경우 NX-OS)용 NSSA(Not-So-Stubby-Area)인 영역 1 이 포함된 ACI OSPF 의 구성 예시를 나타냅니다. 특히 OSPF 의 두 가지 필수 구성 요소는 다음과 같습니다.

- **영역 및 영역 유형**
  한 개의 L3Out 이 OSPF 영역을 의미한다는 뜻입니다. Figure 50 과 같이 여러 OSPF 영역이 구성되어야 할 경우, L3Out 도 여러 개로 구성되어야 합니다.
- **인터페이스에서 OSPF 활성화**
  논리 인터페이스 프로필에서 OSPF I/F 정책을 생성함으로써 수행됩니다. 논리 인터페이스 프로필에서 구성된 인터페이스의 독립 실행형 NX-OS 명령어 "**ip router ospf default area x**"를 수행하는 것에 해당합니다. 사용자는 인증과 인터페이스 네트워크 유형 등을 구성할 수 있지만 독립 실행형 NX-OS 와 마찬가지로 OSPF I/F 정책에서도 일반적으로 모든 값을 기본값으로 둘 수 있습니다.

ACI 에서 OSPF 인접 라우터를 성공적으로 설정하는 기타 요점은 OSPF 인접 라우터 기준이 MTU, 네트워크 마스크, 영역 ID, 영역 유형 등 인접 라우터와 일치하는지 확인하는 데 있습니다.

Figure 49 에는 APIC GUI 구성의 예시가 나와 있습니다.

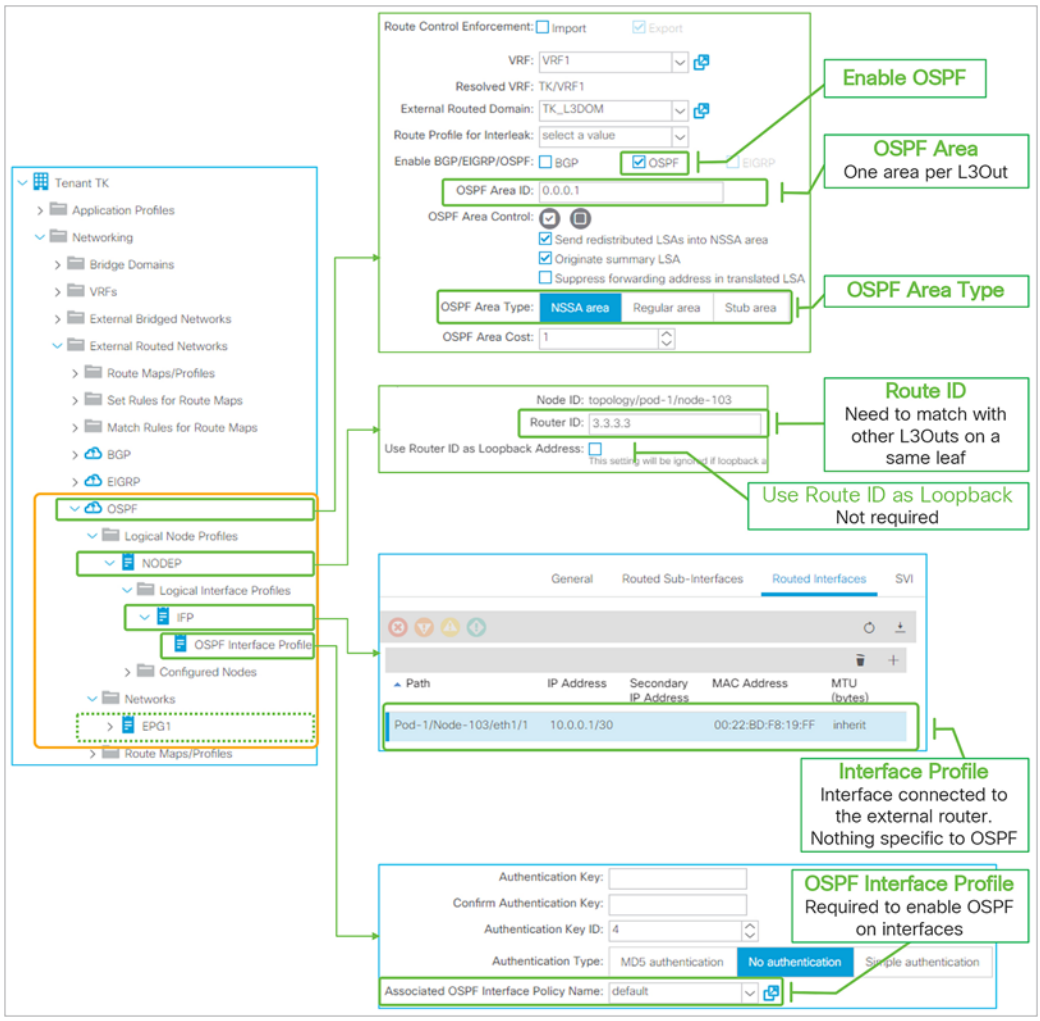

Figure 49.
GUI(APIC Release 3.2) 내 OSPF 의 기본 구성

제한 및 지침

- 각 OSPF L3Out 은 한 개의 OSPF 영역을 나타냅니다.

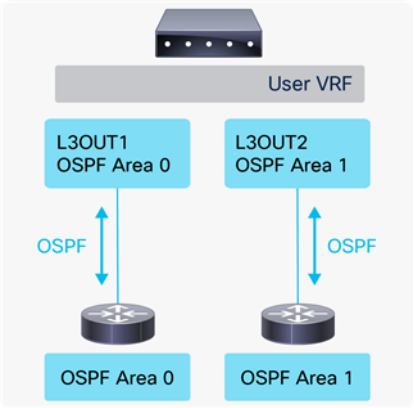

Figure 50.
L3Out OSPF 영역

  - 두 개의 OSPF L3Out 이 동일한 리프에 있다면 서로 다른 OSPF 영역에 위치해야 합니다.
  - 두 개의 OSPF L3Out 이 서로 다른 리프 스위치에 있다면 동일한 OSPF 영역에 위치할 수 있습니다.

- 동일한 L3Out 에서 OSPF 가 BGP 로서 활성화된 경우, OSPF 는 L3Out 루프백과 인터페이스 서브넷을 보급할 목적으로만 프로그래밍됩니다. 이러한 경우 기타 L3Out 은 동일한 VRF 내 동일한 보더 리프에서 OSPF 를 사용할 수 없습니다(F0467 오류 메시지 표시).
  OSPF 가 BGP 피어 연결 가능성을 지원하는 것 외에도 전송 라우팅을 수행하거나 BD 서브넷을 보급해야 하는 경우, OSPF 는 다른 L3Out 을 통해 IP 주소 등 동일한 매개변수가 포함된 BGP L3Out 으로 동일한 인터페이스에서 활성화되어야 합니다(SVI 의 경우 "캡슐화 범위 VRF"도 사용).
- 동일한 SVI/VLAN 이 포함된 OSPF L3Out 에 여러 개의 외부 라우터가 연결되면 동일한 L3Out BD 내에서 외부 라우터는 서로 간에 직접 인접 관계를 형성하게 됩니다. 자세한 내용은 "L3Out 브리지 도메인" 섹션의 Figure 20 을 참조하시기 바랍니다.
  이러한 경우 외부 라우터에서는 ACI L3Out BD 를 통해 OSPF LSA 를 송신하여 경로를 바로 교환합니다. 따라서 "경로 제어 서브넷 내보내기"가 포함된 전송 라우팅과 유사한 상황이 "경로 제어 서브넷 내보내기" 없이 발생할 수도 있습니다.
- BD 서브넷을 보급하거나 전송 라우팅을 수행할 때 경로는 보더 리프에서 자동으로 생성된 경로 맵을 통해 OSPF LSDB(연결 상태 데이터베이스)로 재배포됩니다. 이 경로 맵은 동일한 VRF 내 동일 리프에 있는 다른 OSPF L3Out 및 EIGRP 와 공유되는데, 이는 한 개의 L3Out 에 있는 서브넷 보급 구성이 다른 L3Out 에도 영향을 미칠 수 있음을 의미합니다. 따라서 동일한 VRF 의 동일 리프에 다른 L3Out 이

있을 경우 이 부분이 필요하다는 것을 인지해야 합니다. 자세한 내용은 "L3Out 전송 라우팅" 섹션의 Figure 93 을 참조하시기 바랍니다.

- IPv6 (OSPFv3)은 APIC Release 1.1(1)부터 지원됩니다.

OSPF 프로토콜 옵션(인터페이스 수준)

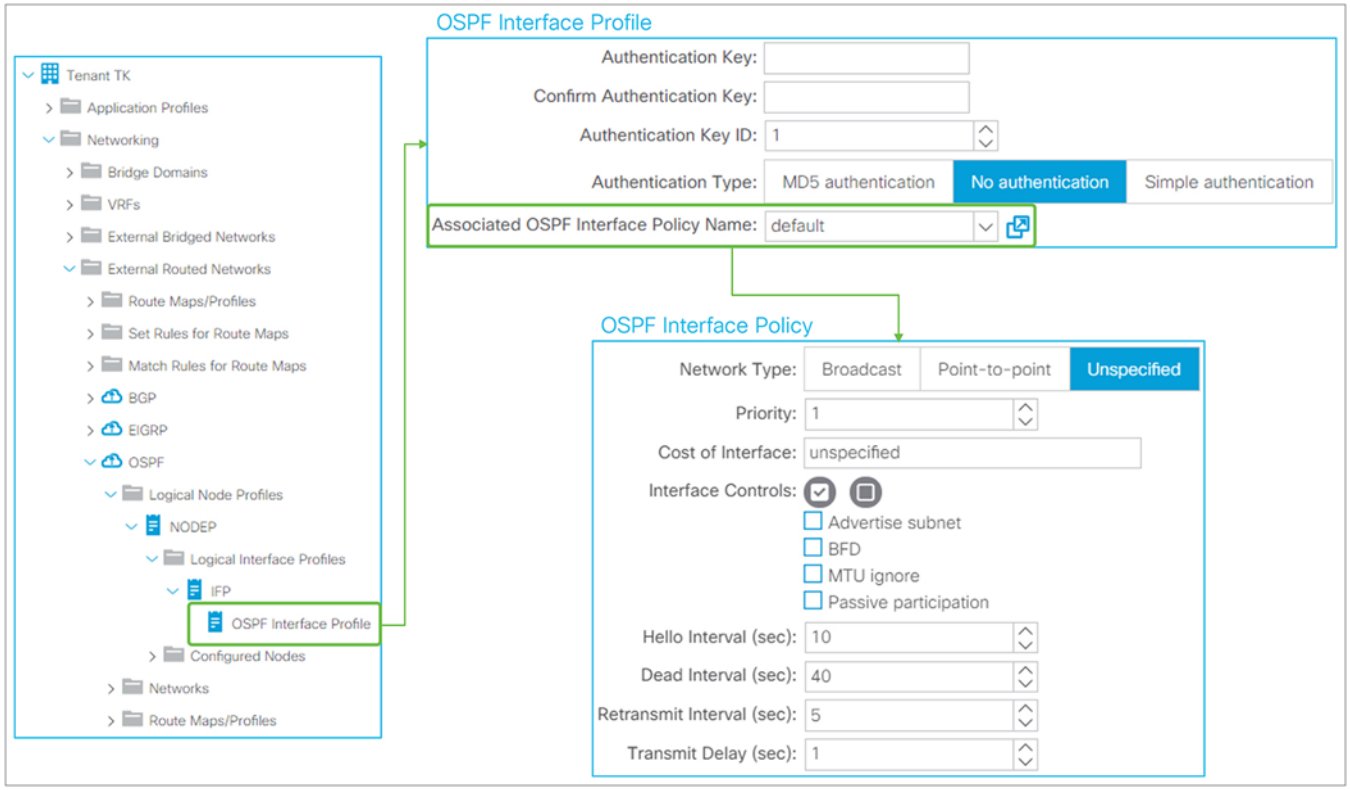

Figure 51.
GUI(APIC Release 3.2) 내 OSPF 인터페이스 프로필 및 정책

OSPF 인터페이스 프로필의 인터페이스 수준 OSPF 구성은 연결된 논리 인터페이스 프로필 내 모든 인터페이스에 적용됩니다. **OSPF 인터페이스 정책**은 **"Tenant > Policies > OSPF > OSPF Interface"**에 위치합니다.

- **인증**

  각 인터페이스 수준의 OSPF 인증입니다.

  - **인증 키:** 단순 및 MD5 인증에 모두 사용되는 암호입니다.
  - **인증 키 ID:** MD5 인증용 키 ID 로, 인접 장치와 일치해야 합니다.
  - **인증 유형:** 단순 또는 MD5 인증이 포함되지 않습니다.

독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
interface eth1/1
  ip ospf authentication
  ip ospf authentication-key <password>

interface eth1/1
  ip ospf authentication message-digest
  ip ospf message-digest-key <key id> md5 <password>
```

- **네트워크 유형**
  - 브로드캐스트

    이더넷 등의 브로드캐스트 트래픽을 허용하는 공유 매체로 통신할 수 있는 여러 개의 라우터가 포함된 네트워크입니다. 일반적으로 인터페이스 유형 SVI 에 사용됩니다. 이 유형에서는 OSPF DR(지정 라우터) 또는 BDR(예비 지정 라우터) 선택이 이루어집니다.
  - 지점 간

    두 개의 라우터 사이에만 존재하는 네트워크로, 일반적으로 라우팅된 인터페이스 또는 하위 인터페이스 유형에 사용됩니다. 이 유형에서는 OSPF DR 또는 BDR 선택이 이루어지지 않습니다.
  - 지정되지 않음

    네트워크 유형이 지정되지 않아 기본값인 브로드캐스트를 취합니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
interface eth1/1
  ip ospf network <broadcast or point-to-point>
```

- **우선 순위**

  OSPF DR 또는 BDR 선택을 위한 우선 순위입니다. 더 높은 수를 보유한 라우터가 DR 또는 BDR 로 선택됩니다. 인접 라우터의 우선 순위가 동일할 때는 IP 주소가 대신 사용됩니다. 우선 순위가 0 이라는 것은 이 인터페이스가 DR 선택에 관련되지 않았다는 의미입니다. 기본값은 1 입니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
interface eth1/1
  ip ospf priority <0-255>
```

- **인터페이스 비용**

  인터페이스에서의 OSPF 비용 또는 행렬입니다. 숫자가 낮을수록 행렬이 더 우수합니다. 기본값은 0 으로, 이는 인터페이스의 대역폭을 기준으로 비용이 계산된다는 의미입니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
interface eth1/1
ip ospf cost <1-65535>
```

- **인터페이스 제어**
  - 서브넷 보급

    이를 통해 OSPF 가 루프백에서 지점 간으로 네트워크 유형을 변경하지 않고, /32 대신 서브넷으로 루프백 IP 주소를 보급할 수 있습니다. 그러나 ACI 에서는 루프백 IP 주소가 항상 /32 로 구성되므로 이 옵션은 ACI 내 루프백 IP 에 /32 가 사용되지 않을 때까지 아무런 기능을 하지 않습니다.

    독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
interface loopback1
  ip ospf advertise-subnet
```

  - BFD

    APIC Release 1.2(2)에서 도입된 기능으로, OSPF 인터페이스에서 BFD 를 활성화하는 데 사용됩니다. 자세한 내용은 "L3Out BFD" 섹션을 참조하시기 바랍니다.

    독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
interface eth1/1
  ip ospf bfd
```

  - MTU 무시

    이 옵션을 통해 일치하지 않는 MTU 로도 OSPF 인접 라우터가 형성될 수 있습니다. 이 옵션은 낮은 MTU 로 OSPF 인터페이스에서 활성화되어야 합니다. 이는 일반적으로 권장되지 않는데, 그 이유는 네트워크 경로에 있는 MTU 가 OSPF 뿐만 아니라 대량의 페이로드를 보유할 가능성이 있는 기타 트래픽에 대해서도 항상 일치해야 하기 때문입니다. 특히 OSPF 의 경우, 인접 라우터가 설정되었더라도 더 높은 MTU 만큼 큰 OSPF DBD 패킷이 더 낮은 MTU 측면에서 삭제될 수 있습니다.

    독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
interface eth1/1
  ip ospf mtu-ignore
```

  - 수동 참여

    OSPF 수동 인터페이스로서 인터페이스를 구성하기 위한 옵션입니다.

    독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
interface eth1/1
  ip ospf passive-interface
```

- **Hello 간격(초)**

  OSPF Hello 패킷의 간격으로, 모든 OSPF 인접 라우터에서 일치해야 합니다. 기본값은 브로드캐스트 및 지점 간 OSPF 네트워크 유형의 기본값인 10 초입니다.

- **Dead 간격(초)**
  OSPF Hello 가 이 간격 내에서 수신되지 않으면 인접 라우터는 중지된 것으로 간주합니다. 기본값은 브로드캐스트 및 지점 간 OSPF 네트워크 유형의 기본값(4 x Hello 간격)인 40 초입니다.

- **재전송 간격(초)**
  OSPF LSA(연결 상태 보급) 재전송 간의 간격입니다. 라우터가 LSA 를 수신한 인접 라우터의 LSAck 를 기다리는 동안 재전송 간격이 발생합니다. 간격이 종료될 때까지 LSAck 가 수신되지 않으면 LSA 가 재송신됩니다. 기본값은 5 초입니다.
- **전송 지연(초)**
  이 시간은 초과 업데이트에 대한 LSU(연결 상태 업데이트) 패킷에서 복사될 때 각 LSA 의 LS 기간에 추가됩니다. 이는 각 LSA 가 인접 라우터에 도달할 때 적절한 기간이 확보되도록 전송 지연(LSU 가 인접 라우터에 도달하는 데 소요되는 시간)을 고려하기 위함입니다. 그렇지 않으면 인접 라우터의 LSA 가 LSA 의 공급자보다 이력이 더 짧을 수도 있습니다. 기본값은 1 초입니다. 빠른 최신 네트워크에서는 이 값이 변경될 필요가 없습니다.

  상기 타이머에 대한 독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
interface eth1/1
  ip ospf hello-interval <sec>
  ip ospf dead-interval <sec>
  ip ospf retransmit-interval <sec>
  ip ospf transmit-delay <sec>
```

OSPF 프로토콜 옵션(L3Out 수준)

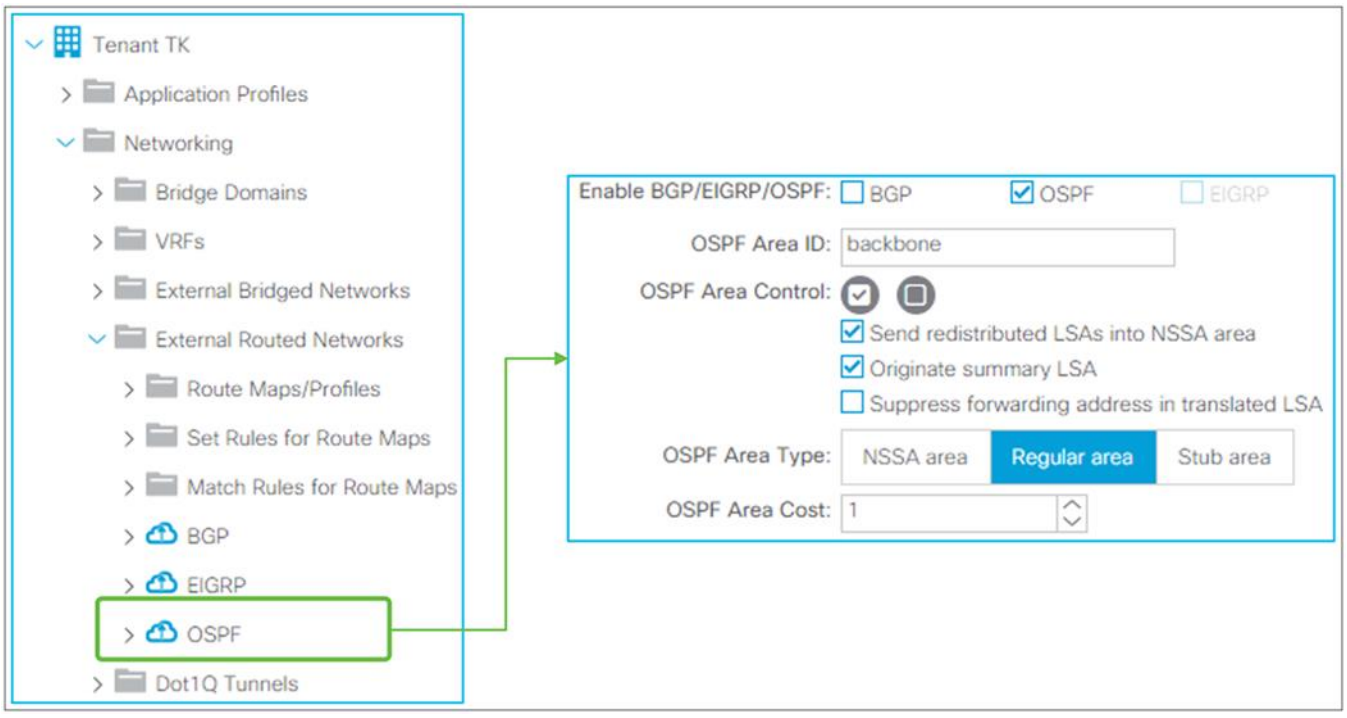

Figure 52.
GUI(APIC Release 3.2) 내 OSPF 프로토콜 옵션

- **OSPF 영역 ID**

  본 L3Out 내 모든 인터페이스에 대한 OSPF 영역 ID 입니다. 영역 0 은 "backbone" 문자열로도 구성할 수 있으며, 숫자를 사용하는 방법도 있습니다.

- **OSPF 영역 제어**

  - 재배포된 LSA 를 NSSA 영역에 송신

    OSPF NSSA(not-so-stubby area)를 위한 옵션으로, 표준 OSPF 동작과 정렬되도록 기본값으로 활성화되어 있습니다. 이 옵션이 비활성화되면 재배포된 경로는 보더 리프에서 이 NSSA 영역으로 송신되지 않습니다. 이는 일반적으로 **요약 LSA 시작** 옵션이 함께 비활성화되었을 때 사용되는데, 그 이유는 **요약 LSA 시작** 옵션을 해제하면 기본 경로가 생성되어 NSSA 또는 스텁 영역으로 송신되기 때문입니다.

    이 옵션을 비활성화하는 독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router ospf 1
  vrf TK:VRF1
    area 0.0.0.1 nssa no-redistribution
```

  - 요약 LSA 시작

    OSPF NSSA 또는 스텁 영역을 위한 옵션으로, 표준 OSPF 동작과 정렬되도록 기본값으로 활성화되어 있습니다. 이 옵션이 비활성화되면 보더 리프에서 유형 4 와 5 외에 유형 3 LSA 도 NSSA 또는 스텁 영역으로 송신되지 않습니다. 대신 보더 리프에서 기본 경로를 생성하여 해당 영역으로 송신합니다. 초기에 이 영역에 유형 3 LSA 가 없는 경우에는 기본 경로가 생성되지 않습니다.

    이 옵션을 비활성화하는 독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router ospf 1
  vrf TK:VRF1
    area 0.0.0.1 nssa no-summary
```

  - 변환된 LSA 에서 전환 주소 저지

    OSPF NSSA 에 대한 옵션으로, 기본적으로 비활성화되어 있습니다. OSPF NSSA ABR(영역 보더 라우터)에서는 유형 7 LSA 를 유형 5 로 변환하여 NSSA 외부 영역에 송신합니다. 이때 재배포된 경로의 공급자 ASBR(자치 시스템 보더 라우터)의 IP 주소가 전환 주소로서 LSA 에 추가됩니다. 유형 5 LSA 를 수신하는 OSPF 라우터가 전환 주소 IP 에 대한 경로를 보유하지 않고, 유형 5 의 경로가 라우터의 경로 테이블에 설치되지 않도록 차단하는 경우도 있습니다. 이 문제는 유형 7 에서 유형 5 로 변환이 이루어질 때 ACI 보더 리프(OSPF NSSA ABR)가 전환 주소를 LSA 에 추가하지 못하도록 막는 이 옵션을 활성화하여 방지할 수 있습니다.

    APIC Release 1.2(2)에서 도입된 옵션으로,

    이 옵션을 활성화하는 독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router ospf 1
  vrf TK:VRF1
```

```
area 0.0.0.1 nssa translate type7 suppress-fa
```

- **OSPF 영역 유형**

  ACI 에서는 다음 세 가지 OSPF 영역 유형을 모두 지원합니다. 일반, NSSA, 스텁 영역

- **OSPF 영역 비용**

  이 옵션은 보더 리프가 기본 경로를 생성하는 OSPF 스텁 영역인 경우와 같이, 보더 리프에서 생성된 기본 경로에 대한 OSPF 비용을 설정합니다.

  이 옵션을 활성화하는 독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router ospf 1
  vrf TK:VRF1
    area 0.0.0.1 default-cost <cost>
```

OSPF 프로토콜 옵션(VRF 수준)

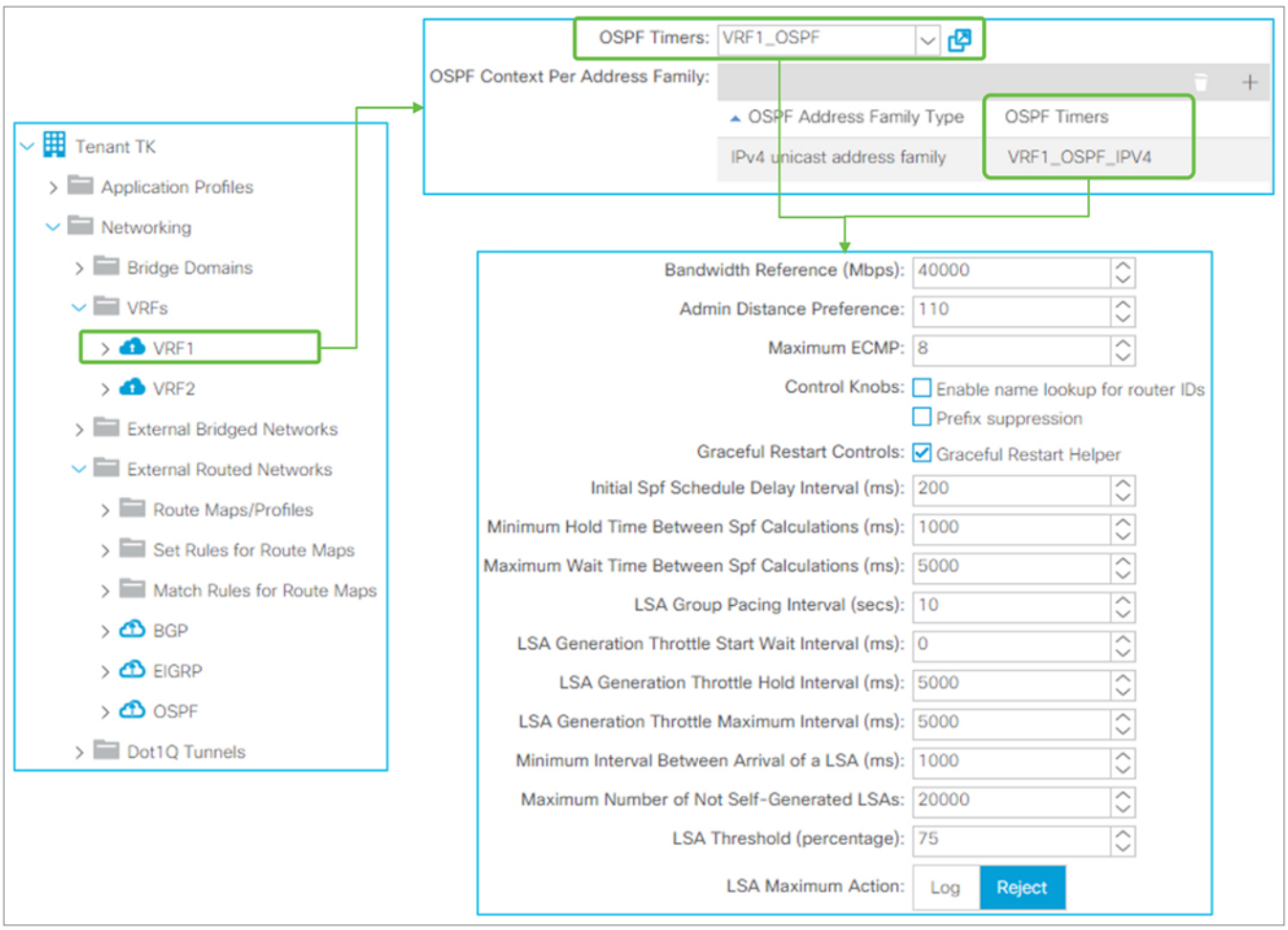

Figure 53.

OSPF 타이머 정책

OSPF 타이머 정책(각 VRF 와 주소 패밀리)

이 정책은 VRF 에서 사용되지만 OSPF 타이머 정책은 **"Tenant > Policies > OSPF > OSPF Timers"**에 위치합니다. 주소 패밀리가 아닌 VRF 마다 구성되면 정책은 OSPFv2 와 OSPFv3 에 모두 적용됩니다. 주소 패밀리마다 구성되면 정책은 주소 패밀리에만 적용됩니다(주소 패밀리가 IPv4 인 경우 OSPFv2 에 정책이 적용됨). 두 가지가 모두 구성되면 VRF 별 정책보다 주소 패밀리별 정책이 더 많이 사용됩니다.

OSPF 타이머 정책에는 타이머 외에도 몇 가지 구성 매개변수가 있습니다. 다음 내용은 각 매개변수에 대한 설명입니다.

- **광대역 참조(Mbps)**
  OSPF 인터페이스에 대한 기본 행렬을 계산하는 데 사용되는 참조 광대역으로, 기본값은 40,000Mbps(40Gbps)입니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router ospf 1
  vrf TK:VRF1
    auto-cost reference-bandwidth <number> Mbps
```

- **관리 거리 설정**
  OSPF 에 대한 관리 거리로, 기본값은 110 입니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router ospf 1
  vrf TK:VRF1
    distance <number>
```

- **최대 ECMP**
  OSPF 가 라우팅 테이블에 설치할 수 있는 ECMP 의 최대 수로, 기본값은 8 개 경로입니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router ospf 1
  vrf TK:VRF1
    maximum-paths <number>
```

- **제어 노브**
  APIC Release 1.2(2)에서 도입된 두 개의 노브입니다.

  ◦ 라우터 ID 에 대한 이름 검색 활성화
  OSPF 표시 명령어 내에서 라우터 ID 를 DNS 이름으로 표시하는 기능으로, 기본적으로 비활성화되어 있습니다.
  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router ospf 1
  vrf TK:VRF1
    name-lookup
```

- 식별 번호 저지

라우팅 테이블에서 설치 또는 보급되는 경로의 수를 최소화하는 옵션입니다. 기본적으로 비활성화되어 있지만 활성화되면 다음과 같은 저지 작업이 이루어집니다.

유형 1 LSA: 지점 간 링크에 대한 연결된 서브넷을 나타내는 자체 생성된 유형 1 LSA 의 "스텁 네트워크 연결 링크"라는 링크 유형은 인접 라우터로 보급되지 않습니다.

유형 2 LSA: LS 유형 "네트워크 링크"가 있는 자체 생성된 LSA 는 브로드캐스트 링크에 대한 연결된 서브넷을 나타내며 실제 네트워크 마스크가 아닌 /32 네트워크 마스크로 보급됩니다. 식별 번호 저지를 지원하는 플랫폼에서는 이 /32 LSA 가 라우팅 테이블에 설치되지 않습니다.

독립 실행형 NX-OS 에 대응하는 명령어는 없으나 IOS 에 대응하는 명령어는 다음과 같습니다.

```
router ospf 1
  prefix-suppression
```

- **정상 재시작 제어(정상 재시작 도우미)**

OSPF 라우터가 정상 재시작을 유도하면 OSPFv2 의 불투명 LSA 또는 OSPFv3 의 정상 LSA 를 인접 라우터로 송신합니다. 이 LSA 에는 인접 라우터 인터페이스가 재시작 중인 라우터의 LSA 를 유지하는 시간인 정상 기간이 포함됩니다. 재시작 중인 라우터에서 정상 기간을 수신하는 인접 라우터를 정상 재시작 도우미라고 부릅니다. ACI 에서는 정상 재시작 도우미 기능만 제공됩니다. 정상 기간 동안 정상 재시작 도우미는 재시작 중인 라우터에서 시작된 모든 LSA 를 유지합니다.

독립 실행형 NX-OS 에 대응하는 명령어는 없습니다. 독립 실행형 NX-OS 에서 정상 재시작 라우터와 도우미 기능을 한 번에 활성화하는 명령어는 다음과 같습니다.

```
router ospf 1
  vrf TK:VRF1
    graceful-restart
```

- **최초 SPF 일정 지연 간격(마이크로초)**
- **SPF 계산 간 최소 보류 시간(마이크로초)**
- **SPF 계산 간 최대 대기 시간(마이크로초)**

SPF 계산 타이머에 대한 독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router ospf 1
  vrf TK:VRF1
    timers throttle spf <initial delay> <minimum hold> <maximum wait>
```

- **LSA 그룹 속도 간격(초)**

LSA 그룹 속도에 대한 독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router ospf 1
```

```
  vrf TK:VRF1
    timers lsa-group-pacing <msec>
```

- **LSA 세대 제한 시간 대기 간격(마이크로초)**
- **LSA 세대 제한 보류 간격(마이크로초)**
- **LSA 세대 제한 최대 간격(마이크로초)**

LSA 생성 타이머에 대한 독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router ospf 1
  vrf TK:VRF1
    timers throttle lsa <start> <hold> <maximum>
```

- **LSA 의 도착 간 최소 간격(마이크로초)**

최소 LSA 도착 간격에 대한 독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router ospf 1
  vrf TK:VRF1
    timers lsa-arrival <msec>
```

- **자체 생성되지 않은 LSA 의 최대 수**
- **LSA 임곗값(퍼센트)**
- **LSA 최대 작업(로그 또는 거부)**

최소 LSA 도착 간격에 대한 독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router ospf 1
  vrf TK:VRF1
    max-lsa <max lsa> <threshold> {warning-only}
```

OSPF 경로 요약

APIC Release 1.2(2)에서 도입된 기능으로, ACI BGP L3Out 에서 BD 서브넷 및/또는 전송 경로에 대한 요약된 식별 번호만 외부로 보급합니다. OSPF 에서 ACI 는 두 가지 요약 방법을 지원합니다.

- 재배포된 경로 요약: "**summary-address <prefix>/<mask>**"에 해당합니다.
- 영역 간 경로 요약: "**area <ID> range <prefix>/<mask>**"에 해당합니다.

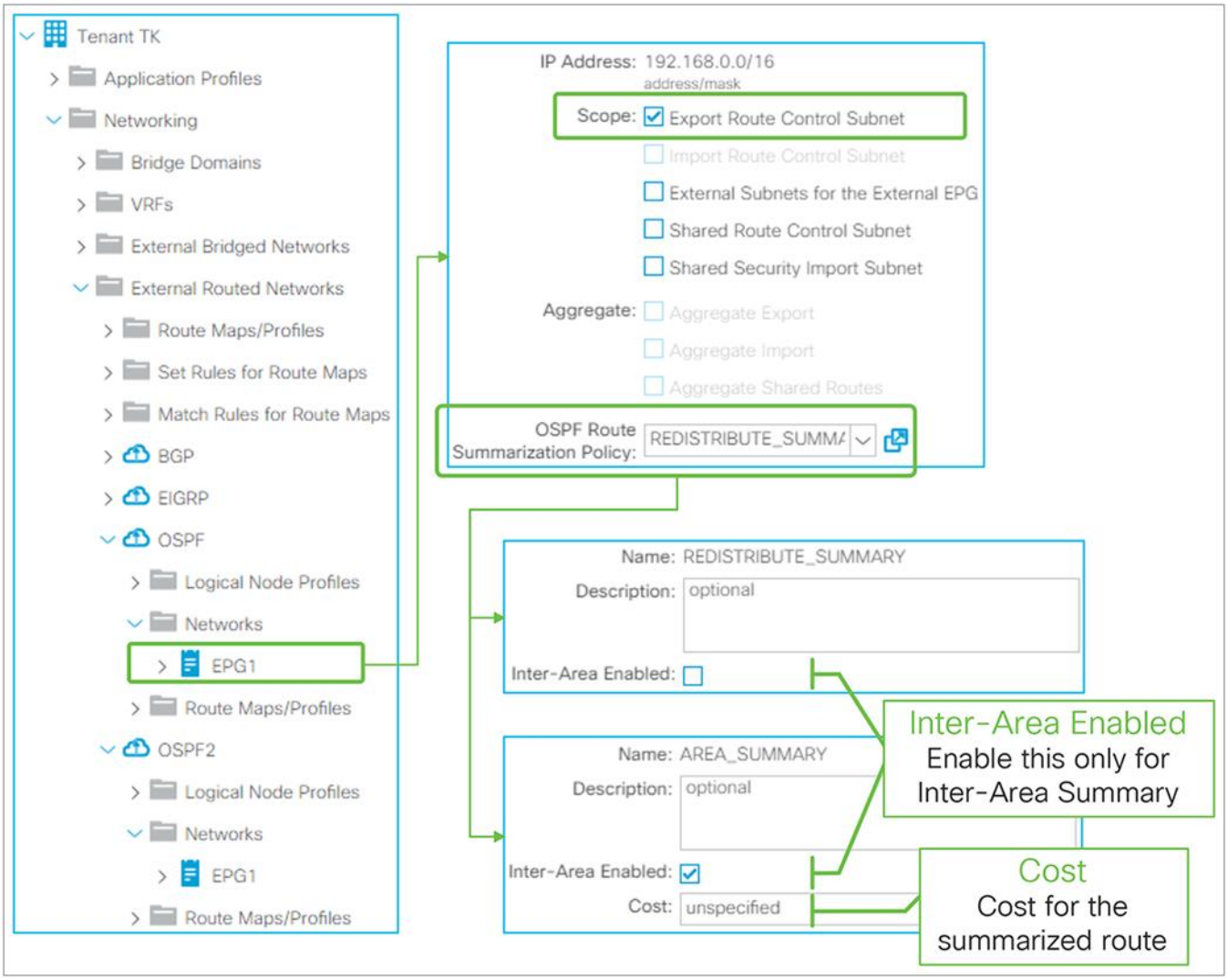

Figure 54.

GUI(APIC Release 3.2) 내 OSPF 경로 요약

ACI 내 OSPF 경로 요약은 "경로 제어 서브넷 내보내기" 범위를 사용해 경로 요약 정책을 L3Out 서브넷에 추가함으로써 구성되는데, 그 이유는 ACI 에서 외부로 경로를 보급하는(내보내는) 데 사용되기 때문입니다. "경로 제어 서브넷 내보내기" 범위에 대한 자세한 내용은 "L3Out 전송 라우팅" 섹션을 참조하시기 바랍니다.

Figure 54 에서와 같이, L3Out 서브넷에 경로 요약 정책을 추가하면 보더 리프가 요약된 경로(Figure 54 의 192.168.0.0/16)에 대한 Null-0 항목을 생성하며, 이는 OSPF 피어로 보급됩니다. Null-0 다음 홉이 있는 요약된 경로는 인프라 MP-BGP 를 통해 다른 리프 스위치로 보급되지 않습니다. 일반적인 OSPF 라우터와 마찬가지로, 보더 리프의 VRF 에 대한 OSPF 데이터베이스에 기여 경로가 존재하지 않는 경우에는 요약이 발생하지 않는다는 점에 유의해야 합니다.

BGP 나 EIGRP 와는 달리, OSPF 가 경로를 외부에 보급하는 데 재배포를 사용하지 않는 예외적인 시나리오가 한 가지 존재합니다. 동일한 보더 리프에 있는 두 개의 OSPF L3Out 간 전송 라우팅을 수행하는 경우입니다(자세한

내용은 "L3Out 전송 라우팅" 섹션 참조). 따라서 위에서 언급한 대로 ACI 는 두 가지 방법의 OSPF 경로 요약을 지원합니다. 두 가지 요약 방법에 대한 자세한 구성 지침과 토폴로지는 다음과 같습니다.

OSPF 경로 요약(재배포된 경로)

재배포된 경로 요약은 동일한 보더 리프에 두 개의 OSPF L3Out 이 있는 경우를 제외하고 모든 OSPF 요약에 대해 사용됩니다. OSPF 재배포된 경로 요약(Figure 54 와 Figure 55 의 192.168.0.0/16)에서는 "**영역 간 활성화됨**" 옵션 없이 OSPF 경로 요약 정책을 사용합니다. 해당 옵션을 사용하지 않으면 이는 독립 실행형 NX-OS 의 "**요약 주소 192.168.0.0/16**"에 해당합니다. 이는 재배포된 외부 경로인 유형 5 또는 유형 7 LSA 에서 구성된 서브넷(Figure 54 또는 Figure 55 의 192.168.0.0/16)에 있는 모든 경로의 요약을 시도하게 됩니다. 이 방법으로 요약할 수 있는 LSA 가 없을 경우 요약은 일어나지 않으며 192.168.0.0/16 에 대한 Null-0 항목도 생성되지 않습니다. 이는 OSPF 요약이 일어나려면 한 개 이상의 서브넷이 OSPF L3Out(Figure 55 내 L3Out 3)으로 재배포되어야 한다는 의미입니다.

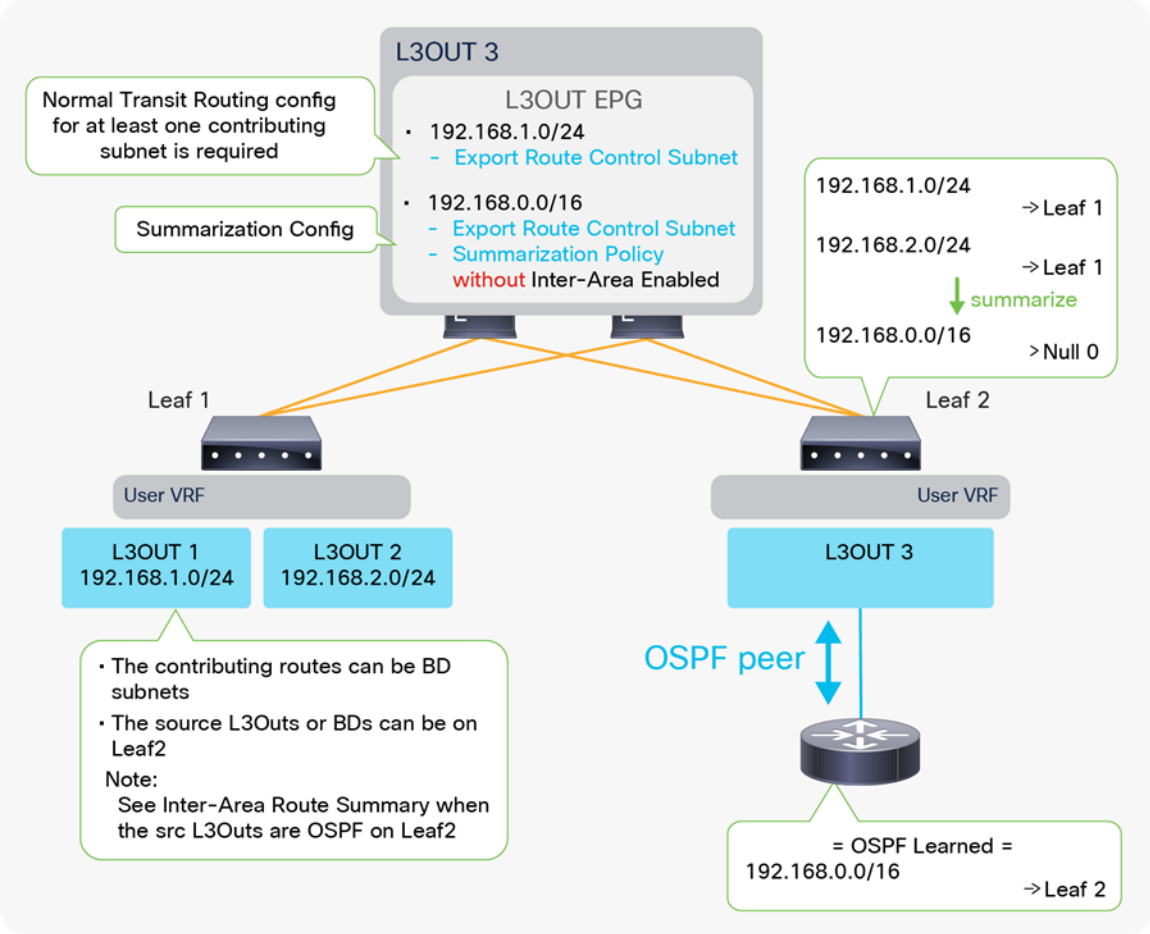

Figure 55.
OSPF 경로 요약 토폴로지(경로 재배포) 예시

Figure 55 는 L3Out 3 가 L3Out 1 과 2(192.168.1.0/24 및 192.168.2.0/24)에서 전송 경로에 대해 요약된 서브넷(192.168.0.0/16)만 보급하는 경우를 나타냅니다. 요약을 수행하려면 L3Out 3 에 대한 OSPF LSDB 내에 한 개 이상의 기여 서브넷이 필요합니다. 따라서 Figure 55 에서는 한 개 이상의 구성 서브넷에 대한 전송 라우팅

구성("경로 제어 서브넷 가져오기" 범위)이 필요합니다. BD 서브넷을 요약하는 경우, 적합한 BD 서브넷 보급 구성이 한 개 이상의 서브넷에 필요합니다("ACI BD 서브넷 보급" 섹션 참조).

독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router ospf 1
  vrf TK:VRF1
    summary-address <prefix>/<mask>
```

OSPF 경로 요약(영역 간 경로)

동일한 보더 리프에 여러 개의 OSPF L3Out 이 있는 경우 각 L3Out 은 서로 다른 OSPF 영역을 관리합니다. 따라서 L3Out 간의 전송 라우팅에서는 재배포 대신 영역 필터가 사용됩니다. 이러한 경우, 이전 요약 옵션은 재배포된 유형 5 와 유형 7 LSA 에 대한 것이므로 이전 옵션을 사용해 경로 요약을 수행할 수 없습니다. 이러한 문제를 해결하기 위해 ACI 에서는 영역 간 경로 요약을 제공합니다.

참고:

여러 개의 OSPF L3Out 이 동일한 보더 리프가 아닌 서로 다른 보더 리프 스위치에 배포될 경우 한 개의 OSPF L3Out 은 인프라 MP-BGP 를 통해 다른 OSPF L3Out 에서 전송 경로를 수신하게 됩니다. 따라서 재배포를 계속 사용하며 영역 간 경로 요약이 아닌 재배포된 경로 요약에 의존합니다. OSPF L3Out 이 전송 라우팅을 구현하는 방식에 대한 자세한 내용은 "L3Out 전송 라우팅" 섹션을 참조하시기 바랍니다.

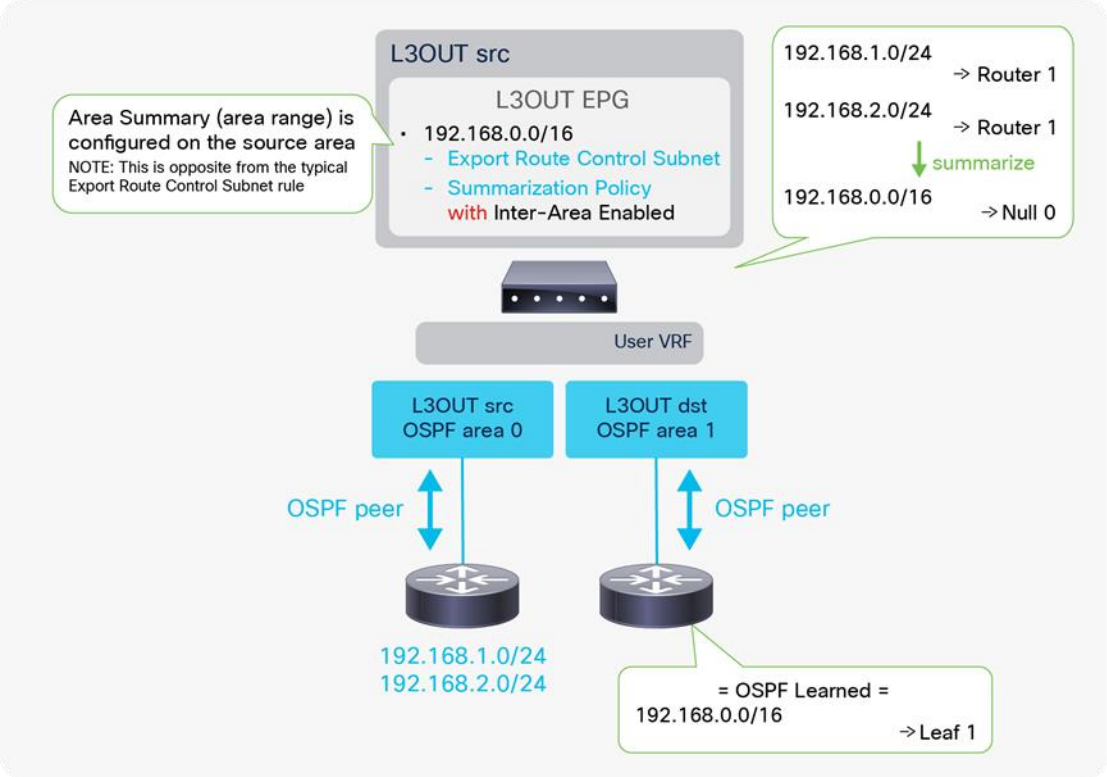

Figure 56.

OSPF 경로 요약 토폴로지(영역 간 경로)에 대한 예시

OSPF 영역 간 경로 요약에서는 "**영역 간 활성화됨**" 옵션을 통한 OSPF 경로 요약 정책을 사용합니다. 이 옵션을 사용하면 독립 실행형 NX-OS 의 "**area 0 range 192.168.0.0/16**"에 대응하는 기능이 됩니다. 영역 범위 명령어가 요약되어야 할 경로를 보유한 원본 영역에서 구성되므로 ACI 에서의 이 구성은 다른 L3Out 경로 요약과는 달리 원본 L3Out 에서도 구성됩니다(Figure 56 의 "L3Out src"). 원본 L3Out 이 요약되어야 할 경로를 학습 중이라고 가정하면(Figure 56 의 192.168.x.0/24) 해당 요약은 별도의 ACI 구성 없이 이루어지며 요약된 경로(Figure 56 의 192.168.0.0/16)는 대상 L3Out(L3Out dst)에서 외부로 보급됩니다.

참고:

동일한 VRF 의 동일한 보더 리프에 다른 OSPF L3Out 이 있을 경우, 원본 L3Out 을 제외하고 모든 OSPF L3Out 에서 요약된 경로가 보급됩니다. 이는 동일한 보더 리프에서 OSPF L3Out(OSPF 영역) 간의 전송 경로를 제어하는 영역 필터가 동일한 VRF 의 동일한 보더 리프에서 모든 OSPF L3Out 에 대해 동일한 경로 맵을 사용하기 때문입니다. 영역 필터에 대한 공유된 경로 맵에서는 원본 L3Out 의 "경로 제어 서브넷 내보내기" 범위로 인해 요약된 식별 번호(Figure 56 의 192.168.0.0/16)가 허용됩니다. 이는 동일한 VRF 의 동일한 보더 리프에 있는 모든 L3Out 이 공유된 경로 맵으로 인해 요약된 식별 번호의 허용을 시도한다는 것을 뜻합니다. 이는 대상 L3Out 에서 구성이 불필요한 이유이기도 합니다. 자세한 내용은 "L3Out 전송 라우팅" 섹션의 "전송 라우팅에 대한 내부 경로 맵"을 참조하시기 바랍니다.

참고:

이는 "경로 제어 서브넷 내보내기" 범위를 사용하는 매우 이례적인 방법입니다. 이 범위는 일반적으로 경로가 외부로 보급 또는 내보내기되어야 하는 대상 L3Out(이 예시에서는 "L3Out dst")에서 구성되기 때문입니다. "경로 제어 서브넷 내보내기"의 일반적인 사용법에 대한 자세한 내용은 "L3Out 서브넷 범위 옵션" 섹션 또는 "L3Out 전송 라우팅" 섹션을 참조하시기 바랍니다.

영역 간 경로 요약의 경우 요약된 경로에 대한 비용을 구성할 수 있습니다. 지정되지 않은 경우, 요약 정책을 통한 원본 L3Out 은 기여 경로의 최대 비용을 사용합니다. 이는 요약된 경로의 비용을 확인하도록 RFC 2328 에서 정의된 방법입니다.

독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router ospf 1
  vrf TK:VRF1
    area <source area id> range <prefix>/<mask> {cost <num>}
```

OSPF 기본 경로 보급

기본 경로(0.0.0.0/0)를 OSPF L3Out 에서 외부로 보급하는 데는 여러 가지 방법이 있습니다. 여기에서는 OSPF 내 기본 경로 유출 정책의 기초를 살펴본 후 각 OSPF 영역 유형에 사용되는 방법을 간략하게 설명합니다. OSPF 내 기본 경로를 보급하는 방법으로 기본 경로 유출 정책이 반드시 정답은 아니라는 점에 유의해야 합니다. 예를 들어 OSPF 스텁 영역에 대해서는 아무런 조치를 취하지 않는데 그 이유는 기본 경로 유출 정책이 근본적으로 "default-information originate" 또는 "area <ID> nssa default-information-originate"와 동일하기 때문입니다. 따라서 표준 OSPF 영역 동작을 반드시 이해해야 합니다.

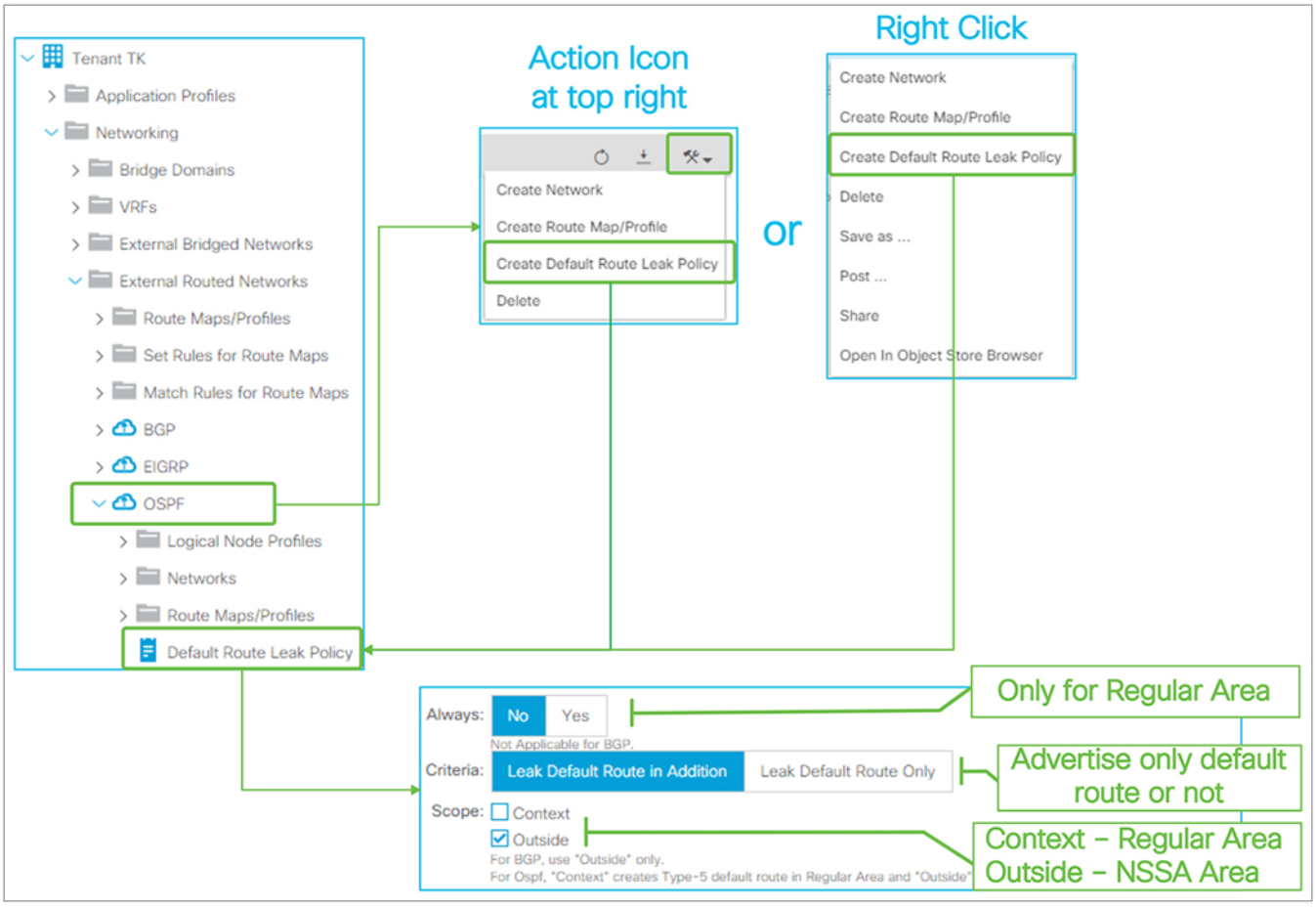

Figure 57.

GUI(APIC Release 3.2) 내 OSPF 에 대한 기본 경로 유출 정책

기본 경로 유출 정책은 APIC Release 1.1(1)에서 도입되었으며 다음 수단 중 한 가지를 사용해 L3Out 에서 생성될 수 있습니다.

- L3Out 의 우측 상단에서 드롭다운 메뉴의 "기본 경로 유출 정책 생성" 선택
- L3Out 자체의 우클릭 메뉴에서 "기본 경로 유출 정책 생성" 선택

기본 경로 유출 정책에는 다음과 같은 매개변수가 포함됩니다.

- **항상**
  OSPF 정규 영역에만 적용 가능합니다. **항상**이 "예"로 설정되어 있을 경우, 라우팅 테이블에 기본 경로가 없더라도 OSPF LSDB 에서 기본 경로가 생성됩니다.
- **기준**
  다른 경로 외에 기본 경로도 보급해야 하는 경우 "**기본 경로 추가로 유출**"을 사용합니다. 기본 경로만 보급해야 하는 경우 "**기본 경로만 유출**"을 사용합니다.

  "**기본 경로만 유출**"이 선택되면 해당 L3Out 내 모든 재배포 및 영역 필터에 대한 경로 맵에 모두 거부가 적용되어 다른 경로가 보급되는 것을 방지합니다.
- **범위**
  OSPF 정규 영역에 대해 "컨텍스트"를 선택합니다. OSPF NSSA 영역에 대해 "외부"를 선택합니다.

OSPF 정규 영역에 대한 독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router ospf 1
  vrf TK:VRF1
    default-information originate [always]
```

OSPF NSSA 영역에 대한 독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router ospf 1
  vrf TK:VRF1
    area 0.0.0.1 nssa default-information-originate
```

OSPF 스텁 영역의 기본 경로

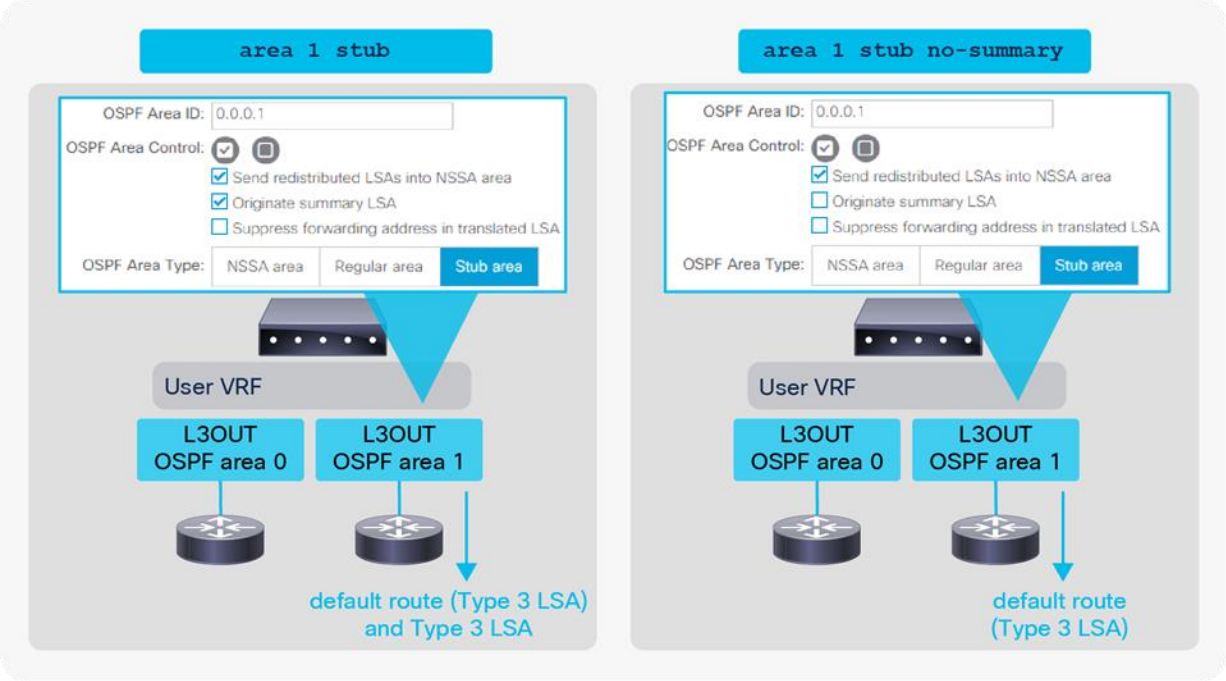

Figure 58.
OSPF 스텁 영역 내 기본 경로 보급

- **기본 스텁 동장(Figure 58 의 좌측)**
  OSPF ABR 에서는 기본값으로 기본 경로를 생성해 이를 다른 유형 3 LSA 와 함께 스텁 영역으로 송신합니다.
- **완전한 스텁** 동작**(Figure 58 의 우측)**
  L3Out 의 루트 아래에 있는 "**요약 LSA 시작**" 옵션을 비활성화하면 스텁 영역은 완전한 스텁 영역이 됩니다. 이후 기본 경로가 생성되고 기본 경로만 보급됩니다.

OSPF NSSA 영역의 기본 경로

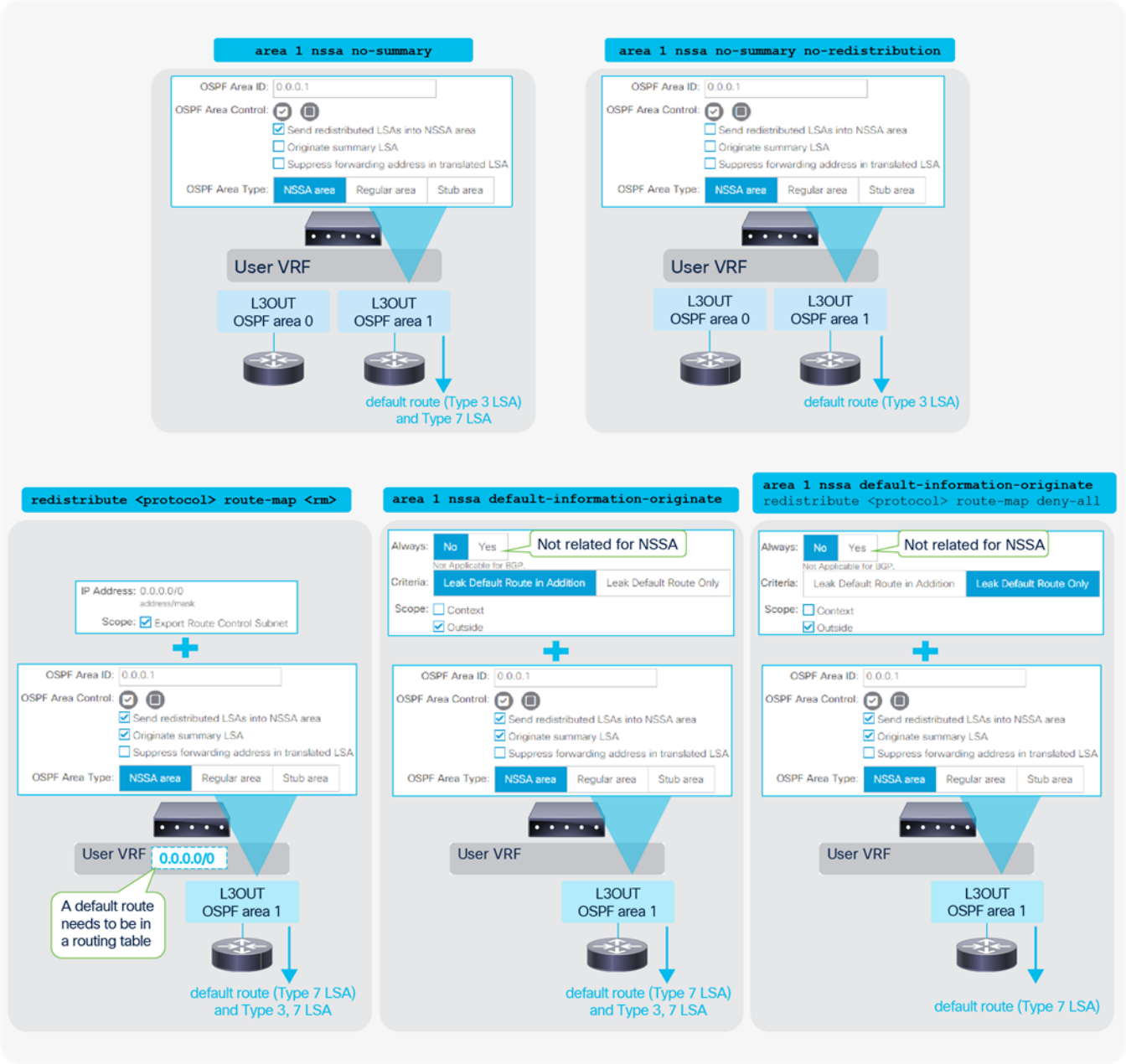

Figure 59.

OSPF NSSA 영역 내 기본 경로 보급

- **완전한 NSSA 동작(상단의 두 도표)**

  L3Out 의 루트 아래에 있는 "**요약 LSA 시작**" 옵션을 비활성화하면 NSSA 영역은 완전한 NSSA 영역이 됩니다. 이후 기본 경로가 생성되고 다른 유형 3 LSA 가 저지됩니다. 보더 리프가 ASBR 이면서 ABR 인 경우 기본 경로 외에도 유형 7 LSA 가 보급될 수 있습니다. 이 유형 7 LSA 는 "**재배포된 LSA 를 NSSA 영역으로 송신**" 옵션을 비활성화하여 저지할 수도 있습니다.

- **전송 라우팅(좌측 하단의 도표)**
  다른 L3Out 또는 고정 경로에서 "경로 제어 서브넷 내보내기" 범위를 통해 기본 경로를 내보내는 옵션입니다. 자세한 내용은 "L3Out 전송 라우팅" 섹션을 참조하시기 바랍니다.
- **기본 경로 유출 정책(우측 하단의 두 도표)**
  L3Out 에서 기본 경로 유출 정책을 사용하는 옵션입니다. 기본 경로 유출 정책은 위 내용을 참고하시기 바랍니다.

OSPF 정규 영역의 기본 경로

Figure 60.
OSPF 정규 영역의 기본 경로 보급

- **전송 라우팅(좌측의 도표)**
  다른 L3Out 에서 "경로 제어 서브넷 내보내기" 범위를 통해 기본 경로를 내보내는 옵션입니다. 자세한 내용은 "L3Out 전송 라우팅" 섹션을 참조하시기 바랍니다.
- **기본 경로 유출 정책(우측의 4 가지 도표)**
  L3Out 에서 기본 경로 유출 정책을 사용하는 옵션입니다. 기본 경로 유출 정책은 위 내용을 참고하시기 바랍니다.

참고:

기본 경로 유출 정책이 한 개의 L3Out 에서 **컨텍스트** 범위와 함께 구성되면 동일한 보더 리프의 동일한 VRF 에서 OSPF 정규 영역이 있는 모든 L3Out 에 적용됩니다. 이는 VRF 에서 모든 정규 영역에 적용되는 표준 NX-OS 의 "기본 정보 시작"에 해당합니다.

L3Out EIGRP

기본 구성 예시

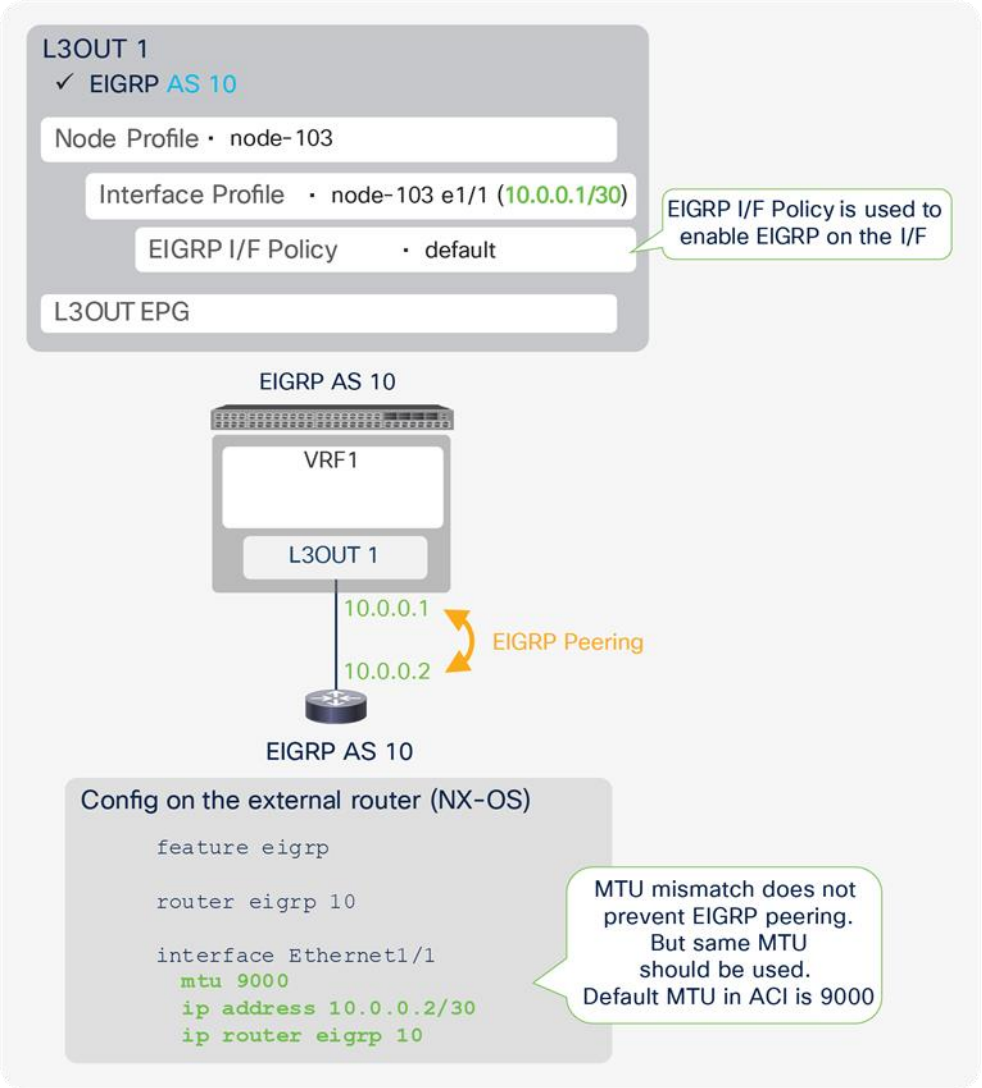

Figure 61.
EIGRP 구성 도표

Figure 61 에서는 AS 10 이 포함된 EIGRP 의 구성 예시가 나와있습니다. 주요 구성 요소는 AS 번호가 일치하도록 일반적인 라우터와 동일합니다. EIGRP 인접 관계를 확보하기 위해 MTU 가 동일할 필요는 없지만, 인접 관계 설정 후 경로 변경 등의 프로토콜 패킷이 삭제되지 않도록 하기 위해 동일한 값을 설정하는 것을 권장합니다.

Figure 62 에는 APIC GUI 구성의 예시가 나와있습니다.

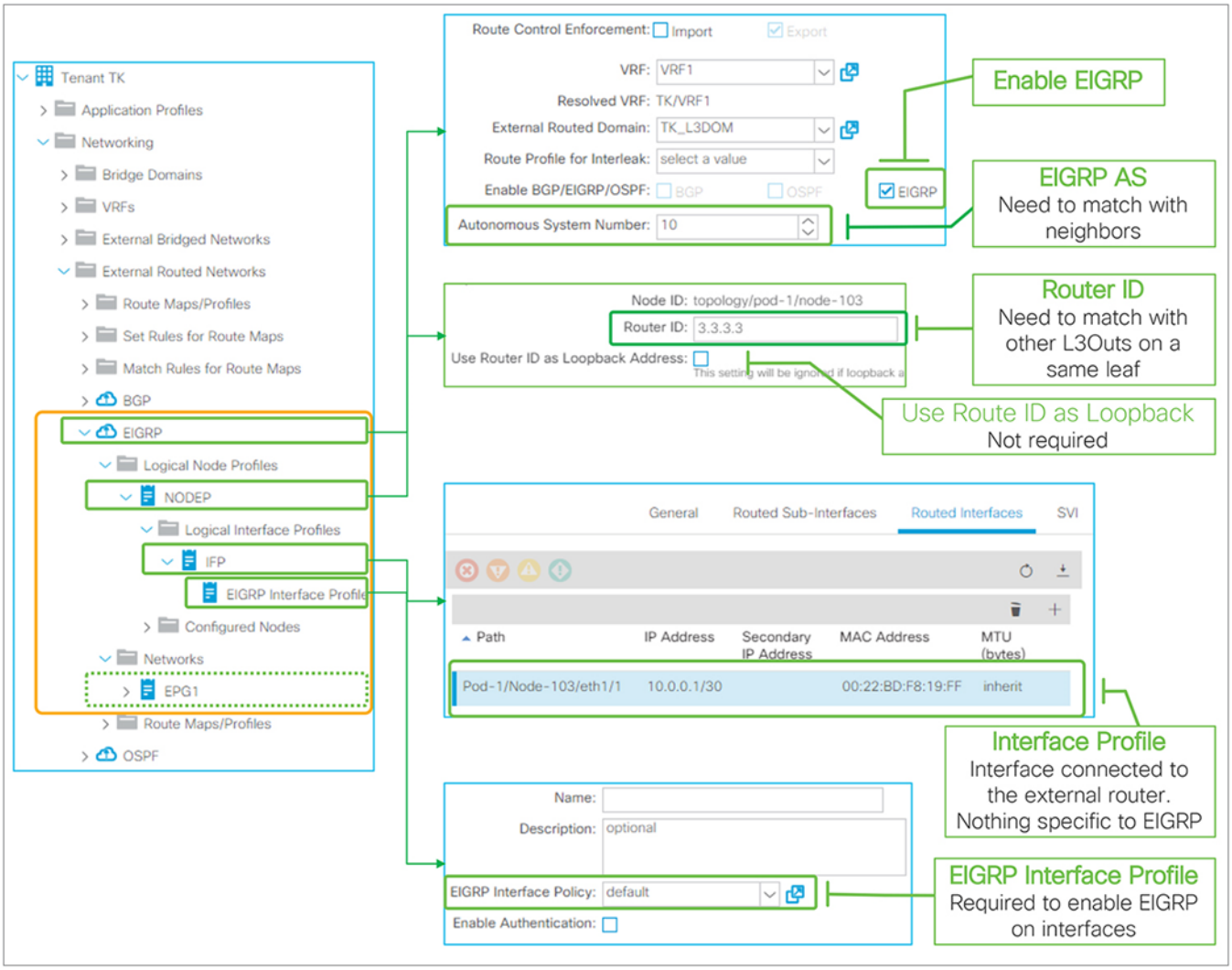

Figure 62.

GUI(APIC Release 3.2) 내 EIGRP 의 기본 구성

다음은 EIGRP 별 세 가지 구성 요소입니다.

- EIGRP 활성화: L3Out 내 보더 리프 스위치에서 EIGRP 프로토콜을 활성화하기 위해 확인합니다.
- EIGRP AS 번호: 인접 라우터를 설정하는 데 사용되는 EIGRP AS 번호입니다.
- EIGRP 인터페이스 프로필: 논리 인터페이스 프로필 내 인터페이스에서 EIGRP 를 활성화합니다. 미세 조정이 필요한 경우가 아니라면 기본값을 사용할 수 있습니다.

일반적인 라우터와 마찬가지로 EIGRP 의 작동을 위해 루프백이 특별히 필요한 것은 아닙니다.

제한 및 지침

- EIGRP(IPv4)는 APIC Release 1.1(1)부터 지원됩니다.
- EIGRP(IPv6)는 APIC Release 1.2(2)부터 지원됩니다.
- VRF 별 보더 리프에는 한 개의 EIGRP L3Out 만 배포될 수 있습니다. 그 이유는 한 개의 EIGRP L3Out 이 한 개의 EIGRP AS 를 나타내기 때문입니다.
- 동일한 VLAN 이 포함된 EIGRP L3Out 에 여러 개의 외부 라우터가 연결되면 동일한 L3Out BD 내에서 외부 라우터가 서로 간에 직접 인접 관계를 형성하게 됩니다. 자세한 내용은 "L3Out 노드 및 인터페이스 프로필" 섹션의 "L3Out 브리지 도메인"서브섹션 내 Figure 20 을 참조하시기 바랍니다.

  이러한 경우 외부 라우터에서는 ACI L3Out BD 를 통해 경로를 직접 교환합니다. 따라서 "경로 제어 서브넷 내보내기"를 통한 전송 라우팅과 유사한 상황이 "경로 제어 서브넷 내보내기" 없이 발생할 수도 있습니다.
- BD 서브넷을 보급하거나 전송 라우팅을 수행할 때는 경로가 보더 리프에서 자동으로 생성된 경로 맵을 통해 EIGRP 토폴로지로 재배포됩니다. 이 경로 맵은 동일한 VRF 의 동일 리프에서 OSPF L3Out 과 공유되는데, 이는 한 개의 L3Out 에 있는 서브넷 보급 구성이 다른 L3Out 에도 영향을 미칠 수 있다는 의미입니다. 따라서 동일한 VRF 의 동일 리프에 다른 L3Out 이 있을 경우 이 부분이 필요하다는 것을 인지해야 합니다. 자세한 내용은 "L3Out 전송 라우팅" 섹션의 Figure 93 을 참조하시기 바랍니다.

기타 제한에 대한 자세한 내용은 Cisco APIC 계층 3 네트워크 구성 가이드의 "EIGRP 프로토콜 지원" 섹션을 참조하시기 바랍니다.

EIGRP 프로토콜 옵션(인터페이스 수준)

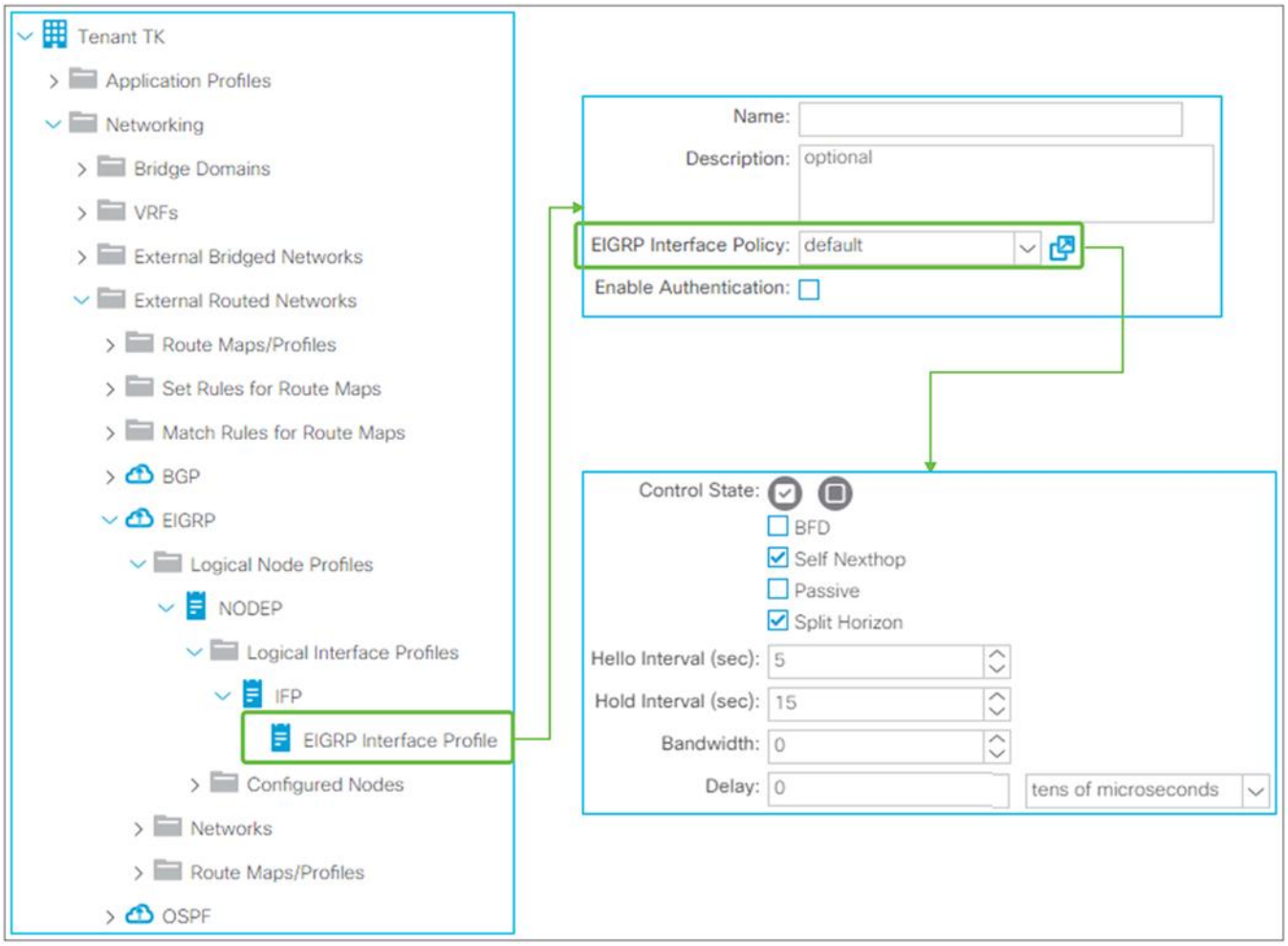

Figure 63.
GUI(APIC Release 3.2) 내 EIGRP 인터페이스 프로필 및 정책

EIGRP 인터페이스 프로필의 인터페이스 수준 EIGRP 구성은 연결된 논리 인터페이스 프로필의 모든 인터페이스에 적용됩니다. **EIGRP 인터페이스 정책**은 **"Tenant > Policies > EIGRP > EIGRP Interface"**에 위치합니다.

EIGRP 인터페이스 정책

- **제어 상태**
  - BFD

    APIC Release 1.2(2)에서 도입된 기능으로, EIGRP 인터페이스에서 BFD 를 활성화하는 데 사용됩니다. 자세한 내용은 "L3Out BFD" 섹션을 참조하시기 바랍니다.

    독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
interface eth1/1
  ip eigrp <instance> bfd
```

- 자체 다음 홉

  이 옵션은 기본적으로 활성화되어 있습니다. EIGRP 는 경로 보급 시 로컬 IP 주소를 다음 홉으로 설정하는 것이 기본값이며, 이 옵션을 비활성화하면 보더 리프가 다음 홉을 덮어쓰지 않으며 원본 다음 홉 IP 를 유지합니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
interface eth1/1
  ip next-hop-self eigrp <instance>
```

- 수동

  인터페이스를 EIGRP 수동 인터페이스로 구성하기 위한 옵션으로, 기본적으로 비활성화되어 있습니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
interface eth1/1
  ip passive-interface eigrp <instance>
```

- 스플릿 호라이즌

  EIGRP 업데이트 또는 쿼리를 학습된 장소인 인터페이스로 송신하지 않는 방법으로 라우팅 루프를 방지하는 기능으로, 기본적으로 비활성화되어 있습니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
interface eth1/1
  ip split-horizon eigrp <instance>
```

- **Hello 간격(초) 및 보류 간격(초)**

  Hello 간격은 EIGRP Hello 메시지가 송신되는 간격으로, 기본값은 5 초입니다. **보류 간격**은 Hello 메시지에서 보급되며, 인접 라우터에게 송신자를 유효하게 간주해야 하는 시간의 길이를 알립니다. 보류 간격의 기본값은 Hello 간격의 세 배인 15 초입니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
interface eth1/1
  hello-interval eigrp <instance> <sec>
  ip hold-interval eigrp <instance> <sec>
```

- **대역폭 및 지연**

  EIGRP 행렬 계산에 대한 대역폭과 지연을 구성합니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
interface eth1/1
  ip bandwidth eigrp <instance> <bandwidth>
  ip delay eigrp <instance> <delay>
```

EIGRP 인증

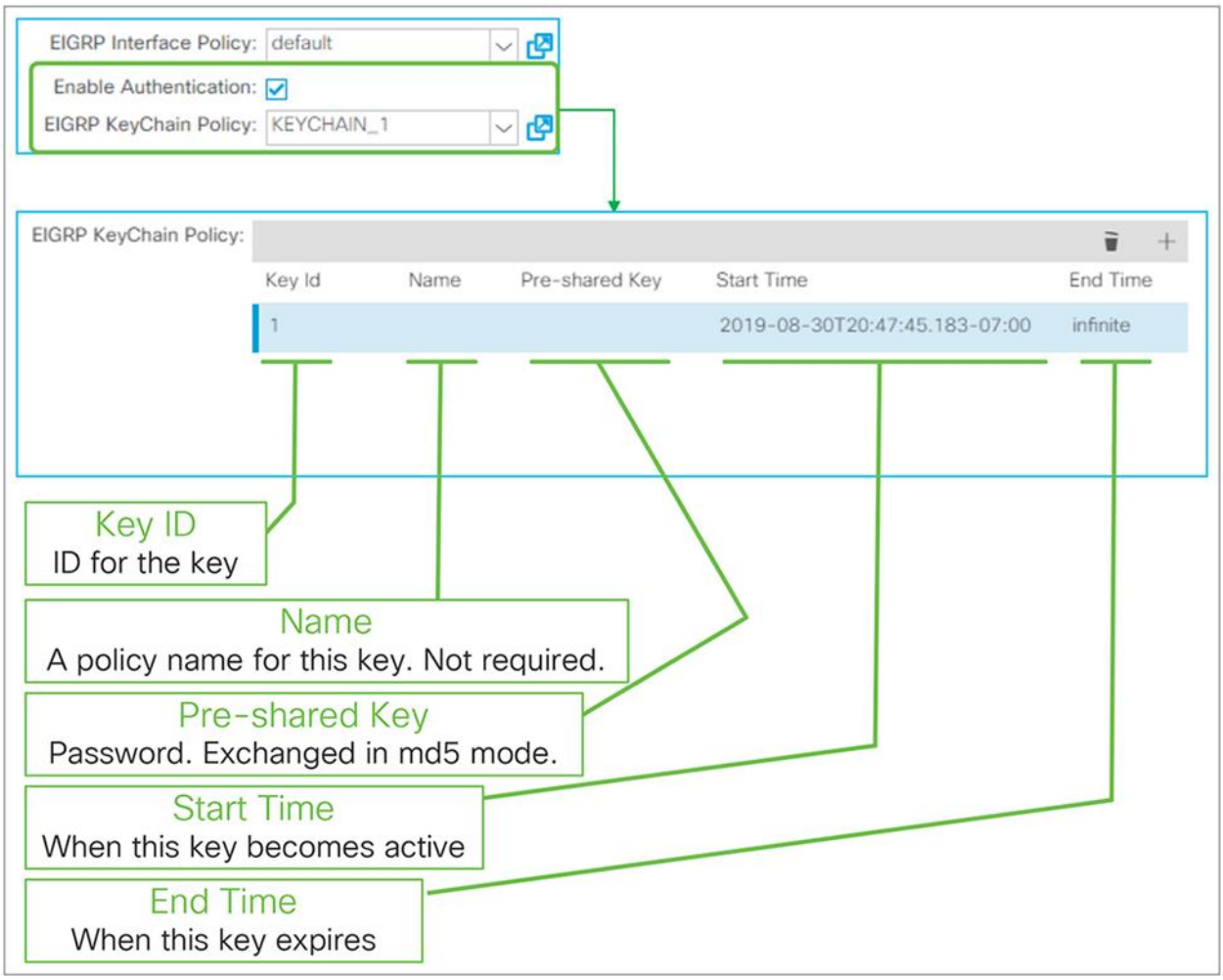

Figure 64.
GUI(APIC Release 3.2) 내 EIGRP 키 인증

EIGRP 인증은 다음의 개선 사항과 함께 APIC Release 3.2(4)에서 도입되었습니다.

CSCvk43721 ACI 에 대한 EIGRP 인증 지원

키 집합으로 EIGRP 인터페이스 프로필마다 활성화됩니다. 지원되는 EIGRP 인증 모드는 MD5 이며, EIGRP 키 집합 정책은 "**Tenant > Policies > EIGRP > EIGRP KeyChains**"에 위치합니다.

- 키 ID: 키 집합에서 키가 여러 키를 관리할 수 있게 해주는 ID 입니다.
- 이름: 각 키의 객체 모델에서 사용되는 이름으로 옵션 사항입니다.
- 사전 공유된 키: 인접 라우터와 일치해야 하는 암호입니다.
- 시작 시간: 이 키가 활성화되는 시점으로 빈 칸일 경우 즉시 시작됩니다.
- 종료 시간: 이 키가 만료되는 시점으로 빈 칸일 경우 무한값이 사용됩니다.

독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
key chain <keychain name>
  key <id>
    key-string <password>
    send-lifetime <start-time> <end-time>

interface eth1/1
  ip authentication mode eigrp <instance> md5
  ip authentication key-chain eigrp <instance> <keychain name>
```

EIGRP 프로토콜 옵션(VRF 수준)

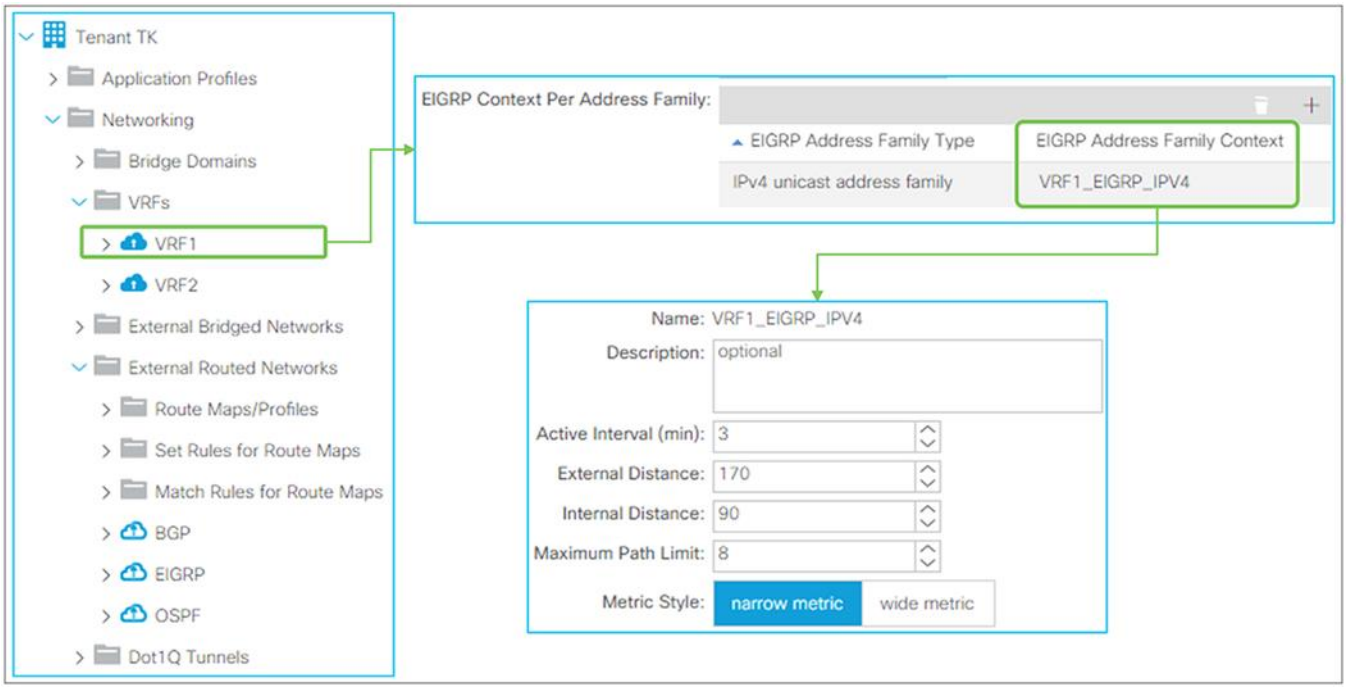

Figure 65.

GUI(APIC Release 3.2) 내 EIGRP 주소 패밀리 컨텍스트 정책

EIGRP 주소 패밀리 컨텍스트 정책

이 정책은 VRF 에서 사용되나 **EIGRP 주소 패밀리 컨텍스트 정책**은 "**Tenant > Policies > EIGRP > EIGRP Address Family Context**"에 위치합니다.

각 매개변수에 대한 자세한 내용은 다음과 같습니다.

- 활성화 간격(분)
  활성 상태 유지(SIA)를 선언하고 인접 관계를 재설정하기 전에 EIGRP 쿼리를 송신한 후 보더 리프가 대기하는 간격으로 기본값은 3 분입니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router eigrp 10
  vrf TK:VRF1
    address-family ipv4 unicast
      timers active-time <min>
```

- **외부 거리 및 내부 거리**
  외부 및 내부 EIGRP 경로에 대한 관리 거리(AD)로, 기본값은 외부에서 170, 내부에서 90 입니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router eigrp 10
  vrf TK:VRF1
    address-family ipv4 unicast
      distance <internal> <external>
```

- **최대 경로 제한**
  EIGRP 가 라우팅 테이블에 설치할 수 있는 ECMP 의 최대 수로, 기본값은 8 개 경로입니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router eigrp 10
  vrf TK:VRF1
    address-family ipv4 unicast
      maximum-paths <num>
```

- **행렬 스타일**
  EIGRP 는 기본 K 값과 대역폭 및 지연을 토대로 행렬을 계산합니다. 그러나 32 비트의 원래 구현 값은 10 기가비트 이더넷보다 빠른 인터페이스를 구별해내지 못합니다. 이 원 구현을 전형적 또는 제한적 행렬이라고 부릅니다. 이러한 문제를 해결하기 위해 EIGRP 에서 개선된 수식이 포함된 64 비트의 값이 도입되었습니다. 이를 폭넓은 행렬이라고 하며, 제한적 행렬이 기본값입니다.

독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router eigrp 10
  vrf TK:VRF1
    address-family ipv4 unicast
      metric version 64bit
```

EIGRP 경로 요약

APIC Release 1.2(2)에서 도입된 기능으로, ACI OSPF L3Out 에서 BD 서브넷 및/또는 전송 경로에 대한 요약된 식별 번호만 외부로 보급합니다.

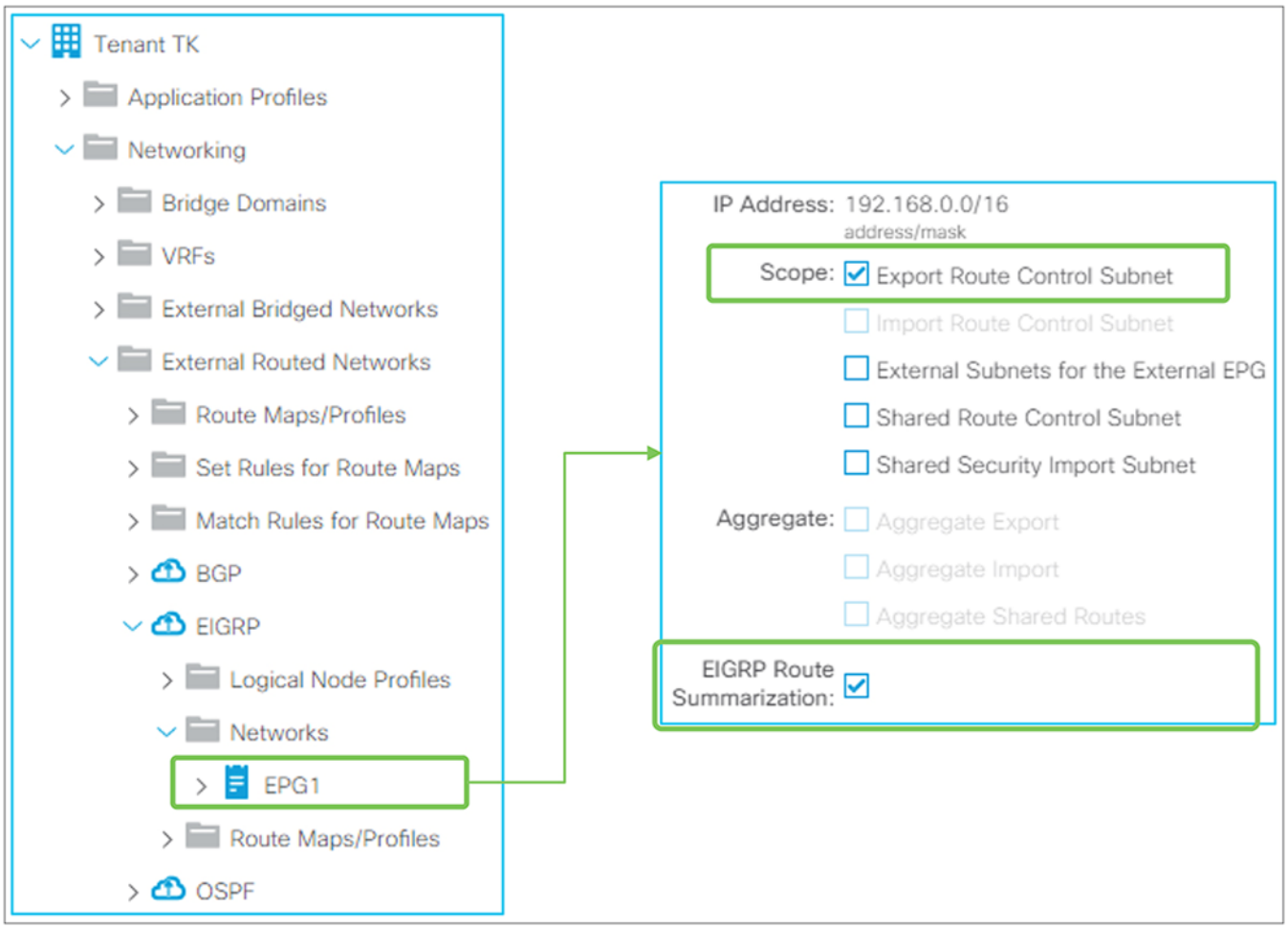

Figure 66.

GUI(APIC Release 3.2) 내 EIGRP 경로 요약

ACI 내 EIGRP 경로 요약은 "경로 제어 서브넷 내보내기" 범위를 사용해 경로 요약 정책을 L3Out 서브넷에 추가함으로써 구성되는데, 그 이유는 이것이 ACI 에서 경로를 외부로 보급하는(내보내는) 데 사용되기 때문입니다. "경로 제어 서브넷 내보내기" 범위에 대한 자세한 내용은 "L3Out 전송 라우팅" 섹션을 참조하시기 바랍니다.

Figure 66 에서와 같이, L3Out 서브넷에 경로 요약 정책을 추가하면 보더 리프가 요약된 경로(Figure 66 의 192.168.0.0/16)에 대한 Null-0 항목을 생성하며, 이것은 EIGRP 피어에 보급됩니다. Null-0 다음 홉이 있는 요약된 경로는 인프라 MP-BGP 를 통해 다른 리프 스위치로 보급되지 않습니다. 일반적인 EIGRP 라우터와 마찬가지로 보더 리프에 있는 사용자 VRF 에 대한 EIGRP 토폴로지 테이블에 기여 경로가 존재하지 않는 경우에는 요약이 발생하지 않는 점에 유의해야 합니다.

EIGRP 요약은 인터페이스마다 구현되므로 ACI 는 L3Out 내 모든 인터페이스에 요약 정책을 배포하게 됩니다.

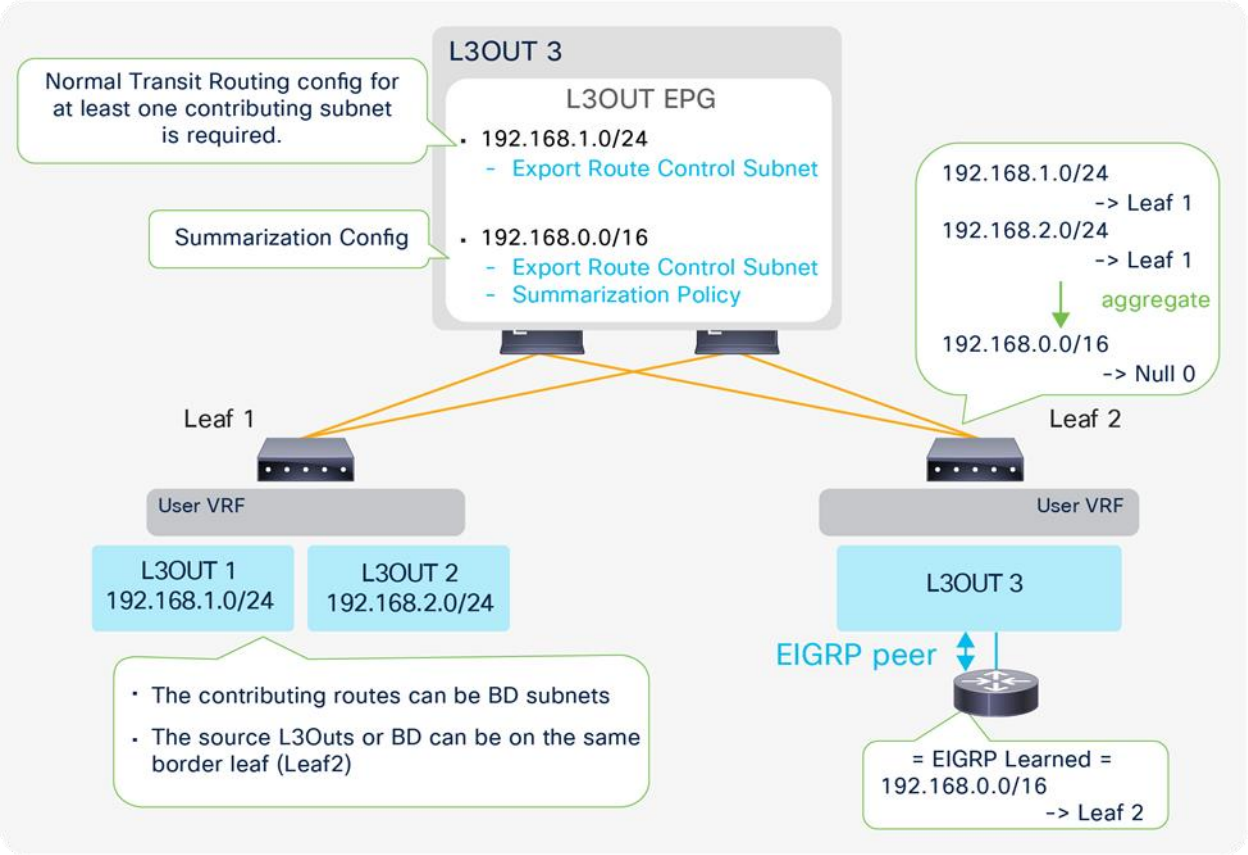

Figure 67.
EIGRP 경로 요약 토폴로지에 대한 예시

Figure 67 에는 L3Out 3 가 L3Out 1 과 2(192.168.1.0/24 및 192.168.2.0/24)에서 전송 경로에 대해 요약된 서브넷(192.168.0.0/16)만 보급하는 상황이 나와있습니다. 요약을 수행하려면 L3Out 3 용 EIGRP 토폴로지 테이블에 한 개 이상의 기여 서브넷이 필요합니다. 따라서 한 개 이상의 구성 서브넷에 대한 전송 라우팅

구성("경로 제어 서브넷 가져오기" 범위)이 필요합니다. BD 서브넷을 요약하는 경우, 적합한 BD 서브넷 보급 구성이 한 개 이상의 서브넷에 필요합니다("ACI BD 서브넷 보급" 섹션 참조).

독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
interface eth1/1
  ip summary-address eigrp <instance> <prefix>/<mask>
```

참고:

동일한 VRF 의 동일 리프에서 OSPF 경로 요약이 EIGRP L3Out 으로서 구성되면, EIGRP L3Out 에 경로 요약이 없더라도 OSPF 경로 요약이 EIGRP 로 보급됩니다. 그 이유는 다음과 같습니다.

1. Null-0 다음 홉이 포함된 요약된 경로가 동일한 보더 리프의 OSPF 로 인해 라우팅 테이블에서 이미 생성되었습니다.
2. OSPF L3Out 이 요약된 경로에 대해 경로 맵 항목을 생성합니다.
3. 이 경로 맵은 전송 라우팅 또는 "경로 제어 서브넷 내보내기" 범위에 대한 것이므로 동일한 VRF 의 동일 리프에 있는 OSPF 와 EIGRP 간에 공유됩니다. 자세한 내용은 "L3Out 전송 라우팅" 섹션의 "전송 라우팅에 대한 내부 경로 맵"을 참조하시기 바랍니다.

이러한 이유로 EIGRP 는 동일한 리프에서 EIGRP 경로 요약 없이 OSPF 요약된 경로를 재배포합니다. 이 현상은 EIGRP L3Out 에 경로 요약 구성이 존재하지만 동일한 VRF 의 동일 리프에 있는 OSPF L3Out 이 존재하지 않을 때도 발생합니다.

EIGRP 기본 경로 보급

기본 경로(0.0.0.0/0)를 EIGRP L3Out 에서 외부로 보급하는 데는 두 가지 방법이 있습니다.

1. 전송 라우팅
2. 기본 경로 유출 정책

전송 라우팅은 다른 L3Out 또는 다른 L3Out 에서 구성된 고정 경로에서 학습된 기본 경로를 보급합니다. 전송 라우팅에 대한 자세한 내용은 "L3Out 전송 라우팅" 섹션을 참조하시기 바랍니다.

기본 경로 유출 정책은 독립 실행형 NX-OS 의 "default-information originate"에 해당합니다.

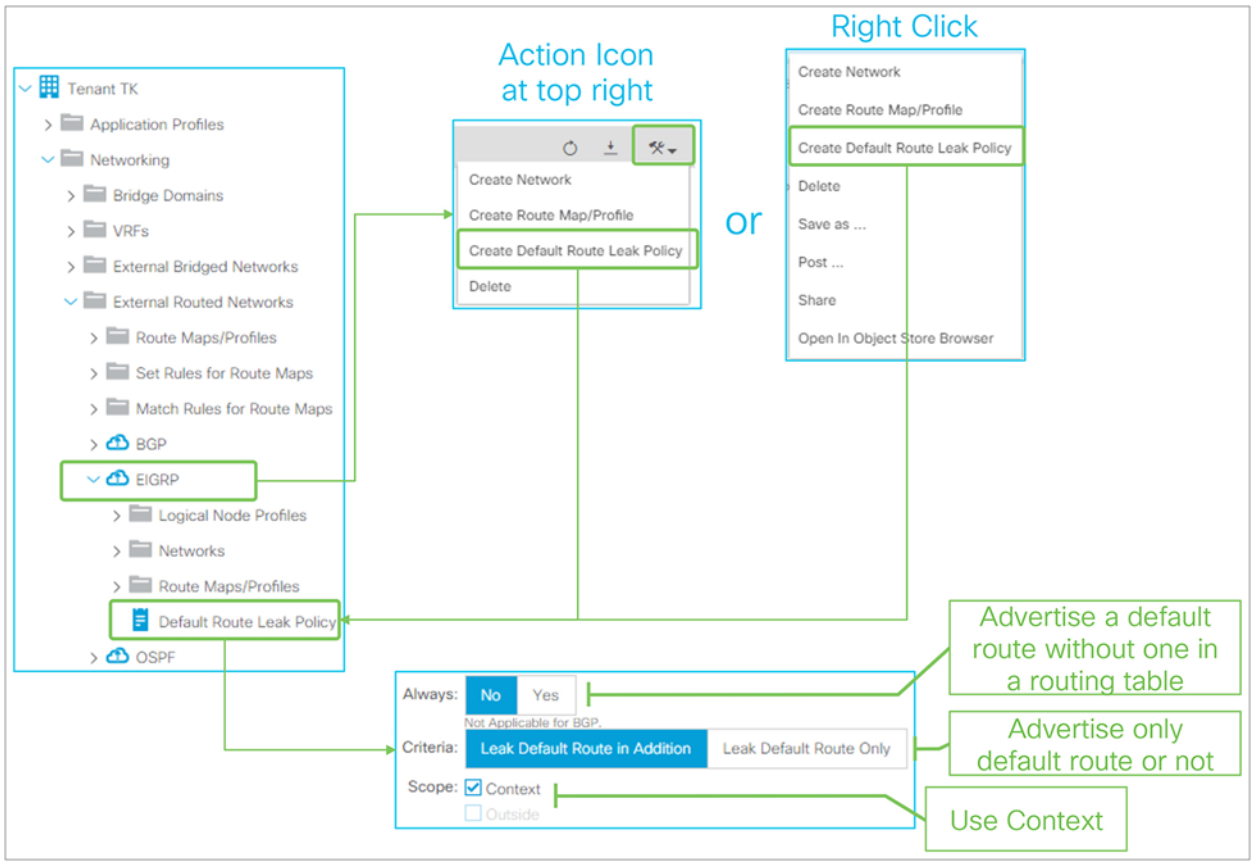

Figure 68.

GUI(APIC Release 3.2) 내 EIGRP 에 대한 기본 경로 유출 정책

기본 경로 유출 정책은 APIC Release 1.1(1)에서 도입되었으며 다음 중 한 가지 수단을 사용해 L3Out 에서 생성될 수 있습니다.

- L3Out 의 우측 상단에서 드롭다운 메뉴의 "기본 경로 유출 정책 생성" 선택
- L3Out 자체의 우클릭 메뉴에서 "기본 경로 유출 정책 생성" 선택

기본 경로 유출 정책에는 다음과 같은 매개변수가 포함됩니다.

- **항상**

  독립 실행형 NX-OS 의 "default-information originate"에 대한 "항상" 옵션에 해당합니다. "예"로 설정한 경우 라우팅 테이블에 기본 경로가 없더라도 기본 경로는 보급됩니다.

- **기준**

  다른 경로 외에 기본 경로도 보급해야 하는 경우 "**기본 경로 추가로 유출**"을 사용합니다. 기본 경로만 보급해야 하는 경우 "**기본 경로만 유출**"을 사용합니다.

  "**기본 경로만 유출**"이 선택되면 해당 EIGRP L3Out 에 대한 보더 리프에는 재배포 규칙이 배포되지 않습니다.

- **범위**

  EIGRP 의 경우 "**컨텍스트**"를 사용합니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
router eigrp 10
  vrf TK:VRF1
    default-information originate [always]
```

ACI BD 서브넷 보급

이 섹션에서는 L3Out 에서 ACI 패브릭이 라우팅 프로토콜을 통해 BD 서브넷을 보급하는 방법을 자세히 설명합니다. 기본적인 내용과 구성은 "L3Out 의 기본 구성 요소" 섹션을 참조하시기 바랍니다.

BD 서브넷을 보급하는 데는 세 가지 방법이 있습니다.

1. **L3Out 과 BD 의 연결**("L3Out 의 기본 구성 요소" 섹션에서 설명된 방법) 이용
2. L3Out EPG 의 서브넷 내 "**경로 제어 서브넷 내보내기**" 범위 이용
3. 명시적 식별 번호 목록이 포함된 내보내기 방향의 **경로 맵 및 프로필** 이용

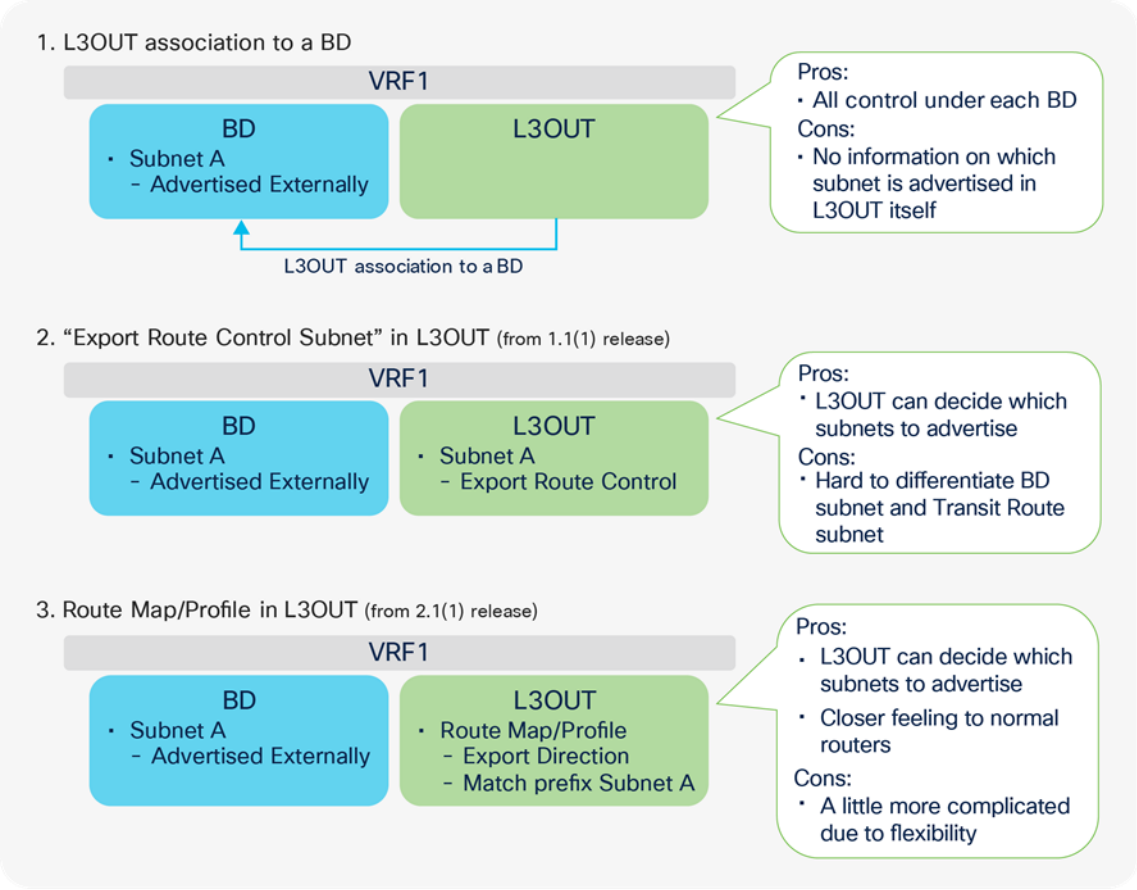

Figure 69.

BD 서브넷 보급 방법

Figure 69 에는 BD 서브넷을 외부로 보급하는 세 가지 방법과 각 방법의 장단점이 나와있습니다. 세 가지 방법 모두 리프에 배포되는 사항은 동일합니다. ACI 가 BD 서브넷에 대해 IP 식별 번호 목록을 생성하고(서브넷이 "외부로 보급됨" 범위로 구성되었을 경우에 한정) 해당 식별 번호 목록을 보더 리프의 경로 맵에 삽입합니다(자세한 내용은 아래 Figure 70 및 Figure 71 에서 설명). 따라서 사용자는 선호하는 방법을 선택해서 사용할 수 있지만 세 가지 방법을 혼용하는 것은 권장하지 않는데, 이는 혼합된 구성을 관리하는 것이 매우 까다롭기 때문입니다.

첫 번째 방법인 L3Out 과 BD 의 연결은 가장 기본적인 방법으로, 첫 APIC Release 1.0 부터 지원되었습니다. L3Out 에 보급될 BD 서브넷(b)에 대한 일체의 제어 권한은 BD(a)에만 부여합니다. 다중 테넌시의 이유로 BD 및 L3Out 구성 요소 간에 운영 팀이 분리될 경우 이 방법은 단일 팀 및 구성 요소 내에서 완수될 수 있습니다. 그러나 L3Out 과 BD 의 연결은 BD 에서 구성되므로 L3Out 구성 요소는 보급 중인 BD 서브넷에 대한 가시성이 저하됩니다.

"경로 제어 서브넷 내보내기" 범위를 사용하는 두 번째 방법의 경우, 서브넷이 BD 서브넷인지, 또는 다른 L3Out(전송 라우팅)의 외부 경로인지 여부에 관계없이 L3Out 구성을 통해 외부로 보급되는 서브넷을 관리할 수 있습니다. 이에 따라 구성이 통합될 수는 있지만 구성에 관한 문제를 해결하고자 하는 경우에는 혼란스러울 수 있고, L3Out 서브넷을 관찰하여 전송 라우팅 서브넷과 BD 서브넷을 구별해야 합니다. BD 서브넷은 "외부로 보급됨"으로 표시되어야 하는 점에 유의해야 합니다.

내보내기 방향의 경로 맵 및 프로필을 사용하는 세 번째 방법에서는 경로 맵 및 IP 식별 번호 목록을 직접 구성할 때 일반 라우터와 같은 구성 방식을 제공합니다. 이 옵션에서는 L3Out 과 BD 의 연결이나 L3Out 경로 제어 서브넷 내보내기가 아닌 경로 프로필 및 명시적 식별 번호 목록(식별 번호 기준 일치)을 사용합니다. 자세한 내용은 "L3Out 경로 프로필 및 경로 맵" 섹션을 참조하시기 바랍니다. 두 번째 방법의 장단점이 이 방법에도 동일하게 적용되며, BD 서브넷은 "외부로 보급됨"으로 표시되어야 합니다.

BD 서브넷 보급에 대한 내부 경로 맵

이 섹션에서는 BD 서브넷을 보급하는 과정에서 보더 리프에서 발생하는 현상을 자세히 설명합니다.

BD 서브넷이 L3Out 을 통해 외부로 표시되려면 APIC 에서 세 가지 요소로 보더 리프를 구성해야 합니다(Figure 70 에 다양한 색상으로 표시).

- 경로 맵(최초에는 빈 상태일 수 있음)이 포함된 재배포 구성, Figure 에서 녹색으로 표시
- 보급할 서브넷이 포함된 경로 맵 내 IP 식별 번호 목록, Figure 에서 청색으로 표시
- L3Out 외부 EPG 및 서버가 위치한 EPG 간 Contract 의 결과로 보더 리프의 APIC 에서 푸시한 BD 서브넷 경로(Figure 에서 회색으로 표시)

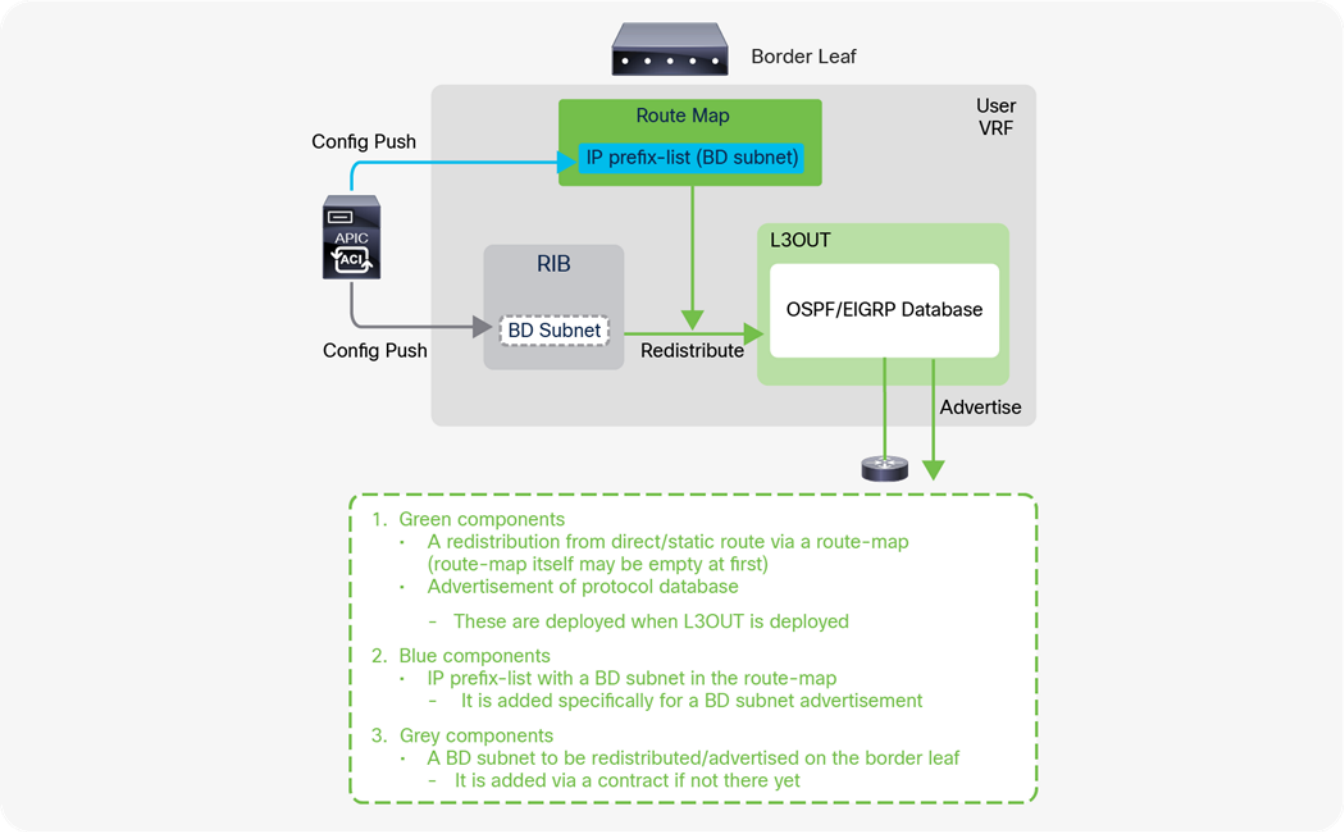

Figure 70.

BD 서브넷 보급 아키텍처(OSPF 및 EIGRP)

Figure 70 에서는 OSPF 와 EIGRP 에서 BD 서브넷 보급 시 표면 아래에서 발생하는 현상에 대해 설명합니다. 녹색 구성 요소(직접 및 고정 경로의 재배포, 프로토콜 데이터베이스 내 경로의 보급에 대한 경로 맵)는 BD 서브넷이 보급되도록 구성되는지 여부에 관계없이 보더 리프에 배포됩니다. 그러나 보급되도록 구성된 BD 서브넷이 없으면(예: L3Out 과 BD 의 연결이 없는 경우) 직접 및 고정 재배포에 대한 경로 맵은 빈 상태이며 BD 서브넷 보급 또한 완료되지 않은 상태입니다. 청색 구성 요소(경로 맵 내 BD 서브넷에 대한 IP 식별 번호 목록)는 L3Out 과 BD 의 연결 등 BD 서브넷 보급 구성이 실제로 추가한 것입니다. 따라서 BD 서브넷이 보더 리프에 배포되어 있을 경우 BD 서브넷은 라우팅 프로토콜로 재배포되고 외부로 보급될 수 있습니다. L3Out 외부 EPG 및 BD 용 EPG 간의 Contract 의 결과로서, 또는 단순히 보더 리프의 BD 에 연결된 로컬 엔드포인트가 존재하기 때문에 BD 서브넷은 보더 리프에 존재할 수 있습니다.

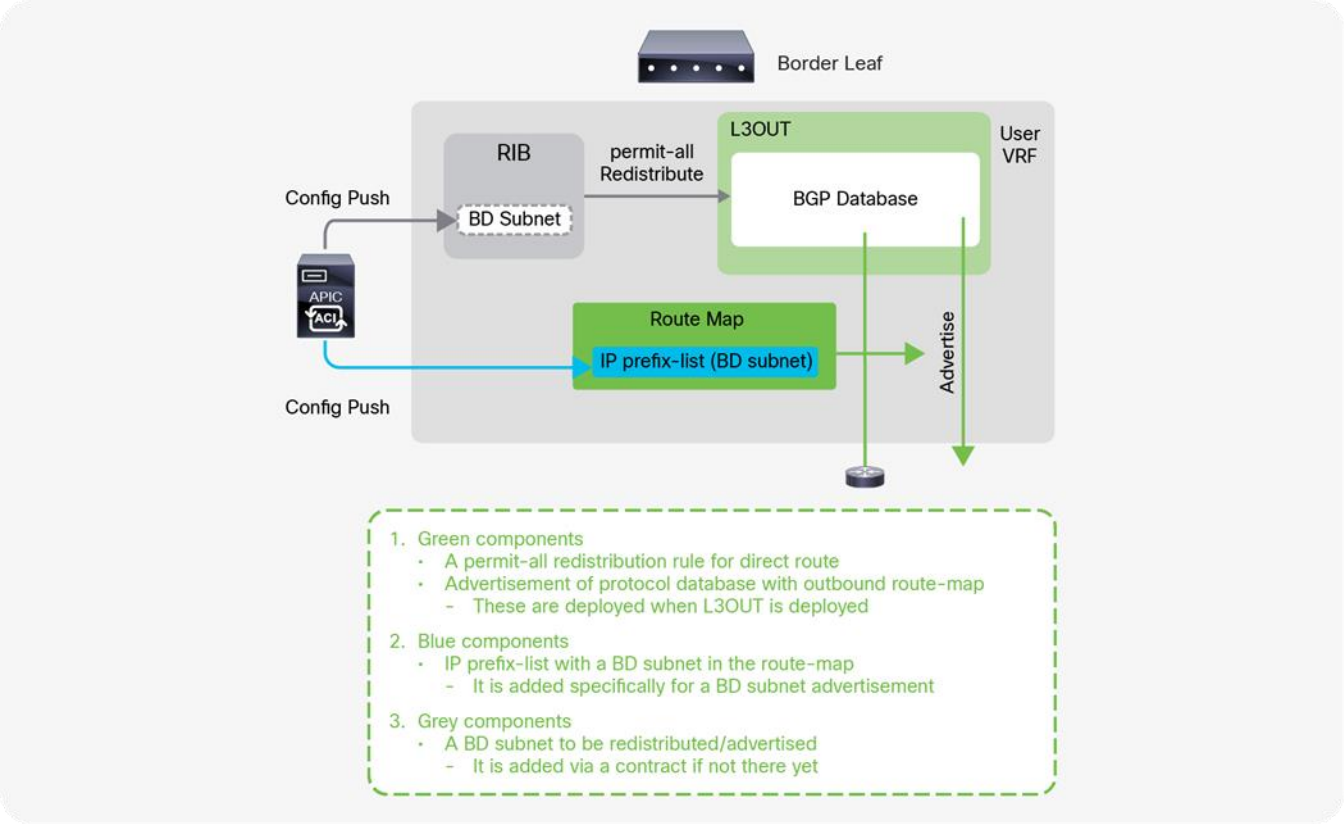

Figure 71.
BD 서브넷 보급 아키텍처(BGP)

Figure 71 에서는 BGP 에서 BD 서브넷 보급 시 표면 아래에서 발생하는 현상에 대해 설명합니다. 제어판의 프로그래밍과 보더 리프의 데이터 평면은 대체로 OSPF 와 EIGRP 를 이용하는 것과 동일하지만, BGP 용 APIC 가 배경에서 수행한 구성의 경우 인프라 MP-BGP 의 사용으로 인해 약간 다른 접근법이 필요합니다. 모든 직접 및 고정 경로는 인프라 MP-BGP 를 위해 BGP IPv4 AF 로 먼저 재배포되고 나면 APIC 가 아웃바운드 경로 맵으로 BGP 피어에 보급할 경로를 구성합니다. 청색 구성 요소는 BD 서브넷에 대한 IP 식별 번호 목록을 아웃바운드 경로 맵에 추가합니다(OSPF 와 EIGRP 의 경우 재배포를 위해 IP 식별 번호 목록이 경로 맵에 추가됨).

참고:

OSPF 및 EIGRP 내 직접 경로 재배포를 위한 경로 맵의 이름은 "exp-ctx-st-<VRF VNID>" 형식이며 동일한 VRF 의 동일 보더 리프에서 OSPF 와 EIGRP 간에 공유됩니다.

```
Leaf1# show ip ospf vrf TK:VRF1 | grep -A 4 Redist
 Redistributing External Routes from
    static route-map exp-ctx-st-2916353     <-- "exp-ctx-st-<VRF VNID>"
    direct route-map exp-ctx-st-2916353     <-- "exp-ctx-st-<VRF VNID>"
    bgp route-map exp-ctx-proto-2916353
    eigrp route-map exp-ctx-proto-2916353
```

BGP 피어 아웃바운드에 대한 경로 맵의 이름은 exp-L3Out-<L3Out name>-peer-<VRF VNID>" 형식이며 동일한 L3Out 내 모든 BGP 피어와 공유됩니다.

```
Leaf1# show bgp ipv4 unicast neighbors vrf TK:VRF1 | egrep 'BGP nei|Outbound'
BGP neighbor is 102.0.0.9,  remote AS 65009, ebgp link,  Peer index 1
  Outbound route-map configured is exp-L3Out-BGP-peer-2916353, handle obtained
        <-- "exp-L3Out-<L3Out name>-peer<VRF VNID>"
```

참고:

보더 리프의 경로 맵에 IP 식별 번호 목록을 추가하는 구성 요소는 많으므로 ACI 패브릭 내 경로 맵에는 일반적으로 한 개 이상의 IP 식별 번호 목록이 존재합니다.

경로 맵에 IP 식별 번호 목록이 없는 경우에는 경로 맵 자체가 아직 존재하지 않더라도 경로 맵 이름은 각 프로토콜(예: BGP 내 피어 아웃바운드에 대한 OSPF 와 EIGRP 에서의 재배포)에서 지정될 수 있습니다.

참고:

BGP IPv4 및 v6 AF 에는 모두 허용 재배포 경로 맵이 있지만 BD 서브넷은 인프라 MP-BGP 를 통해 다른 리프 스위치로 배포되지 않습니다. EPG 의 배포 또는 BD 에 대한 EPG Contract 등 사용자 구성을 토대로 APIC 로만 스파인 프록시 TEP 를 가리키는 고정 및 직접 경로로서 리프 스위치에 BD 서브넷이 배포됩니다.

L3Out 서브넷 범위 옵션

이 섹션에서는 L3Out 서브넷 범위 옵션의 개요를 제시합니다. 각 범위의 자세한 내용은 후반부에서 다룹니다.

"경로 제어 서브넷 내보내기" 또는 "외부 EPG 에 대한 외부 서브넷" 등의 L3Out 서브넷 범위 옵션은 **"Tenant > Networking > External Routed Networks > L3Out > Networks > L3Out EPG > General tab > Subnet"**에 위치합니다.

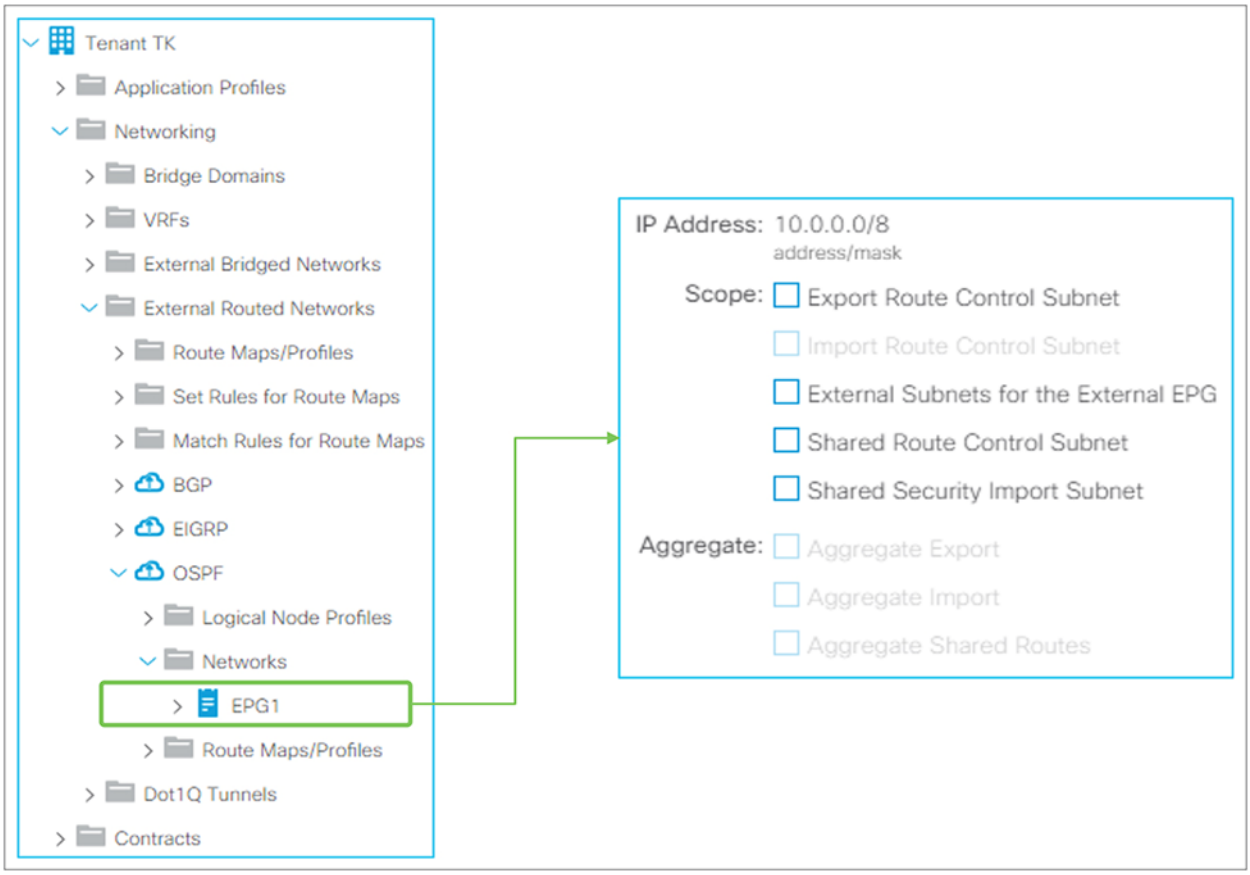

Figure 72.

GUI(APIC Release 3.2) 내 L3Out 서브넷 범위

L3Out 서브넷 범위 요약

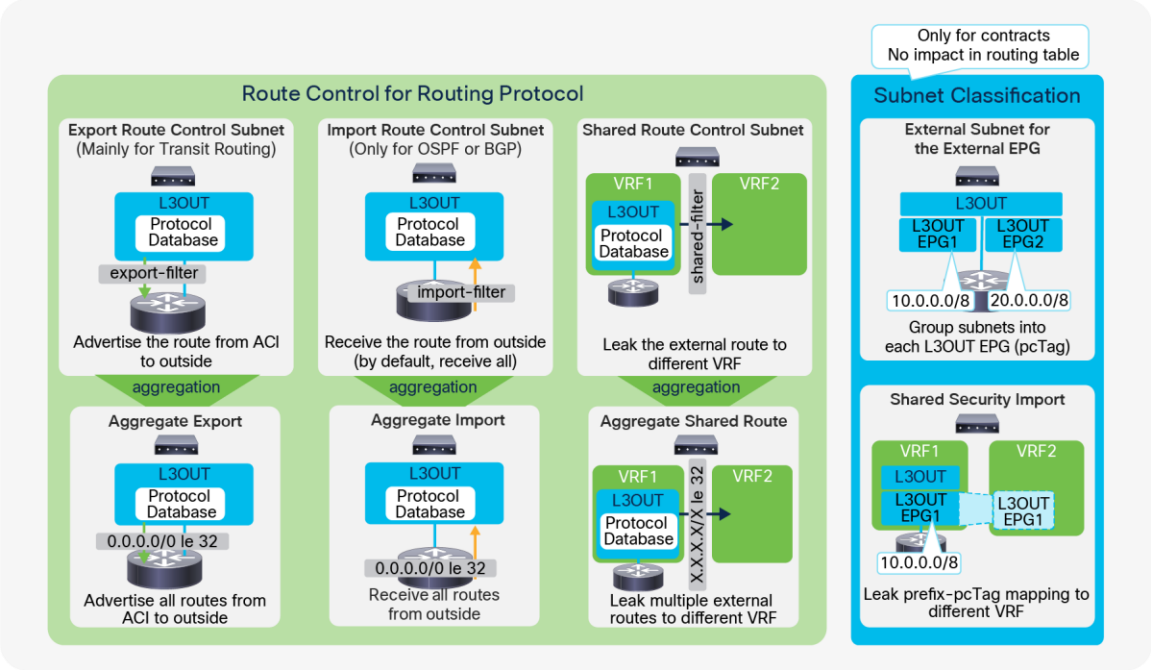

Figure 73.
L3Out 서브넷 범위 요약

Figure 73 에서와 같이, 범위 옵션과 집계 옵션은 두 개의 그룹으로 나뉩니다. 한 그룹(Figure 73 의 녹색 그룹)은 IP 식별 번호 목록 및 보더 리프의 경로 맵을 통해 라우팅 테이블과 라우팅 프로토콜을 조작하기 위한 옵션입니다. 또 다른 그룹(Figure 73 의 청색 그룹)은 Contract 과 관련된 옵션입니다.

라우팅 프로토콜에 대한 경로 제어

이 세 가지 범위(내보내기, 가져오기, 공유됨)는 모두 보더 리프의 지정된 서브넷으로 IP 식별 번호 목록을 생성합니다. 따라서 이들 범위는 정확히 일치하는 경로에만 영향을 미치게 됩니다. 이들 범위를 통해 10.0.0.0/8 로 서브넷을 구성할 경우 ACI 는 10.0.0.0/8 에는 구성을 적용하지만 10.0.0.0/16 에는 적용하지 않습니다. 여러 서브넷을 한 개의 구성 항목으로 매칭해야 하는 경우, 각 범위에 대해 "집계" 옵션을 사용해야 합니다. 내보내기 및 가져오기 범위에 대한 "집계" 옵션은 0.0.0.0/0 서브넷에만 지원됩니다.

- **경로 제어 서브넷 내보내기**

  L3Out 을 통해 ACI 에서 외부로 서브넷을 보급하는(내보내는) 범위입니다. 주로 전송 라우팅을 위한 범위이지만 "ACI BD 서브넷 보급" 섹션에서 설명한 것과 같이 BD 서브넷을 보급하는 데에도 사용할 수 있습니다.

  이 범위는 서브넷을 보급하는 데 사용되는 L3Out 에서 구성되어야 하며 서브넷을 학습 중인 L3Out 을 위한 범위가 아닙니다. 이 범위는 APIC Release 1.1(1)에서 도입되었습니다.

  자세한 내용은 "L3Out 전송 라우팅" 섹션을 참조하시기 바랍니다.

- **경로 제어 서브넷 가져오기**
  L3Out 에서 외부 서브넷을 학습하는(가져오는) 범위입니다. 이 범위는 기본적으로 비활성화되어 있으므로 Figure 72 에서는 회색으로 표시되어 있으며 보더 리프는 라우팅 프로토콜의 모든 경로를 학습합니다. OSPF 와 BGP 를 통해 학습된 외부 경로를 제한해야 하는 경우에 이 범위를 활성화할 수 있습니다. EIGRP 에서는 이 옵션을 사용할 수 없습니다.

  이 범위를 사용하려면 특정 L3Out 에서 "경로 제어 적용 가져오기"를 먼저 활성화해야 합니다(자세한 내용은 다음 "경로 제어 적용" 서브섹션 참조). OSPF L3Out 에서 "경로 제어 적용 가져오기"가 활성화되면, 보더 리프의 OSPF LSDB 에 경로가 존재하더라도 라우팅 테이블에서 해당 서브넷만 사용될 수 있도록 보더 리프가 "경로 제어 서브넷 가져오기"가 포함된 서브넷에 대해 IP 식별 번호 목록이 포함된 테이블 맵을 사용합니다. 이 범위가 BGP L3Out 에서 활성화되면 보더 리프가 L3Out 내 모든 BGP 피어와는 반대로 "경로 제어 서브넷 가져오기"가 포함된 서브넷에 대해 IP 식별 번호 목록이 포함된 인바운드 경로 맵을 사용합니다. 따라서 초기에 구성된 경로만 BGP 테이블에서 학습할 수 있습니다.

  이 옵션은 서브넷을 학습 중인 L3Out 에서 구성되어야 합니다. 이 범위는 APIC Release 1.1(1)에서 도입되었습니다.

- **공유된 경로 제어 서브넷**
  외부 서브넷을 다른 VRF 로 유출하는 범위입니다. ACI 는 MP-BGP 와 경로 대상을 사용해 VRF 간에 외부 경로를 유출합니다. 이 범위는 서브넷으로 IP 식별 번호 목록을 생성하는데, 이것은 MP-BGP 에서 경로 대상으로 경로를 내보내거나 가져오는 필터로 사용됩니다.

  이 범위는 원본 VRF 에서 서브넷을 학습 중인 L3Out 에서 구성해야 합니다.

  자세한 내용은 "L3Out 공유된 서비스(VRF 경로 유출)" 섹션을 참조하시기 바랍니다.

라우팅 프로토콜에 대한 경로 제어(집계)

위에서 언급한 바와 같이 내보내기, 가져오기, 공유된 경로 제어 서브넷은 정확한 매치입니다. 여러 서브넷을 하나의 구성과 매칭하려고 하는 경우 각 경로 제어 서브넷 범위에 대해 "집계" 옵션을 사용할 수 있습니다.

- **집계 내보내기**
  "경로 제어 서브넷 내보내기"가 포함된 0.0.0.0/0 에만 사용할 수 있는 옵션입니다. "경로 제어 서브넷 내보내기"와 "집계 내보내기"가 0.0.0.0/0 에 대해 모두 활성화된 경우, ACI 는 모든 서브넷과 일치하는 "0.0.0.0/0 le 32"가 포함된 IP 식별 번호 목록을 생성합니다. 따라서 이 옵션은 L3Out 이 경로를 외부로 보급(내보내기)해야 할 때 사용할 수 있습니다. 이 범위는 APIC Release 1.1(1)에서 도입되었습니다.

  보다 상세한 집계가 필요한 경우 명시적인 IP 식별 번호 목록이 포함된 경로 맵 및 프로필을 사용할 수 있습니다.

- **집계 가져오기**
  "경로 제어 서브넷 가져오기"가 포함된 0.0.0.0/0 에만 사용할 수 있는 옵션입니다. "경로 제어 서브넷 가져오기"와 "종합 가져오기"가 0.0.0.0/0 에 대해 모두 활성화된 경우, ACI 는 모든 서브넷과 일치하는 "0.0.0.0/0 le 32"가 포함된 IP 식별 번호 목록을 생성합니다. 따라서 이 옵션은 L3Out 이 외부의 경로를 학습해야(가져와야) 할 때 사용할 수 있습니다. 그러나 이는 "경로 제어 적용 가져오기"가 비활성화된

L3Out 구성의 기본값을 유지하는 방법으로도 달성할 수 있습니다. 이 범위는 APIC Release 1.1(1)에서 도입되었습니다.

보다 상세한 집계가 필요한 경우 명시적인 IP 식별 번호 목록이 포함된 경로 맵 및 프로필을 사용할 수 있습니다.

- **공유된 경로 집계**
  "공유된 경로 제어 서브넷"으로 모든 서브넷에 사용할 수 있는 옵션입니다. "공유된 경로 제어 서브넷"과 "공유된 집계 경로 "가 0.0.0.0/8 에 대해 모두 활성화된 경우, ACI 는 10.0.0.0/8, 10.1.0.0/16 등과 일치하는 "0.0.0.0/8 le 32"가 포함된 IP 식별 번호 목록을 생성합니다.

참고:

"경로 제어 서브넷 내보내기" 범위는 라우팅 프로토콜의 경로와 고정 경로, L3Out 인터페이스 서브넷, 그리고 BD 서브넷에 적용되지만 "집계 내보내기"가 OSPF 또는 EIGRP 용 L3Out 에서 사용될 때는 동적 라우팅 프로토콜의 경로에만 적용됩니다. 이 예외 사항은 BGP L3Out 에는 적용되지 않습니다. OSPF 또는 EIGRP L3Out 에서 라우팅 프로토콜이 아닌 BD 서브넷, L3Out 인터페이스 서브넷, 고정 경로 등의 경로에 "경로 제어 서브넷 내보내기" 범위를 적용하고자 할 경우, "경로 제어 서브넷 내보내기" 범위로 특정 서브넷을 구성하면 됩니다. 집계 0.0.0.0/0 에 라우팅 프로토콜의 경로만 포함되는 이 예외가 집계 0.0.0.0/0 에 대한 명시적 식별 번호 목록이 포함된 경로 프로필에도 동일하게 적용됩니다. 기본 내보내기 경로 프로필은 BD 서브넷과 고정 경로 등 직접 경로에 적용되는 예외입니다. 기본 내보내기 경로 프로필은 일반적인 경로 프로필과는 달리, L3Out EPG 또는 L3Out 서브넷에 적용되지 않고도 효력을 발휘하는 사전 정의된 경로 프로필입니다. 자세한 내용은 "L3Out 경로 프로필 및 경로 맵" 섹션을 참조하시기 바랍니다.

Contract 에 대한 서브넷 분류

두 범위("외부 EPG 에 대한 외부 서브넷" 및 "공유된 보안 가져오기")는 Contract 적용에만 사용됩니다. 두 가지 옵션으로 어떤 서브넷이 구성되더라도 라우팅 프로토콜 동작 또는 라우팅 테이블에는 영향을 미치지 않습니다.

ACI 에서는 EPG 간에 Contract 가 적용되며, L3Out 에서는 두 가지 범위를 사용해 특정 L3Out EPG 에서 수신 또는 송신하는 트래픽을 분류합니다. 내부적으로 pcTag(정책 제어 태그)라는 ID 를 각 EPG 및 L3Out EPG 에 대한 식별자로 사용합니다. 자세한 내용은 "L3Out Contract" 섹션을 참조하시기 바랍니다.

- **외부 EPG 에 대한 외부 서브넷**
  Contract 를 보유하고 L3Out 에서 수신 또는 송신되어 구성된 서브넷으로 패킷을 허용하는 데 사용되는 범위입니다.

  L3Out EPG 의 Contract 가 패킷에 적용될 수 있도록 서브넷을 토대로 구성된 L3Out EPG 로 패킷을 분류합니다. 이 범위는 라우팅 프로토콜 제어와 관련된 다른 범위에 대한 IP 식별 번호 목록이 포함된 정확한 매치가 아닌 가장 긴 식별 번호 매치입니다. L3Out EPG A 에서 10.0.0.0/16 이 "외부 EPG 에 대한 외부 서브넷"으로 구성된 경우, 10.0.1.1 등 해당 서브넷의 IP 주소를 보유한 패킷은 모두 L3Out EPG A 로 분류되어 L3Out EPG A 에 대한 Contract 를 적용합니다. 이는 "외부 EPG 에 대한 외부 서브넷" 범위가 라우팅 테이블에서 경로 10.0.0.0/16 을 설치한다는 의미는 아닙니다. 이는 오로지 Contract 적용을 목적으로 EPG(pcTag)에 서브넷을 매핑할 다른 내부 테이블을 생성하게 되며, 이는 라우팅 프로토콜 동작에는 영향을 미치지 않습니다. 따라서 라우팅 프로토콜 또는 고정 경로에 대상 경로가 존재하지 않는 경우에는 "외부 EPG 에 대한 외부 서브넷" 범위 덕분에 패킷이 적합한 Contract 가 포함된 적합한 L3Out EPG 로 분류되더라도 패킷은 전송되지 않습니다.

  이것은 서브넷을 학습 중인 L3Out 에서 구성해야 하는 범위입니다.

  자세한 내용은 "L3Out Contract" 섹션을 참조하시기 바랍니다.

- **공유된 보안 가져오기 서브넷**

  패킷이 L3Out 으로 VRF 전체에 전달될 때 구성된 서브넷을 사용해 패킷을 허용하는 범위입니다. 라우팅 테이블의 경로는 위에서 언급한 바와 같이 "공유된 경로 제어 서브넷"이 포함된 다른 VRF 로 유출됩니다. 그러나 또 다른 VRF 는 유출된 경로가 어느 EPG 에 속해야 하는지를 아직 인지하지 못합니다. "공유된 보안 가져오기 서브넷" 범위는 유출된 경로가 속하는 L3Out EPG 를 다른 VRF 에 통지합니다. 따라서 이 범위는 "외부 EPG 에 대한 외부 서브넷" 범위도 함께 사용될 때만 사용할 수 있으며, 그렇지 않을 경우 원본 VRF 가 서브넷이 속하는 L3Out EPG 를 인식할 수 없습니다. "외부 EPG 에 대한 외부 서브넷" 없이 "공유된 보안 가져오기 서브넷"이 구성된 경우 APIC GUI 가 해당 구성을 차단합니다. 이 범위는 가장 긴 식별 번호 매치이기도 합니다.

  자세한 내용은 "L3Out 공유된 서비스(VRF 경로 유출)" 섹션을 참조하시기 바랍니다.

경로 제어 적용

경로 제어 적용 옵션은 APIC Release 1.1(1)에서 도입되었으며, **Tenant > Networking > External Routed Networks > L3Out** 에 위치합니다. 기술적으로 두 개의 옵션(가져오기와 내보내기)이 있지만, 내보내기는 항상 활성화되어 있으며 비활성화할 수 없으므로 경로 제어 적용은 기본적으로 비활성화되어 있는 경로 제어 적용 가져오기로 간주할 수 있습니다. L3Out 서브넷에 대해 "경로 제어 서브넷 가져오기" 범위를 사용하려면 이 옵션을 반드시 활성화해야 합니다. 이 옵션은 OSPF 와 BGP 에만 지원됩니다.

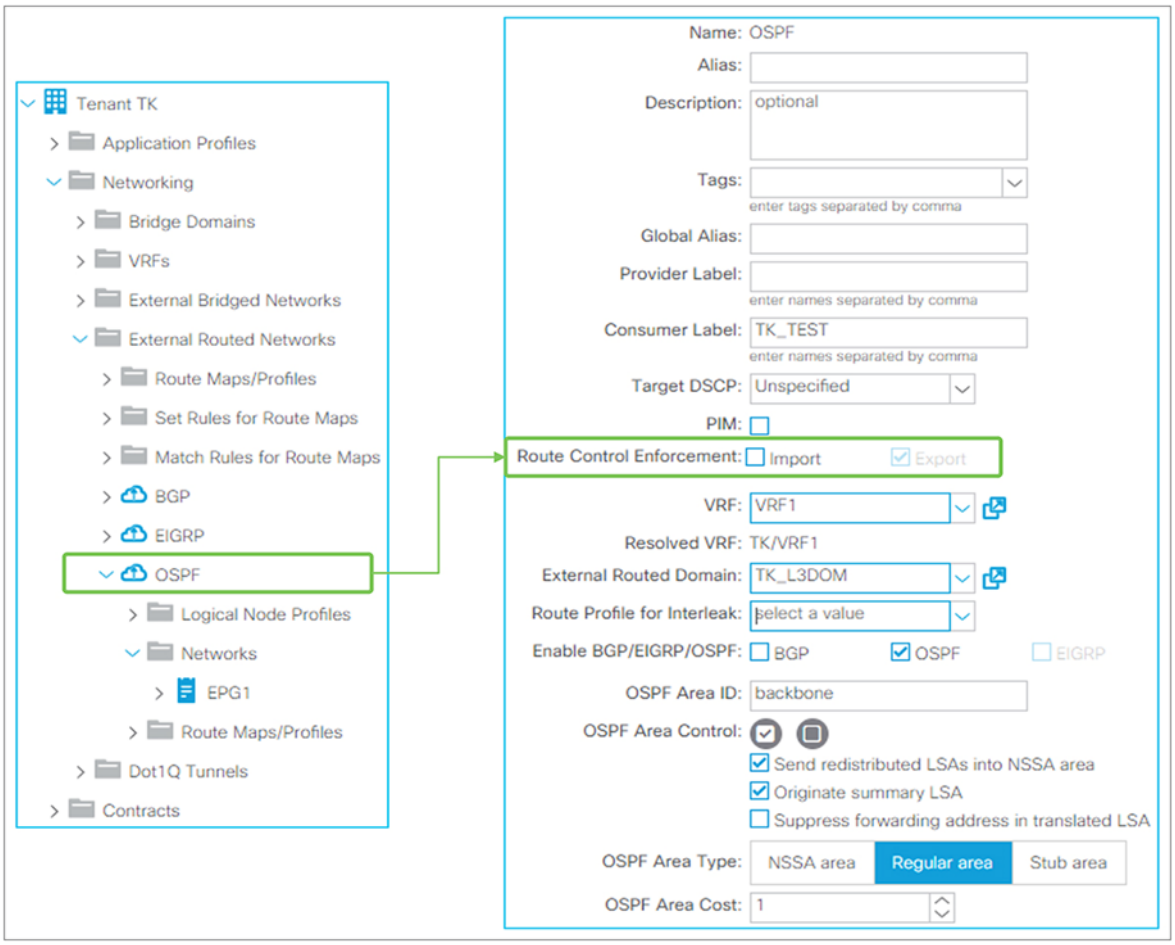

Figure 74.
GUI(APIC Release 3.2) 내 경로 제어 적용

경로 제어 **가져오기** 옵션이 활성화되어 있지 않으면 L3Out 은 라우팅 프로토콜을 통해 외부 경로를 학습하고, 이렇게 학습된 외부 경로가 라우팅 테이블에 설치됩니다.

경로 제어 **가져오기**가 OSPF L3Out 에 대해 활성화되면 OSPF 는 외부 경로를 학습하고, 이 외부 경로는 보더 리프의 OSPF LSDB 에 위치하게 됩니다. 그러나 "경로 제어 서브넷 가져오기" 범위로 경로 서브넷이 구성되지 않으면 이러한 외부 경로는 라우팅 테이블에 설치되지 않습니다. 이는 NX-OS OSPF 의 테이블 맵 기능을 사용해 구현합니다. "경로 제어 서브넷 가져오기" 범위가 포함된 서브넷은 IP 식별 번호 목록이 포함된 경로 맵에서 사용되어 서브넷이 라우팅 테이블에 설치되는 것을 테이블 맵이 허용하게 됩니다.

경로 제어 **가져오기**가 BGP L3Out 에 대해 활성화되면 BGP 는 동일한 L3Out 내 모든 BGP 피어에 대해 인바운드 경로 맵을 사용해 외부 경로 학습을 중단합니다. "경로 제어 서브넷 가져오기" 범위가 포함된 서브넷은 IP 식별 번호 목록이 포함된 경로 맵에서 사용되어 서브넷이 BGP 를 통해 학습될 수 있도록 허용합니다.

참고:

동일한 VRF 의 동일 보더 리프에 OSPF 가 포함된 L3Out 이 여러 개가 있을 경우, 두 L3Out 에서 경로 제어 적용이 일치해야 합니다. 그렇지 않을 경우 F0467 오류 메시지가 표시되며, 그 이유는 다음과 같습니다. 한 개의 보더 리프에는 OSPF 프로세스가 한 개만 존재하며 동일한 VRF 의 동일 보더 리프에 있는 각 OSPF L3Out 은 동일한 프로세스의 서로 다른 OSPF 를 나타냅니다. 그러나 테이블 맵은 각 영역이 아닌 OSPF 프로세스 수준에 적용됩니다. 따라서 동일한 VRF 의 동일 보더 리프에 각기 다른 경로 제어 적용 구성이 포함된 OSPF 영역(L3Out)을 보유하면 충돌이 발생하게 됩니다. 이는 동일한 VRF 의 동일 보더 리프에 두 L3Out 이 모두 배포될 경우, OSPF L3Out A 의 "경로 제어 서브넷 가져오기" 범위 구성이 OSPF L3Out B 에도 적용될 것이라는 것을 나타냅니다.

OSPF 테이블 맵에 대한 경로 맵의 이름은 "**exp-ctx-<VRF VNID>-deny-external-tag**" 형식입니다.

L3Out Contract

L3Out Contract 에 대한 대략적인 개요는 "L3Out 의 기본 구성 요소" 섹션의 5 단계에서 다루며, 이 섹션에서는 L3Out Contract 아키텍처를 자세히 설명합니다.

ACI 의 Contract 는 EPG 간 트래픽을 허용하는 데 사용됩니다. 일반적으로 패킷은 수신되는 VLAN 및 인터페이스에 기반해 적합한 EPG 로 분류됩니다. 미세 세분화를 위한 IP 기반 EPG 등 예외사항도 있지만 본 문서에서는 다루지 않습니다. 하드웨어에서는 각 EPG 를 pcTag(정책 제어 태그)라는 번호로 나타내며, 두 번호 간에 Contract 가 적용됩니다.

예시: **"EPG A → EPG B"**는 **"pcTag 49150 → pcTag 49151"**을 의미함

각 EPG 에 대한 pcTag 는 "Tenant > Application Profiles > Application EPGs > EPG > Policy tab > General tab > pcTag (sclass)"에서 확인할 수 있습니다.

L3Out 을 통해 ACI 패브릭을 출입하는 트래픽을 분류하기 위한 EPG 를 일반적으로 L3Out EPG 또는 외부 EPG 라고 하며, 이는 **"Tenant > Networking > External Routed Networks > L3OU > Networks > L3Out EPG"**에 위치합니다. APIC GUI 에서는 "외부 네트워크 인스턴스 프로필"(Figure 75)로 표시됩니다. L3Out 은 패킷을 적합한 L3Out EPG 로 분류하는 데 VLAN 과 인터페이스를 사용하지 않으며, 원본 식별 번호와 서브넷을 기반으로 분류합니다. 따라서 L3Out EPG 를 식별 번호 기반 EPG 라고 부르기도 합니다. 패킷이 L3Out EPG 로 분류되고 서브넷을 기반으로 pcTag 가 할당되면 일반적인 EPG 와 마찬가지로 원본 및 대상 EPG(pcTag) 결합을 기반으로 Contract 가 적용됩니다.

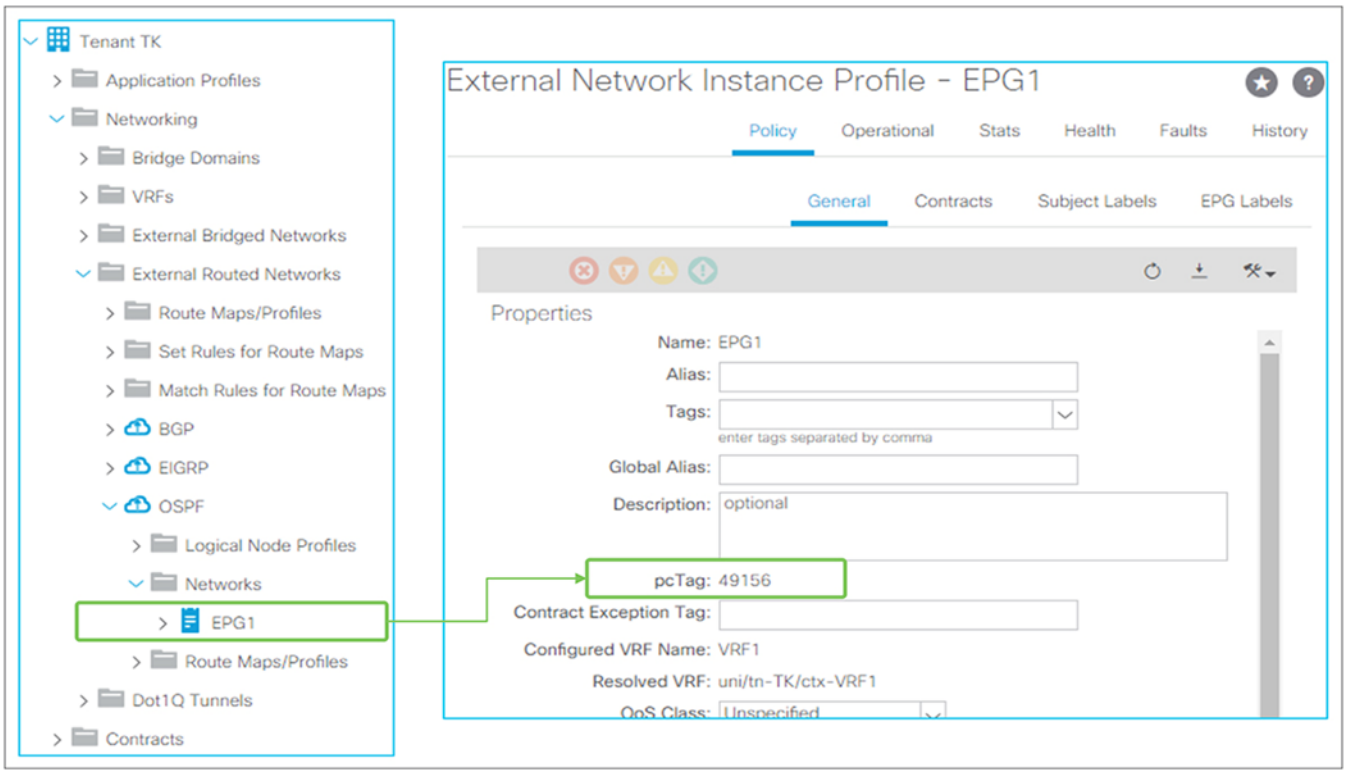

Figure 75.
GUI(APIC Release 3.2) 내 L3Out EPG 및 pcTag

참고:

pcTag 는 기본적으로 VRF 내에서 고유하므로 VRF 전체에서 pcTag 의 중첩이 발생할 수 있습니다. 이는 문제가 되지 않지만 VRF 경로 유출, 즉 공유된 서비스를 수행할 때는 문제가 됩니다. 이러한 상황에서 ACI 는 글로벌 pcTag 라고 하는 pcTag 를 사용합니다. ACI 는 명시적인 사용자 구성 없이 적합한 유형의 pcTag 를 생성하여 이를 EPG 로 할당한다는 점에 유의해야 합니다. 0x4000(16384)보다 범위가 작은 pcTag 를 글로벌 pcTag 라고 하며, 이는 전체 VRF 전체에서 고유합니다. 자세한 내용은 "L3Out 공유된 서비스(VRF 경로 유출)" 섹션을 참조하시기 바랍니다.

L3Out EPG(식별 번호 기반의 EPG)

이 섹션에서는 서브넷을 기반으로 패킷이 L3Out EPG 로 분류되는 방식을 자세히 설명합니다.

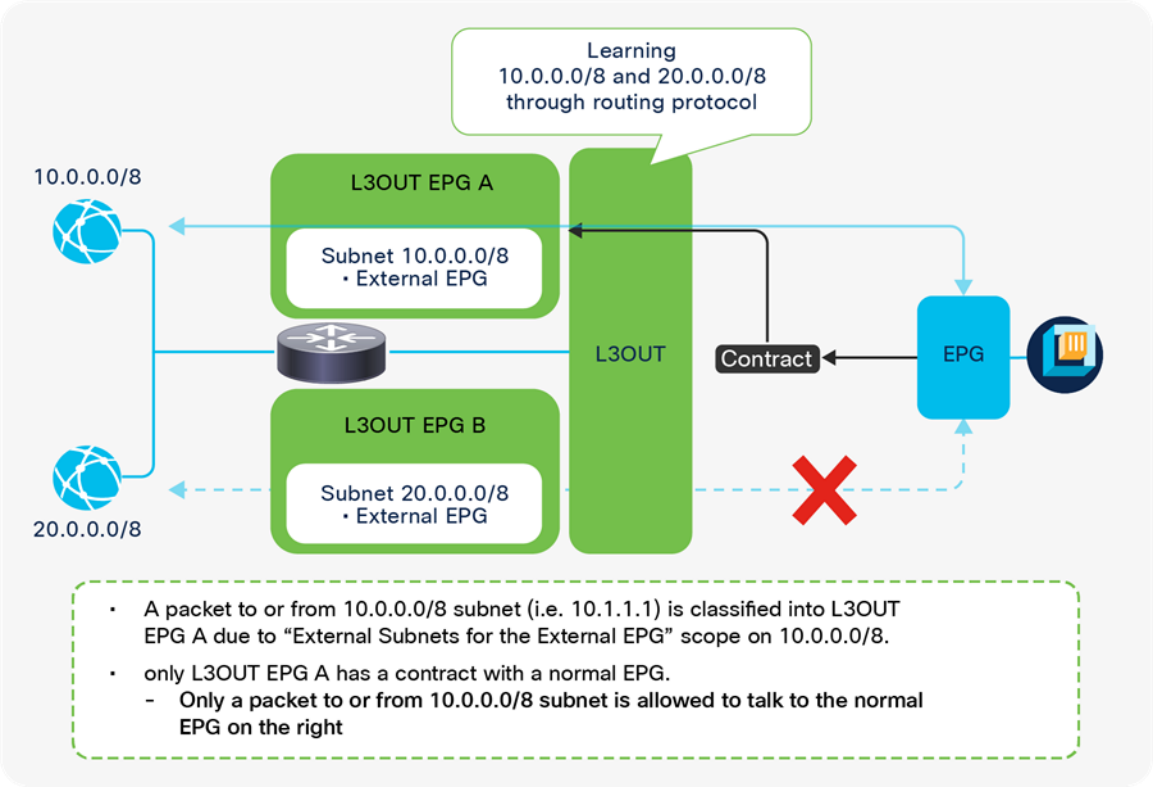

Figure 76.

L3Out EPG 에 대한 식별 번호 기반 분류

L3Out 은 엔드 호스트가 아닌 외부 라우팅 장치에 연결하는 구성 요소입니다. 이는 그 뒤에 많은 서브넷이 존재한다는 점을 나타내며, 이를 위해 Contract 정책에 대해 서브넷을 상세히 분류해야 합니다. L3Out EPG 를 통해 식별 번호를 토대로 외부 트래픽을 분류할 수 있습니다. Figure 76 은 각기 다른 서브넷과 일치하도록 L3Out EPG 를 구성하는 방법을 설명합니다.

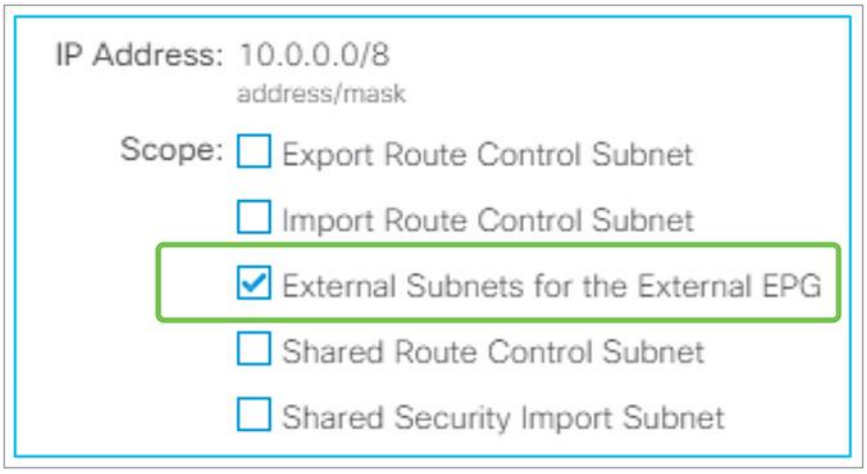

Figure 77.

외부 EPG 에 대한 외부 서브넷

각 L3Out EPG 의 트래픽 분류는 L3Out EPG 의 L3Out 서브넷에서 "외부 EPG 에 대한 외부 서브넷" 범위로 구성됩니다(Figure 77).

외부 EPG 에 대한 외부 서브넷 및 식별 번호(pcTag 매핑)

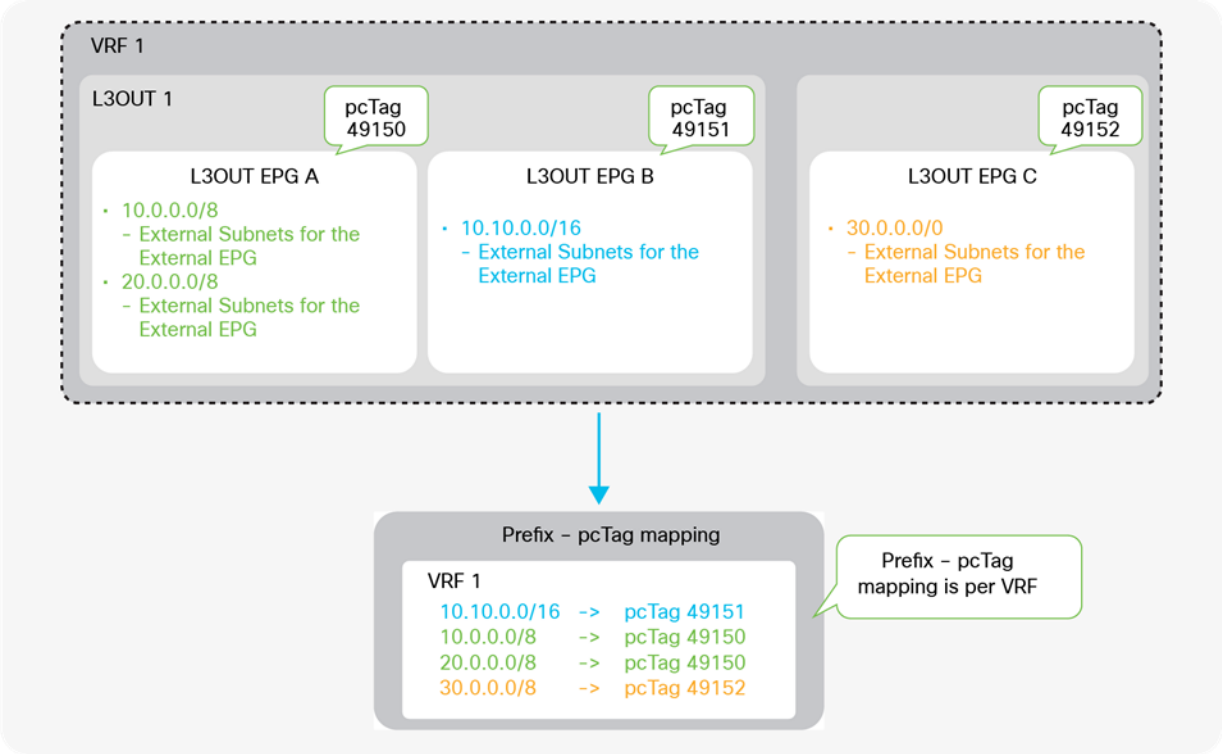

Figure 78.
L3Out 식별 번호(pcTag 매핑)

L3Out 서브넷이 "외부 EPG 에 대한 외부 서브넷"으로 구성되면 ACI 는 해당 L3Out 의 pcTag 와 식별 번호를 매핑하는 테이블을 내부적으로 생성합니다. 이 매핑 테이블은 가장 긴 식별 번호 매칭(LPM) 테이블이며, 각 VRF 에 별도의 매핑 테이블이 구성됩니다. 따라서 "외부 EPG 에 대한 외부 서브넷" 범위가 포함된 서브넷은 동일한 VRF 내 모든 L3Out 의 모든 L3Out EPG 에서 고유해야 합니다. Figure 78 에서 L3Out EPG A 와 마찬가지로 L3Out EPG C 에도 "외부 EPG 에 대한 외부 서브넷" 범위가 포함된 10.0.0.0/8 이 존재한다면, 10.0.0.0/8 을 pcTag 49150(L3Out EPG A) 또는 pcTag 49152(L3Out EPG C)로 매핑해야 하는지 여부를 ACI 가 식별할 수 없게 됩니다. 그러나 Figure 78 에서는 LPM 의 측면에서 볼 때 10.0.0.0/8 과 동일한 항목이 아니므로 10.10.0.0/16 이 L3Out EPG B 에서 구성될 수 있습니다. IP 10.10.0.1 이 포함된 패킷은 L3Out EPG A 가 아닌 L3Out EPG B 로 분류됩니다.

각 리프 스위치의 식별 번호 pcTag 매핑을 확인하는 데 다음 명령어를 사용할 수 있습니다.

```
Leaf1# vsh_lc -c 'show system internal aclqos prefix' | egrep 'Vrf|10.0.0.0'
Vrf-Vni VRF-Id Table-Id    Addr        Class  Shared Remote Complete
2097152 8      0x8         10.0.0.0/8  49200  0      1      No

 === APIC release 3.2(1)부터는 이 명령어를 사용합니다 ===
Leaf1# vsh –c 'show system internal policy-mgr prefix'
```

- Vrf-Vni: VRF VNID
- Addr: "외부 EPG 에 대한 외부 서브넷" 범위가 포함된 L3Out 서브넷 및 식별 번호
- 클래스: L3Out EPG 에 대한 pcTag

주의:

ACI 패브릭에서 엔드포인트가 학습되면 해당 엔드포인트에 대한 EPG 의 pcTag 도 엔드포인트 테이블에 저장됩니다. 이는 ACI 가 L3Out 에 대한 pcTag 매핑의 식별 번호를 확인할 때 pcTag 매핑에 대한 엔드포인트 IP 도 함께 확인된다는 의미입니다. 이 매핑 역시 가장 식별 번호 매치 사용에 기반합니다. L3Out EPG A 에 "외부 EPG 에 대한 외부 서브넷"의 10.0.0.0/8 이 존재하는 Figure 78 의 예시와 같이, 트래픽 경로 설계 오류 또는 IP 스푸핑 등으로 인해 10.1.1.1 과 같은 외부 IP 가 일반적인 엔드포인트로서 학습되는 경우, L3Out 1 로 송/수신되는 IP 10.1.1.1 이 포함된 패킷은 L3Out EPG A 가 아니라 엔드포인트 10.1.1.1 의 일반 EPG 에 대한 pcTag 를 사용하게 되는데, 그 이유는 엔드포인트가 /32 항목으로, LPM 의 /8 항목보다 우선적으로 사용되기 때문입니다.

이처럼 원치 않는 엔드포인트 학습 동작을 방지하는 방법은 ACI 패브릭 엔드포인트 학습 백서를 참조하시기 바랍니다.

외부 EPG 에 대한 외부 서브넷이 포함된 0.0.0.0/0 의 예외

사용자는 0.0.0.0/0 을 "외부 EPG 에 대한 외부 서브넷" 범위가 포함된 서브넷으로 사용하여 발생하는 고유 동작에 관해 신중을 기해야 합니다. 권장하는 방법은 아니지만, 동일한 VRF 의 여러 L3Out EPG 에서 "외부 EPG 에 대한 외부 서브넷"으로 0.0.0.0/0 를 구성할 수 있습니다. 그러나 0.0.0.0/0 이 아닌 서브넷의 경우에는 불가능합니다. 예를 들어 동일한 VRF 의 "외부 EPG 에 대한 외부 서브넷"이 포함된 0.0.0.0/0 이 아닌 서브넷으로는 여러 개의 L3Out EPG 를 구성할 수 없습니다. 0.0.0.0/0 가 예외인 이유는 "외부 EPG 에 대한 외부 서브넷"이 포함된 0.0.0.0/0 가 각 L3Out EPG 에 대한 pcTag 를 사용하지 않고 항상 예약된 pcTag 를 사용하기 때문입니다. 이러한 구성이 허용되기는 하지만, 동일한 VRF 내 여러 개의 L3Out EPG 에서 "외부 EPG 에 대한 외부 서브넷"이 포함된 0.0.0.0/0 을 구성함으로써 Contract 배포가 의도치 않게 발생할 수도 있습니다. Figure 79 에 이러한 시나리오가 나와있습니다.

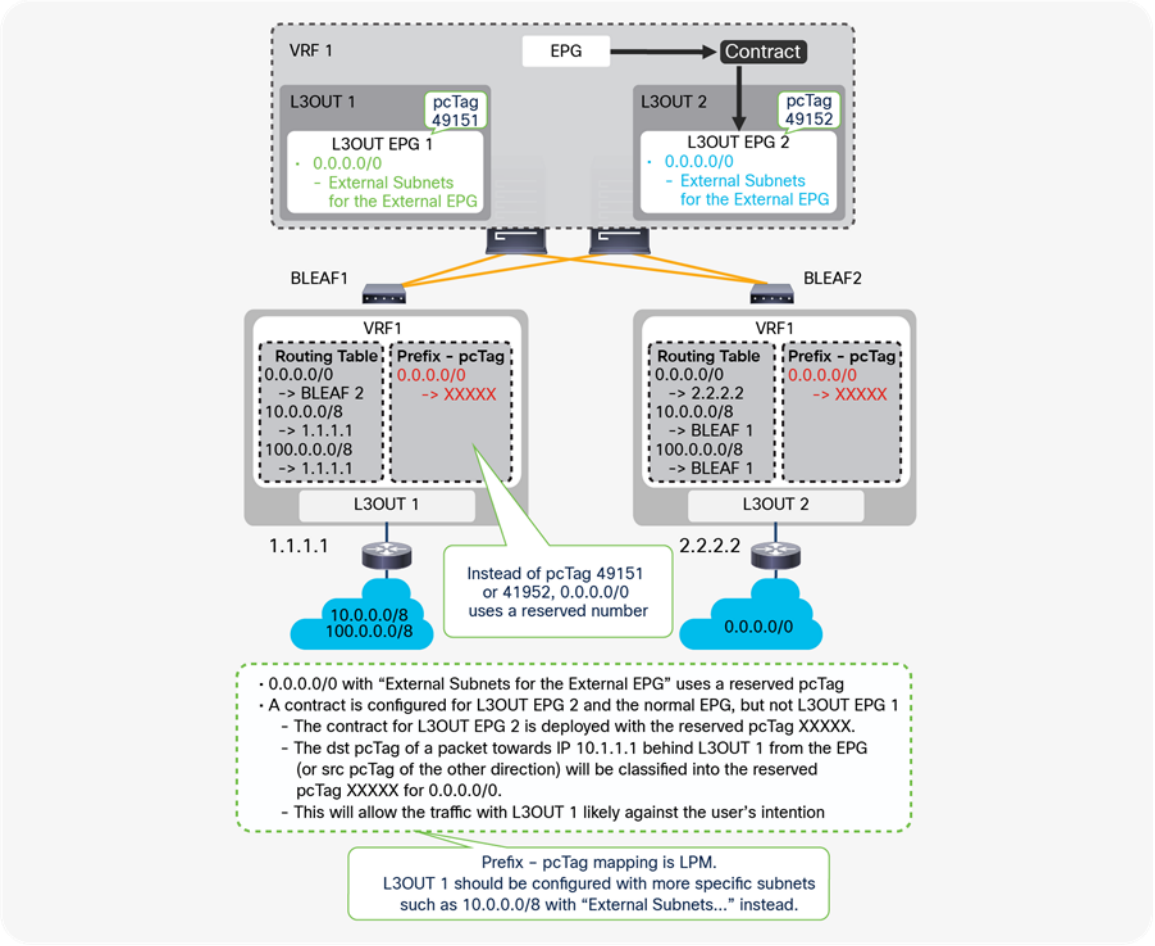

Figure 79.

"외부 EPG 에 대한 외부 서브넷"이 포함된 0.0.0.0/0 의 경고

Figure 79 에서는 "외부 EPG 에 대한 외부 서브넷" 범위가 포함된 0.0.0.0/0 가 L3Out 1 과 L3Out 2 에서 모두 구성되는데, 여기서 일반 EPG 에 대한 Contract 는 L3Out EGP 2 로만 구성됩니다. 따라서 누락된 Contract 로 인해 일반 EPG 와 L3Out 1 라우터 간의 패킷이 삭제될 수 있습니다. 그러나 L3Out 2 라우터의 패킷과 마찬가지로 일반 EPG 와 L3Out 1 라우터 간의 모든 패킷이 허용되는데, 그 이유는 pcTag 분류가 L3Out 이 아닌 각 VRF 에 적용되는 prefix-pcTag 매핑 테이블만 사용하기 때문입니다.

이 구성이 포함된 보더 리프 스위치의 식별 번호 pcTag 매핑 테이블에는 49151(L3Out EPG1)이나 49152(L3Out EPG2)가 아닌 0.0.0.0/0 에 대한 예약된 pcTag 가 포함된 항목이 한 개만 존재하게 됩니다. 이후 일반 EPG 와 L3Out EPG 2 간의 Contract 는 0.0.0.0/0 에 대한 예약된 pcTag 와 일반 EPG 에 대한 pcTag 로 배포됩니다. 패킷이 일반 EPG 의 L3Out 1 뒤에서 10.1.1.1 로 송신될 때, 대상 pcTag 는 식별 번호 pcTag 매핑에 기반해 예약 상태가 됩니다(Figure 79 의 "XXXXX"). 따라서 L3Out EPG 2 와 일반 EPG 간 Contract 규칙으로 인해 L3Out EPG 1 에 대한 패킷이 허용됩니다. 이에 더해 L3Out EPG 1 에 "외부 EPG 에 대한 외부 서브넷" 범위가 포함된 10.0.0.0/8 이 존재할 경우, 식별 번호 pcTag 매핑 테이블에는 두 개의 항목이 존재하게 되는데, 하나는 예약된 pcTag 가 포함된 0.0.0.0/0 에 대한 것이고, 다른 하나는 49151(L3Out EPG1 pcTag)이 포함된 10.0.0.0/8 에 대한

것입니다. LPM 규칙으로 인해 패킷은 pcTag 49151 로 분류됩니다. 이후 이 패킷은 누락된 Contract 로 인해 삭제됩니다.

따라서 "외부 EPG 에 대한 외부 서브넷" 범위가 포함된 0.0.0.0/0 를 VRF 마다 한 개의 L3Out EPG 에서만 사용하고, 다른 L3Out EPG 에는 좀 더 구체적인 서브넷을 사용하는 것이 좋습니다.

참고:

이 동작은 정책 제어 적용 방향 옵션에 따라 달라질 수 있습니다. 비 기본인 "송신"이 사용될 경우 Contract 가 각 보더 리프에 적용될 수 있습니다. 두 개의 L3Out 이 서로 다른 보더 리프 스위치에 배포될 경우 각 보더 리프 스위치에는 자체 Contract 규칙만 존재하게 됩니다. 따라서 적어도 각 보더 리프에는 부적합한 Contract 가 적용되지 않지만 두 L3Out 에 대해 Contract 규칙을 가질 수 있는 비 보더 리프 스위치에 Contract 가 적용되는 시나리오는 많이 있습니다. 따라서 0.0.0.0/0 을 "외부 EPG 에 대한 외부 서브넷" 범위가 동일하게 유지되는 서브넷으로 사용하는 것이 좋습니다.

참고:

"외부 EPG 에 대한 외부 서브넷" 범위가 포함된 0.0.0.0/0 에 대한 예약된 pcTag 는 패킷의 방향에 따라 달라집니다. 대상 pcTag 분류(ACI 패브릭에서 L3Out 으로 송신되는 패킷)의 경우, ACI 는 0.0.0.0/0 에 대한 고정 값으로 항상 pcTag 15 을 사용합니다. 원본 pcTag 분류(L3Out 에서 ACI 패브릭의 엔드포인트로 송신되는 패킷)의 경우 ACI 는 0.0.0.0/0 에 대해 VRF 의 pcTag 또는 L3Out BD(L3Out BD 의 pcTag 는 VRF 와 동일)를 사용합니다. pcTag 15 이 원본과 대상에 모두 사용되지 않는 이유는 원본과 대상이 0.0.0.0/0 pcTag-prefix 매핑에 속하는 트래픽의 허용을 방지하기 위해서입니다. 원본과 대상의 값이 동일한 경우 동일 EPG 내에서 트래픽은 통신으로 추정되고 해당 통신이 허용됩니다.

0.0.0.0/0 을 포함하는 직접 연결된 서브넷의 예외

이전 섹션에서는 ACI 가 L3Out 을 통해 외부에서 패브릭으로 입력되는 트래픽을 분류하는 방식을 설명했으며, 해당 트래픽이 패브릭으로부터 여러 홉 떨어진 곳에서 시작되고 외부에서 보더 리프로 라우팅된다고 가정했습니다. 트래픽을 시작하는 장치가 L3Out 인터페이스 서브넷(직접 연결된 서브넷)의 보더 리프에 직접 연결되면 트래픽이 분류되는 방식은 이전 섹션에서 설명한 것과 다소 달라지며 리프 하드웨어에 따라 달라집니다.

세부 내용을 다루기에 앞서, 만일의 상황에 대비해 L3Out 인터페이스 서브넷을 "외부 EPG 에 대한 외부 서브넷"으로 항상 구성하는 것이 좋습니다.

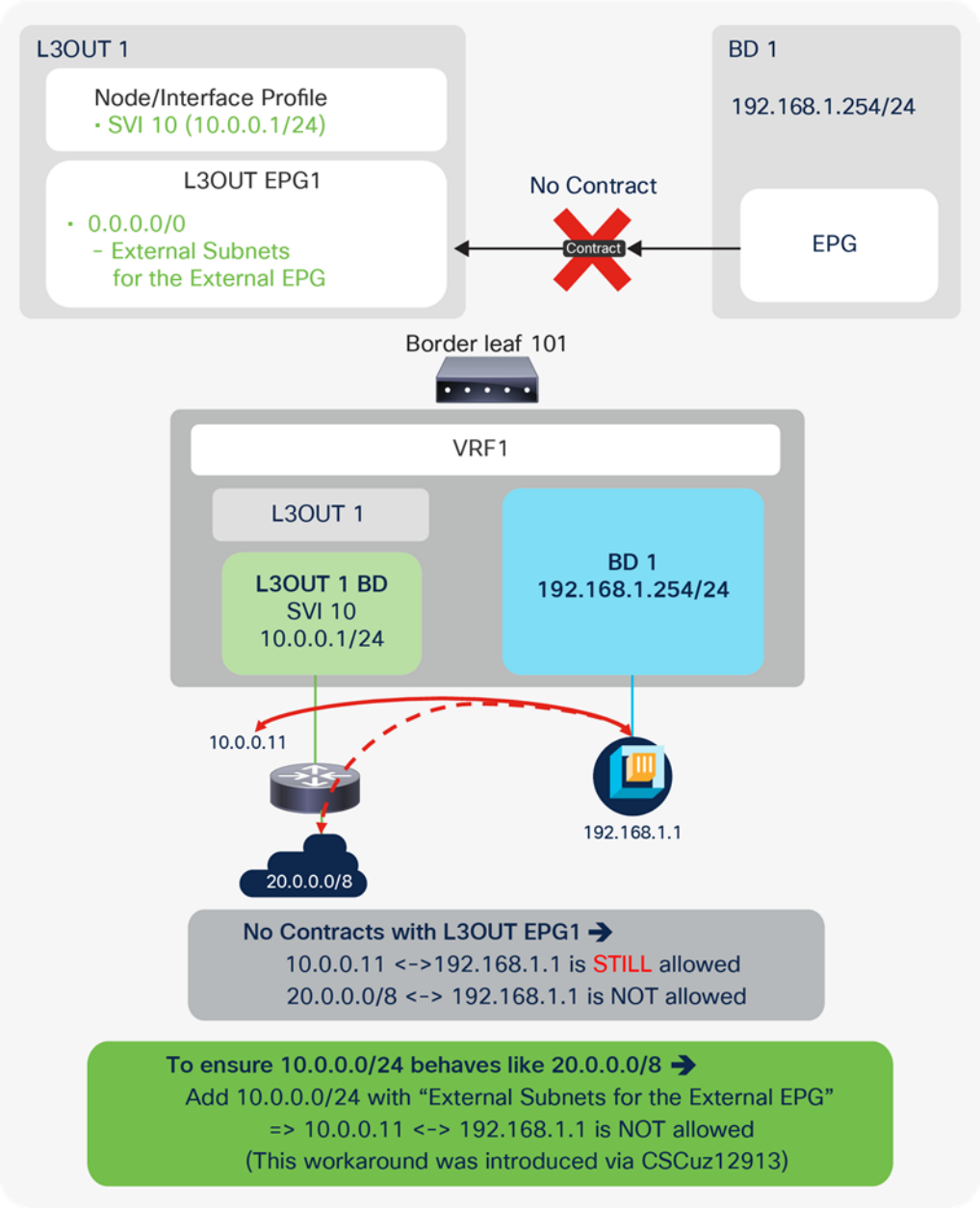

Figure 80.

L3Out Contract 및 직접 연결된 서브넷(예기치 않은 허용)

Figure 80 에서와 같이, 직접 연결된 L3Out 서브넷(10.0.0.11)의 IP 와 다른 IP(예: 192.168.1.1) 간 트래픽은 Contract 없이도 허용될 수 있습니다. 다른 IP 는 이 예시 또는 다른 L3Out 의 IP 등 일반 엔드포인트(EP)가 될 수 있습니다. 그 이유는 기본값으로 직접 연결된 서브넷이 할당된 pcTag 1 로, 이것이 Contract 를 우회하는 특별 pcTag 이기 때문입니다. 이는 코너 케이스 시나리오에서 라우팅 프로토콜 통신을 암시적으로 허용하는 것이 목적입니다. 그러나 Figure 80 에서와 같이, 이로 인해 보안 문제가 발생할 수 있으므로 이 동작을 결함 ID CSCuz12913 를 통해 상세하게 설명하며 해결 방법 구성을 함께 소개합니다.

CSCuz12913 ACI: Contract 는 L3Out 에서 직접 연결된 서브넷에 적용되지 않습니다.

CSCuz12913 의 개선 기능을 활용하면 "'외부 EPG 에 대한 외부 서브넷' 범위로 직접 연결된 서브넷을 다루는 0.0.0.0/0 이 아닌 서브넷을 구성"하는 방법을 통해, 직접 연결된 서브넷도 pcTag 1 이 아닌 L3Out EPG 의 pcTag 를 사용하도록 강제할 수 있습니다. 원치 않은 트래픽이 ACI 패브릭을 통과하는 것을 방지하려면 "외부 EPG 에 대한 외부 서브넷"으로 직접 연결된 서브넷을 명시적으로 구성하고 CSCuz12913 의 개선 기능을 활용하는 것이 좋습니다. 이 개선 기능은 2 세대 리프 스위치부터 사용할 수 있습니다.

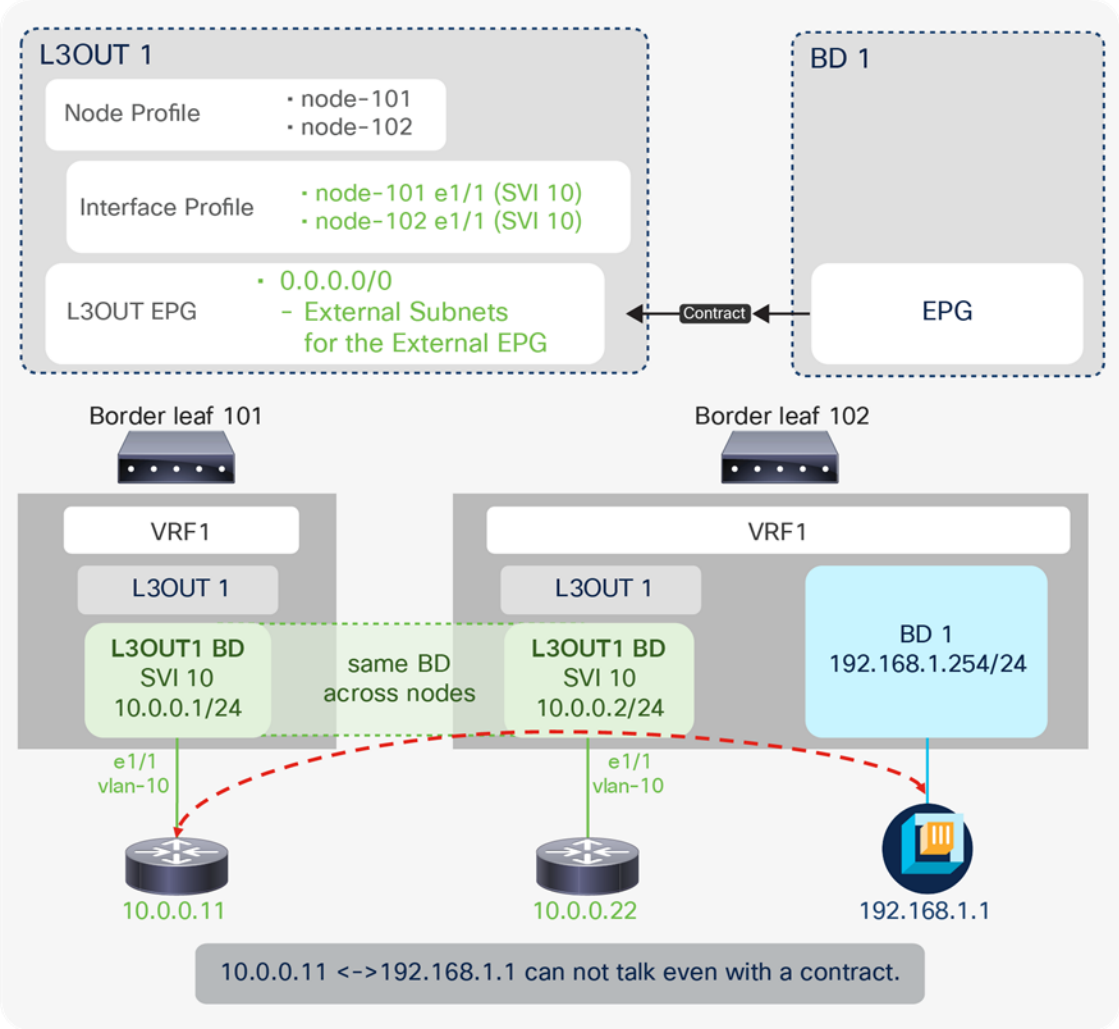

Figure 81.

L3Out Contract 및 직접 연결된 서브넷(예기치 않은 거부)

직접 연결된 서브넷에 대한 이 pcTag 1 으로 인해 특수한 상황의 Contract 에서도 허용이 아닌 삭제가 예기치 않게 발생할 수 있습니다(Figure 81). 이 경우 L3Out BD 는 두 개의 보더 리프 스위치 전체를 아우릅니다. 한 개의 보더 리프(리프 102)에서 다른 리프(리프 101)의 직접 연결된 IP 10.0.0.11 로 트래픽이 전송됩니다. 다음은 일어나는 현상을 단계별로 설명한 것입니다.

4. 리프 102 는 동일한 L2 도메인(L3Out BD)에 위치하므로 10.0.0.11 에 대한 ARP 항목을 보유합니다.
5. 리프 102 는 대상 10.0.0.11 을 조회하고, ARP 항목을 사용해 다음 홉 MAC 주소를 해결한 후 이를 리프 101 로 송신합니다.

6. 이때 직접 연결된 서브넷에 대한 pcTag1 으로 인해 리프 102 에서 Contract 가 우회됩니다. 10.0.0.11 은 리프 102 에 기술적으로 직접 연결되지는 않지만, L3Out BD 를 통해 ARP 항목을 보유하므로 직접 연결로 간주하게 됩니다.
7. 패킷이 리프 101 에 도달합니다. 대상 MAC 는 ACI MAC 주소가 아닌 외부 라우터(10.0.0.11)에 이미 속해있습니다. 이전 노드에서 우회되었으므로 Contract 는 아직 적용되지 않습니다.
8. 조회는 리프 101 이 인식하는 대상 MAC 주소에 기반합니다. 그러나 L3Out Contract 가 서브넷에 기반하여 L3Out BD 의 MAC 주소에 대한 Contract 가 존재하지 않으므로 리프 101 에서 삭제됩니다.

이러한 문제를 방지하기 위해 CSCuz12913 의 해결 방법을 적용할 수 있습니다. 직접 서브넷을 아우르는 0.0.0.0/0 이 아닌 서브넷이 "외부 EPG 에 대한 외부 서브넷" 범위로 구성되면 리프 101 과 리프 102 는 pc Tag 1 이 아닌 L3Out EPG 의 pcTag 를 인식하게 되며, 이에 따라 리프 102 는 외부 BD 에서 트래픽을 브리징하기 전에 Contract 를 적용하게 됩니다. Contract 는 우회되지 않고 서브넷을 기반으로 적절하게 적용되며, 트래픽은 VXLAN 헤더의 "정책 적용" 비트 설정을 통해 리프 101 로 전송됩니다. 이후 리프 101 이 트래픽을 전송합니다. 이는 직접 연결된 서브넷에만 적용됩니다. 트래픽이 외부 라우터(10.0.0.11) 뒤에서 다른 서브넷으로 송신되는 경우에는 이러한 문제가 발생하지 않습니다. Figure 82 는 멀티 포드와 관련하여 이러한 문제에 대한 일반적인 토폴로지 예시 중 하나입니다.

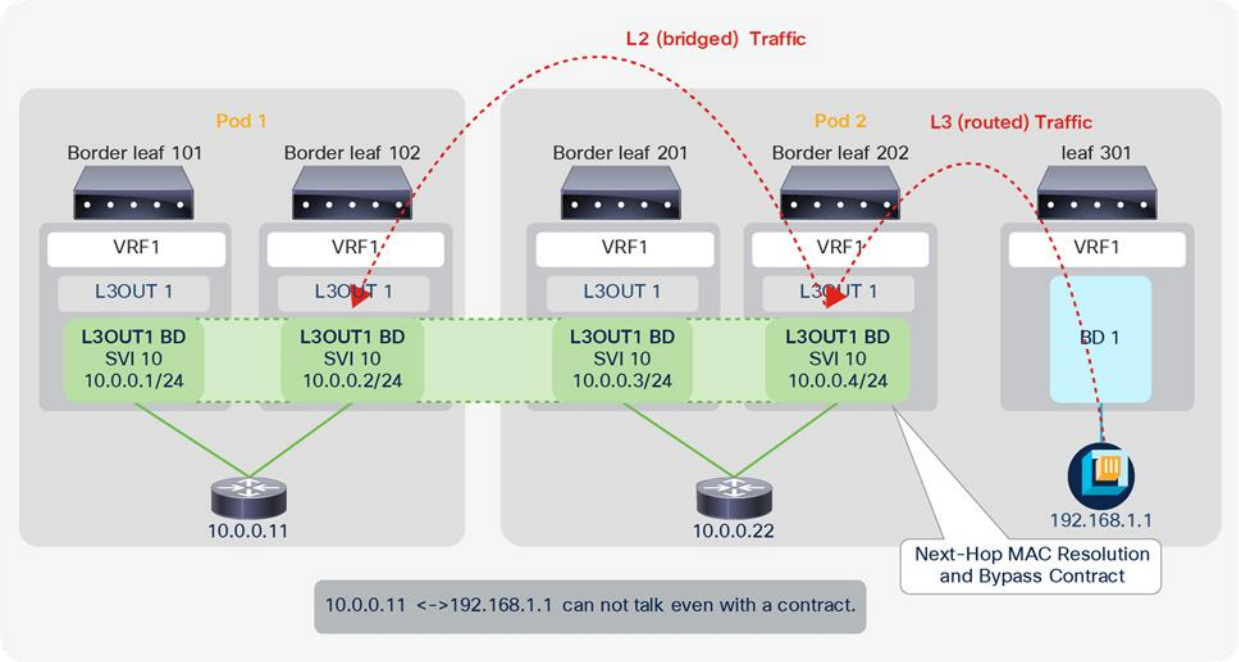

Figure 82.

L3Out Contract 및 직접 연결된 서브넷(예기치 않은 거부-2)

정책 제어 적용 방향

정책 제어 적용 방향 옵션은 APIC Release 1.2(1)에서 도입되었으며, **"Tenant > Networking > VRFs > VRF"**에 위치합니다. "**수신**" 또는 "**송신**"으로 설정될 수 있는데, "**송신**" 옵션은 Release 1.2(1) 이전의 동작에 해당합니다. 따라서 모든 업그레이드 버전에서 동작을 동일하게 유지하려면 VRF 가 Release 1.2(1) 이전에 생성되었고 ACI 패브릭이 1.2(1) 이후 버전으로 업그레이드된 경우 "**송신**"으로 설정해야 합니다. APIC Release 1.2(1)부터는 "**수신**"이 기본 구성입니다.

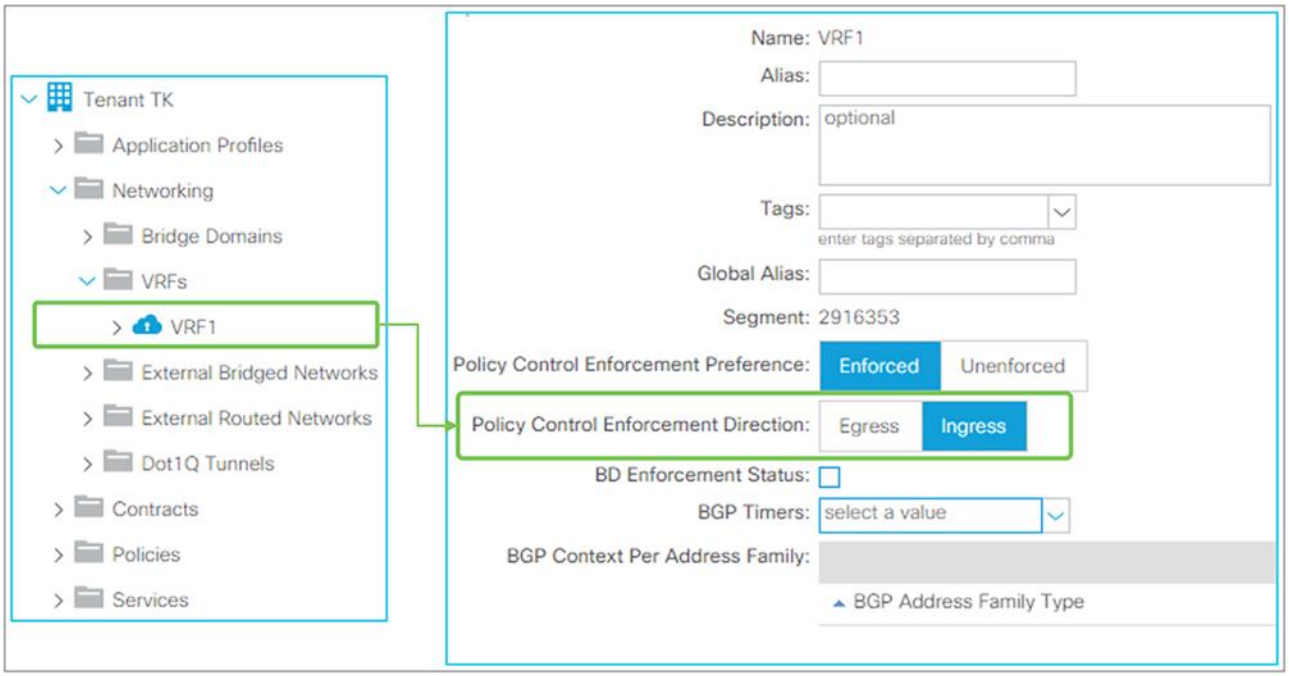

Figure 83.
GUI(APIC Release 3.2) 내 정책 제어 적용 방향

정책 제어 적용 방향은 보더 리프 스위치의 Contract 에 대한 TCAM 리소스를 저장하는 기능입니다. 따라서 이는 L3Out 에서 수신 또는 송신되는 트래픽에만 영향을 미칩니다. EPG 간 트래픽에서는 이 옵션으로 인한 동작 변화가 없습니다. "**수신**"이 TCAM 리소스를 저장하는 기본 모드이므로 일반적으로는 사용자가 이 구성의 모드를 변경할 필요가 없습니다.

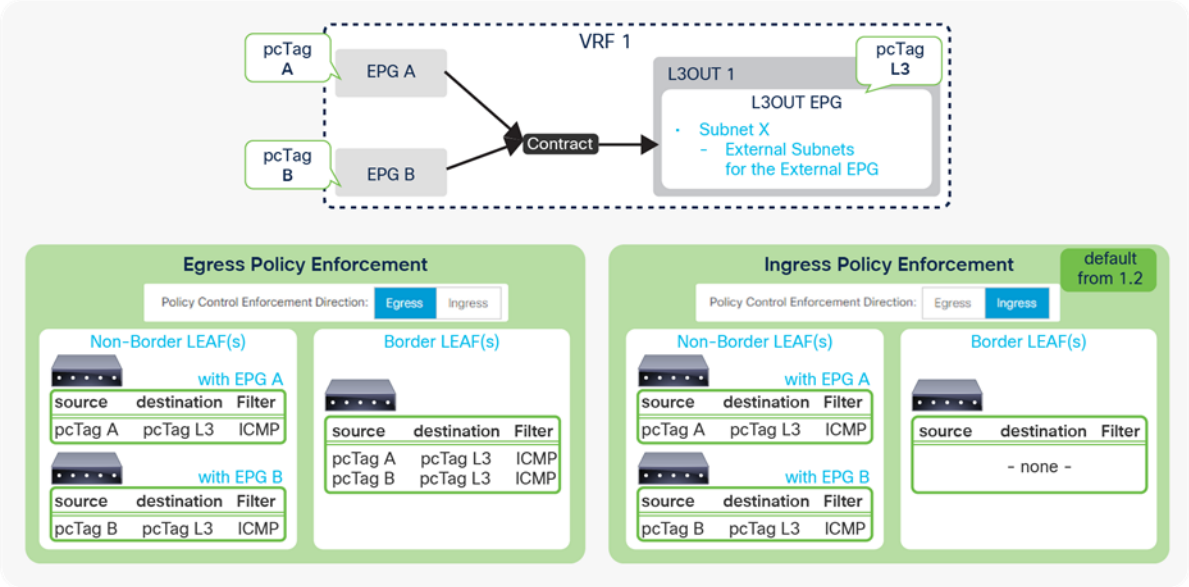

Figure 84.

정책 제어 적용 방향 및 Contract

정책 제어 적용 방향이 "**송신**"으로 설정되어 있으면(Figure 84 의 좌측 하단 참조) L3Out 에 대한 Contract 규칙이 보더 리프 및 비 보더 리프 스위치에 모두 배포됩니다. 이러한 상황에서 L3Out 과 통신해야 하는 EPG 가 많으면 보더 리프 스위치의 Contract 에 대한 TCAM 리소스가 병목 상태를 일으킬 수 있는데, 그 이유는 비 보더 리프 스위치의 Contract 가 대개 다수의 리프 스위치로 배포되는 반면 보더 리프는 모든 Contract 를 배포하기 때문입니다. 그러나 "**수신**"으로 설정하면 Contract 규칙이 비 보더 리프 스위치에만 배포되므로 보더 리프 스위치의 Contract 에 대한 TCAM 리소스와 관련된 문제가 해결됩니다.

즉 이 기능이 "**수신**"으로 설정되어 있을 때는 L3Out 에서 송/수신되는 패킷에 대한 Contract 가 항상 비 보더 리프에 적용됩니다. Figure 85 에는 각 시나리오에서 Contract 가 적용되는 방식과 상황이 자세히 나와 있습니다.

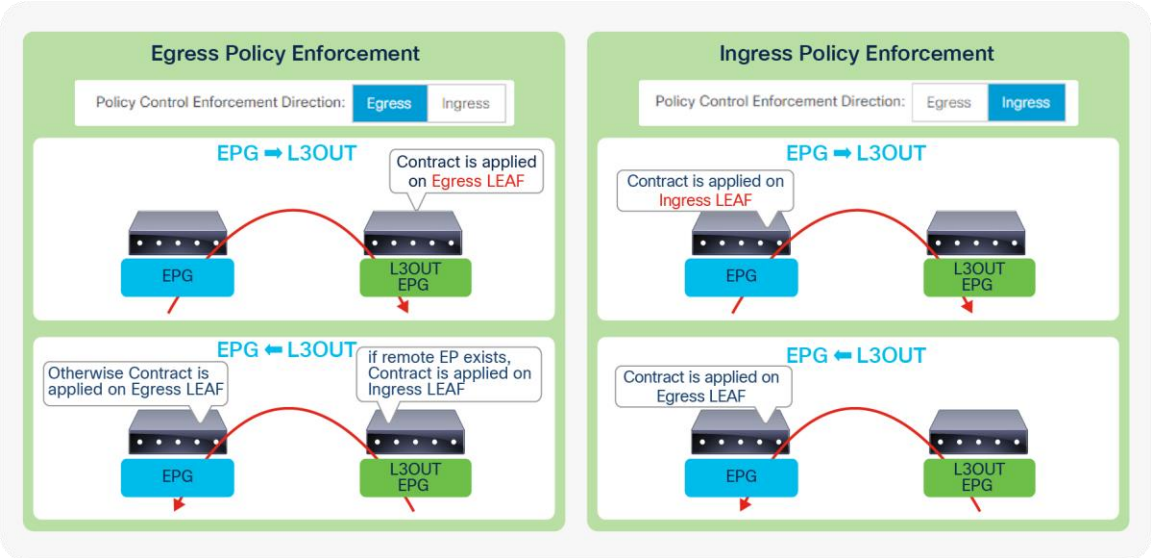

Figure 85.
정책 제어 적용 방향 및 패킷 플로

먼저 일반 EPG 에서 L3Out 으로 송신되는 패킷을 집중적으로 설명하겠습니다(Figure 85 상단의 두 도표 참조). 이 플로에서 비 보더 리프는 수신 리프이고, 보더 리프는 송신 리프입니다. 이 기능의 "**송신**" 옵션을 통해 이 플로에 대한 Contract 가 보더 리프에 항상 적용됩니다(송신 리프). "**수신**" 옵션을 통해서는 이 플로에 대한 Contract 가 비보더 리프에 항상 적용됩니다(수신 리프).

반대 방향의 트래픽 플로(L3Out 에서 일반 EPG 로)의 경우, 대상이 일반적인 엔드포인트이므로 Contract 가 수신 리프(이 경우 보더 리프) 또는 송신 리프(이 경우 비 보더 리프) 중 어느 리프에 적용되는지는 이 기능이 "**송신**"으로 설정되어 있을 때 수신(보더) 리프에서 원격 엔드포인트의 학습에 따라 달라집니다. 원격 엔드포인트가 수신 리프에서 학습되면 수신 리프는 원본(L3Out)과 대상(EPG) pcTag 를 둘 다 인식해 Contract 를 적용합니다. 따라서 수신 리프가 Contract 를 적용할 수 있으며, 그렇지 않으면 송신(비 보더) 리프에 Contract 가 적용됩니다. 그러나 "**수신**" 모드에서는 수신 리프에 적용할 Contract 규칙이 없기 때문에 항상 송신 리프에 적용됩니다.

L3Out 전송 라우팅

전송 라우팅은 APIC Release 1.1(1)에서 도입되었습니다. 외부 라우팅 도메인 간에 학습된 외부 경로를 보급함으로써 ACI 패브릭이 전송 네트워크가 될 수 있도록 허용하는 기능입니다. 이 기능 이전에 ACI 패브릭은 스텁 네트워크의 역할만 수행했습니다. L3Out EPG 서브넷의 "경로 제어 서브넷 내보내기" 범위는 이 기능을 위해 도입되었으며, **"Tenant > Networking > External Routed Networks > L3Out > Networks > L3Out EPG > Subnets"**에 위치합니다.

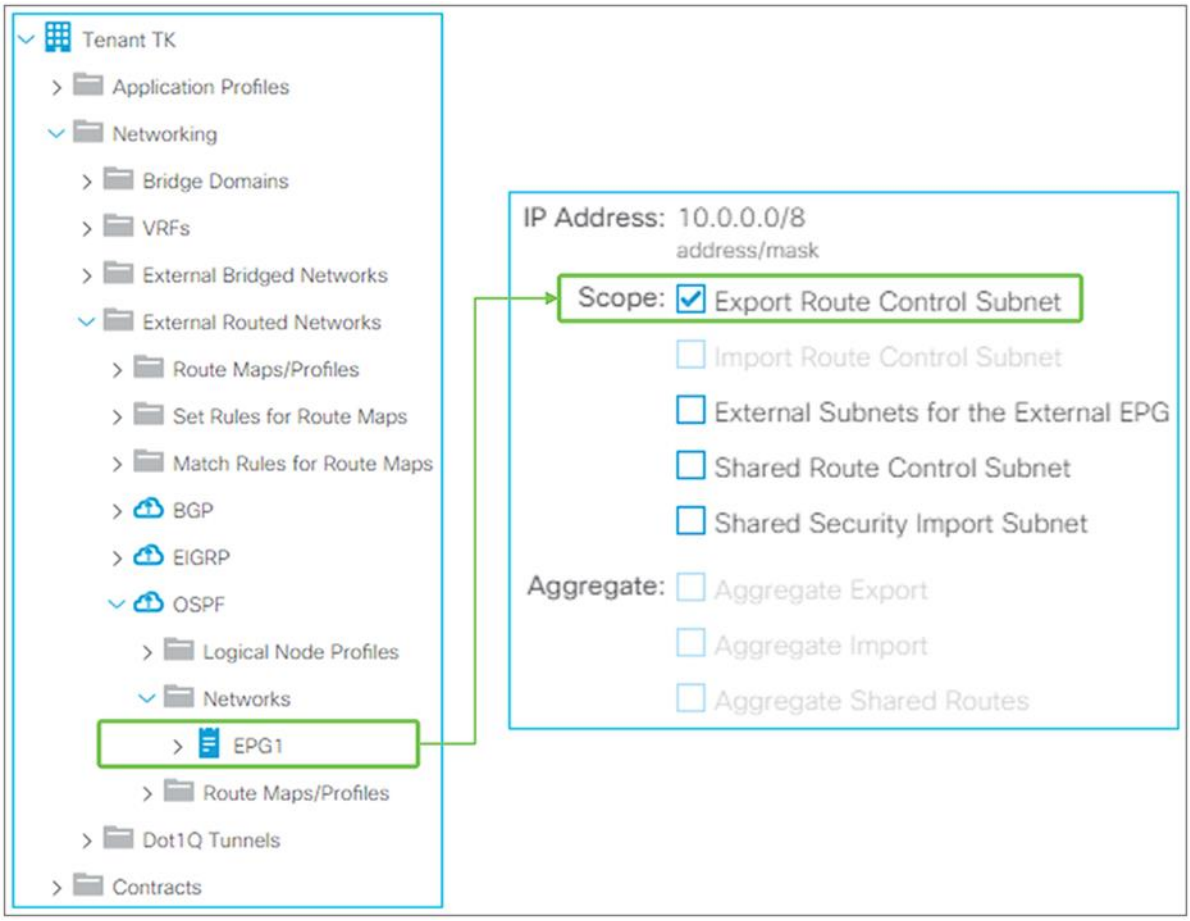

Figure 86.
GUI(APIC Release 3.2) 내 전송 라우팅

참고:

ACI 가 보급하는 외부 경로뿐만 아니라 ACI 가 학습할 수 있는 외부 경로에 대해서도 제어를 제공하기 위해 L3Out EPG 의 "경로 제어 서브넷 가져오기" 범위가 전송 라우팅의 일환으로 도입되었습니다. 그러나 대부분의 경우에는 ACI 가 모든 외부 경로를 학습하는 기본 가져오기 동작으로도 충분하기 때문에 "경로 제어 서브넷 가져오기" 범위는 자주 사용되지 않습니다.

참고:

전송 라우팅에서 지원되는 라우팅 프로토콜 조합을 자세히 알아보려면 Cisco APIC 계층 3 구성 가이드의 "전송 라우팅" 섹션에서 **지원되는 전송 조합 행렬**을 참조하시기 바랍니다.

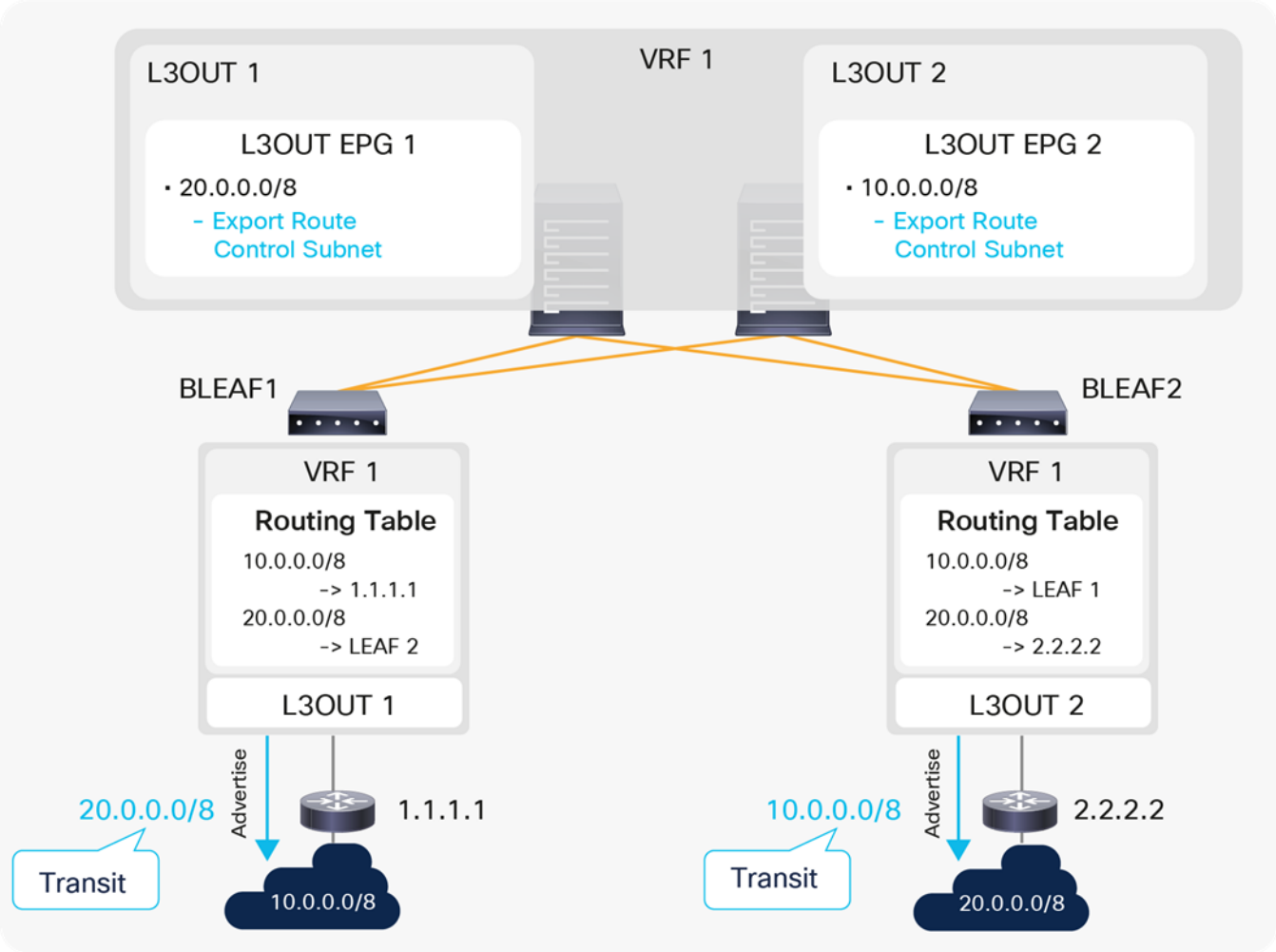

Figure 87.
전송 라우팅 도표에 대한 간단한 예시

Figure 87 은 Contract 가 없는 전송 라우팅에 대한 간단한 예시입니다. Figure 87 에서는 "경로 제어 서브넷 내보내기" 범위가 L3Out 간에 경로를 보급하는 데 사용된다는 점이 설명되어 있습니다. "경로 제어 서브넷 내보내기" 범위는 경로를 학습하는 L3Out 이 아닌 경로를 보급해야 하는 L3Out 에서만 사용되는 점에 유의해야 합니다.

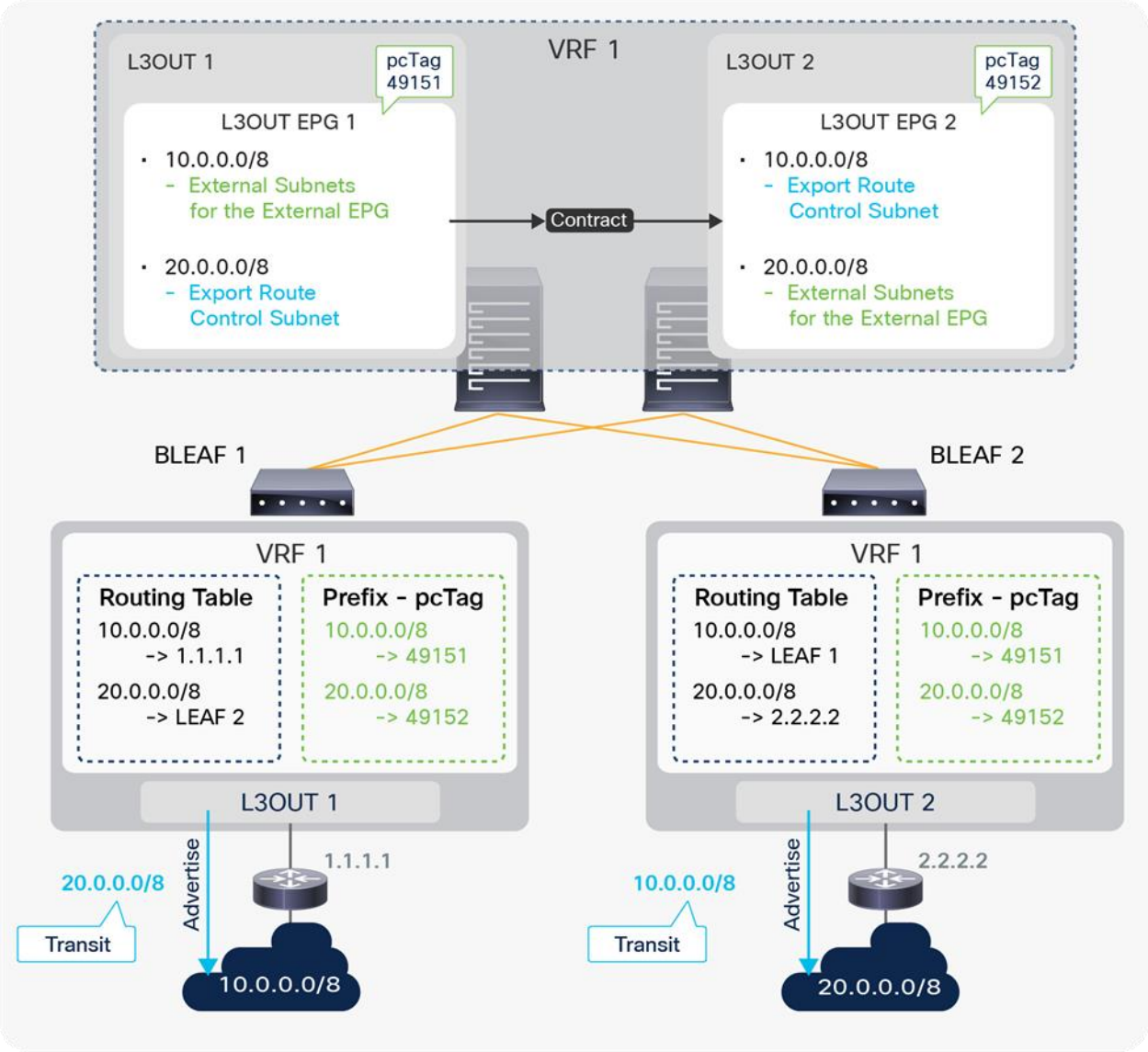

Figure 88.
전송 라우팅의 예시

Figure 88 은 Figure 87 의 전송 라우팅 예시와 동일하며, 여기에는 트래픽 필터링에 대한 Contract 부분이 포함됩니다. L3Out 1 과 2 는 두 개의 서로 다른 보더 리프 스위치의 동일한 VRF 에 존재합니다. ACI 패브릭은 L3Out 1 에서 경로 10.0.0.0/8 을 학습하며 L3Out 2 에서는 경로 20.0.0.0/8 을 학습합니다. 이 경우 10.0.0.0/8 과 20.0.0.0/8 의 장치가 ACI L3Out 1 과 2 를 통해 서로 통신할 수 있어야 합니다. 이를 위해 필요한 두 가지 구성이 있는데, 다른 L3Out 시나리오와 마찬가지로 라우팅과 Contract 입니다. 전송 라우팅에서 라우팅을 완수하기 위해 ACI 는 "경로 제어 서브넷 내보내기" 범위를 사용합니다. 여기서 L3Out 1 은 20.0.0.0/8 을 피어에 보급해야 하므로 "경로 제어 서브넷 내보내기" 범위가 포함된 20.0.0.0/8 이 L3Out 1 에서 구성됩니다. 인프라 MP-BGP 로 인해 20.0.0.0/8 이 보더 리프 1 에서 이미 사용 가능한 경우에는 L3Out 1 라우팅 프로토콜로 재배포되고 L3Out 1 을 통해 보급됩니다. 흔히 하는 실수로, 경로의 보급 출처가 되어야 하는 L3Out 1 이 아닌 20.0.0.0/8 을 학습 중인 L3Out 2 에서 "경로 제어 서브넷 내보내기" 범위를 사용해 20.0.0.0/8 을 구성하는 경우가 있습니다. 이는

L3Out 2 에서 "경로 제어 서브넷 내보내기" 범위가 포함된 10.0.0.0/8 에도 적용됩니다. L3Out 2 에서 구성되고, 해당 경로가 보더 리프 2 에서 사용 가능하다면 L3Out 2 는 10.0.0.0/8 을 외부로 보급하기 시작합니다. Contract 구성은 전송 라우팅에만 적용되는 것이 아닙니다.

EPG-to-L3Out 통신에서의 원칙도 여기에 적용됩니다. 사용자는 서브넷이 각 L3Out EPG(pcTag)로 매핑할 수 있도록 "외부 EPG 에 대한 외부 서브넷" 범위로 L3Out 1 과 2 를 구성합니다. 이 두 개의 L3Out EPG(pcTag) 간에 Contract 가 적용됩니다.

주의:

"L3Out 의 기본 구성 요소" 섹션의 4 단계에서 언급된 바와 같이 L3Out 의 동일한 서브넷에서 "경로 제어 서브넷 내보내기" 범위와 "외부 EPG 에 대한 외부 서브넷" 범위를 구성하는 것은 OSPF 영역 간 경로 요약을 제외하고 잘못된 구성으로, 이로 인해 라우팅 루프가 발생할 수 있습니다. "외부 EPG 에 대한 외부 서브넷" 범위는 해당 서브넷이 이 L3Out 뒤의 라우팅 도메인에 속한다는 점을 나타냅니다. 그러나 ACI 는 서브넷을 L3Out 으로 다시 보급(내보내기)하려고 시도하고 있습니다. 이러한 보급은 각 라우팅 프로토콜에서 라우팅 루프 방지 메커니즘을 통해 절대적으로 차단되지만 보급이 발생할 수도 있으므로 이러한 구성은 피해야 합니다.

"경로 제어 서브넷 내보내기" 범위와 "집계 내보내기" 옵션을 사용해 모든 서브넷을 내보내는 경우, 내보내는 서브넷은 불가피하게 자체 서브넷을 포함하게 됩니다. 따라서 이러한 구성을 수행할 때는 재배포를 위해 다른 라우팅 장치를 다룰 때와 같이 특별히 주의해야 합니다.

전송 라우팅 토폴로지

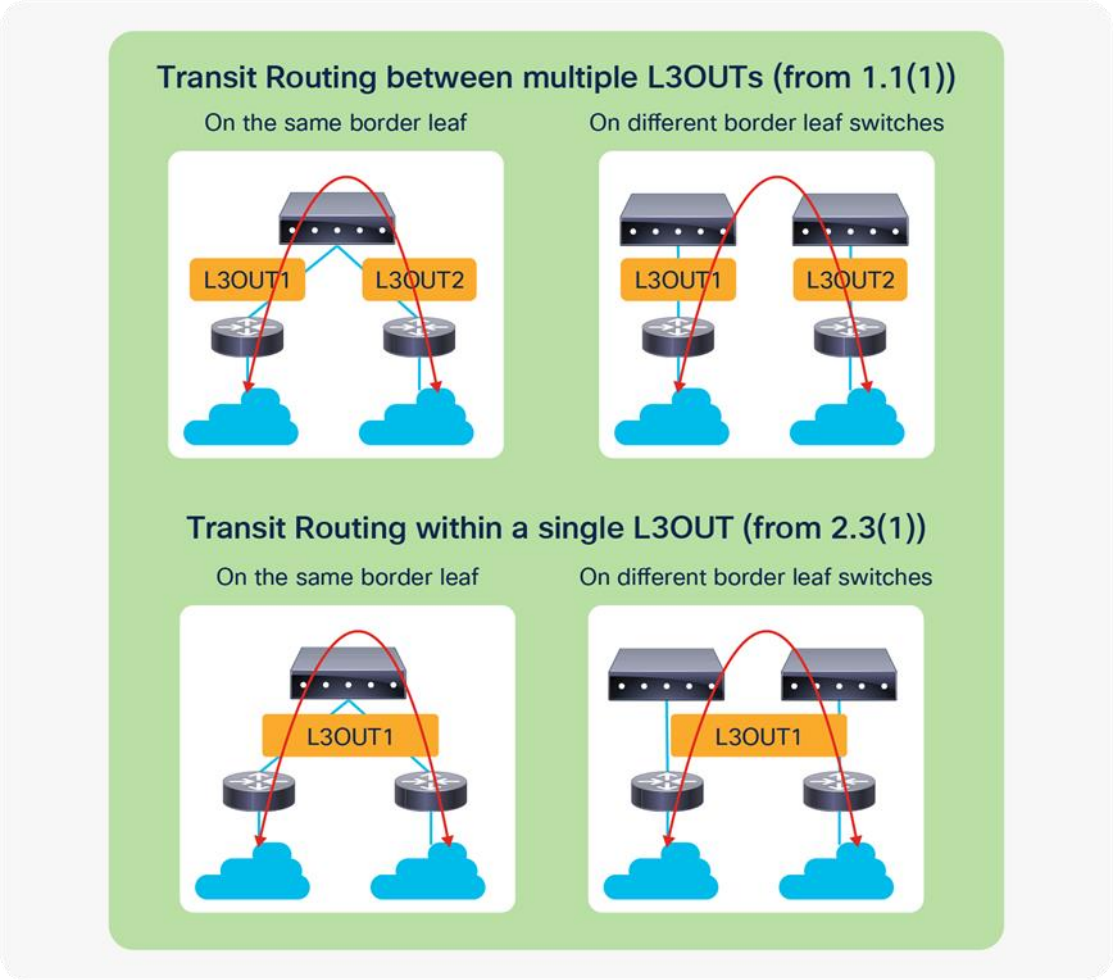

Figure 89.
전송 라우팅의 유형

Figure 89 에는 전송 라우팅의 4 가지 주요 토폴로지가 나와있습니다. 다수의 L3Out 이 포함된 상단의 두 가지는 원본 전송 라우팅 토폴로지입니다. 다수의 라우팅 장치(하단의 두 가지) 간 한 개의 L3Out 내 전송 라우팅은 APIC Release 2.3(1)에서 도입되었으나, "외부 EPG 에 대한 외부 서브넷" 범위가 포함된 0.0.0.0/0 에 대한 Contract 에 제한이 있습니다. 0.0.0.0/0 에 따른 제한 사항을 자세히 알아보려면 Cisco APIC 계층 3 네트워크 구성 가이드의 "전송 라우팅" 섹션에서 **전송 라우팅 지침** 또는 CSCuy16355 를 참조하시기 바랍니다.

참고:

두 개의 OSPF L3Out 에 걸쳐 동일한 보더 리프에서 전송 라우팅이 수행될 때, 인프라 MP-BGP 를 거치지 않고 OSPF 영역 간 경로 교환이 이루어지게 되므로 그중 한 개는 OSPF 영역이 0 이어야 합니다.

VRF 태그 및 전송 라우팅

VRF 태그는 전송 라우팅과 함께 잠재적인 라우팅 루프를 방지하기 위한 메커니즘으로서 도입되었습니다. 이 기능은 OSPF 또는 EIGRP 경로 태깅을 활용하므로 BGP 가 아닌 주로 두 개의 프로토콜을 위한 사항입니다.

ACI 에서는 VRF 마다 자체 VRF 태그가 있으며, 모든 VRF 에 대해 VRF 태그의 기본값은 4294967295 로 동일합니다. ACI 는 L3Out 을 통해 보급하는 서브넷에서 VRF 태그를 설정합니다. 여기에는 BD 서브넷과 전송 경로가 모두 포함됩니다. 전송 라우팅을 수행할 때 보더 리프의 OSPF 또는 EIGRP 는 재배포(또는 OSPF 영역 필터)를 사용해 다른 L3Out 에서 외부 경로를 수신합니다. 이때 ACI 는 VRF 태그를 재배포된 경로에 경로 태그로 설정합니다. ACI 가 자체 VRF 태그를 보유한 외부 경로를 인식할 경우, 루프를 방지하기 위해 라우팅 테이블에서 해당 경로를 사용하지 않습니다.

해당 경로를 사용하지 않는 이 동작은 NX-OS 의 테이블 맵 기능으로 구현된 것으로, OSPF 와 EIGRP 에 대한 "경로 제어 서브넷 가져오기" 범위에도 사용됩니다. 따라서 VRF 태그와 "경로 제어 서브넷 가져오기" 범위는 테이블 맵에서 동일한 경로 맵을 공유합니다.

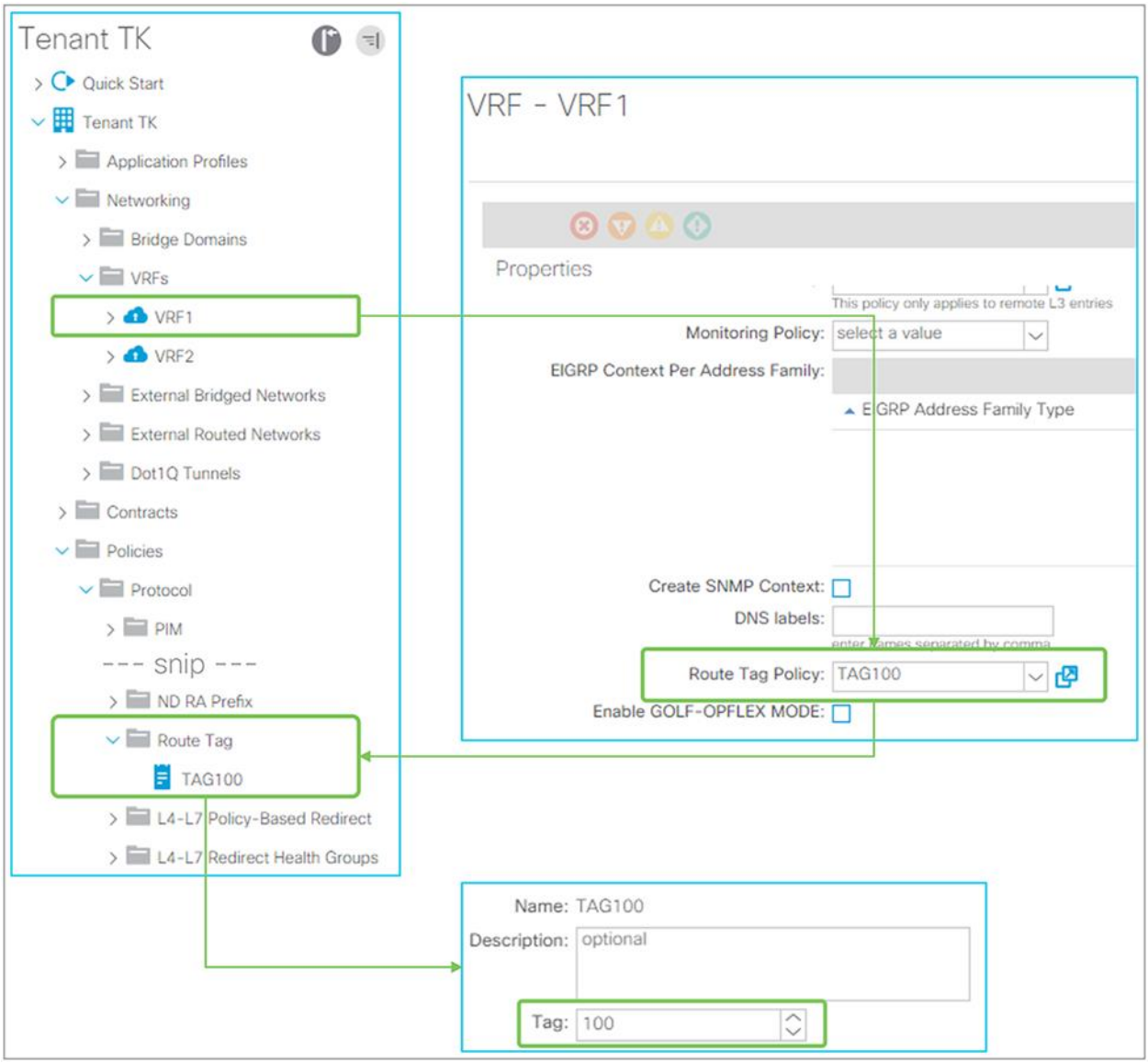

Figure 90.

GUI(APIC Release 3.2) 내 VRF 태그

Figure 90 에는 VRF 1 에 대한 VRF 태그를 변경하는 방법이 설명되어 있습니다. 경로 태그 정책은 **"Tenant > Policies > Protocol > Route Tag"**에 위치합니다. 이 정책은 기본값에서 VRF 태그를 변경해야 하는 각 VRF 에서 구성됩니다. 이 예시에서 VRF 1 의 VRF 태그는 100 으로 변경되었습니다. 다른 VRF 에서 ACI 로 다시 변경하여 전송 경로가 학습되어야 하는 경우에는 VRF 태그가 기본값에서 변경되어야 합니다. 그렇지 않으면 모든 VRF 가 기본적으로 동일한 기본 VRF 태그를 사용하기 때문에 경로가 라우팅 테이블에 표시되지 않습니다. Figure 91 의 예시에 이러한 문제가 나와있습니다.

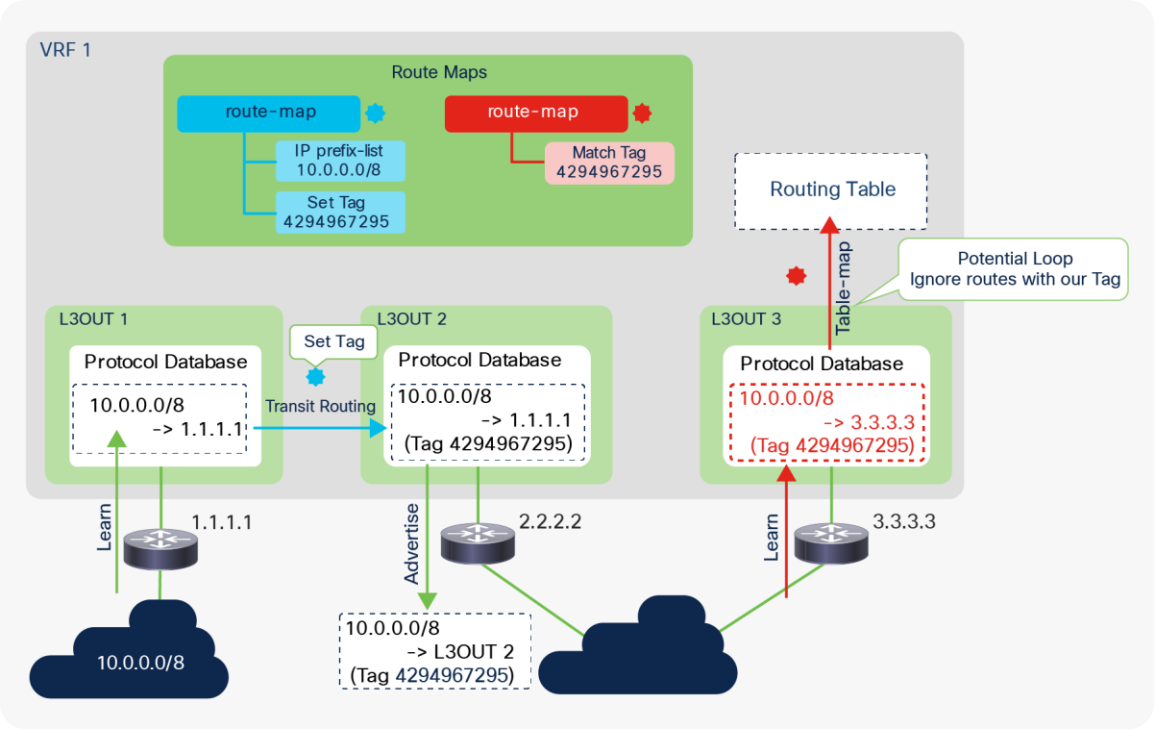

Figure 91.

전송 라우팅에서 VRF 태그를 사용해 루프 방지

Figure 91 은 ACI 가 VRF 태그를 사용하여 루프를 방지하는 방법에 관한 예시입니다. 이 예시에서 전송 라우팅은 L3Out 1 에서 학습된 경로 10.0.0.0/8 에 대해 L3Out 2 에서 구성됩니다. ACI 는 L3Out 2 가 L3Out 1 에서 경로를 수신할 때 10.0.0.0/8 에 VRF 태그를 설정합니다. 이 태그는 표준 경로 태그이므로 외부 라우터를 통해 전송됩니다. 어떤 이유로 이 경로가 ACI 로 다시 보급될 경우, ACI 는 경로 태그로 인한 루프의 발생 가능성을 인식합니다. OSPF 또는 EIGRP 의 테이블 맵 덕분에 이러한 잠재적 루프 경로는 라우팅 테이블에 표시되지 않습니다. 전송 라우팅이 구현되는 방식에 대한 자세한 내용은 다음에 나오는 "전송 라우팅에 대한 내부 경로 맵" 서브섹션을 참조하시기 바랍니다(Figure 91 의 L3Out 1 에서 L3Out 2 로).

전송 라우팅에 대한 내부 경로 맵

이 섹션에서는 "경로 제어 서브넷 내보내기" 범위가 구성되어 있을 때 보더 리프가 전송 라우팅 기능을 구현하는 방법을 자세히 설명합니다. ACI 는 경로 맵을 통한 재배포와 같이, 표준 라우팅 프로토콜 메커니즘을 활용합니다. 사용자가 ACI 패브릭을 실행하기 위해 이러한 수준의 지식을 갖추어야 하는 경우는 드물지만, 한계점을 목록으로 외우기보다는 ACI L3Out 과 전송 라우팅의 한계점을 이해하는 것이 더 유용합니다.

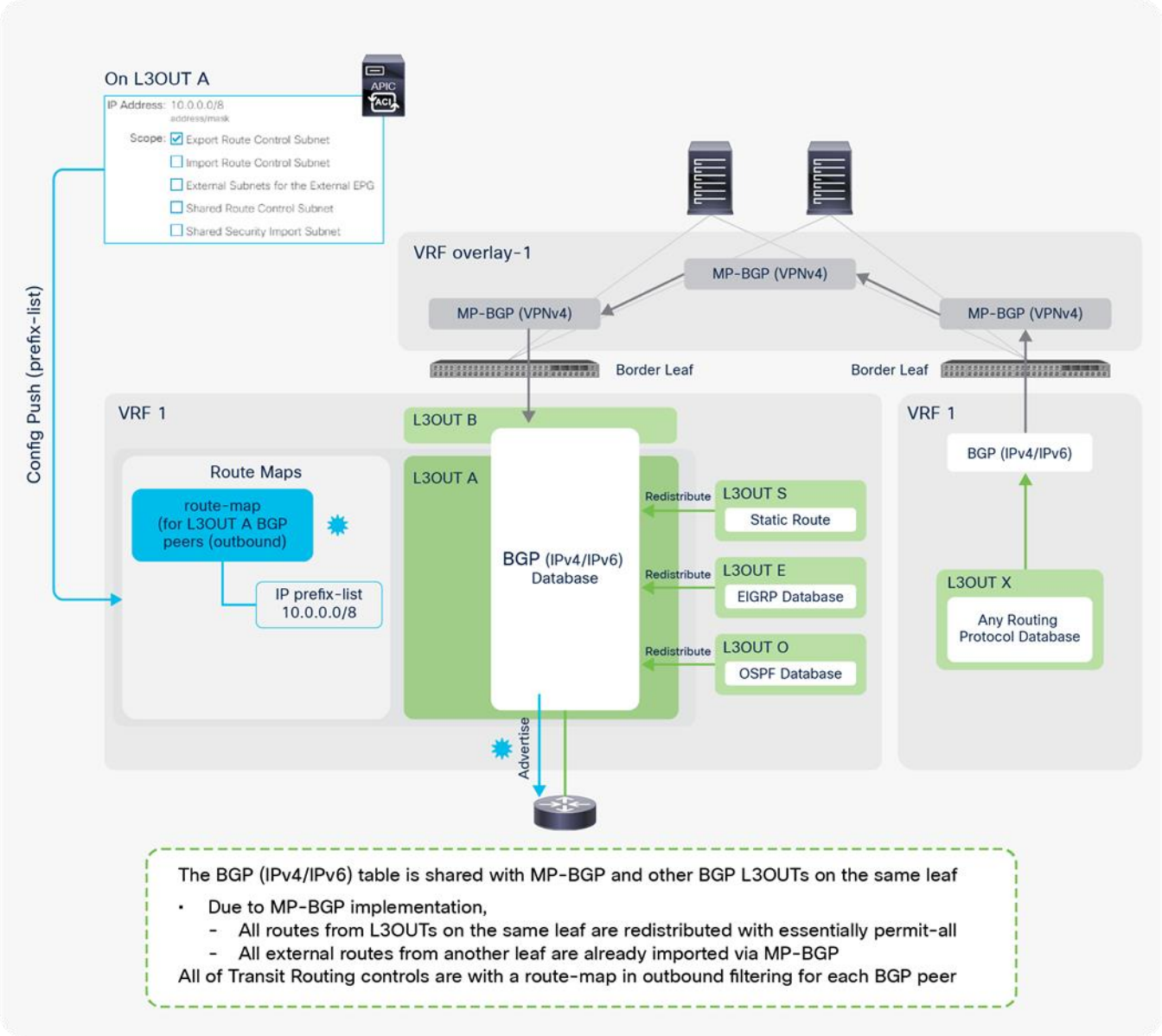

Figure 92.

BGP 가 포함된 전송 라우팅에 대한 경로 맵 구현

Figure 92 에서는 전송 라우팅과 관련된 L3Out 의 모든 조합이 설명되어 있습니다. 여기서는 BGP L3Out A 를 통한 경로 보급을 중점으로 설명하는데, 다른 모든 L3Out 이 동시에 배포되어야 한다는 의미는 아닙니다.

BGP L3Out 의 구현은 OSPF, EIGRP 등 다른 L3Out 과는 다소 다른데, 그 이유는 사용자 VRF 의 BGP 가 인프라 MP-BGP 와 사용자 L3Out 에 활용되기 때문입니다. 인프라 MP-BGP 의 구현으로 인해 사용자 VRF 의 BGP IPv4 및 IPv6 데이터베이스에는 전송 라우팅 구성 없이도 동일한 보더 리프와 다른 보더 리프 스위치의 다른 L3Out 에서 수신된 모든 외부 경로가 있습니다. 따라서 BGP L3Out 을 통한 전송 라우팅 제어는 보더 리프의 BGP 피어 인접 라우터 세션에 적용되는 아웃바운드 경로 맵을 통해 수행됩니다. ACI 는 기본값으로 각 BGP L3Out 마다 한 개의 아웃바운드 경로 맵을 생성하며, 이 경로 맵은 동일한 L3Out 의 모든 BGP 피어에 적용됩니다. 이는 새로운 기능으로 변경하여 각 피어별로 BGP 경로 맵을 구성할 수 있는데, 이는 APIC Release 4.2(1)에서 도입되었습니다.

참고:

BGP 에 대한 아웃바운드 경로 맵은 BD 서브넷 보급을 통해 공유됩니다. BGP 및 BD 서브넷 보급을 위한 전송 라우팅을 적합한 서브넷으로 구성하여 예기치 않은 보급을 방지하는 것이 중요합니다. 자세한 내용은 "BD 서브넷 보급" 섹션을 참조하시기 바랍니다.

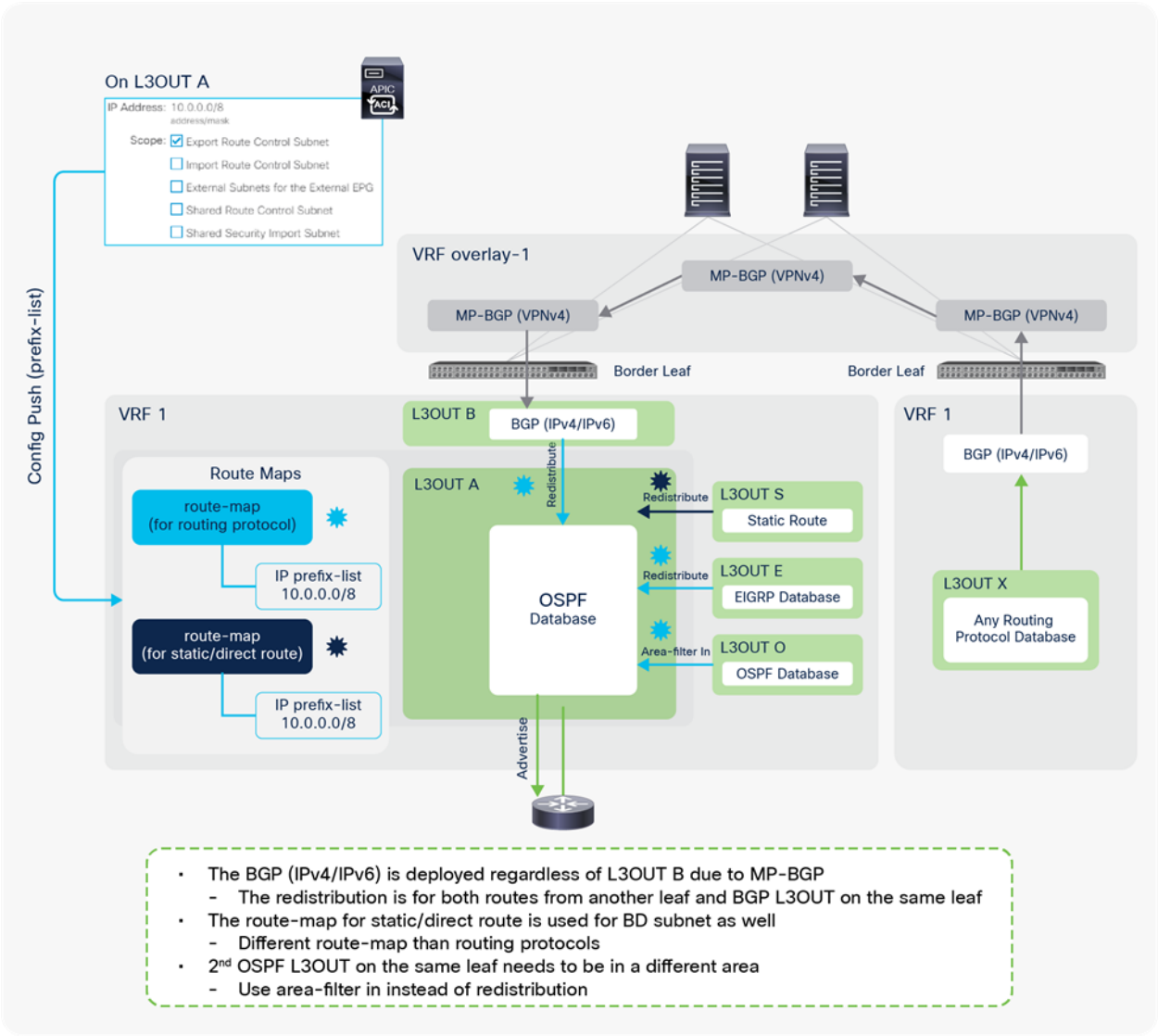

Figure 93.
OSPF 를 통한 전송 라우팅에 대한 경로 맵 구현

Figure 93 에서는 전송 라우팅과 관련된 L3Out 의 모든 조합이 설명되어 있습니다. 여기서는 OSPF L3Out A 를 통한 경로 보급을 중점적으로 설명하는데, 다른 모든 L3Out 이 동시에 배포되어야 한다는 의미는 아닙니다.

전송 라우팅에 대한 OSPF L3Out 구현은 주로 재배포를 이용합니다. Figure 93 에서 다른 보더 리프의 외부 경로는 인프라 MP-BGP 로 인해 BGP IPv4 및 IPv6 테이블에서 제공되어야 합니다. 이 BGP 테이블은 BGP L3Out B 에서도 사용됩니다. BGP 테이블이 이들 경로는 라우팅 테이블에서 사용될 수 있지만 OSPF 데이터베이스(LSDB: 연결 상태 데이터베이스)에서는 불가능합니다. OSPF 가 전송 라우팅을 위해 외부로 보급할 수 있도록 지원하기 위해 ACI 는 BGP 에서 OSPF 로 "경로 제어 서브넷 내보내기" 범위를 사용해 이러한 경로를 재배포합니다. 동일한 보더 리프에 있는 EIGRP 나 고정 경로 등 다른 L3Out 의 경우에도 재배포를 사용합니다. 그러나 동일한 보더 리프에 OSPF L3Out 이 하나 더 있는 경우에는 라우팅 프로토콜이 동일하기 때문에 재배포가 불가능해집니다. 이 경우 동일한 보더 리프에 있는 각 OSPF L3Out 이 각기 다른 OSPF 영역에 속해야 하므로, ACI 는 "내부" 방향을 통해 영역 필터를 사용합니다.

참고:

OSPF 와 EIGRP 에서 ACI 는 내부에서 두 개의 경로 맵을 생성하는데, 하나는 라우팅 프로토콜을 위한 것이고, 다른 하나는 고정 또는 직접 경로를 위한 것입니다. "경로 제어 서브넷 내보내기" 범위는 두 경로 맵에서 동일한 IP 식별 번호 목록 항목을 배포합니다.

BD 서브넷은 고정 및 직접 경로이기도 하므로, 고정/직접 경로에 대한 경로 맵은 BD 서브넷 보급과 공유됩니다. 의도한 서브넷만 보급되도록 전송 라우팅과 BD 서브넷 보급이 적합한 서브넷으로 구성되었는지 확인하는 것이 중요합니다. 자세한 내용은 "BD 서브넷 보급" 섹션을 참조하시기 바랍니다.

또한 두 경로 맵은 동일한 보더 리프에서 동일한 VRF 의 모든 OSPF 및 EIGRP L3Out 과 공유됩니다.

OSPF 와 EIGRP 간 공유된 경로 맵의 주소를 지정할 수 있도록 개선해달라는 사용자의 요청이 있었습니다.

CSCuy63998 ACI: EIGRP 의 서브넷 내보내기가 동일한 노드에서 OSPF 에 적용됩니다.

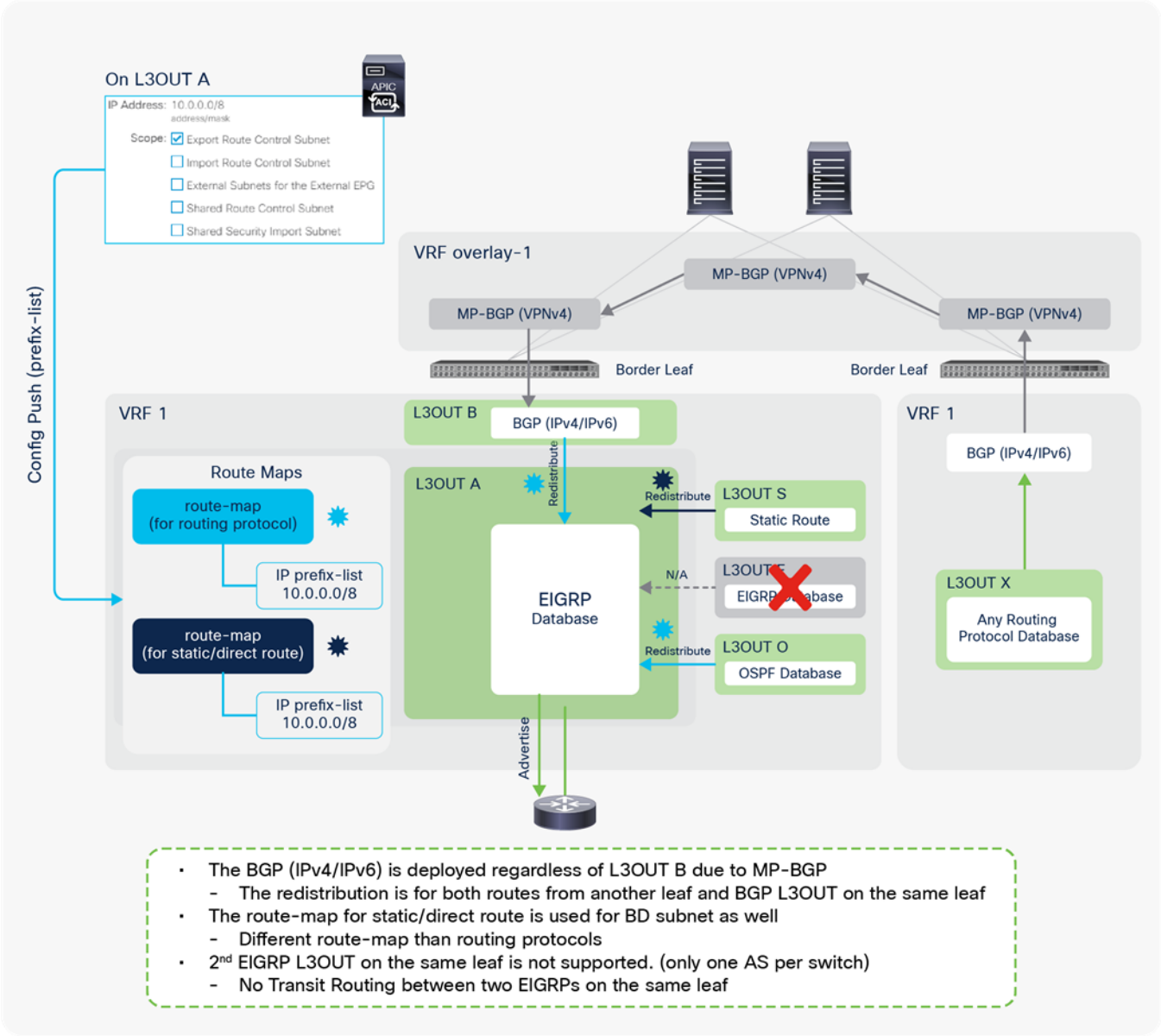

Figure 94.

EIGRP 를 통한 전송 라우팅에 대한 경로 맵 구현

Figure 94 에서는 전송 라우팅과 관련된 L3Out 의 모든 조합이 설명되어 있습니다. 여기서는 EIGRP L3Out A 를 통한 경로 보급을 중점으로 설명하는데, 다른 모든 L3Out 이 동시에 배포되어야 한다는 의미는 아닙니다.

전송 라우팅에 대한 EIGRP L3Out 구현은 OSPF 와 거의 동일하며, 동일한 보더 리프의 동일한 프로토콜을 사용하는 동일한 L3Out 간 전송 라우팅이 EIGRP 에서는 지원되지 않는다는 점만 다릅니다. 그 이유는 두 번째 EIGRP L3Out 이 동일한 보더 리프에서 구성될 수 없기 때문인데, EIGRP AS 번호가 각 L3Out 마다 적용되며 동일한 스위치 노드에 두 개의 EIGRP AS 가 존재할 수 없기 때문입니다. 내부적으로 생성되는 경로 맵 등 자세한 내용은 OSPF L3Out 구현과 동일합니다.

L3Out 경로 프로필 및 경로 맵

경로 프로필 및 경로 맵 기본 사항

ACI 는 이전 섹션에서 언급한 바와 같이 인프라 MP-BGP, 외부로 BD 서브넷 보급, 전송 라우팅 등 갖가지 목적으로 경로 맵을 내부적으로 사용합니다. ACI 는 사용자에게 이러한 내부 경로 맵에 대해 사용자 정의된 매칭을 추가하거나 규칙을 설정하는 기능을 제공합니다. 이는 일명 경로 제어 프로필 또는 경로 맵이라고 하는 경로 프로필을 사용해 수행됩니다. 다음은 이 기능에 대한 사용 사례 예시입니다.

- L3Out 을 통해 BD 서브넷을 외부로 재배포(내보내기)해야 하는 경로 맵
- L3Out 간 외부 경로를 재배포(내보내기)해야 하는 경로 맵(전송 라우팅)
- L3Out 을 통해 외부에서 외부 경로 학습(가져오기)을 제한하는 경로 맵
- 인프라 MP-BGP 등에 대해 L3Out 에서 BGP 로 외부 경로를 재배포(Interleak)하는 경로 맵

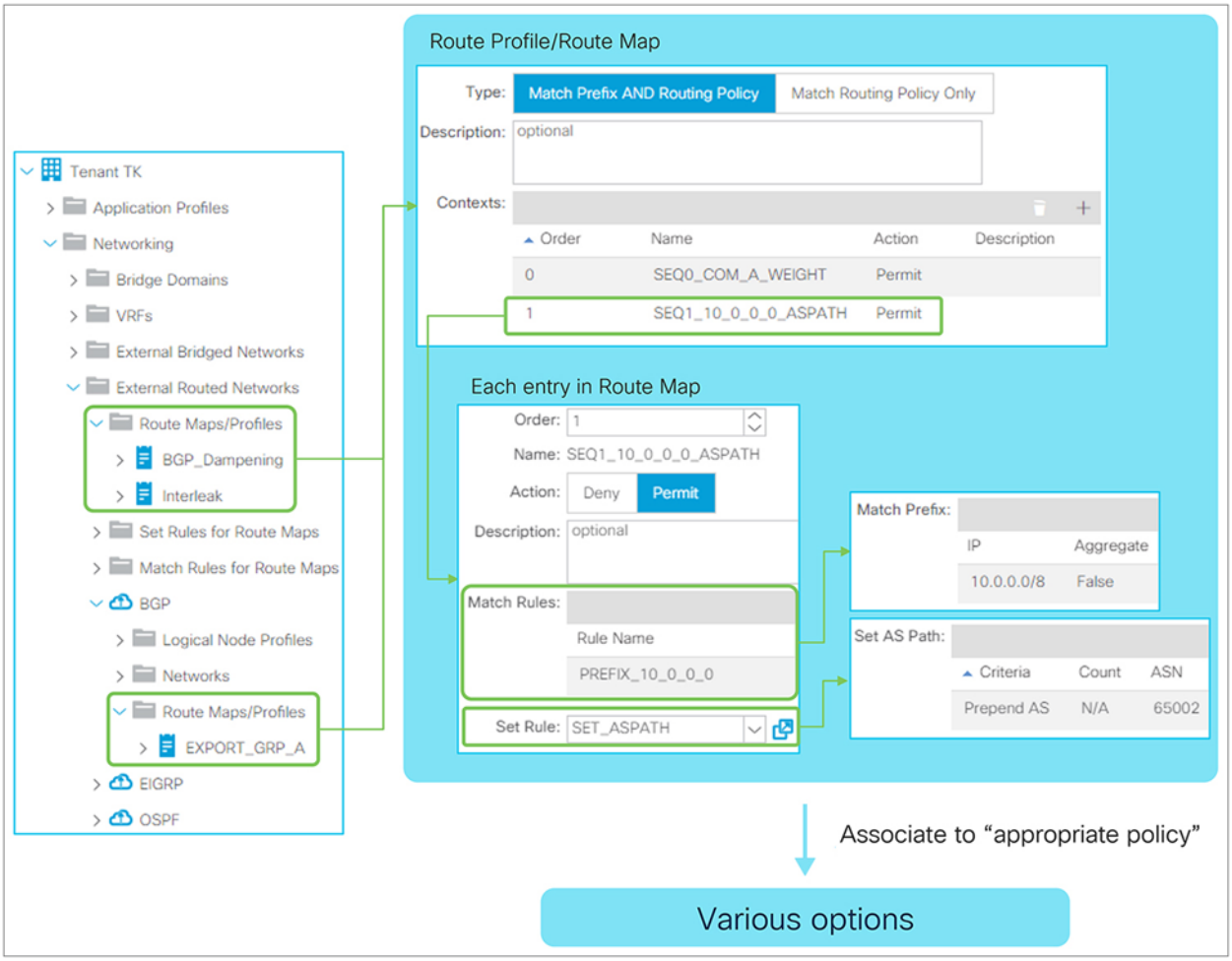

Figure 95.

GUI(APIC Release 3.2) 내 경로 프로필 구조

Figure 95 에서와 같이, 경로 프로필을 구성하는 곳은 두 군데입니다. 하나는 테넌트 수준으로, **"Tenant > External Routed Networks > Route Maps/Profiles"**에 위치하며 APIC Release 1.2(2)에서 도입되었습니다. 다른 하나는 L3Out 수준으로, **"Tenant > External Routed Networks > {L3Out} > Route Maps/Profiles"**에 위치합니다. 두 가지 모두 테넌트 수준으로 **"Tenant > External Routed Networks > Set Rules (or Match Rules) for Route Maps"**에 위치한 규칙 매칭 및/또는 설정을 사용합니다. 차이점은 다음과 같습니다.

- 테넌트 수준 경로 프로필: Interleak(OSPF 또는 EIGRP 에서 인프라 MP-BGP 로 재배포) 및 BGP 경로 댐프닝에 적용
- L3Out 수준 경로 프로필: 다른 모든 부분에 적용

Figure 96 에는 일반적인 라우터의 경로 맵에서 구성 요소를 나타내는 각 경로 프로필의 구성 요소가 나와있습니다. 이들 구성요소는 전송 라우팅 등 다른 APIC 정책을 구현하는 데 사용되는 경로 맵으로 병합됩니다.

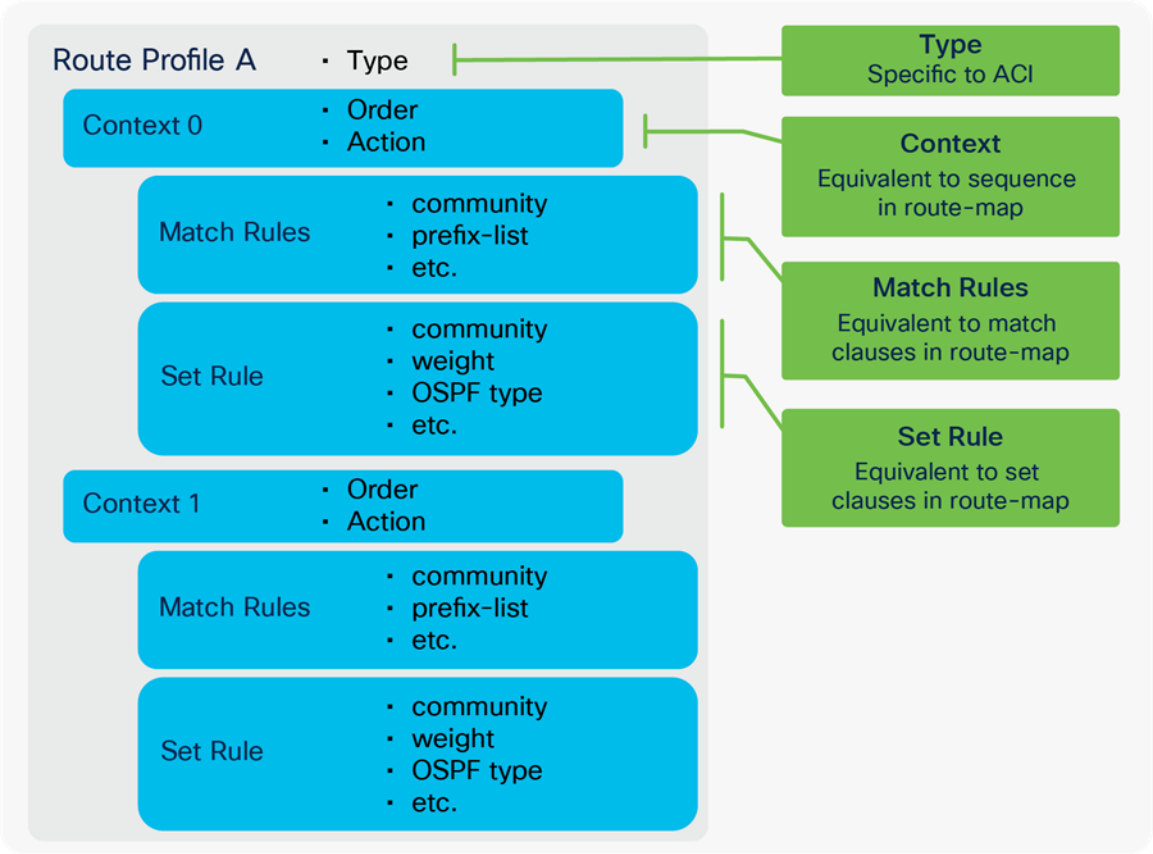

Figure 96.
경로 프로필 구성 요소

다음은 컨텍스트 정책의 두 가지 옵션에 대한 설명입니다.

- **순서:** 적용될 컨텍스트 정책의 순서를 결정합니다. 일반적인 경로 맵의 시퀀스 번호에 해당하지만 절대 경로 맵으로 병합되기 때문에 실제 시퀀스 번호는 이 순서 번호와 동일하지 않습니다.
- **작업:** 허용 또는 거부 작업은 APIC Release 2.3(1)에서 도입되었습니다. 이 옵션이 나오기 일부 이전 버전에서는 규칙 설정이 작업으로 표기되었습니다. 이는 일반적인 경로 맵의 허용 또는 거부에 해당합니다.

경로 프로필 유형

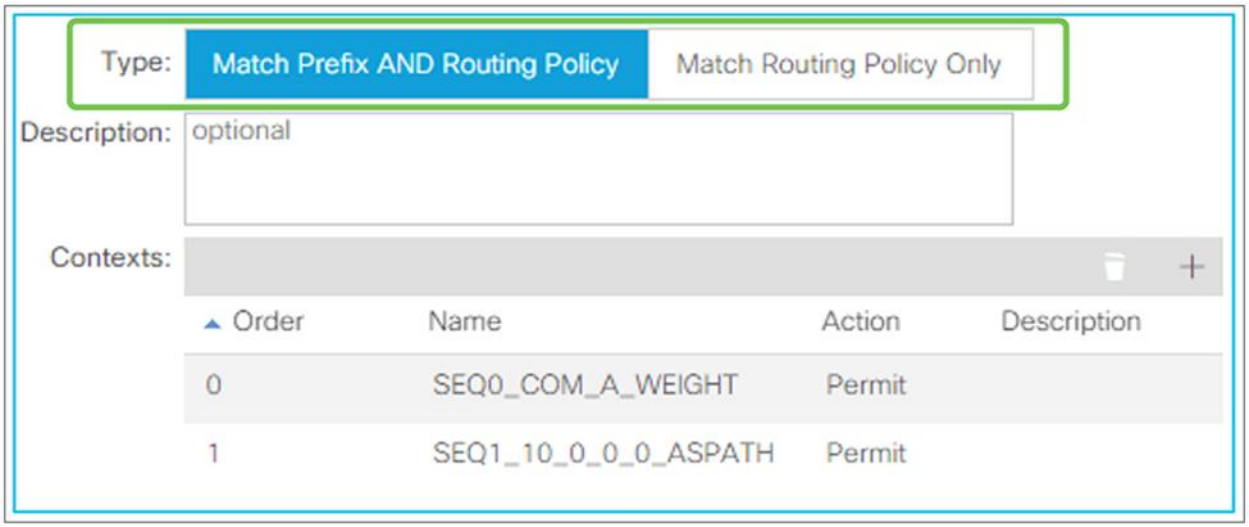

Figure 97.
GUI(APIC Release 3.2) 내 경로 프로필 유형

경로 프로필 유형은 APIC Release 1.2(2)에서 도입되었습니다. 1.2(2) 이전에는 모든 경로 프로필(경로 맵)이 "**식별 번호 AND 라우팅 정책 매치**"와 동일한 방식으로 작동했습니다.

경로 프로필이 L3Out EPG 나 L3Out 서브넷과 같은 구성 요소와 관련이 있을 때는 경로 프로필의 규칙 매치가 구성 요소에 대한 내부 경로 맵에 병합됩니다. 다른 구성 요소에서 내부적으로 생성된 경로 맵에 대한 자세한 예시는 기타 섹션("L3Out 전송 라우팅" 섹션 등)에서 확인할 수 있습니다. 경로 프로필 유형 옵션은 APIC 가 L3Out 서브넷에서 "경로 제어 서브넷 내보내기" 범위 등의 다른 APIC 정책에서 배포된 경로 맵으로 구성된 경로 프로필 규칙을 병합하는 방식을 정의합니다.

- **식별 번호 AND 라우팅 정책 매치**
  이 유형은 경로 프로필이 경로 프로필에서 구성된 매치 기준인 AND 와 연관되어 있는 구성 요소의 식별 번호를 결합합니다. 예를 들어 경로 프로필이 "경로 제어 서브넷 내보내기" 범위와 L3Out 서브넷 10.0.0.0/8 및 20.0.0.0/8 이 포함된 L3Out EPG 에 내보내기 방향으로 연관될 경우, 리프에서 각 내부 경로 맵 시퀀스의 매치 절에는 연관된 구성 요소(10.0.0.0/8 및 20.0.0.0/8) AND 와 경로 프로필 내 각 컨텍스트 정책의 식별 번호에 대한 매치 기준이 포함됩니다.

- **라우팅 정책만 매치**

  이 유형은 경로 프로필에서 구성된 매치 기준만 사용하며 경로 프로필이 연관된 구성 요소의 식별 번호는 무시합니다. 예를 들어 경로 프로필이 "경로 제어 서브넷 내보내기" 범위가 포함된 L3Out 서브넷 10.0.0.0/8 및 20.0.0.0/8 과 L3Out EPG 에 내보내기 방향으로 연결될 경우, APIC 는 10.0.0.0/8 과 20.0.0.0/8 을 무시하고 이에 대해 경로 프로필 내 컨텍스트 정책의 매치 기준만 사용해 새로운 경로 맵으로 내부 경로 맵 시퀀스를 덮어씁니다. BGP 경로 댐프닝 정책 등 서브넷 구성이 포함되지 않는 일부 구성 요소는 이 유형으로 구성해야 합니다.

Figure 98 에는 L3Out EPG 내 각 유형의 차이점이 설명되어 있습니다.

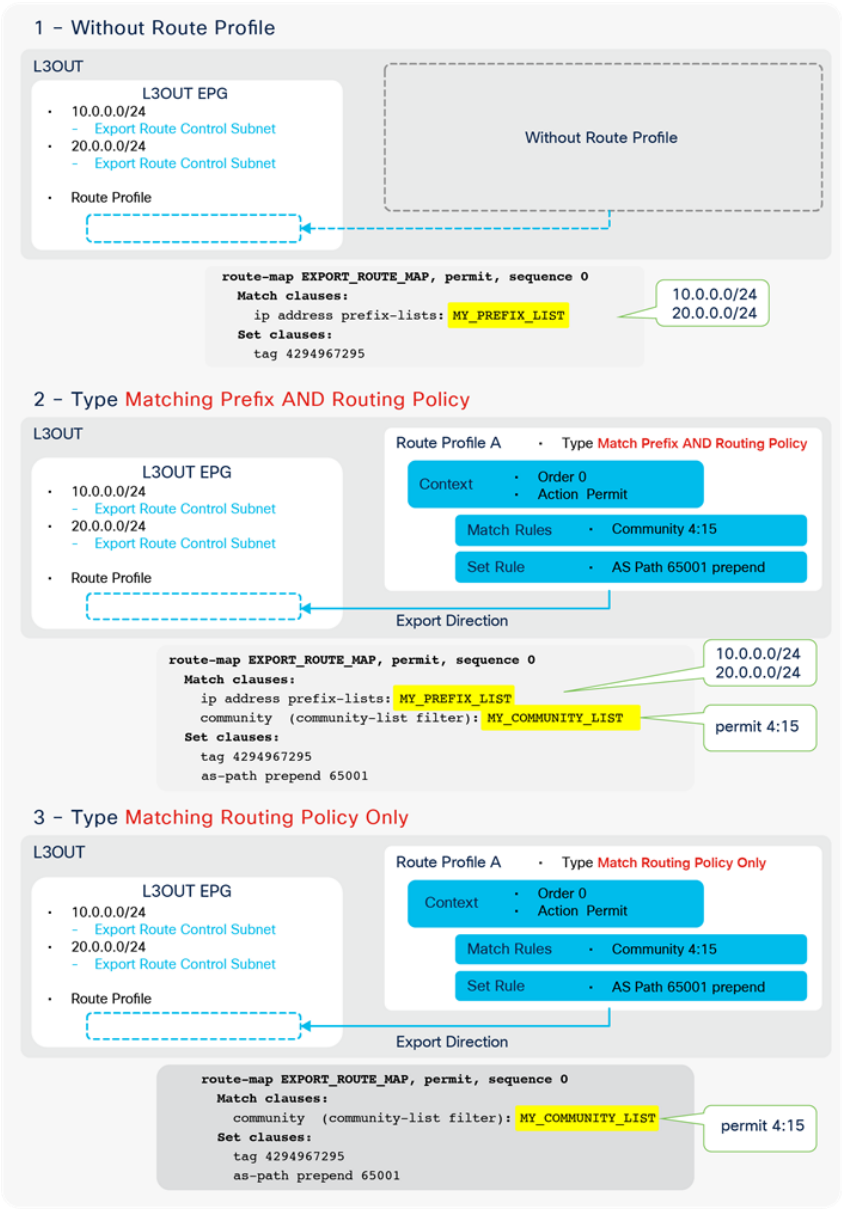

Figure 98.

경로 프로필 유형의 비교

Figure 98 에서와 같이 "라우팅 정책만 유형 매치"(시나리오 3)에서는 "**경로 제어 서브넷 내보내기**" 범위가 포함된 L3Out 서브넷을 완전히 무시합니다. 따라서 이 경우에는 "경로 제어 서브넷 내보내기" 범위가 포함된 L3Out 서브넷을 구성하는 의미가 없습니다. 사용되어야 하는 유형에 관한 자세한 지침은 다음 섹션의 경로 프로필 연결에 따른 각 시나리오에 제시되어 있습니다.

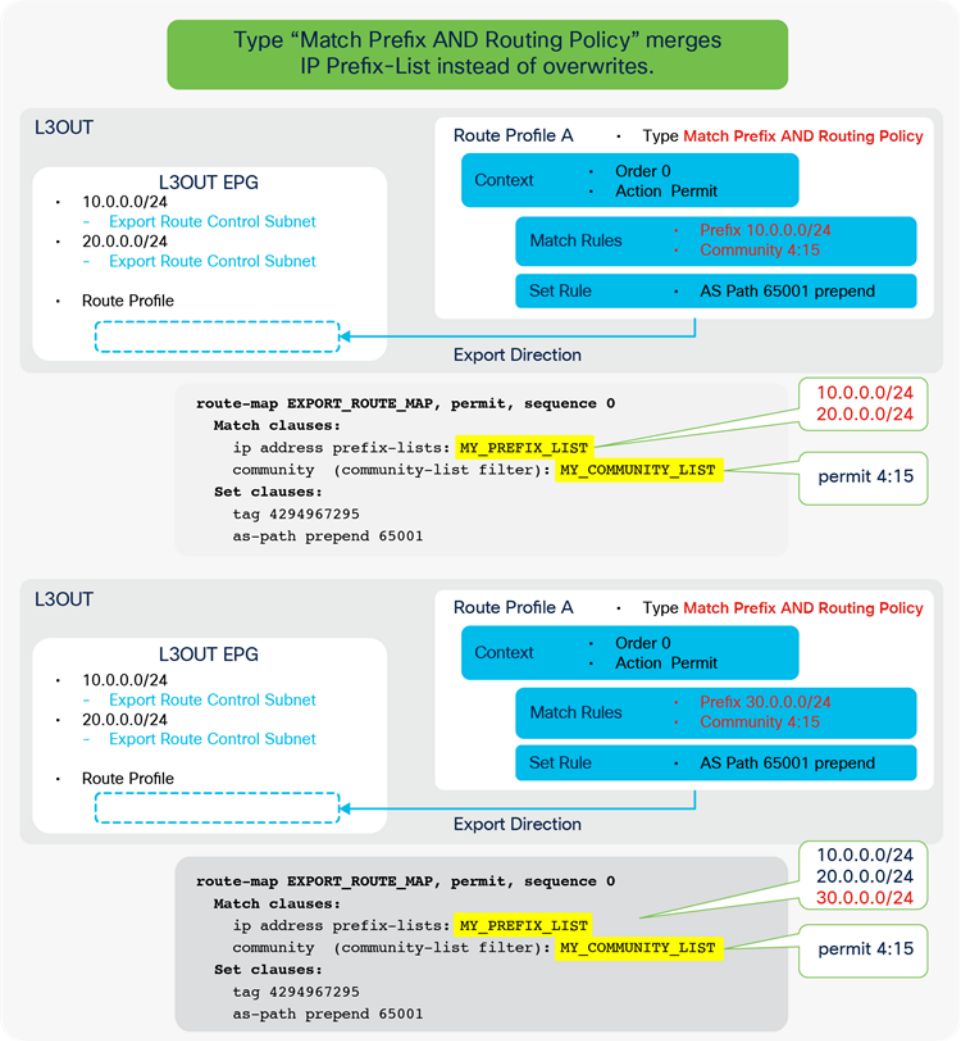

Figure 99.

명시적인 식별 번호 목록 및 매치 식별 번호 AND 라우팅 정책

Figure 99 는 명시적인 식별 번호 목록(매치 식별 번호 기준)과 함께 "매치 식별 번호 AND 라우팅 정책" 유형의 동작에 관한 설명입니다. 설명된 바와 같이 명시적인 식별 번호 목록에서 L3Out 서브넷과 식별 번호 간 "논리적 AND"를 덮어쓰거나 실행하지 않고 경로 맵이 두 객체의 식별 번호를 병합할 뿐입니다.

경로 프로필 매치 및 규칙 설정

경로 프로필 매치 규칙 옵션

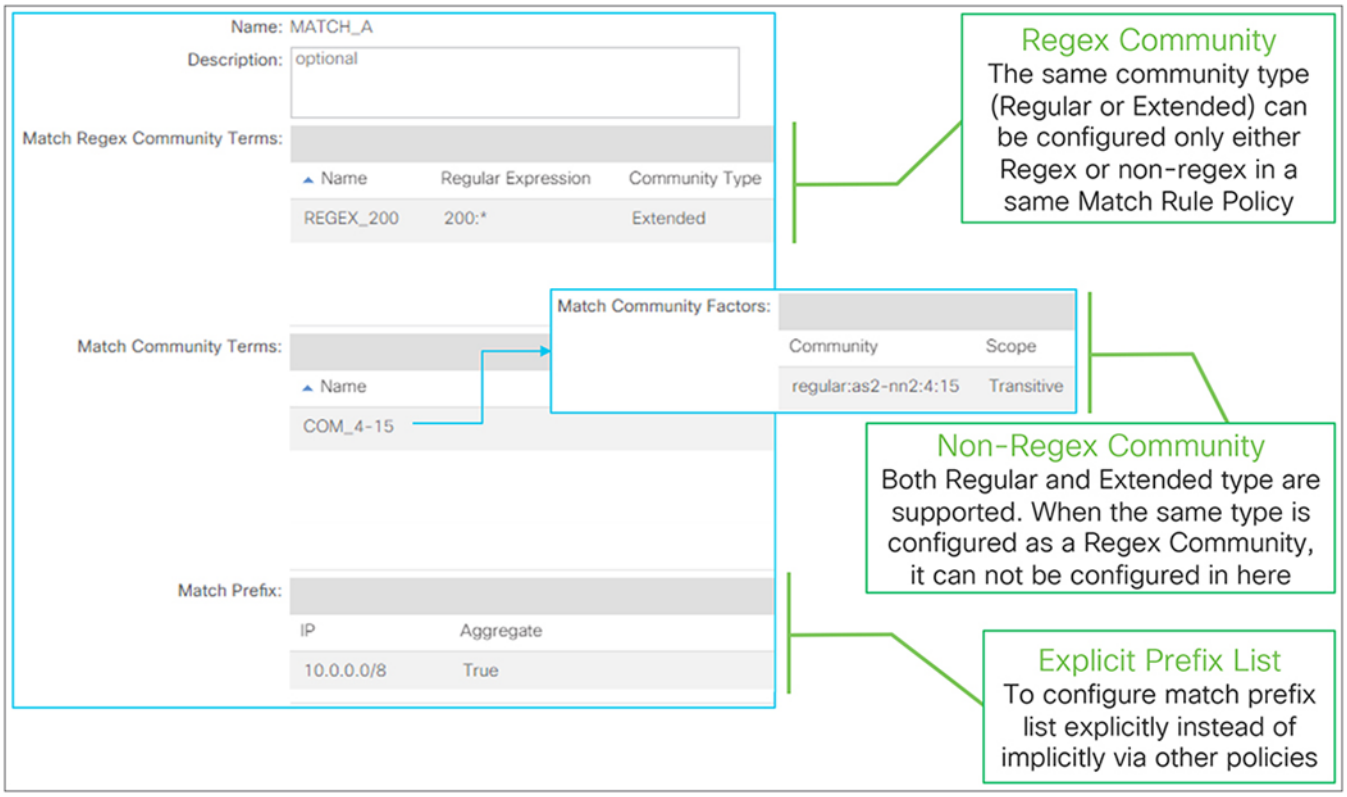

Figure 100.
GUI(APIC Release 3.2) 내 경로 프로필 매치 옵션

매치 규칙은 APIC Release 1.2(2)부터 경로 프로필에 추가되었으며, 이전 버전에서는 규칙 설정만 지원되었습니다.

- **정규식 커뮤니티 매치**
  일반적인 표현식(정규식) 커뮤니티를 사용해 매치 기준을 생성합니다. 동일한 유형의 커뮤니티(일반 또는 확장형)가 동일한 규칙 정책 매치 내 비 정규식 커뮤니티 매치로서 구성될 경우, 정규식 커뮤니티 매치로 구성될 수 없습니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
ip community-list expanded <list-name> permit <regular expression>
ip extcommunity-list expanded <list-name> permit <regular expression>

route-map <rm-name>
  match community <list-name>
  match extcommunity <list-name>
```

- **커뮤니티 매치**

  BGP 커뮤니티를 사용해 매치 기준을 생성합니다. ACI 는 일반 및 확장형 커뮤니티 유형을 모두 지원합니다. 커뮤니티의 형식은 확장형 커뮤니티에서 AS2:NN2(2 바이트 AS 및 2 바이트 사용자 정의 네트워크 번호) 또는 AS4:NN2(4 바이트 AS 번호 및 2 바이트 사용자 정의 네트워크 번호)입니다.
  APIC 에서 구성 시 커뮤니티 구문은 다음과 같습니다.

  ◦ 일반: regular:as2-nn2:<2 바이트 AS 번호>:<2 바이트 네트워크 번호>

  ```
  Ex.) "regular:as2-nn2:65001:100"
  ```

  ◦ 확장형: extended:as4-nn2:<4 바이트 AS 번호>:<2 바이트 네트워크 번호>

  ```
  Ex.) "extended:as4-nn2:65536:100"
  ```

  확장형 커뮤니티 유형은 다음 두 가지 범위를 지원합니다.

  ◦ 전이: 커뮤니티가 eBGP 피어링 전반(AS 전체)에 전파됩니다.

  ◦ 비 전이: 커뮤니티가 eBGP 피어링 전반(AS 전체)에 전파되지 않습니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

  ```
  ip community-list standard <list-name> permit <as2:nn community>
  ip extcommunity-list standard <list-name> permit 4bytegeneric {transitive | nontransitive} <as4:nn community>

  route-map <rm-name>
    match community <list-name>
    match extcommunity <list-name>
  ```

- **식별 번호 매치(명시적인 식별 번호 목록)**

  IP 식별 번호 목록을 사용해 매치 기준을 생성합니다. APIC Release 2.1(1)에서 도입된 옵션으로, "경로 제어 서브넷 내보내기" 등 기타 APIC 정책에서 암시적으로 생성한 IP 식별 번호 목록과 비교 시 절대 식별 번호 목록으로 불립니다.
  "집계" 옵션이 활성화되면 IP 식별 번호 목록이 식별 번호에 "le 32"를 추가합니다. 이 식별 번호는 0.0.0.0/0 일 필요가 없습니다. 이는 0.0.0.0/0 이 아닌 서브넷에 집계가 필요한 경우 "경로 제어 서브넷 내보내기 및 가져오기" 범위에 대해 "내보내기 및 가져오기 집계"의 대안으로 사용될 수 있습니다. "경로 제어 서브넷 내보내기 및 가져오기" 범위에서는 "내보내기 및 가져오기 집계" 옵션을 사용하는 데 0.0.0.0/0 만 지원됩니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

  ```
  ip prefix-list <list-name> permit <prefix>/<mask> {le 32}

  route-map <rm-name>
    match ip address prefix-list <list-name>
  ```

경로 프로필 규칙 설정 옵션

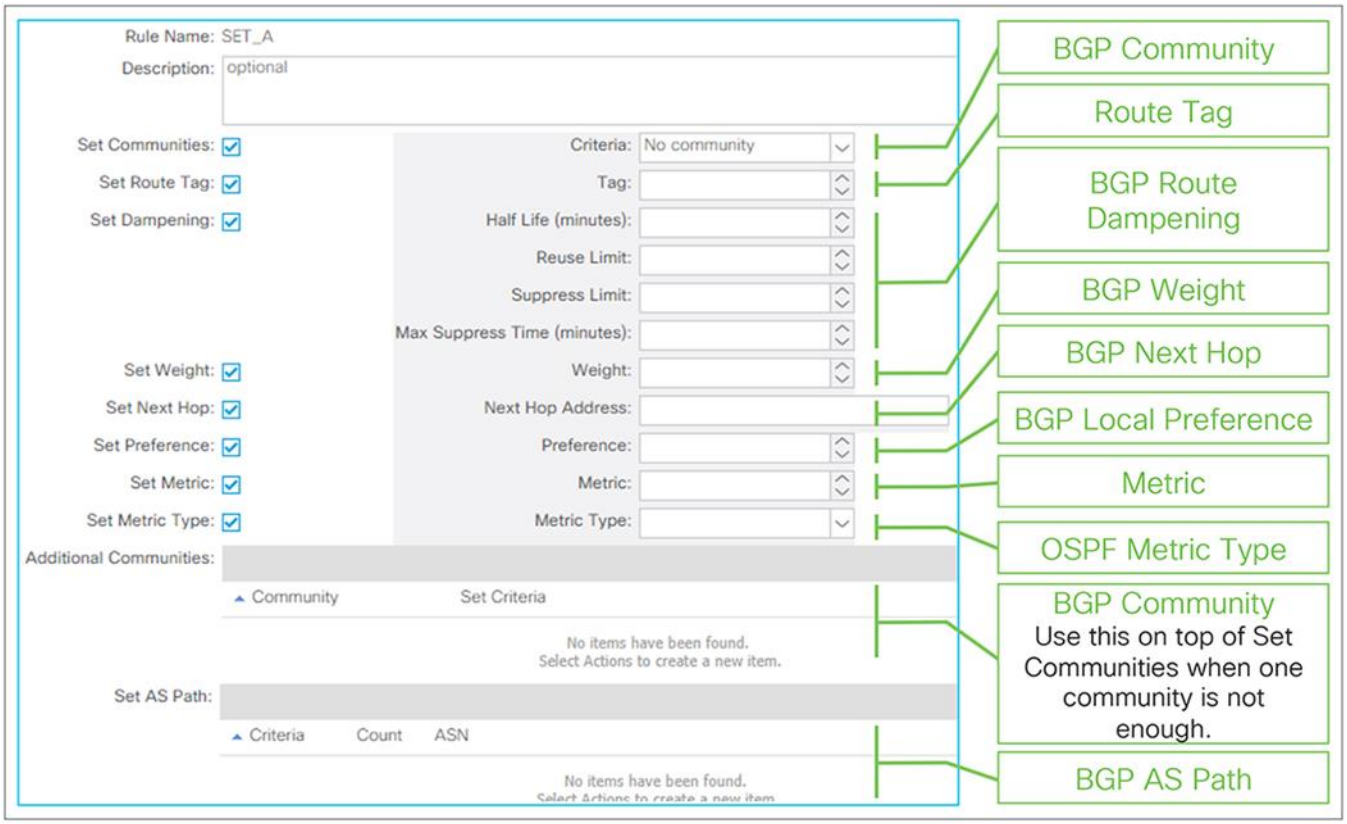

Figure 101.

GUI(APIC Release 3.2) 내 경로 프로필 설정 옵션

- **커뮤니티 설정(BGP 커뮤니티)**

  BGP Community 를 설정하며, 구문은 위에서 언급된 매치 커뮤니티와 동일합니다. 사용 가능한 옵션은 다음과 같습니다.

  - 커뮤니티 제거: 기존 커뮤니티를 제거합니다.
  - 커뮤니티 추가: 기존 커뮤니티에 커뮤니티를 추가합니다.
  - 커뮤니티 교체: 기존 커뮤니티를 새로운 커뮤니티로 교체합니다.

  여러 명령어를 설정해야 할 경우 이 옵션에 더해 **추가적인 커뮤니티** 옵션을 사용합니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
route-map <rm-name>
  set community <community> {none | additive]
  set extcommunity <extcommunity> 4bytes-generic transitive {additive}
```

- **경로 태그 설정**

  경로 태그를 설정하며, 이는 외부로 보급(내보내기)되는 경로 등 VRF 태그 정책으로부터 태그를 부여받은 경로에는 적용되지 않습니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
route-map <rm-name>
  set tag <num>
```

- **댐프닝 설정(BGP 경로 댐프닝)**

  BGP 경로 댐프닝에 대한 매개 변수를 설정합니다. 자세한 내용은 "L3Out BGP" 섹션의 "BGP 경로 댐프닝"을 참조하시기 바랍니다.

- **가중치 설정(BGP 가중치)**

  BGP 가중치를 설정합니다. 특정 BGP 피어의 모든 경로에 대해 BGP 가중치를 동일하게 설정해야 할 경우, BGP 피어 연결성 프로필에서 가중치를 설정할 수 있습니다. 자세한 내용은 "BGP 프로토콜 옵션(인접 라우터 수준)" 섹션을 참조하시기 바랍니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
route-map <rm-name>
  set weight <num>
```

- **다음 홉 설정(BGP 다음 홉)**

  BGP 경로 내 다음 홉 IP 를 덮어씁니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
route-map <rm-name>
  set ip next-hop <next-hop ip>
```

- **환경 설정 지정(BGP 로컬 환경 설정)**

  BGP 로컬 환경 설정을 지정합니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
route-map <rm-name>
  set local-preference <num>
```

- **행렬 설정**

  OSPF 또는 BGP 경로에 대한 행렬을 설정하거나 EIGRP 경로에 대한 최소 대역폭을 설정합니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
route-map <rm-name>
  set metric <num>
```

- **행렬 유형 설정(OSPF 행렬 유형)**
  OSPF 외부 행렬 유형(유형 1 또는 유형 2)을 설정합니다. OSPF 는 유형 2 를 사용하도록 기본 설정되어 있습니다. 유형 2 에는 외부 경로를 시작한 ASBR 에 도달하는 비용(행렬)이 포함되지 않지만 유형 1 에는 ASBR 에 대한 비용이 포함됩니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
route-map <rm-name>
  set [type-1 | type-2]
```

- **추가적 커뮤니티**
  여러 개의 커뮤니티를 설정해야 할 때 **커뮤니티 설정**과 함께 사용됩니다. APIC Release 2.2(2)에서 도입된 옵션으로, 사용 가능한 구성 매개 변수에 대한 내용은 **커뮤니티 설정**을 참조하시기 바랍니다.

- **AS 경로 설정(BGP AS 경로)**
  BGP 경로에서 BGP AS 경로 앞에 추가하는 기능으로, APIC Release 3.0(1)에서 도입되었습니다. 사용 가능한 옵션은 다음과 같습니다.
  - AS 앞에 추가: 앞에 추가할 각 AS 번호를 수동으로 지정합니다.
  - 마지막 AS 앞에 추가: 마지막 AS 번호 앞에 자동으로 여러 차례 추가합니다.

  독립 실행형 NX-OS 에 대응하는 명령어는 다음과 같습니다.

```
route-map <rm-name>
  set as-path prepend <AS> <AS> ...
  set as-path prepend last-as <count>
```

경로 프로필 매치 규칙 AND 및 OR

이 서브섹션에는 경로 프로필에서 다수의 매치 기준이 처리되는 방식이 설명되어 있습니다. 이는 경로 프로필의 L3Out 서브넷(식별 번호)과 매치 기준에 관한 경로 프로필 유형 "식별 번호 AND 라우팅 정책 매치" 또는 "라우팅 정책만 매치"에 관한 내용이 아니라, 단일 경로 프로필 내 매치 기준에 관한 내용입니다.

다음 Figure 102 는 매치 기준이 "AND"로 처리되는 상황을 나타내며, 이는 동일한 경로 맵 시퀀스에서 다수의 매치 기준이 구성되는 경우를 뜻합니다. 이 경우 매치 기준은 단일 컨텍스트 정책의 단일 매치 규칙 정책에서 구성되어야 합니다.

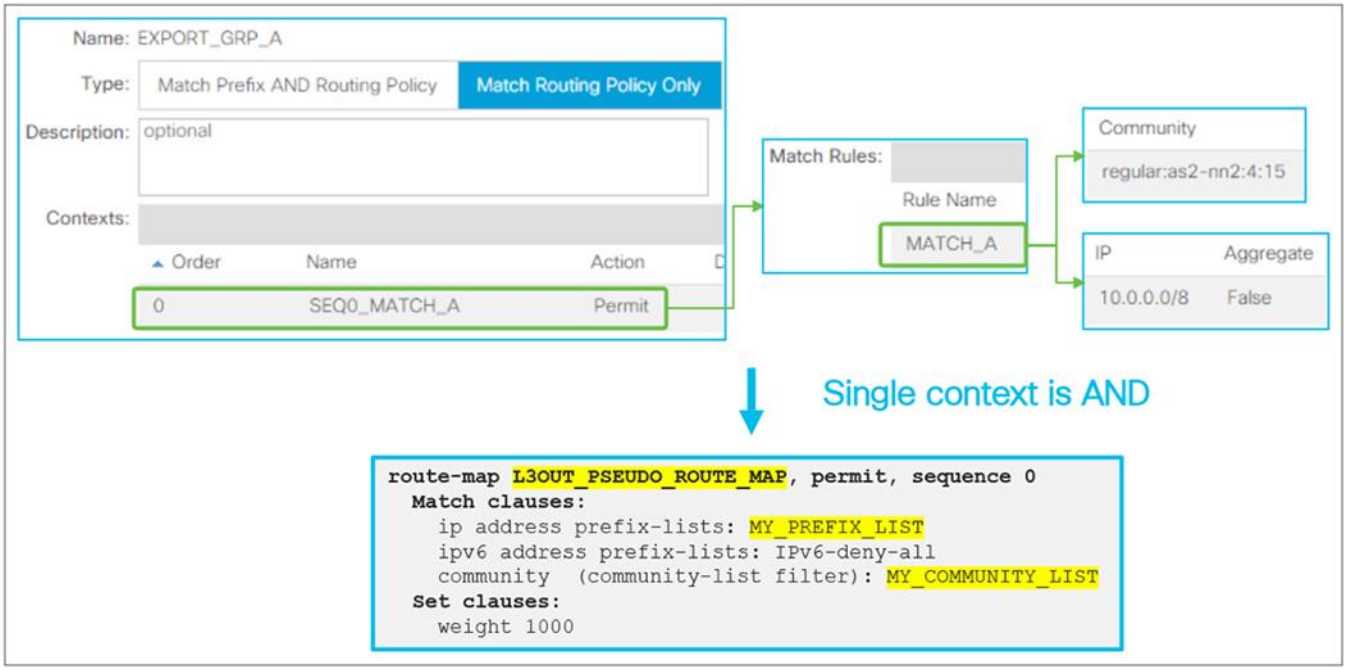

Figure 102.

경로 프로필 AND 매치 규칙

다음 Figure 103 은 매치 기준이 "OR"로 처리되는 상황을 나타내며, 이는 별도의 경로 맵 시퀀스에서 다수의 매치 기준이 구성되는 경우를 뜻합니다. 이 경우 매치 기준은 별도의 컨텍스트 정책에서 구성되어야 합니다. 각 컨텍스트의 순서 옵션은 우선으로 적용될 컨텍스트(경로 맵 시퀀스)를 정의합니다.

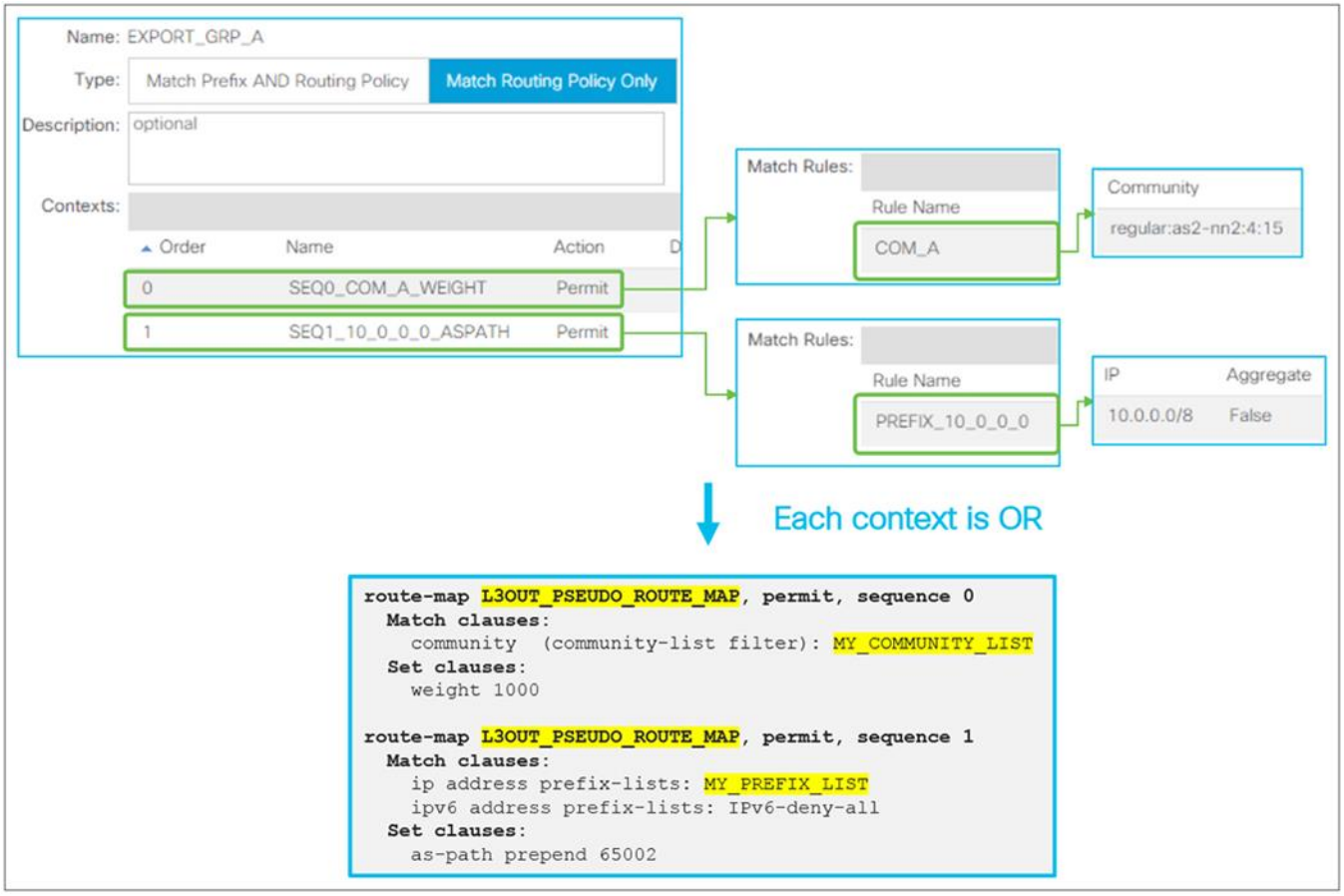

Figure 103.

경로 프로필 OR 매치 규칙-1

참고:

매치 규칙이 "OR"이어야 하는 경우 사용자는 단일 컨텍스트 정책에서 별도의 매치 규칙에 있는 매치 기준을 구성할 수 있습니다. 하지만 이 경우 매치 기준의 순서는 결정적이지 않으므로 각 매치 기준의 순서가 무관한 경우가 아닌 한, "OR"에 대해 이 구성을 선택하는 것은 적합하지 않습니다.

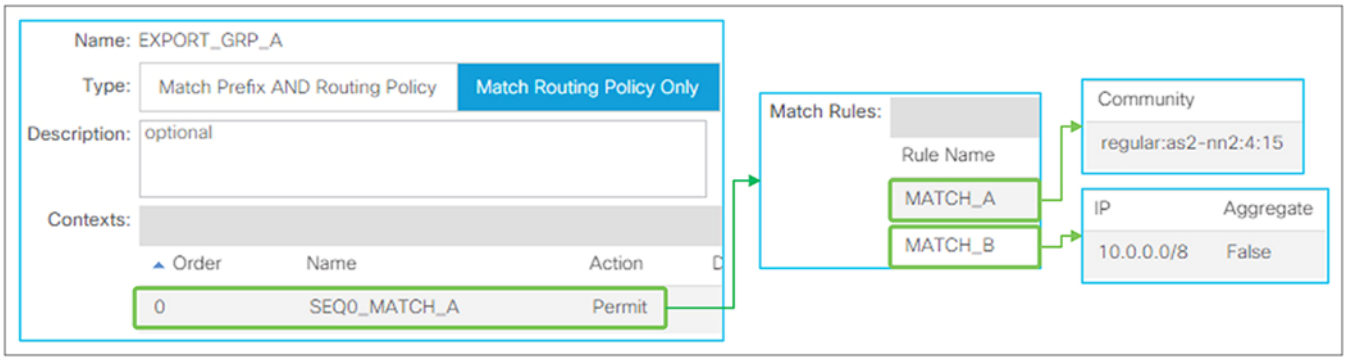

Figure 104.
경로 프로필 OR 매치 규칙-2

L3Out EPG 의 경로 프로필(경로 내보내기 및 가져오기)

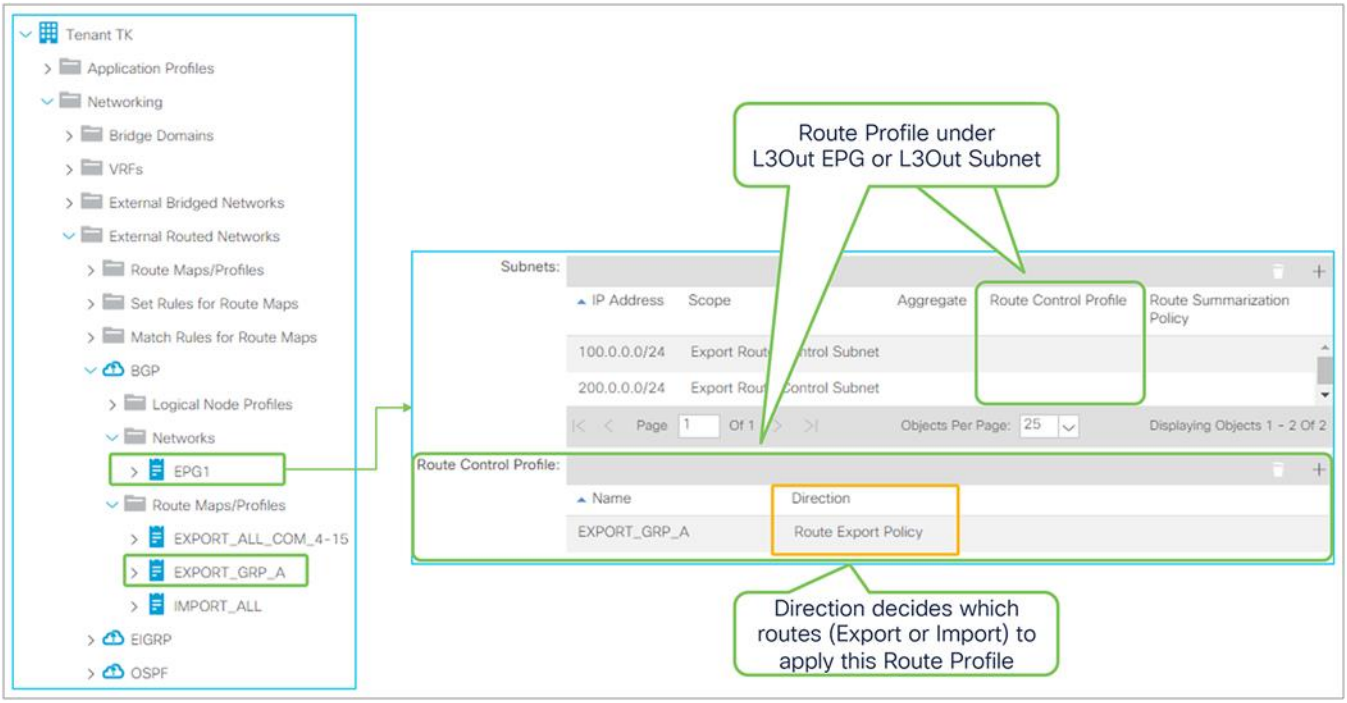

Figure 105.
GUI(APIC Release 3.2) 내 L3Out 의 경로 프로필

L3Out EPG 에서 "경로 제어 서브넷 내보내기" 또는 "경로 제어 서브넷 가져오기" 범위에 사용되는 내부 경로 맵에 규칙 매치 및/또는 설정을 추가하기 위해 각 L3Out 의 경로 프로필이 사용됩니다. 각 서브넷 범위에 대한 자세한 내용은 "L3Out 전송 경로" 섹션을 참조하시기 바랍니다. L3Out EPG 에 대한 경로 프로필에는 두 가지 요소가 있습니다. 첫 번째는 방향, 두 번째는 경로 프로필이 연결된 구성 요소입니다.

- **경로 프로필 방향**
  경로 프로필이 적용될 서브넷 유형을 결정합니다.
  - 경로 내보내기 정책: 경로 프로필은 "경로 제어 서브넷 내보내기" 범위가 포함된 서브넷에 적용됩니다.
  - 경로 가져오기 정책: 경로 프로필은 "경로 제어 서브넷 가져오기" 범위가 포함된 서브넷에 적용됩니다.
- **경로 프로필 연결**
  경로 프로필의 범위를 결정합니다. 다음 내용은 명시적인 식별 번호 목록(식별 번호 기준 매치) 없이 경로 프로필이 "**식별 번호 AND 라우팅 정책 매치**" 유형을 사용하는 경우의 동작에 관한 설명이며, 권장하는 구성방식입니다.
  - L3Out EPG

경로 프로필은 L3Out EPG 내 매치 방향 범위를 통해 구성된 모든 L3Out 서브넷에 적용됩니다. Figure 105 에서는 L3Out EPG 1 의 내보내기 방향이 포함된 경로 프로필 "EXPORT_GRP_A"가 "경로 제어 서브넷 내보내기" 범위가 포함된 L3Out 서브넷 100.0.0.0/024 와 200.0.0.0/24 에 모두 적용됩니다. Figure 105 에서 경로 프로필의 방향이 "가져오기"인 경우, 일치하지 않는 방향으로 인해 경로 프로필이 두 개의 서브넷에 적용되지 않습니다.

- L3Out 서브넷

  경로 프로필은 이 서브넷에 적용됩니다. 서브넷 범위와 경로 프로필 방향이 일치하지 않을 경우 경로 프로필은 적용되지 않습니다.

참고:

두 개의 연결 수준 외에도 한 개의 수준이 더 존재합니다. 일명 **기본 내보내기 또는 기본 가져오기**라고 하는 특수 경로 프로필로, 전체 L3Out 과 연결된 BD 에 적용됩니다. 다음 서브섹션에 **기본 내보내기 및 가져오기**가 자세히 설명되어 있습니다. 경로 프로필이 여러 개의 수준으로 연결될 때는 보다 세부적인 범위가 우선시됩니다. 즉, **L3Out 서브넷 > L3Out EPG > 기본 내보내기 및 가져오기**를 의미합니다.

구성 옵션 예시

다음 일련의 도표(Figure 106~Figure 110)에는 권장 구성 방식과 경로 프로필의 규칙이 적용되는 방식이 설명되어 있습니다. 이 예시에서 가운데의 L3Out 1 이 L3Out 2 에서 외부 경로와 BD1 서브넷의 보급 시도하고 있습니다.

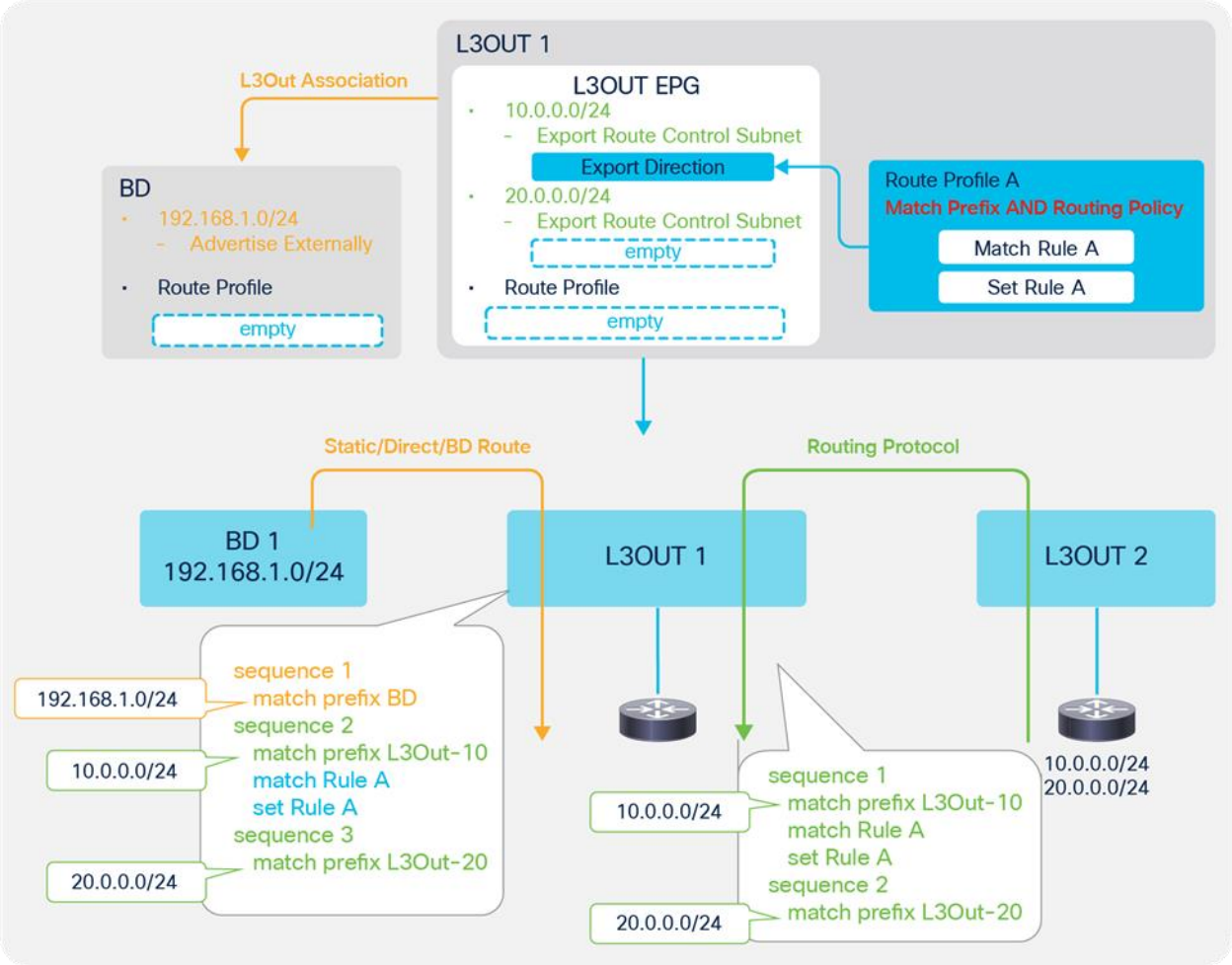

Figure 106.

L3Out 서브넷의 경로 프로필 예시(식별 번호 AND 라우팅 정책 매치)

이 예시에서 경로 프로필은 경로 프로필 A 를 통해 L3Out 서브넷 10.0.0.0/24 에만 적용되며, "경로 제어 서브넷 내보내기" 범위가 BD 서브넷을 보급하는 데 사용될 수 있으므로 BD 서브넷(Figure 106 의 주황색 화살표)을 위한 재배포의 일부분에도 적용됩니다. 이 예시에서 경로 프로필은 BD 서브넷 선언에는 영향을 미치지 않는데, 그 이유는 BD 서브넷이 IP 식별 번호 목록 서브넷(Figure 의 매치 식별 번호 L3Out-10)과 다르며, L3Out 과 BD 의 연결을 통해 보급이 구성되기 때문입니다.

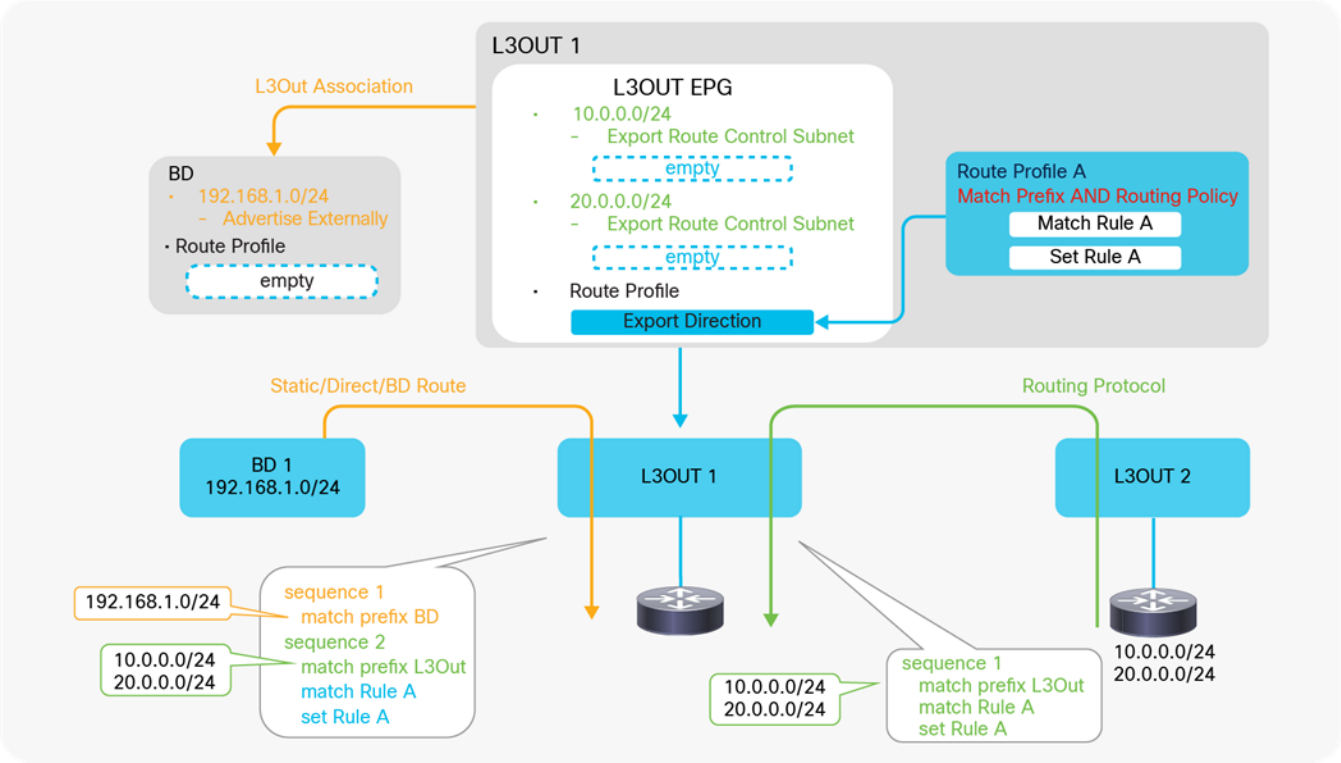

Figure 107.

L3Out EPG 의 경로 프로필 예시(식별 번호 AND 라우팅 정책 매치)

이 예시에서 경로 프로필은 매치 방향 범위인 "경로 제어 서브넷 내보내기"가 포함된 모든 L3Out 서브넷에 적용됩니다. 또한 "경로 제어 서브넷 내보내기" 범위가 BD 서브넷을 보급하는 데 사용될 수 있으므로 BD 서브넷(Figure 107 의 주황색 화살표)을 위한 재배포의 일부분에도 적용됩니다. 이 예시에서 경로 프로필은 BD 서브넷 선언에는 영향을 미치지 않는데, 그 이유는 BD 서브넷이 IP 식별 번호 목록 서브넷(Figure 의 **일치 식별 번호 L3Out**)과 다르며, L3Out 과 BD 의 연결을 통해 보급이 구성되기 때문입니다. "경로 제어 서브넷 내보내기" 범위가 L3Out 연결이 아닌 BD 서브넷을 보급하는 데 사용될 경우, 규칙 A 설정 등의 경로 프로필의 규칙이 BD 서브넷 보급에도 적용됩니다.

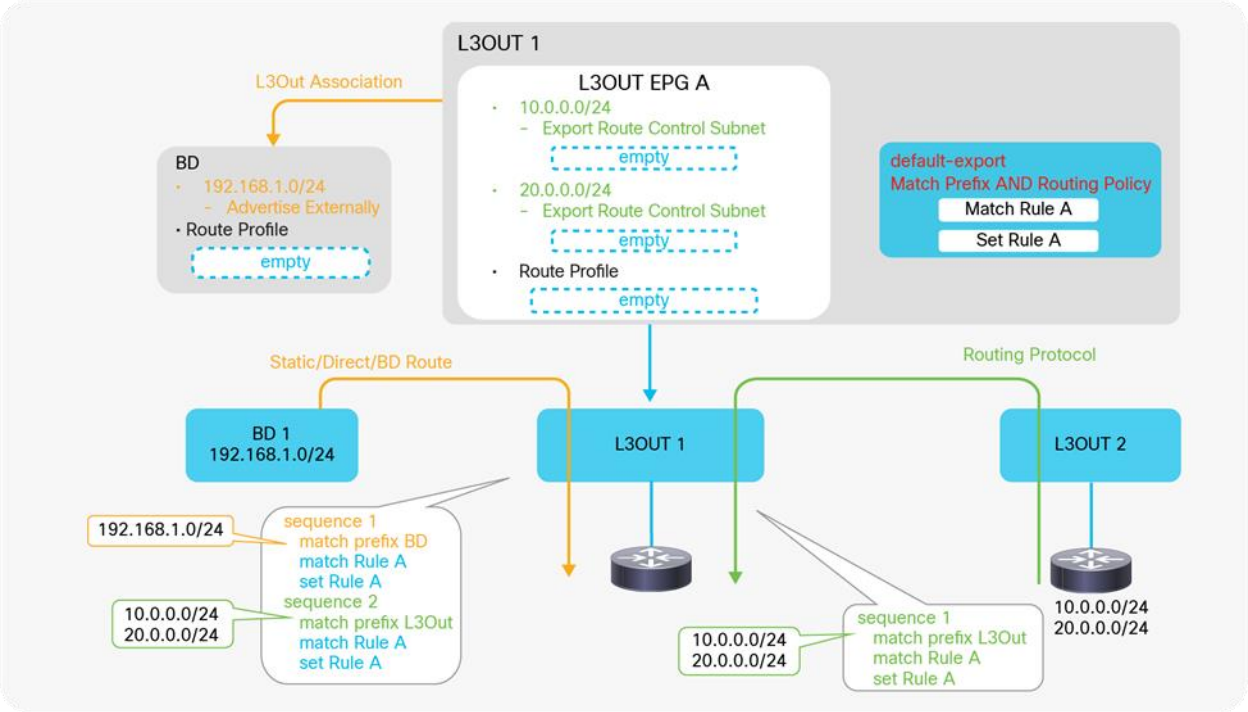

Figure 108.

L3Out 기본 내보내기의 경로 프로필 예시(식별 번호 AND 라우팅 정책 매치)

이 예시에서 경로 프로필은 **기본 내보내기**이며 유형은 "**식별 번호 AND 라우팅 정책 매치**"입니다. 따라서 ACI 는 L3Out 연결 및 "외부로 보급" 범위가 포함된 BD 서브넷을 포함해 이 L3Out 1 과 관련된 모든 서브넷에 경로 프로필을 적용합니다.

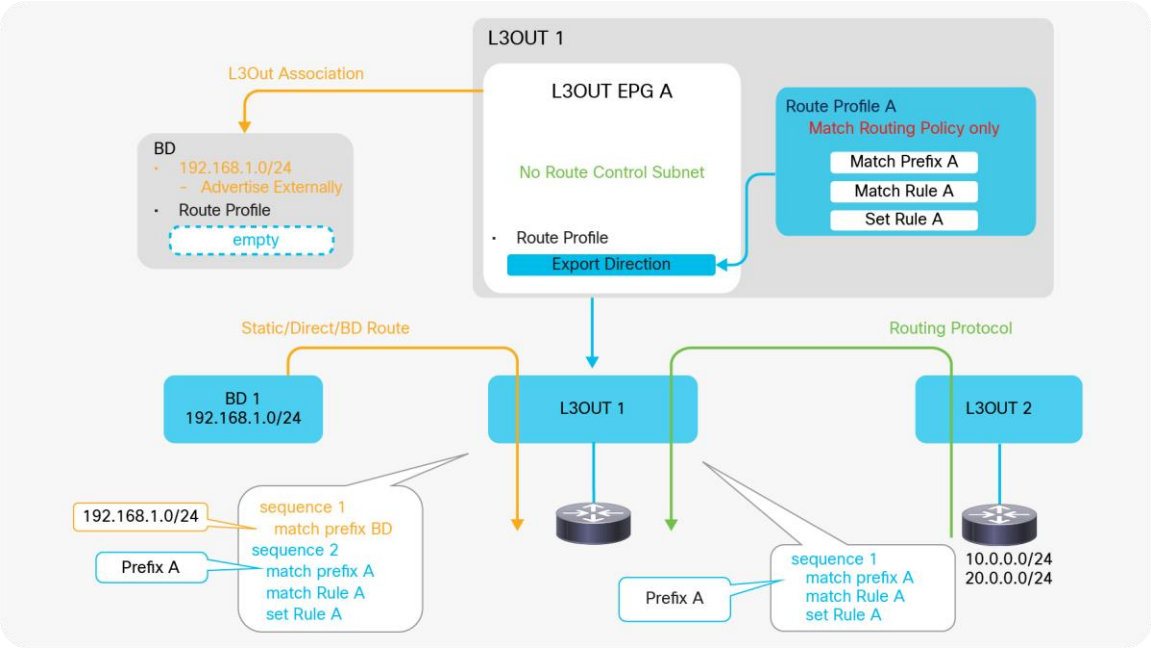

Figure 109.

L3Out EPG(라우팅 정책만 매치)의 경로 프로필 예시

이 예시에서 경로 프로필의 유형은 "라우팅 정책만 매치"이므로 "라우팅 정책만 매치"로 인해 ACI 는 오직 경로 프로필을 기준으로 규칙을 생성합니다. 경로 프로필은 BD 서브넷을 보급하는 데에도 사용될 수 있으므로("ACI BD 서브넷 보급" 섹션 참조) L3Out 경로(Figure 109 의 녹색 화살표)와 BD 서브넷(Figure 109 의 주황색 화살표)의 재배포에도 적용됩니다. 이 예시에서 식별 번호(Figure 의 **식별 번호 A 매치**)는 BD 서브넷과 다르며, L3Out 과 BD 의 연결을 통해 보급이 이루어지기 때문에 BD 서브넷에는 영향을 미치지 않습니다. 또한 이 L3Out EPG 에서는 "경로 제어 서브넷 내보내기" 범위로 L3Out 서브넷을 생성하는 의미가 없습니다. 그 이유는 내보내기 방향의 "라우팅 정책만 매치"가 포함된 경로 프로필로 인해 전송 라우팅과 BD 서브넷 보급에서 L3Out 서브넷이 무시되기 때문입니다.

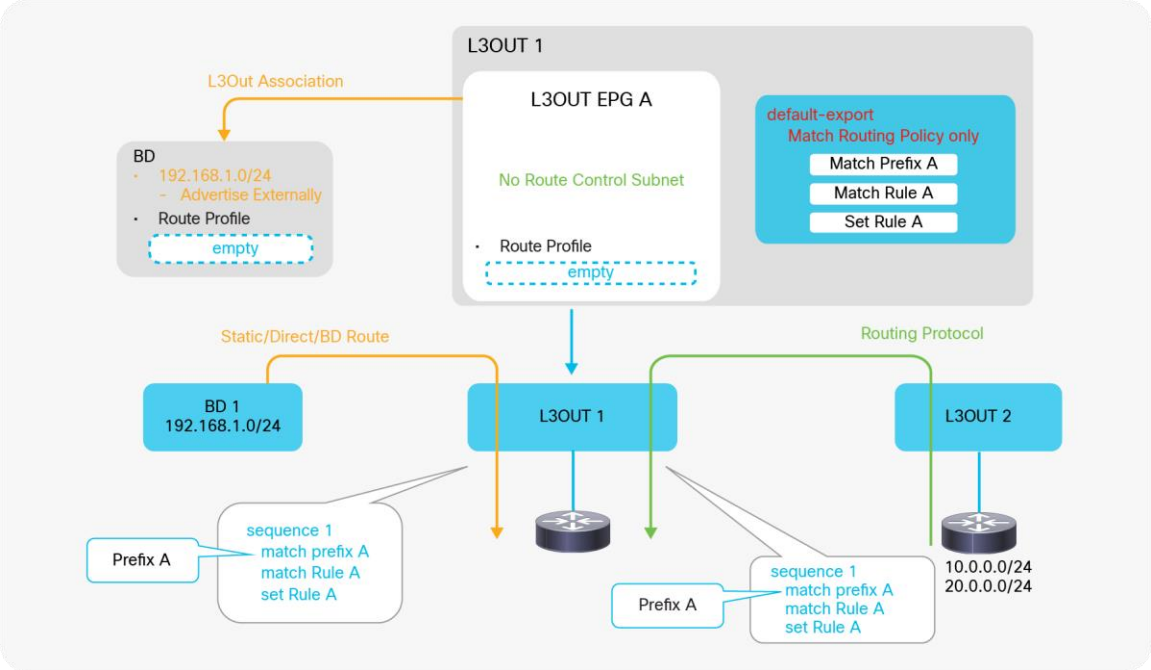

Figure 110.
L3Out 기본 내보내기(라우팅 정책만 매치)의 경로 프로필 예시

이 예시에서 ACI 는 "라우팅 정책만 매치"로 인해 오직 경로 프로필만 기준으로 규칙을 생성합니다. 또한 ACI 는 **기본 내보내기**로 인해 L3Out 1 과 관련된 다른 규칙을 모두 덮어씁니다. 이 예시에서 L3Out 연결은 효과가 없으며 따라서 필요하지 않습니다. 그 이유는 "라우팅 정책만 매치"가 포함된 기본 내보내기에 의해 L3Out 과 BD 연결의 BD 서브넷 재배포가 무시되고 대체되기 때문입니다. 따라서 관리자는 **기본 내보내기**(Figure 110 의 **식별 번호 A 매치**)에 있는 명시적 식별 번호 목록의 BD 서브넷 (192.168.1.0/24)을 포함해야 합니다. 그러나 BD 서브넷의 "외부로 보급됨" 범위는 여전히 필요합니다.

경로 프로필이 전송 라우팅과 BD 서브넷 보급을 제어하는 데 사용되는 경우에는 Figure 110 의 구성이 적합합니다.

참고:

가능한 모든 경로에 경로 프로필을 적용하는 방법에는 여러 가지가 있습니다.

9. 0.0.0.0/0 의 명시적인 식별 번호 목록과 집계 옵션이 포함된 기본 내보내기 및 기본 가져오기 사용(Figure 110)
10. 0.0.0.0/0 의 명시적인 식별 번호 목록과 집계 옵션이 포함된 맞춤형 경로 프로필을 L3Out EPG 에 적용(Figure 109)
11. "경로 제어 서브넷 내보내기 및 가져오기" 범위와 "집계 내보내기 및 가져오기" 옵션이 포함된 0.0.0.0/0 에 대한 L3Out EPG 또는 L3Out 서브넷에 맞춤형 경로 프로필 적용 (APIC Release 4.2 이후 버전에서만 지원됨)

두 번째 옵션을 사용할 때는 다음 동작에 유의해야 합니다.

- 라우팅 프로토콜(Figure 109 와 Figure 110 의 녹색 화살표)의 경로에 적용됨
- 고정 경로, 직접 연결된 서브넷, BD 서브넷(Figure 109 와 Figure 110 의 주황색 화살표)에는 적용되지 않음

이는 라우팅 프로토콜 재배포 및 기타(고정 및 직접 경로)에 대한 내부 경로 맵이 각기 다르기 때문입니다. 자세한 내용은 "L3Out 전송 라우팅" 섹션의 "전송 라우팅에 대한 내부 경로 맵"을 참조하시기 바랍니다.

경로 프로필 유형, L3Out EPG 및 서브넷

다음은 경로 프로필 유형과 명시적인 식별 번호 목록의 조합에 관한 일반적인 권장 사항입니다. 중복 구성을 피하기 위해 "라우팅 정책만 매치"로 명시적인 식별 번호 목록만 사용하는 방법입니다.

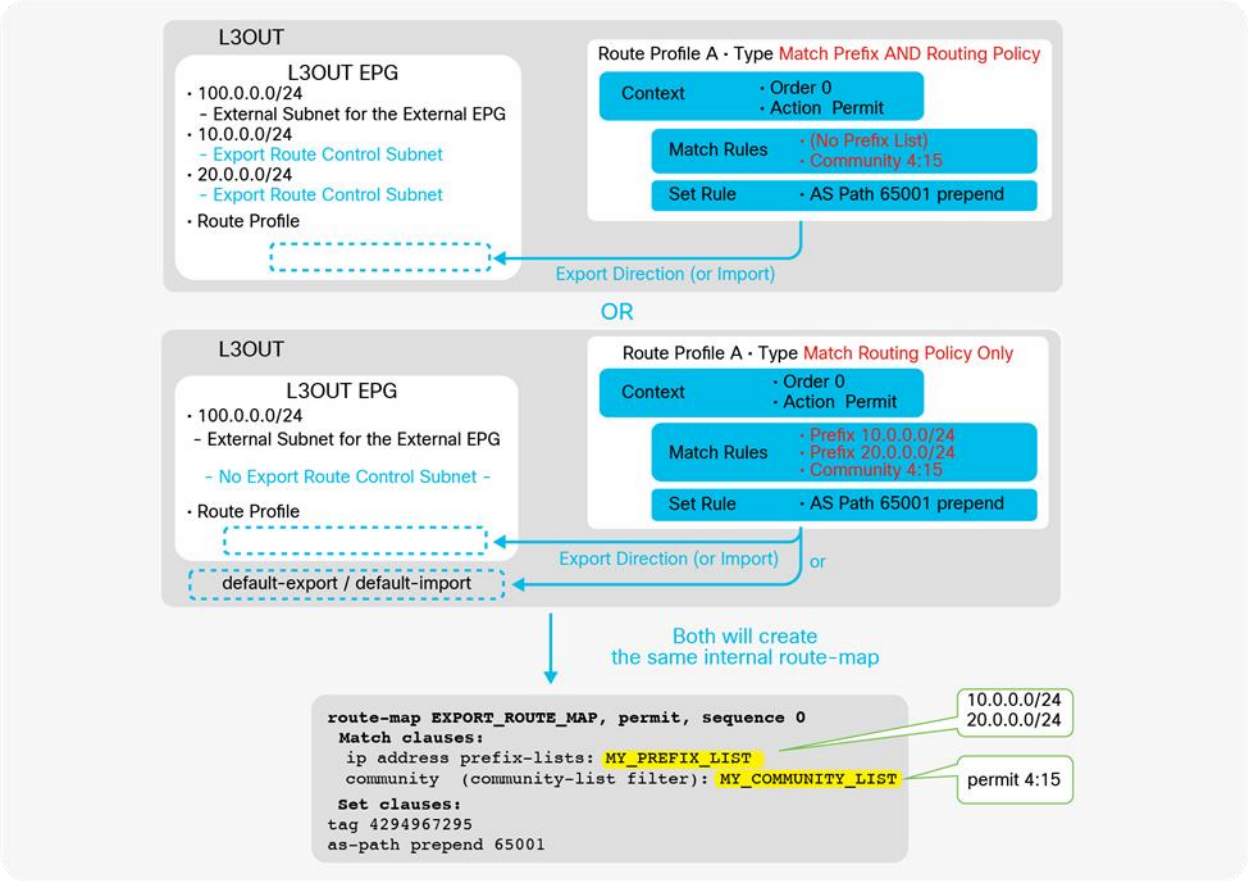

Figure 111.
L3Out 경로 프로필 유형의 차이점 및 권장 사항

- **"식별 번호 AND 라우팅 정책 매치" 유형 사용**
  "경로 제어 서브넷 내보내기 및 가져오기" 범위가 포함된 L3Out 서브넷을 명시적인 식별 번호 목록(식별 번호 기준 일치) 없이 사용하여 커뮤니티 등의 추가적인 매치 규칙이나 규칙 설정을 적용하는 방법입니다. 그렇지 않으면 Figure 99 에서와 같이, 구성이 L3Out 서브넷 및 명시적인 식별 번호 목록의 식별 번호를 병합하기 때문에 구성을 사용 및 유지하기가 어려워집니다.
- **"라우팅 정책만 매치" 유형 사용**
  Figure 98 에서와 같이, "경로 제어 서브넷 내보내기 및 가져오기" 범위가 포함된 L3Out 서브넷은 무시되므로 해당 서브넷 없이 명시적인 식별 번호 목록만 사용하는 방법입니다. L3Out 에서는 항상 맞춤형 경로 프로필이 아닌 "**기본 내보내기**" 또는 "**기본 가져오기**" 경로 프로필로 본 유형을 사용하도록 권장됩니다. L3Out EPG 구성("경로 제어 서브넷 내보내기 및 가져오기" 범위)은 무시되므로 맞춤형 경로 프로필을 사용해 L3Out EPG 에 적용하는 의미가 없기 때문입니다. 두 특정 경로 프로필에 대한 자세한 내용은 아래의 "기본 내보내기 및 기본 가져오기" 서브섹션을 참조하시기 바랍니다.

참고:

L3Out 서브넷에 관한 권장 사항은 "경로 제어 서브넷 내보내기 및 가져오기" 범위에 적용됩니다. "외부 EPG 에

대한 외부 서브넷" 등 기타 범위는 영향을 받지 않으며, 경로 프로필 유형에 관계없이 사용될 수 있습니다.

기본 내보내기 및 기본 가져오기

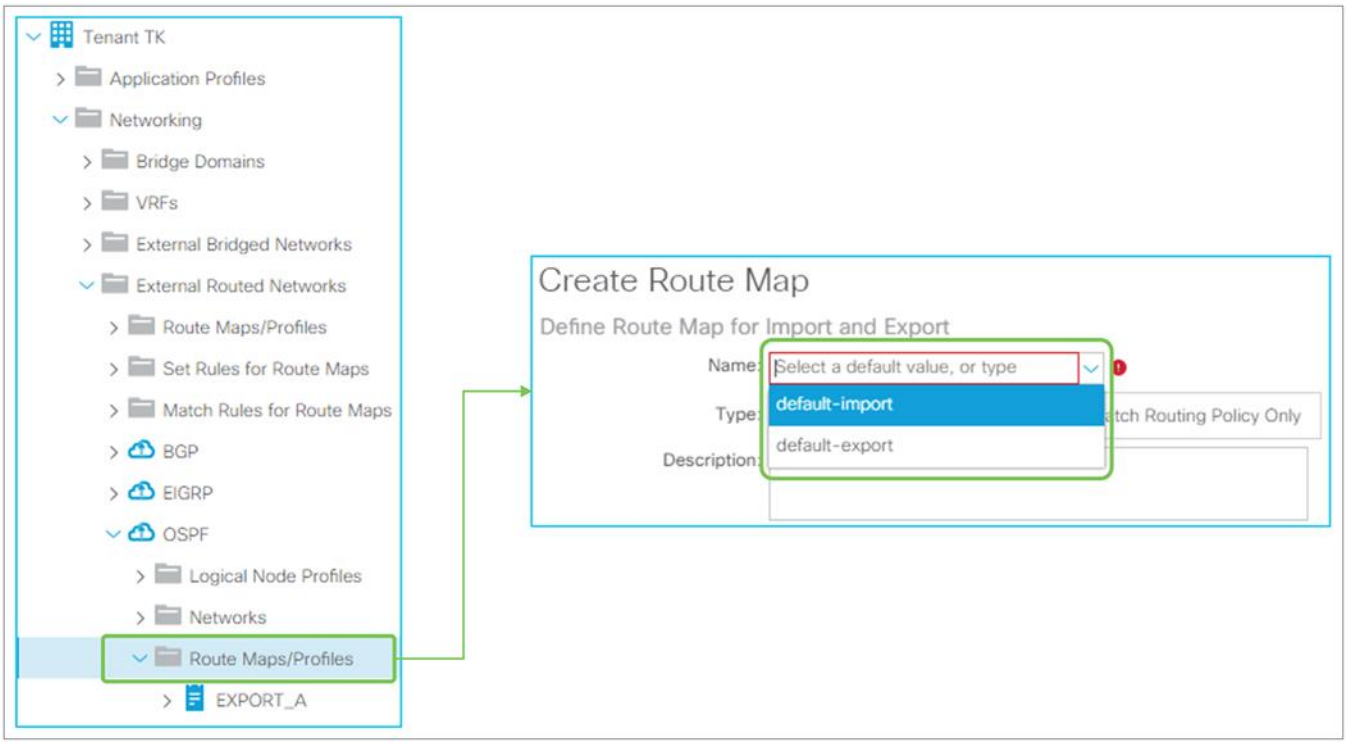

Figure 112.
GUI(APIC Release 3.2) 내 경로 프로필 기본 내보내기 및 기본 가져오기

L3Out 에서 경로 프로필 및 경로 맵을 생성할 때 드롭다운 메뉴에는 **기본 내보내기** 및 **기본 가져오기**의 두 가지 기본 정책 이름이 존재합니다. 이들 경로 프로필의 구성은 다른 경로 프로필의 구성과 동일합니다. 차이점이라면 이 두 개의 특수 경로 프로필이 L3Out EPG 나 L3Out 서브넷 등 다른 구성 요소와 연결되지 않고도 효과를 발휘한다는 것입니다.

참고:

APIC Release 4.2 이전 버전에서는 **기본 내보내기** 및 **기본 가져오기**에 대한 드롭다운 메뉴가 테넌트 수준의 경로 프로필에서도 표시되었습니다. 그러나 적용된 곳이 없어 효과를 발휘하지 못했습니다. APIC Release 4.2 부터는 테넌트 수준 경로 프로필의 **기본 내보내기** 및**기본 가져오기**에 대한 드롭다운 메뉴가 제거되고 두 개의 특수 경로 프로필이 L3Out 에서만 제공되었습니다.

"식별 번호 AND 라우팅 정책 매치" 유형을 통해 생성된 **기본 내보내기**는 각 L3Out 서브넷이나 L3Out EPG 에 연결하지 않고도 "경로 제어 서브넷 내보내기" 범위("경로 제어 서브넷 가져오기"에 대한 **기본 가져오기**)가 포함된 모든 L3Out 서브넷에 적용됩니다. 기본 내보내기 경로 프로필 역시 이 L3Out 에 연결되어 있는 BD 의 "외부로 보급됨" 범위와 함께 BD 서브넷에 적용됩니다. 각 구성 요소(L3Out EPG, L3Out 서브넷, BD 서브넷)에 자체 경로 프로필이 이미 존재할 경우, 이들 경로 프로필은 **기본 내보내기** 또는 **기본 가져오기** 경로 프로필보다

우선시됩니다. Figure 113 은 **기본 내보내기**가 L3Out 에 있는 "식별 번호 AND 라우팅 정책 매치" 유형으로 사용될 때의 내부 경로 맵을 나타냅니다.

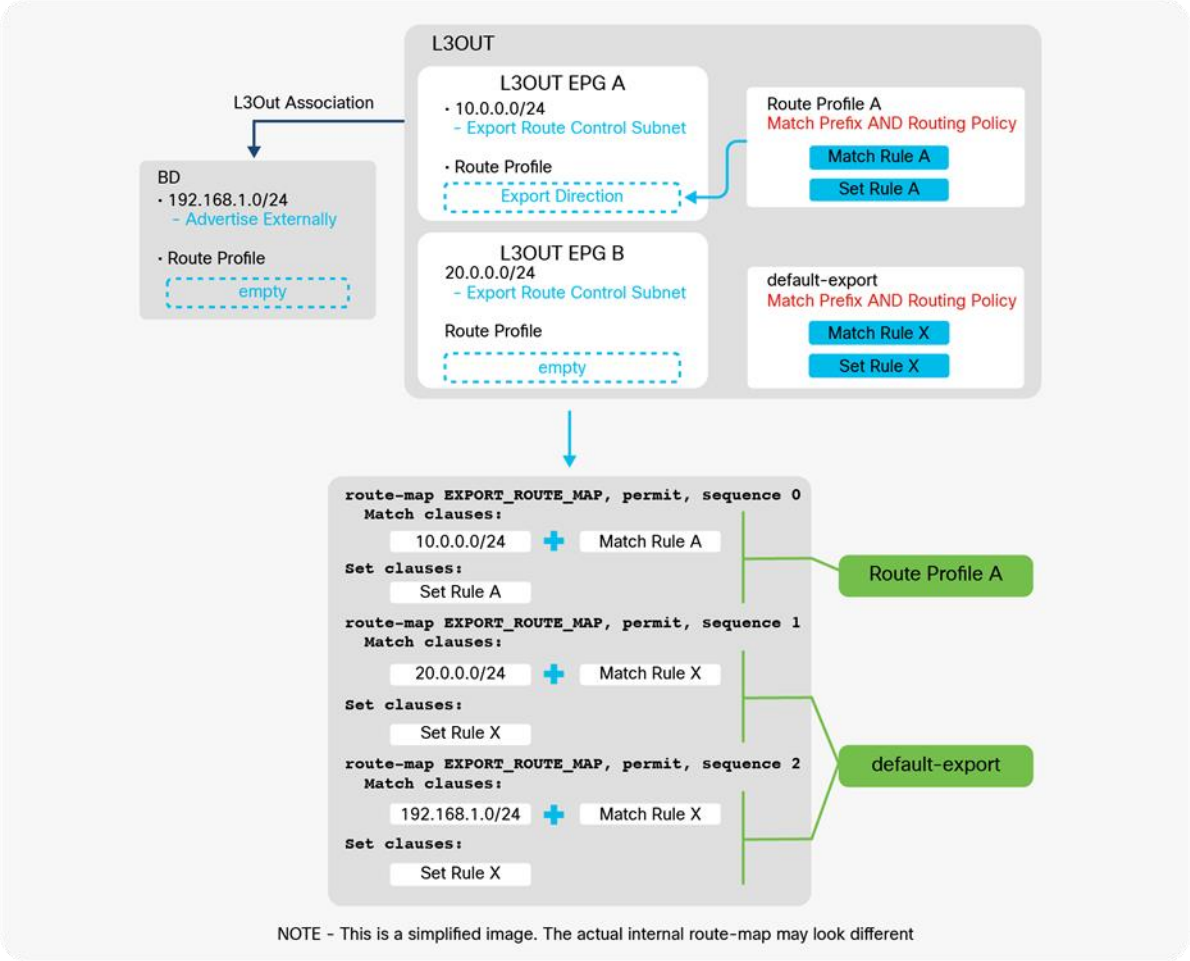

Figure 113.
식별 번호 AND 라우팅 정책 매치가 포함된 L3Out 기본 내보내기 경로 프로필

"라우팅 정책만 매치" 유형으로 생성된 경우, 자체 매치 기준으로만 경로 맵 시퀀스를 생성하고 "경로 제어 서브넷 내보내기" 범위(또는 **기본 가져오기**에 대한 "경로 제어 서브넷 가져오기")가 포함된 L3Out 서브넷에 대한 다른 내부 경로 맵 시퀀스는 모두 무시합니다. **기본 가져오기** 경로 프로필 역시 이 L3Out 에 연결된 BD 의 "외부로 보급됨" 범위를 통해 BD 서브넷의 구성을 무시하게 됩니다. 각 구성 요소(L3Out EPG, L3Out 서브넷, BD 서브넷)에 자체 경로 프로필이 존재할 경우, 이들 경로 프로필은 **기본 내보내기** 또는 **기본 가져오기** 경로 프로필보다 우선시됩니다. Figure 114 에서는 **기본 내보내기**가 L3Out 에 있는 "라우팅 정책만 매치" 유형을 통해 사용될 때의 내부 경로 맵을 나타냅니다.

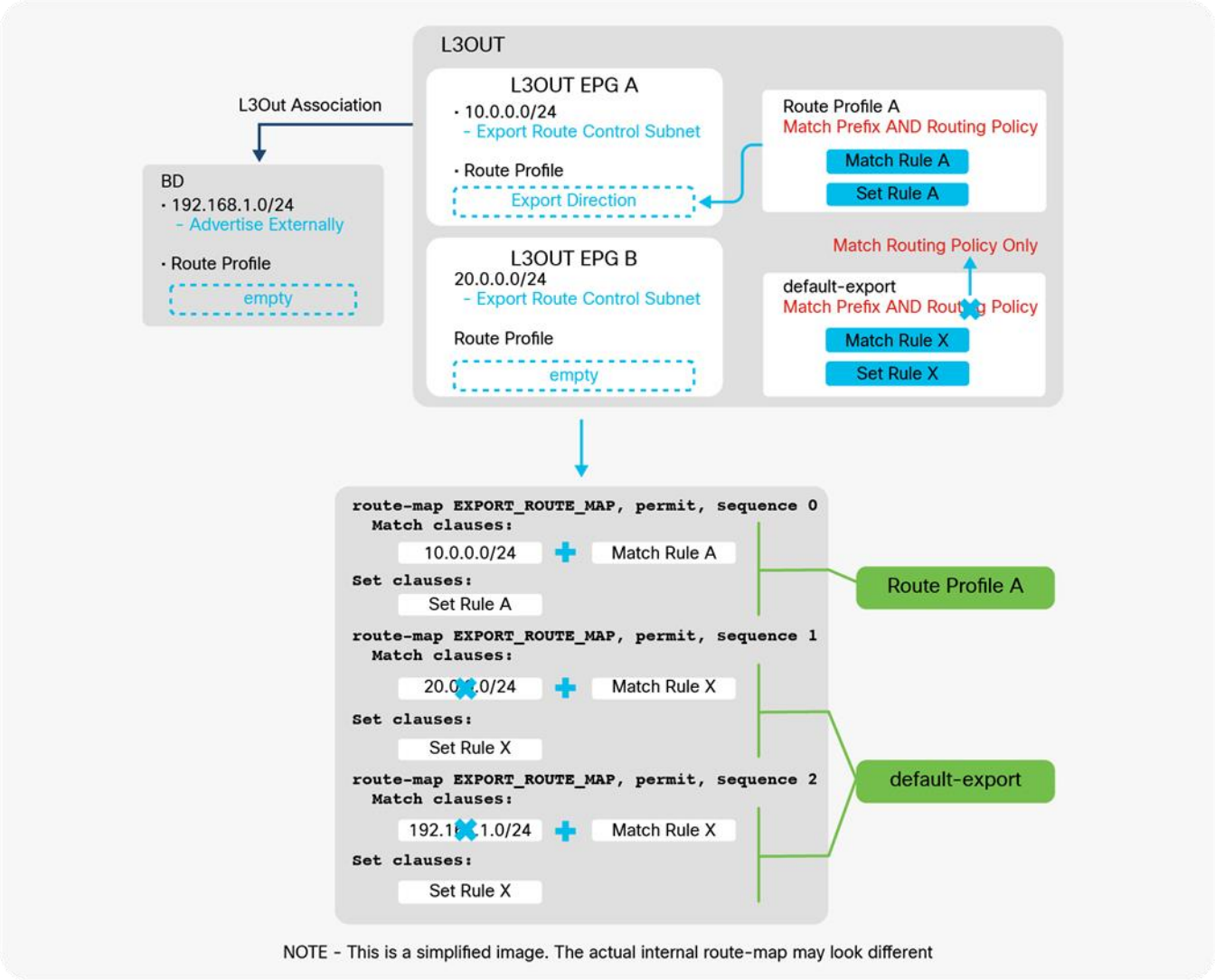

Figure 114.

라우팅 정책만 매치가 포함된 L3Out 기본 내보내기 경로 프로필

단순한 라우팅 제어를 위한 기본 내보내기(권장 구성)

이 서브섹션에서는 **기본 내보내기**를 통해 ACI 에서 서브넷 보급의 구성을 단순화하는 방법을 설명합니다.

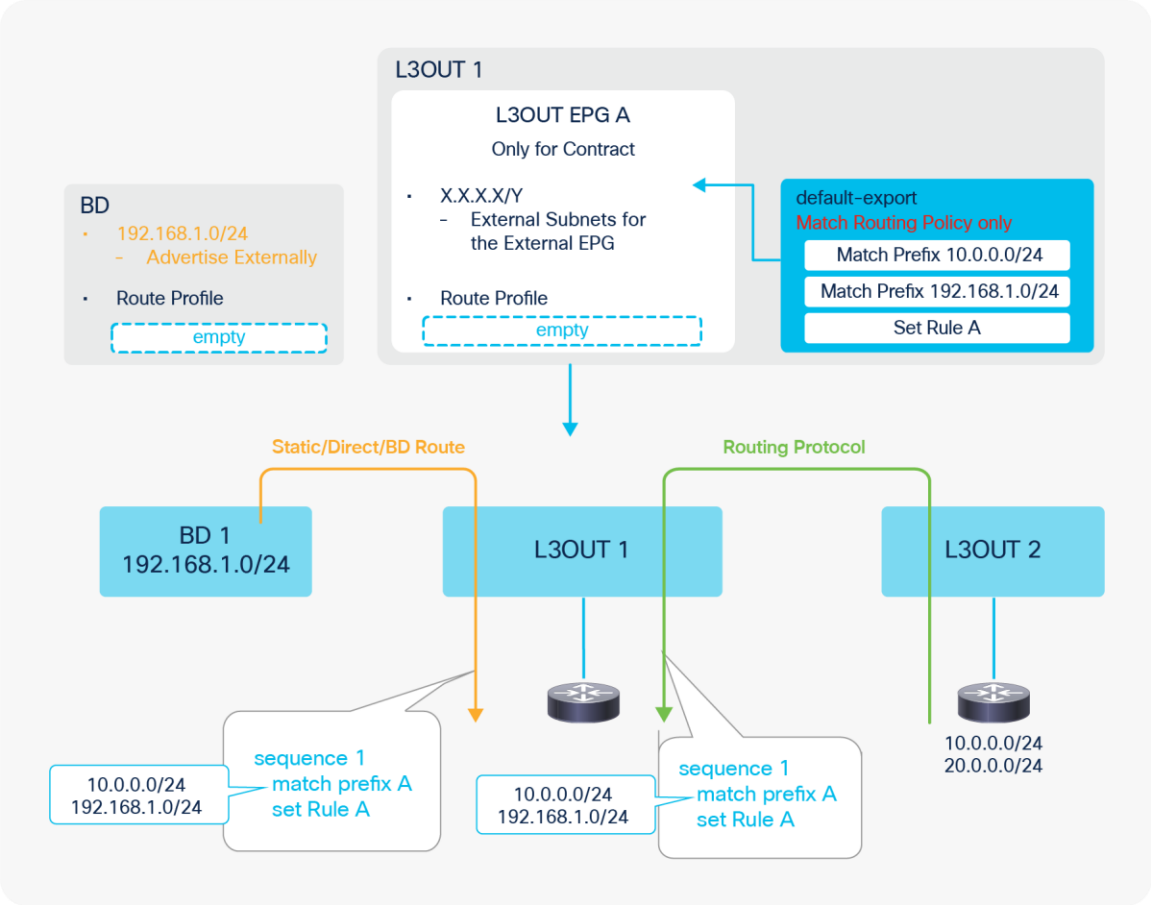

Figure 115.

BD 서브넷과 전송 라우팅에 대한 기본 내보내기

Figure 115 는 "라우팅 정책만 매치" 유형이 포함된 **기본 내보내기** 경로 프로필이 L3Out 의 서브넷 보급 구성을 단순화하는 방법에 관한 예시입니다. 이전 섹션에서 언급한 바와 같이 "라우팅 정책만 매치" 유형이 포함된 **기본 내보내기**는 "경로 제어 서브넷 내보내기" 범위 등의 다른 서브넷 보급 구성을 비롯해 L3Out 과 BD 의 연결을 무시합니다. 이후 **기본 내보내기**는 다른 구성과 병합하지 않고 고정/직접/BD 서브넷에 대한 내부 경로 맵(Figure 의 주황색 화살표)과 라우팅 프로토콜의 경로(Figure 의 녹색 화살표)에 적용됩니다. 따라서 L3Out 의 서브넷 보급에 대한 제어의 단일 소스로 사용될 수 있습니다. 이 예시에서 **기본 내보내기** 경로 프로필은 BD 서브넷(192.168.1.0/24) 및 L3Out 2 의 외부 경로 중 하나(10.0.0.0/24)로 구성됩니다. L3Out 의 추가적인 구성이 없이 L3Out 은 이들 경로를 외부에 보급합니다. BD 서브넷의 "외부로 보급" 범위는 여전히 필요하다는 점에 유의해야 합니다. 규칙 설정을 해당 경로에 적용해야 하는 경우에는 Figure 에서와 같이 동일한 경로 프로필(**기본 내보내기**)에 규칙 설정을 추가하여 간편하게 적용할 수 있습니다.

이러한 접근 방법을 통해 L3Out EPG 는 외부로 보급하는 경로와 반대로 L3Out 을 통해 학습된 서브넷에 대해 "외부 EPG 에 대한 외부 서브넷" 범위를 이용해 보안(Contract) 관리에 집중할 수 있습니다. L3Out 공유된 서비스(VRF 경로 유출)는 여전히 L3Out EPG 에서 구성되어야 합니다.

BD 서브넷을 보급하는 구성 옵션의 비교 사항은 "ACI BD 서브넷 보급" 섹션에서 확인할 수 있습니다.

BD 의 경로 프로필

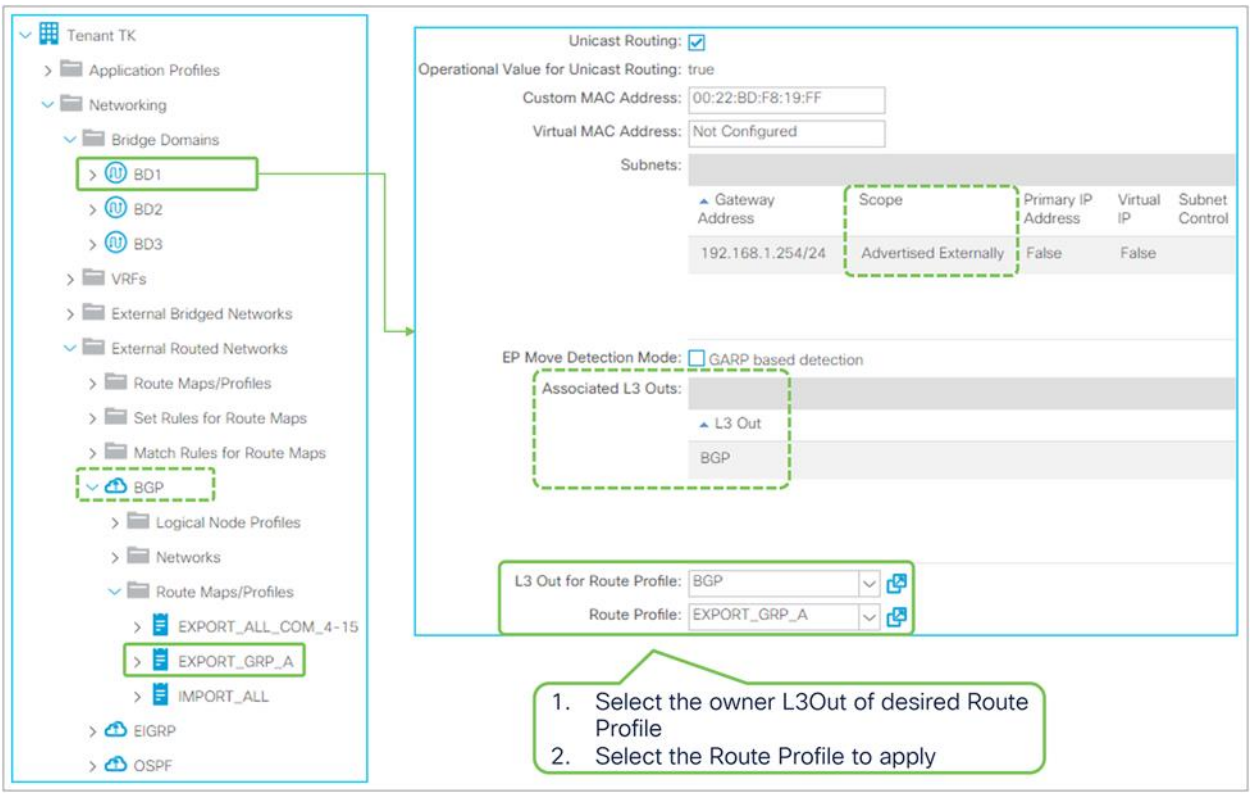

Figure 116.

GUI(APIC Release 3.2) 내 BD 의 경로 프로필

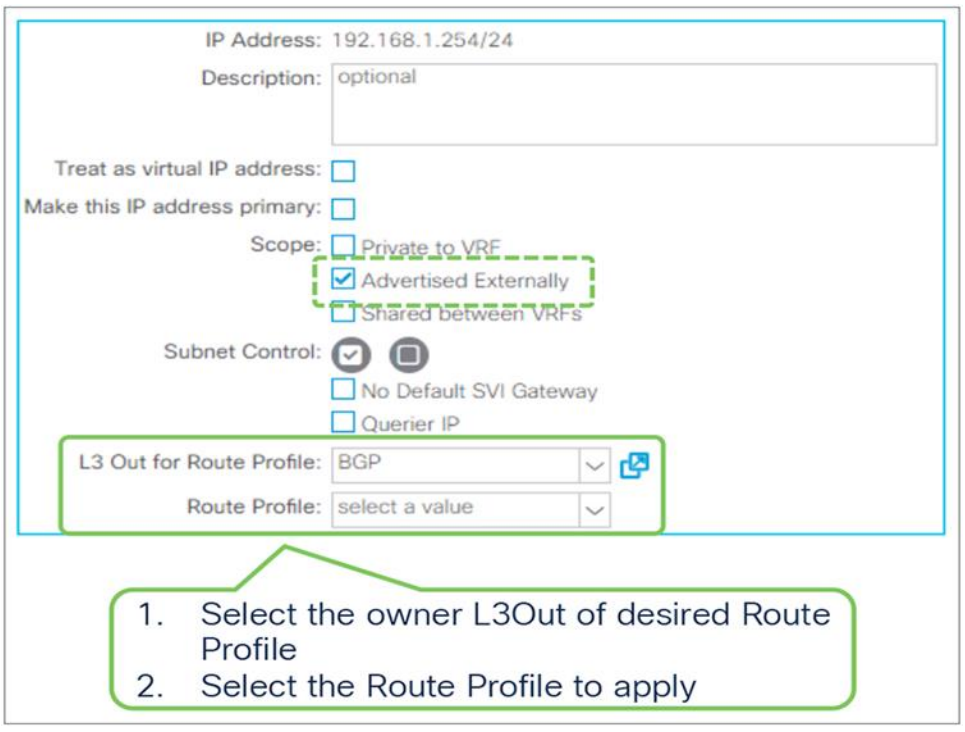

Figure 117.
GUI(APIC Release 3.2) 내 BD 서브넷의 경로 프로필

BD 에서는 경로 프로필을 사용해 내부 경로 맵에 규칙 매치 및 설정을 추가하는데, 이 경로 맵은 L3Out 라우팅 프로토콜에 BD 서브넷을 재배포하는 L3Out 과 BD 의 연결을 통해 BD 서브넷을 외부로 보급하는 데 사용됩니다. 이를 위한 내부 경로 맵에 대한 자세한 내용은 "ACI BD 서브넷 보급" 섹션을 참조하시기 바랍니다.

L3Out EPG 의 경로 프로필과 달리, BD 에는 방향이 없습니다. 한 개의 BD 가 여러 개의 L3Out 에 연결될 수도 있으므로 우선 적용될 경로 프로필을 보유한 L3Out 만 지정하면 됩니다.

참고:

L3Out EPG 에 있는 경로 프로필의 경로 프로필 유형에 대한 권장 사항은 BD 에도 적용됩니다. 명시적인 식별 번호 목록을 사용할 때는 "라우팅 정책만 매치" 유형을 사용하는 것이 좋습니다. 이 경우에는 "ACI BD 서브넷 보급" 섹션의 Figure 69 에 있는 시나리오 3 에 해당합니다.

Interleak 의 경로 프로필

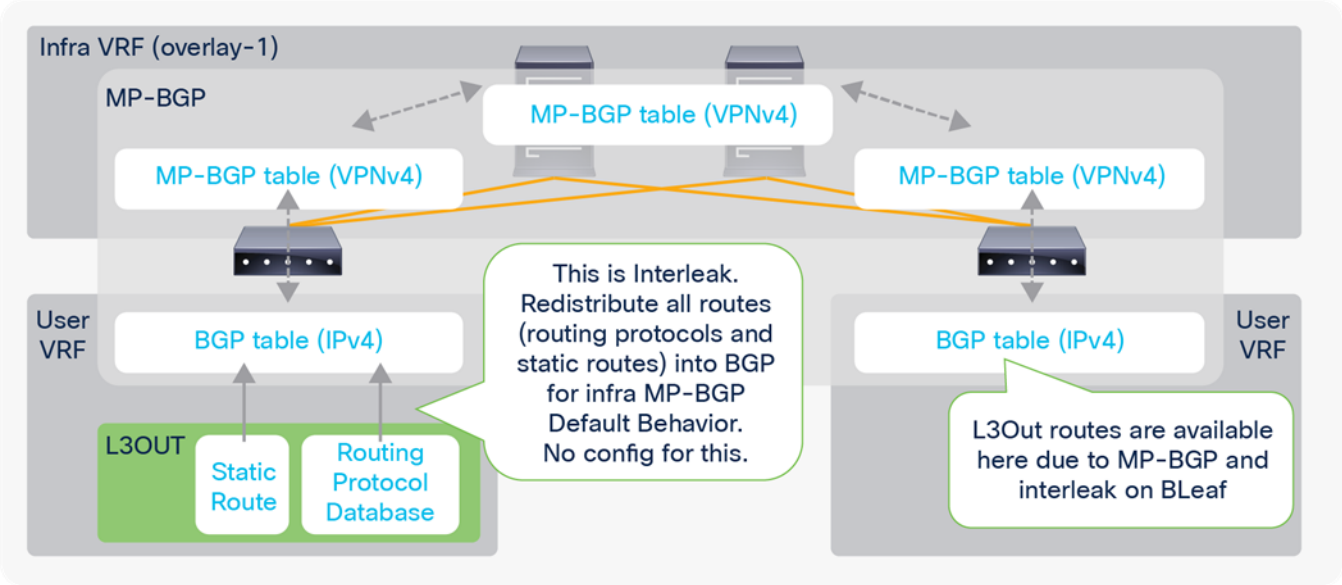

Figure 118.
ACI Interleak

"인프라 MP-BGP" 섹션에서 짧게 언급한 바와 같이 Interleak 는 Cisco ACI 의 최초 발매부터 제공된 L3Out 의 MP-BGP 를 위한 자동 내부 재배포입니다. 경로 프로필을 Interleak 에 적용하는 옵션은 APIC Release 1.2(2)에서 도입되었습니다. 이 옵션은 OSPF 와 EIGRP L3Out 에서 지원됩니다. BGP 테이블에 경로가 이미 존재하기 때문에 BGP L3Out 에는 Interleak 가 필요하지 않습니다. 경로 프로필을 고정 경로의 Interleak 에 적용하는 기능은 APIC Release 4.2(1)에서 도입되었습니다.

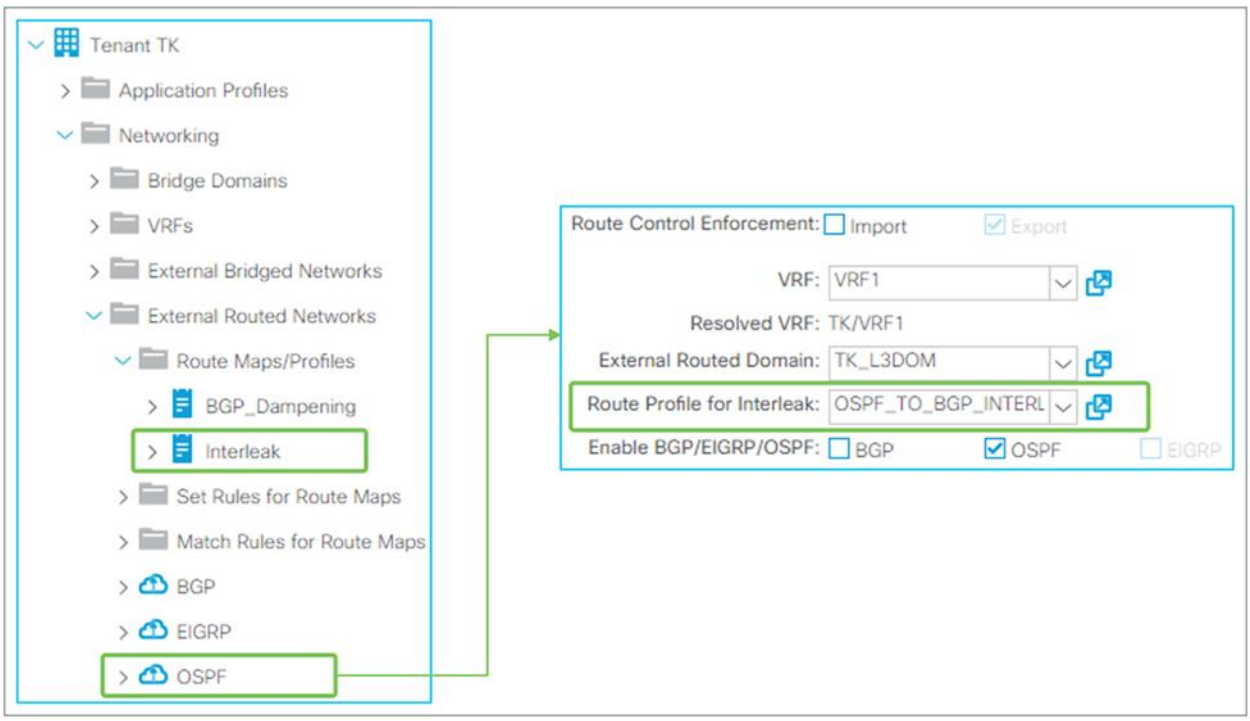

Figure 119.
GUI(APIC Release 3.2) 내 Interleak 에 대한 경로 프로필

Figure 119 에서와 같이 Interleak 의 경우, 경로 프로필이 L3Out 자체에 연결됩니다. Interleak 에 사용되는 경로 프로필은 L3Out 에 있는 경로 프로필이 아닌 테넌트 수준의 경로 프로필입니다.

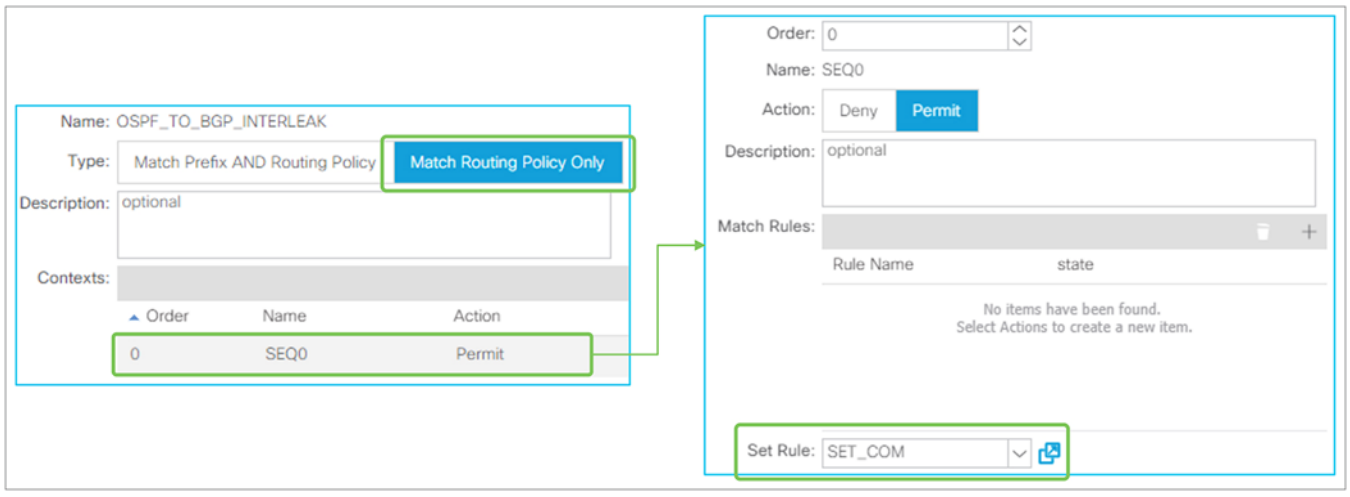

Figure 120.
Interleak 에 대한 경로 프로필 내용

Interleak 에 대한 경로 프로필은 "라우팅 정책만 매치" 유형을 사용해야 합니다. L3Out EPG 에 있는 경로 프로필의 사례와는 달리, 객체 내 참고 가능한 서브넷 정보가 없으므로 "식별 번호 AND 라우팅 정책 매치"를 사용할 의미가 없습니다. Interleak 에 대한 경로 프로필은 다른 보더 리프 스위치가 커뮤니티에 기반해 전송

라우팅을 선별적으로 수행할 수 있도록 인프라 MP-BGP 를 지나 다른 보더 리프 스위치로 전달되는 커뮤니티 규칙을 설정하도록 구성되어 있습니다.

Figure 121 은 L3Out 2 가 다른 두 개의 L3Out(1 및 3)에서 나온 동일한 외부 경로에 대해 각기 다른 행렬을 할당하는 Interleak 에 대한 경로 프로필 사용 사례에 대한 예시입니다.

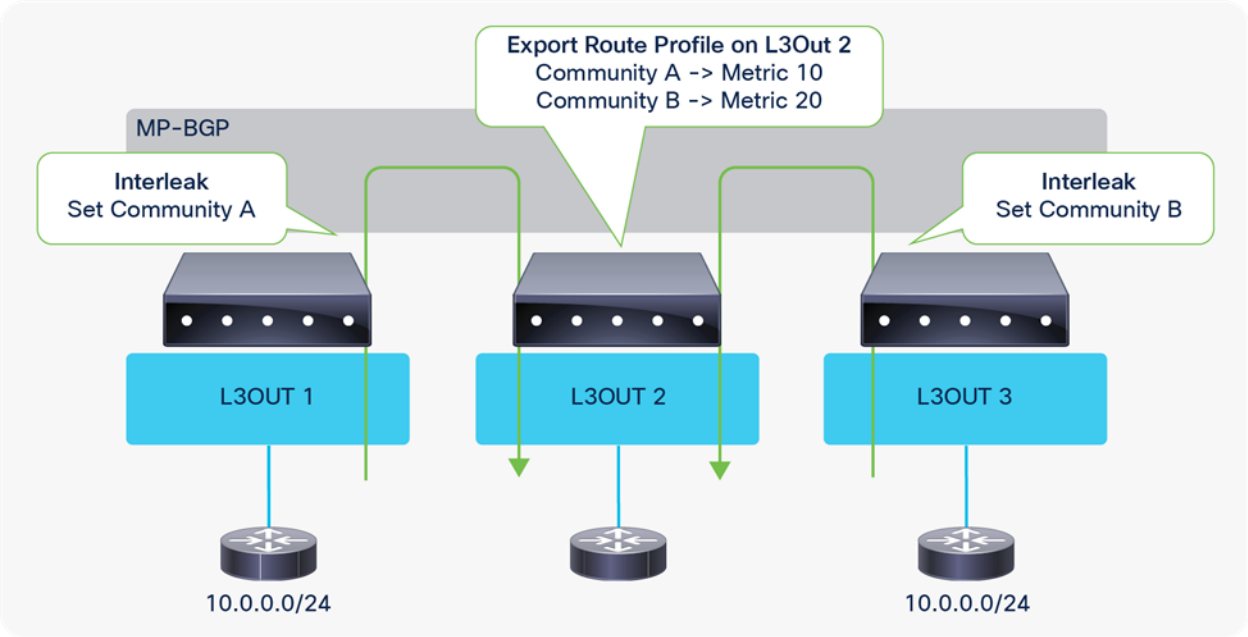

Figure 121.

Interleak 에 대한 경로 프로필 사용 사례

L3Out 공유된 서비스(VRF 경로 유출)

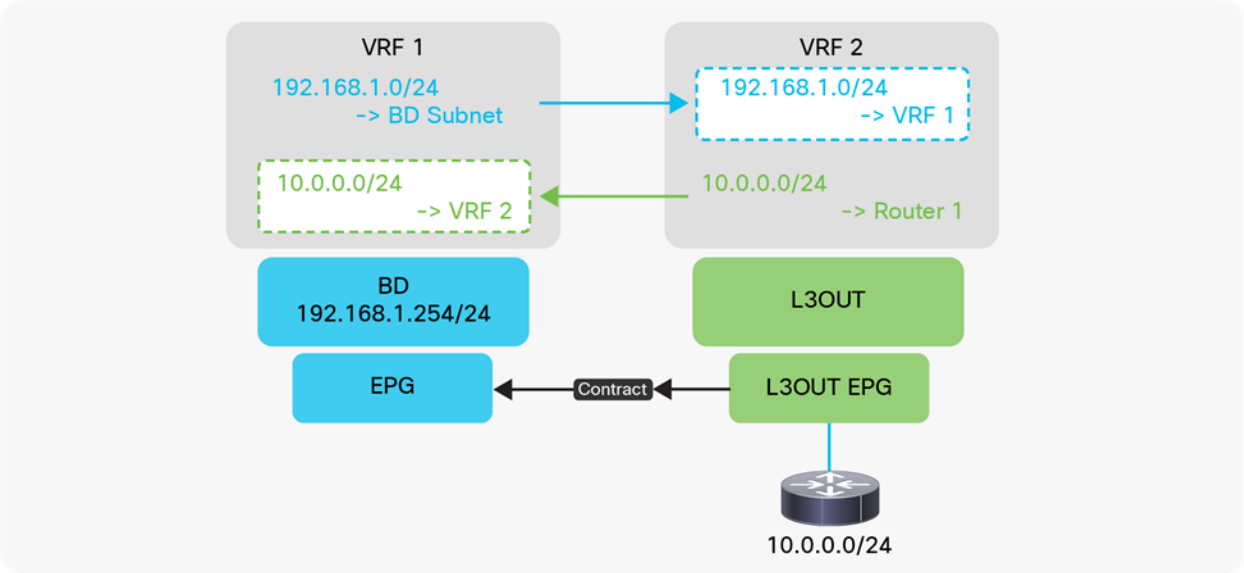

Figure 122.

L3Out 공유된 서비스(VRF 경로 유출)

L3Out 이 포함된 VRF 경로 유출은 APIC Release 1.2(1)에서 도입되었으며, 다른 VRF 에서 EPG 가 사용할 수 있도록 L3Out 을 통해 학습된 외부 경로를 다른 VRF 로 유출할 수 있게 해주는 기능입니다. 이 기능은 L3Out 의 뒤에서 다른 VRF 로 서비스를 공유하기 때문에 L3Out 공유된 서비스 또는 공유된 L3Out 이라고도 합니다. Figure 122 는 다른 VRF(VRF 1)에서 L3Out 이 EPG 로 서비스(10.0.0.0/24)를 제공하는 일반적인 사용 사례입니다. VRF 1 좌측의 EPG 는 VRF 2 의 외부 경로를 사용하는 VRF 1 의 또 다른 L3Out 이 될 수도 있는데, 이는 L3Out 전송 라우팅과 공유된 서비스의 결합입니다. ACI 기본 원칙 가이드의 "공유된 L3Out" 섹션에서 몇 가지 제한 사항을 참조하시기 바랍니다.

참고:

이 기능이 출시되기 전에 "공유된 서비스"라는 용어는 사용자 테넌트가 테넌트 일반의 구성 요소를 사용했다는 점을 암시했습니다. 예를 들어 VRF A 를 사용하고 테넌트 일반에서 테넌트 A 의 BD 에 대해 정의된 테넌트 A 가 있는 경우, 이를 통해 테넌트 A 의 엔드포인트가 테넌트 일반의 서비스(엔드포인트 또는 L3Out)로서 동일한 IP 공간(테넌트 일반 VRF A)에 속할 수 있습니다. 이 경우 모든 구성 요소가 하나의 VRF A 에 존재하기 때문에 상호 테넌트 통신에서 VRF 경로 유출이 불필요했습니다. 그러나 VRF 경로 유출이 출시된 후로 "공유된 서비스"는 테넌트 일반에서의 서비스 공유가 아닌 VRF 경로 유출을 암시하는 경향을 띄고 있습니다. VRF 경로 유출은 테넌트 내 또는 테넌트 간에 일어날 수 있습니다. 테넌트 일반을 사용하는 공유된 원본 서비스는 여전히 사용 가능한 설계이자 구성입니다.

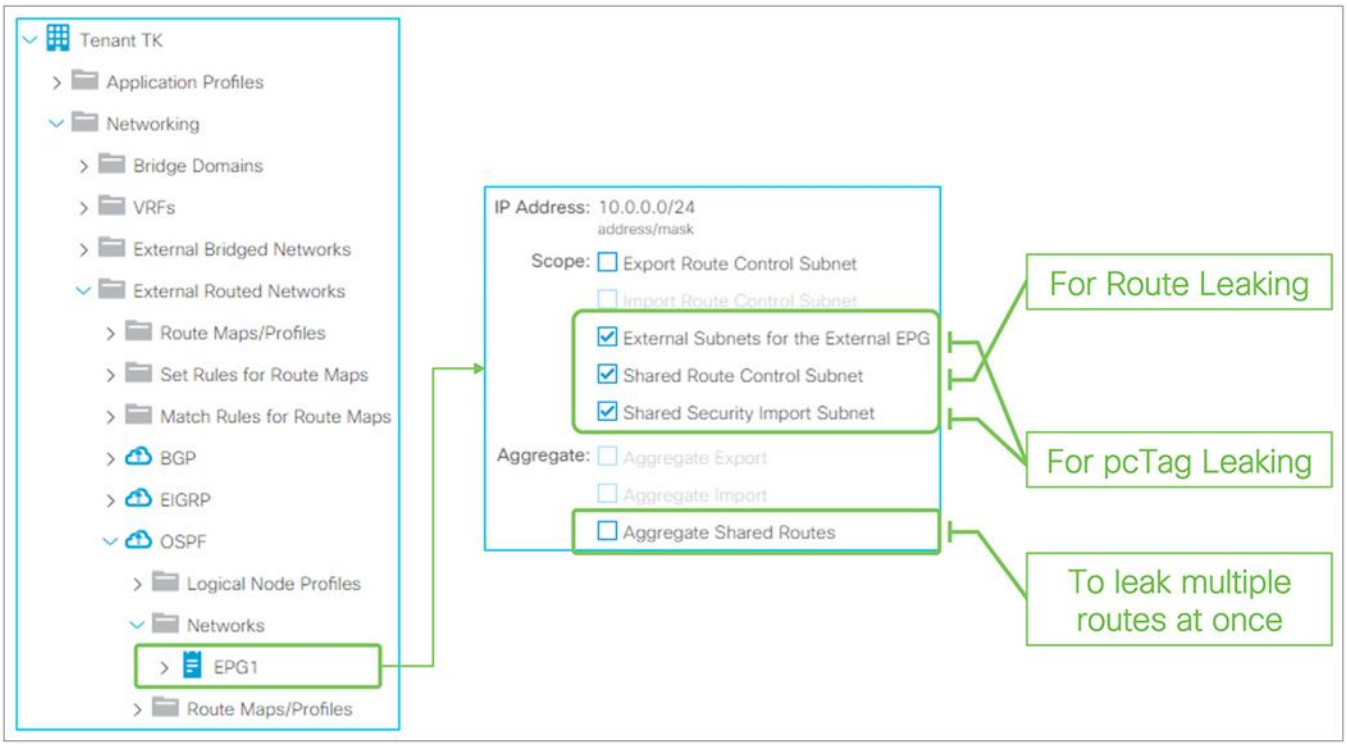

Figure 123.

GUI(APIC Release 3.2) 내 L3Out 서브넷 공유된 서비스

L3Out 공유된 서비스에 대해 두 개의 L3Out 서브넷 범위가 존재합니다.

- 공유된 경로 제어 서브넷: 라우팅 테이블의 경로를 다른 VRF 로 유출합니다.
- 공유된 보안 가져오기 서브넷: prefix-to-pcTag 매핑을 다른 VRF 로 유출하며, 이는 "외부 EPG 에 대한 외부 서브넷" 범위를 통해 사용해야 합니다.

기본 구성 예시

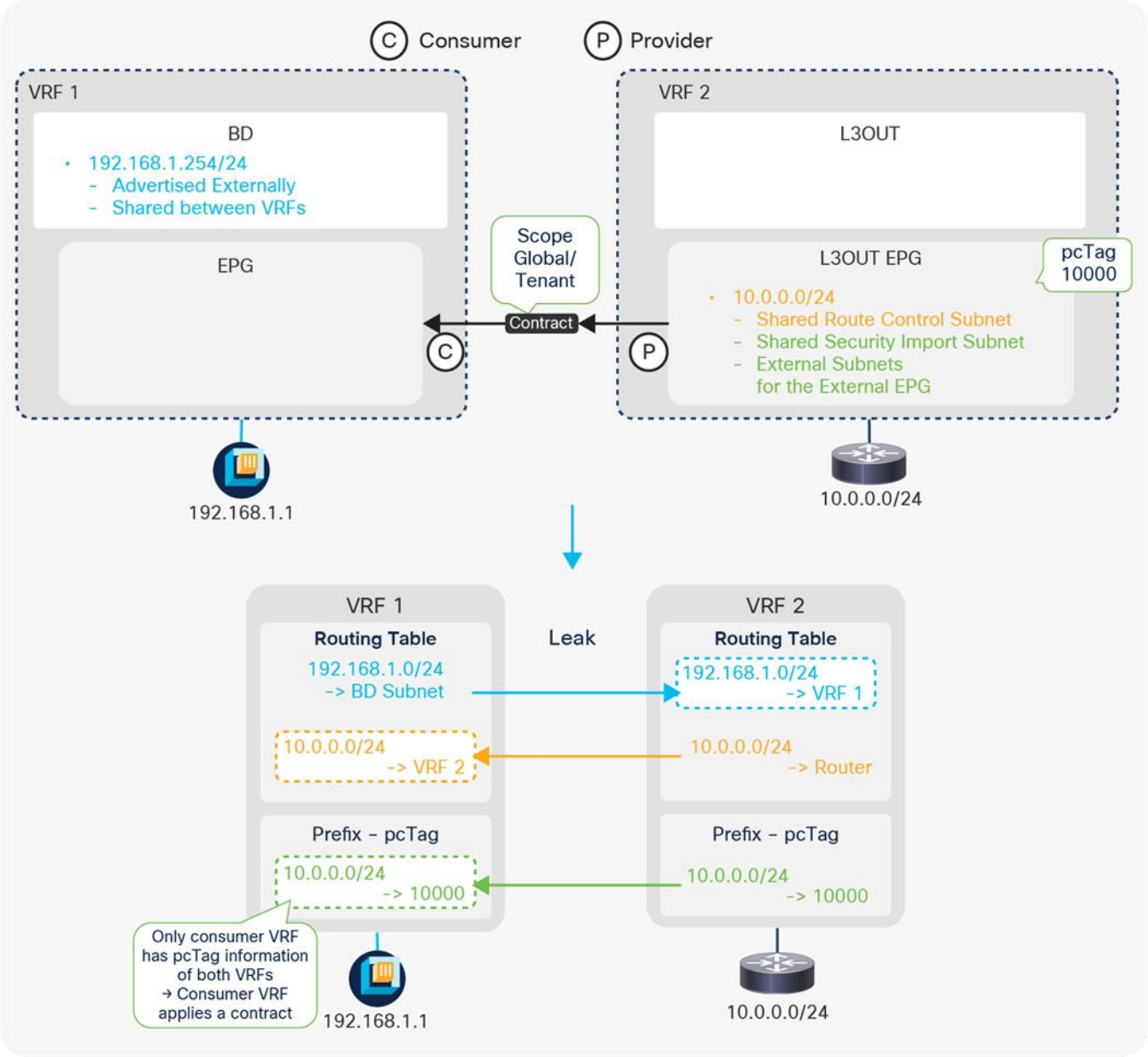

Figure 124.
공유된 L3Out 구성에 대한 예시 도표

Figure 124 는 L3Out 이 VRF 2 에서 VRF 1 의 엔드포인트로 서비스(서브넷 10.0.0.0/24)를 제공하는 공유된 기본 L3Out 구성을 나타냅니다. 앞서 언급한 바와 같이 공유된 L3Out 은 두 가지 부분으로 나뉘는데, 하나는 경로 유출, 다른 하나는 Contract 에 대한 prefix-pcTag 매핑 유출입니다.

경로 유출

일반적인 라우터와 마찬가지로 각 VRF 에서 라우팅 테이블 간에 경로를 유출합니다. 이를 수행하기 위한 세 가지 구성 요소는 다음과 같습니다.

- **"공유된 경로 제어 서브넷" 범위가 포함된 L3Out 서브넷**

  라우팅 테이블 내 유출할 외부 경로(또는 고정 경로)를 정의하며, Figure 124 에서 주황색으로 표시된 부분(VRF 2 의 10.0.0.0/24)입니다. 라우팅 테이블에 위치하지 않은 경로는 유출되지 않습니다.

- **"VRF 간 공유" 및 "외부로 보급됨" 범위가 포함된 BD 서브넷**

  유출할 BD 서브넷을 정의하며, Figure 124 에서 청색으로 표시된 부분(VRF 1 의 192.168.1.0/24)입니다. 경로를 다른 VRF 로 유출하는 범위는 "VRF 간 공유"입니다. 유출된 BD 서브넷이 VRF 2 에서 L3Out 을 통해 외부 라우터로 보급될 수 있도록 "외부로 보급됨" 범위도 필요합니다. 이 경우 L3Out 과 BD 의 연결 또는 Figure 69 에서 언급된 다른 BD 서브넷 보급 구성은 필요하지 않습니다.

- **L3Out EPG 및 BD 내 EPG 간 Contract**

  경로가 어느 VRF 간에 유출되어야 하는지를 정의하며, 주 목적인 Contract 외에도 트래픽을 허용합니다. 두 개의 VRF 가 각기 다른 테넌트에 위치할 때는 Contract 의 범위가 **글로벌**이어야 하며, 동일한 테넌트에 위치할 때는 **테넌트**가 되어야 합니다. L3Out EPG 는 애플리케이션 프로필의 부분이 아니므로 여기서 **애플리케이션 프로필** 범위는 적용되지 않습니다.

Prefix-pcTag(Contract) 유출

prefix-pcTag 매핑을 유출합니다. 기본값으로 pcTag 는 VRF 내에서만 고유하며, Figure 124 의 예시와 같이 VRF 1 의 EPG 와 VRF 2 의 L3Out EPG 는 동일한 pcTag 를 사용할 수 있습니다. 따라서 ACI 에는 일명 글로벌 pcTag 라는 개념이 있으며, 이는 ACI 패브릭 내 모든 VRF 에서 고유합니다. 공유된 L3Out 에는 전체 VRF 에서 Contract 에 대한 이 글로벌 pcTag 를 활용하는 두 가지 요소가 있습니다.

- **"공유된 보안 가져오기 서브넷" 범위가 포함된 L3Out 서브넷**

  유출할 prefix-pcTag 매핑을 정의합니다. 따라서 L3Out 서브넷은 처음부터 prefix-pcTag 매핑을 생성하기 위해 반드시 "외부 EPG 에 대한 외부 서브넷" 범위로도 구성되어야 합니다. Figure 124 에서 녹색으로 표시된 부분(pcTag 10000 으로 10.0.0.0/24)입니다. prefix-pcTag 매핑에 대한 자세한 내용은 "L3Out Contract" 섹션을 참조하시기 바랍니다.

- **L3Out EPG 및 BD 내 EPG 간 Contract**

  prefix-pcTag 매핑이 유출되어야 하는 대상 VRF 와 글로벌 pcTag 를 사용해야 하는 EPG 를 정의합니다. "글로벌" 또는 "테넌트" 범위로 Contract 가 사용되고 VRF 전반에 제공되면 공급자 EPG 의 pcTag 는 글로벌 pcTag 로 변경됩니다. Figure 124 의 예시에서 글로벌 pcTag 가 VRF 2 의 L3Out EPG 에 할당되어 있습니다. 이 글로벌 pcTag 는 VRF 2 에서 prefix-pcTag 매핑을 생성하는 데 사용되며 "공유된 보안 가져오기 서브넷" 범위로 인해 VRF 1 로 유출됩니다.

  이는 Contract 가 사용자와 공급자를 위한 pcTag 정보를 보유한 사용자 VRF 측에 항상 적용된다는 점을 의미합니다. 공급자 측면(Figure 124 의 VRF 2)에서는 사용자 VRF 에 있는 엔드포인트의 pcTag(EPG)가

인식되지 않으며, 사용자가 처리할 것이라고 가정하여 유출된 트래픽을 항상 허용하게 됩니다. Figure 124 의 예시에는 엔드포인트 192.168.1.1 에 대한 prefix-pcTag 매핑 테이블 항목이 존재하지 않는데, 그 이유는 prefix-pcTag 매핑 테이블이 L3Out 외부 경로에만 사용되며 엔드포인트가 엔드포인트 테이블을 사용하기 때문입니다.

Figure 125 에는 이 기본적인 예시의 GUI 구성이 요약되어 있습니다.

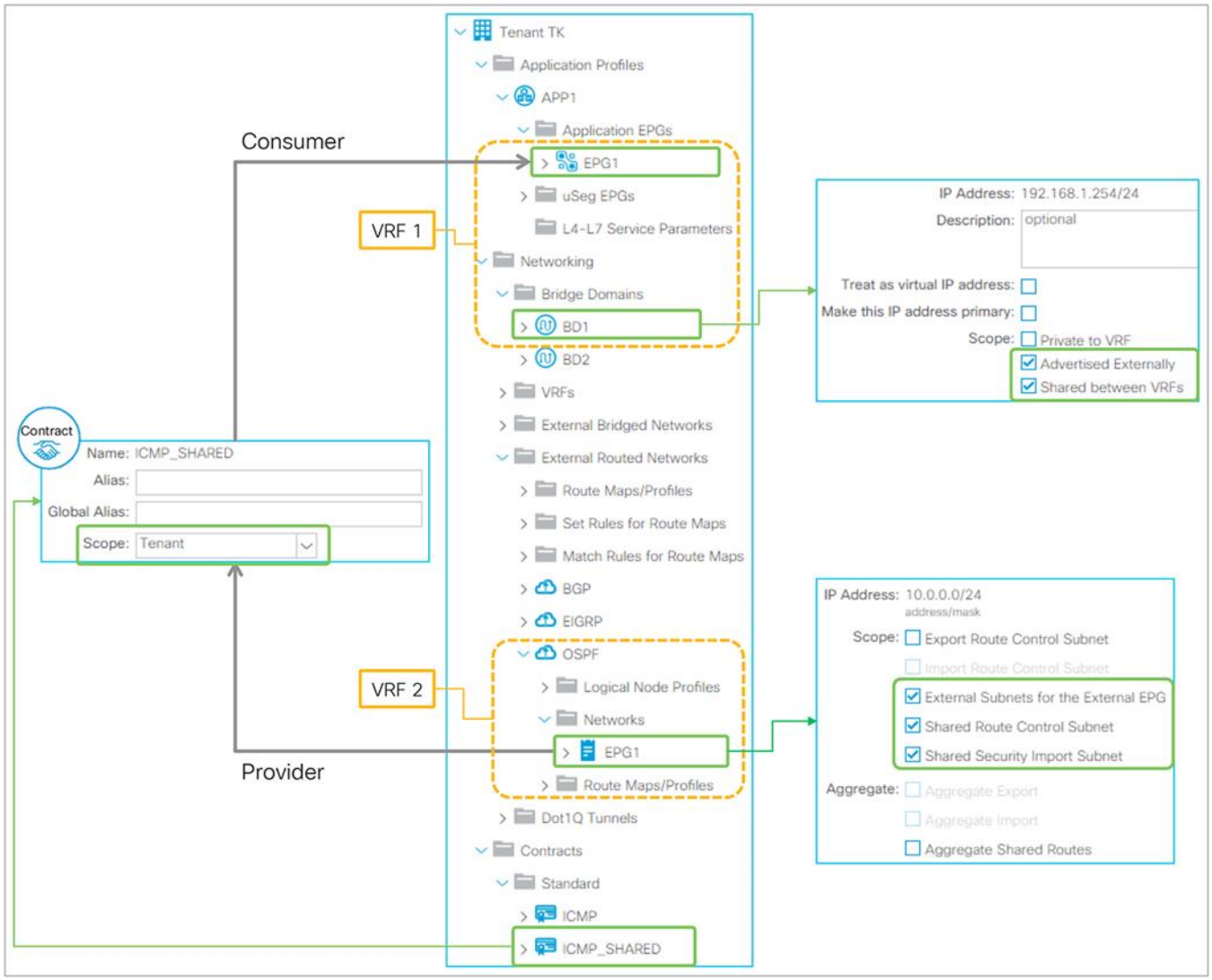

Figure 125.

GUI(APIC Release 3.2) 내 공유된 L3Out 의 구성 예시

참고:

글로벌 pcTag 는 0x4000(16384) 미만의 숫자를 사용하지만 일반 pcTag 는 이것보다 큰 숫자를 사용합니다. 확장성을 위해 다수의 VRF 에서 동일한 번호가 재사용 될 수 있도록 일반 pcTag 의 범위가 각 VRF 마다 적용됩니다. 기존 EPG 의 Contract 로 인해 일반 pcTag 가 글로벌 pcTag 로 변경될 경우, 새로운 글로벌 pcTag 가 있는 스위치의 모든 Contract 규칙을 재작성하는 과정에서 트래픽이 다소 정체될 수 있습니다.

공유된 L3Out 서브넷 범위

"공유된 경로 제어 서브넷" 및 "공유된 보안 가져오기 서브넷"

"공유된 경로 제어 서브넷"과 "공유된 보안 가져오기 서브넷" 범위는 일반적으로 동일한 L3Out 서브넷 항목에서 구성됩니다. 그러나 유출된 서브넷의 하위 집합에 다른 Contract 를 적용해야 할 경우에 대비해 사용자는 "공유된 경로 제어 서브넷"보다 좀 더 세부적인 "공유된 보안 가져오기 서브넷" 범위를 구성할 수 있습니다. 예를 들어 다음 구성은 라우팅 테이블에서 다른 VRF 로 10.0.0.0/8 을 유출하는 데 사용되지만, 각기 다른 Contract 가 각 식별 번호에 적용될 수 있도록 prefix-pcTag 매핑이 10.1.0.0/16 과 10.2.0.0/16 에 대해 각각 생성됩니다.

- "공유된 경로 제어 서브넷" 범위가 포함된 10.0.0.0/8
- "공유된 보안 가져오기 서브넷" 범위(및 "외부 EPG 에 대한 외부 서브넷" 범위)가 포함된 10.1.0.0/16 과 10.2.0.0/16

그러나 이 예시의 10.0.0.0/4 와 같이 "공유된 보안 가져오기 서브넷" 범위는 "공유된 경로 제어 서브넷" 범위보다 덜 상세할 수 없습니다.

"공유된 경로 집계"

이 범위는 "공유된 경로 제어 서브넷" 범위와 함께 사용됩니다. "경로 제어 서브넷 내보내기" 범위와 마찬가지로 "공유된 경로 제어 서브넷" 범위 역시 내부적으로 IP 식별 번호 목록을 사용하기 때문에 정확히 매치됩니다. "공유된 경로 집계" 범위가 "공유된 경로 제어 서브넷" 범위를 통해 활성화될 경우, 구성된 서브넷의 모든 하위 집합과 일치하는 IP 식별 번호 목록 항목에서 "le 32"를 추가합니다. "경로 제어 서브넷 내보내기" 범위와 달리, 공유된 경로에 대한 이 집계 옵션은 0.0.0.0/0 뿐만 아니라 0.0.0.0/0 이 아닌 서브넷에도 사용됩니다.

공유된 L3Out 구성 옵션

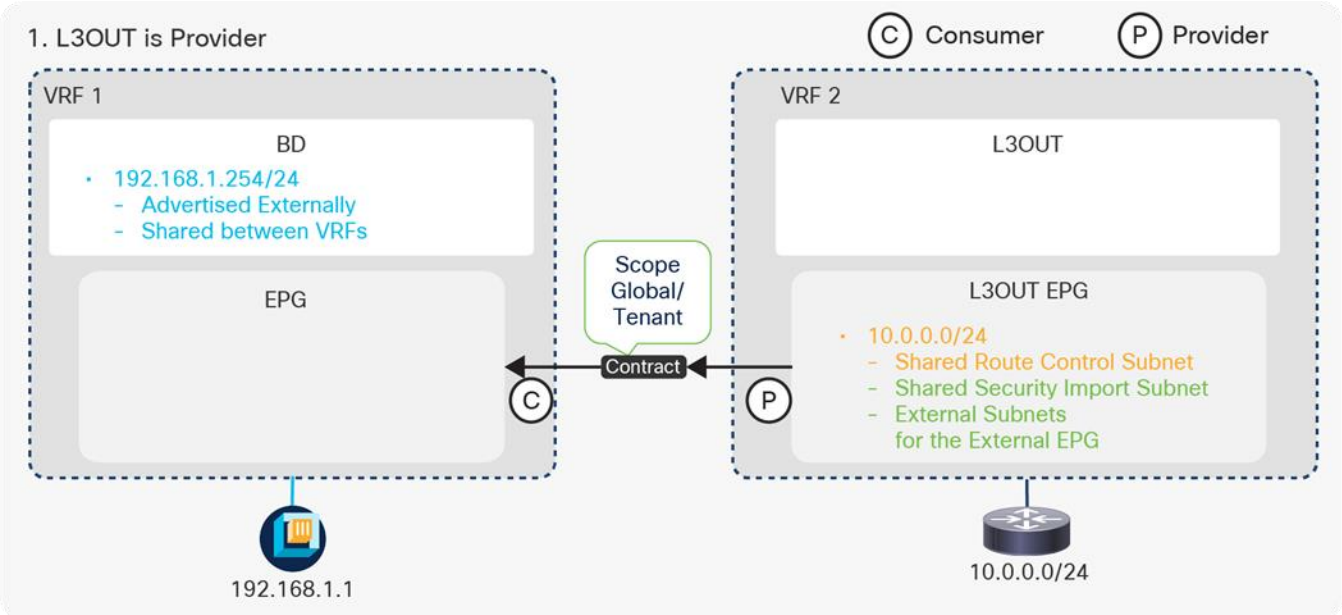

Figure 126.
공유된 L3Out 구성(1. L3Out 이 공급자)

첫 번째 옵션은 L3Out 을 공급자로 사용하는 방법으로, 위에서 설명한 것처럼 가장 기본적인 구성입니다. L3Out 이 공급자이고, EPG 가 사용자 역할을 합니다. 자세한 내용은 위 "기본 구성 예시"에서 확인할 수 있습니다.

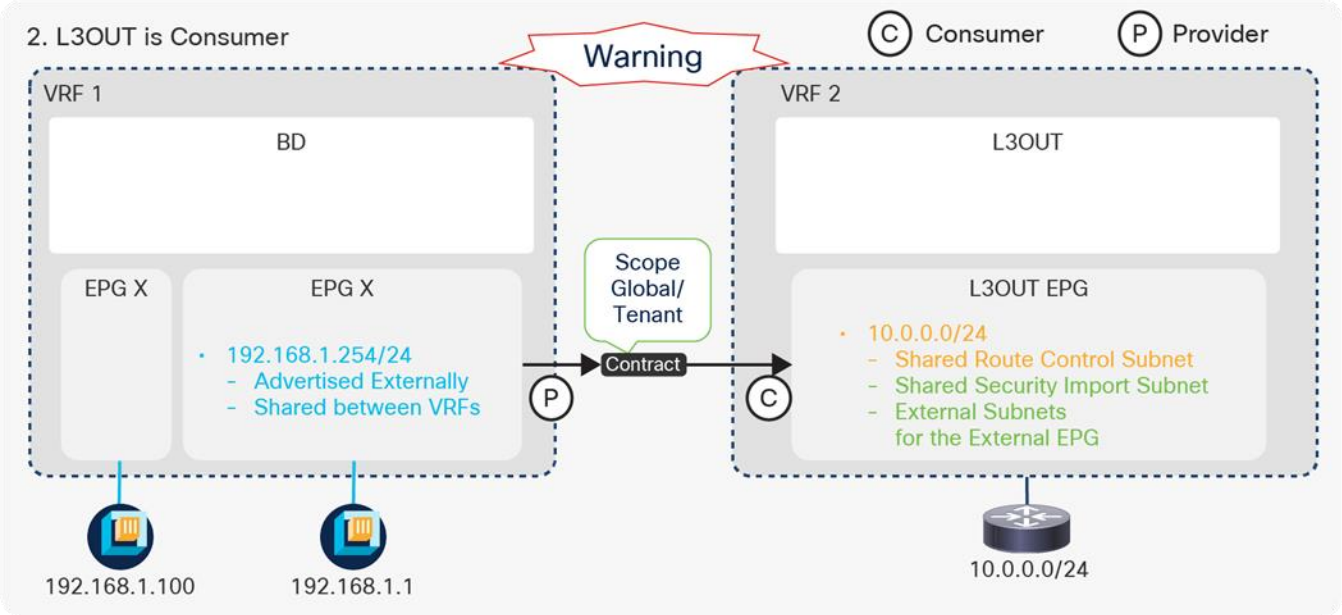

Figure 127.
공유된 L3Out 구성(2. L3Out 이 사용자)

또 다른 옵션은 L3Out 을 사용자로, EPG 를 공급자로 사용하는 방법입니다. 이 옵션을 사용하면 EPG 1 이 공급자이기 때문에 BD 서브넷이 EPG 1 에서 구성됩니다(일반 EPG 간 VRF 경로 유출에 대한 구성 가이드 참조). EPG 의 경우, 동일한 서브넷에 엔드포인트가 있지만 VRF 2 와의 Contract 는 포함되지 않습니다. 서브넷은 EPG 에서 구성되지만 BD SVI 로서 리프 스위치에 배포되고 동일한 BD 의 다른 EPG 역시 동일한 서브넷을 사용할 수 있다는 점에 유의해야 합니다. L3Out EPG 가 사용자인 구성에서는 pcTag 사용과 Contract 의 적용 방식으로 인해 경고가 포함됩니다. 이 설계를 이용하면 EPG 가 공급자이더라도 EPG 1 뿐만 아니라 L3Out EPG 도 글로벌 pcTag 를 사용하게 됩니다(EPG X 는 일반 pcTag 를 계속 사용). Contract 적용 방식에 대한 경고는 아래에서 설명합니다.

- 사용자와 공급자 VRF 모두 동일한 Contract 서 규칙을 갖게 되며, 이 Contract 는 수신 VRF 에 적용됩니다.
- 사용자 VRF(VRF 2)에서는 EPG 1 의 글로벌 pcTag 가 BD(EPG) 서브넷(192.168.1.0/24)에 연결됩니다. 이는 대상 IP 가 EPG 1 에 속하지 않더라도 VRF 2 의 L3Out EPG 에서 192.168.1.0/24 서브넷의 IP 로 전달되는 트래픽이 VRF 2 에서 허용된다는 의미입니다. 예를 들어 EPG 1 이 아닌 EPG X 에 속하는 192.168.1.100 패킷이 VRF 2 에 입력될 때, ACI 는 유출된 서브넷 192.168.1.0/24 를 토대로 pcTag 를 수신하게 됩니다. 이 pcTag 는 공유된 L3Out 에 대한 Contract 를 보유한 EPG 1 의 유출된

pcTag 입니다. 이후 패킷 대상이 유출된 EPG 에 속하지 않더라도 VRF 2 는 유출된 pcTag 를 사용하는 패킷을 허용합니다.

이러한 문제를 방지하려면 전체 BD 서브넷이 아닌 EPG 1 의 IP 주소만 포함된 더 작은 크기의 서브넷을 구성하는 것이 좋습니다. BD SVI 에서 2 차 IP 주소가 불필요하게 생기는 것을 방지하기 위해 이렇게 더 작은 크기의 EPG 서브넷에는 "기본 SVI 게이트웨이 없음"을 활성화해야 합니다. Figure 128 은 더 작은 EPG 서브넷에 대한 예시입니다. 이 경우 BD 가 EPG X 와 같이 EPG 에 대한 퍼베이시브 게이트웨이를 계속 제공할 수 있도록 BD 서브넷 192.168.1.254/24 를 "외부로 보급됨" 및 "VRF 간 공유" 범위 없이 BD 에서 구성해야 합니다.

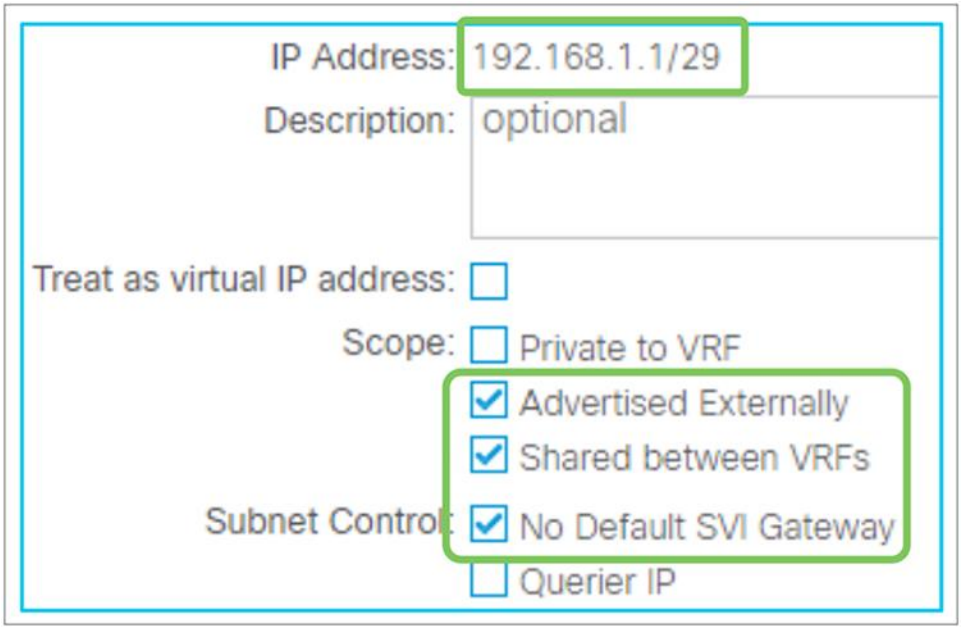

Figure 128.
기본 SVI 게이트웨이 없음이 포함된 EPG 의 더 작은 서브넷

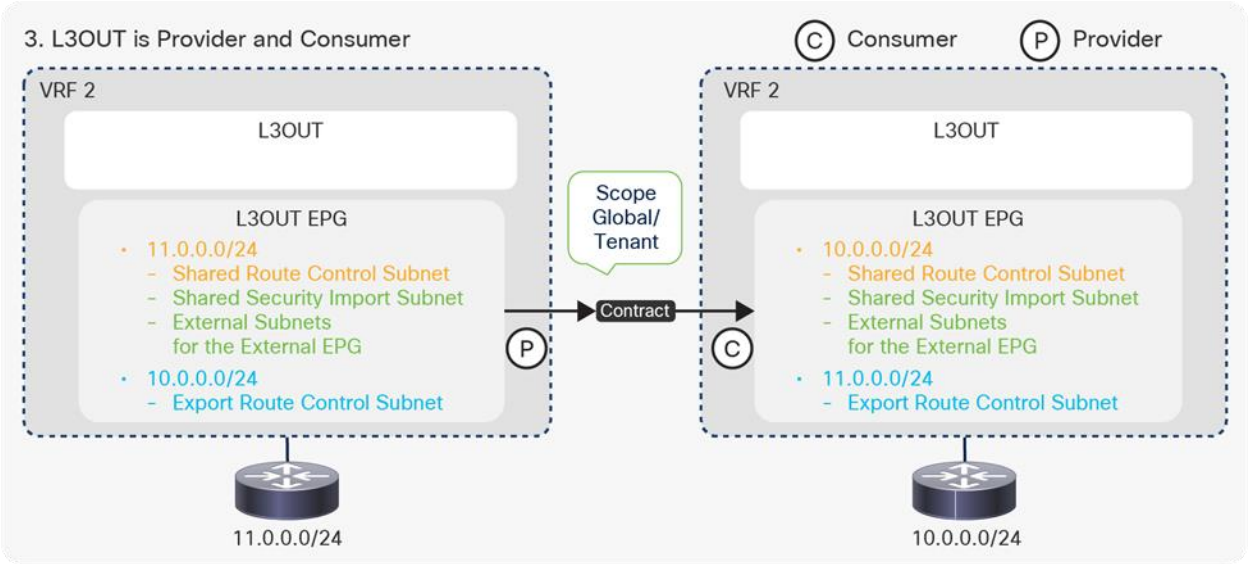

Figure 129.
공유된 L3Out 구성(3. L3Out 이 공급자겸 사용자, 전송 라우팅)

세 번째 옵션은 각기 다른 VRF 간에 전송 라우팅을 구성하는 방식입니다. 이는 전송 라우팅과 결합된 공유 서비스 설계로, APIC Release 2.2(2)부터 지원됩니다. 통신을 완수하기 위해서는 유출된 경로가 외부에 보급될 수 있도록 일반 전송 라우팅 구성("경로 제어 서브넷 내보내기" 범위 또는 유출된 경로용 **기본 내보내기** 등의 경로 프로필)도 각 VRF 에서 구성해야 합니다.

공유된 L3Out 구성 고급 옵션

고급 구성 1(L3Out EPG 분리)

Figure 130 은 VRF 간에 외부 경로의 하위 집합만 액세스할 수 있는 잘못된 구성에 관한 예시입니다. 이 예시의 경우 요구사항은 다음과 같습니다.

- VRF 2 에 L3Out(10.0.0.0/24)과 EPG(172.16.1.1) 간 VRF 내 통신이 존재할 것
- L3Out 경로(10.0.0.128/25)의 절반만 VRF 사이에서 통신이 가능할 것

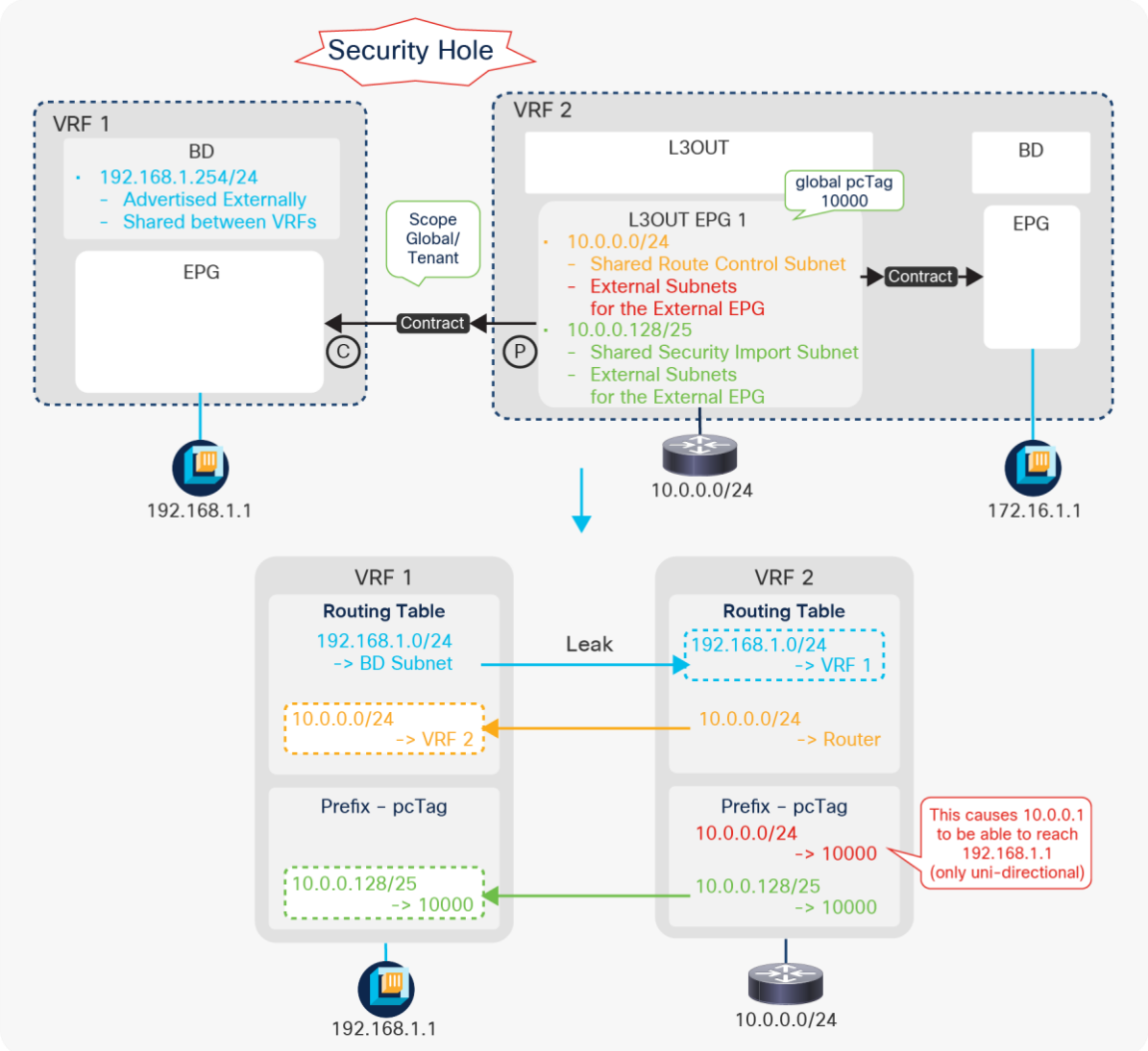

Figure 130.

공유된 L3Out 고급 구성 1(잘못된 예시)

"공유된 보안 가져오기 서브넷" 범위가 10.0.0.128/25 에 대해서만 구성됨에도 불구하고 10.0.0.128/25 뿐만 아니라 VRF 2 의 10.0.0.0/24 전체도 VRF 1 의 192.168.1.1 에 도달할 수 있다는 문제점이 있습니다. 이는 10.0.0.0/24 가 동일한 L3Out EPG 에서 "외부 EPG 에 대한 외부 서브넷"으로 구성되기 때문입니다. 이로 인해 두 식별 번호(10.0.0.0/24 및 10.0.0.128/25)는 VRF 2 에서 한 개의 글로벌 pcTag 10000 으로 매핑됩니다. 패킷(원본 IP 10.0.0.1, 대상 IP 192.168.1.1)이 VRF 2 의 L3Out 에서 도착할 때, 수신 공급자 VRF(VRF 2)는 원본 IP 10.0.0.1 을 글로벌 pcTag 10000 으로 분류합니다. 따라서 사용자 VRF(VRF 1)는 IP 10.0.0.1(10.0.0.128/25 이외 범위)에 대한 prefix-pcTag 매핑을 인식하지 못하지만, 패킷이 Contract 를 적용할 사용자인 VRF 1 에 도달할 때 패킷의 원본은 VRF 2 에 의해 글로벌 pcTag 10000 으로 이미 분류됩니다. 10.0.0.1 은 10.0.0.128/25 범위 밖이지만 10.0.0.128/25 에 대한 Contract 가 pcTag 10000 을 기준으로 적용되며, 패킷이 대상 192.168.1.1 로 송신되도록 허용합니다. 이는 공급자에서 사용자로 향하는 방향에만 적용됩니다. 반대 방향(192.168.1.1 에서 10.0.0.1 로)은 사용자 VRF(VRF 1)에서 삭제됩니다.

VRF 사이에서 의도치 않은 트래픽 허용을 방지하기 위해 Figure 131 과 같이 구성을 변경해야 합니다.

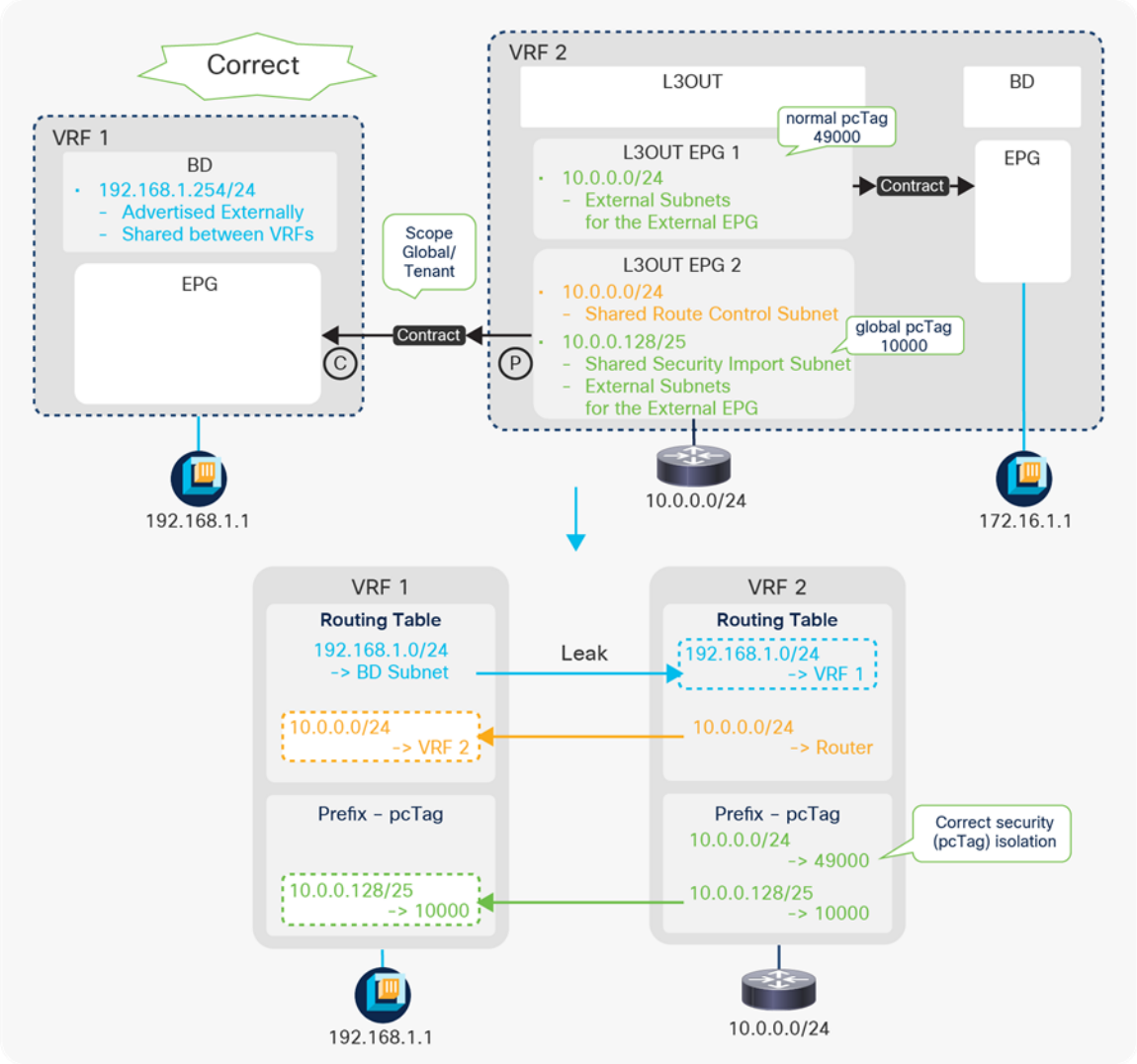

Figure 131.

공유된 L3Out 고급 구성 1(올바른 예시)

Figure 131 에서 구성은 VRF 내 통신(10.0.0.0/24)에 대해 각기 다른 L3Out EPG 를 사용합니다. 이에 따라 패킷(원본 IP 10.0.0.1, 대상 IP 192.168.1.1)이 VRF 2 의 L3Out 에서 도착할 때, 수신 공급자 VRF(VRF 2)는 원본 IP 10.0.0.1 을 일반 pcTag 49000 으로 분류합니다. 그 이유는 일반 pcTag(L3Out EPG 1)에 대한 경로 유출 구성이 없기 때문입니다. 이에 따라 10.0.0.128/25 만 VRF 사이에서 이동할 수 있게 됩니다.

고급 구성 2(다수의 VRF 와 BD 및 공유된 L3Out)

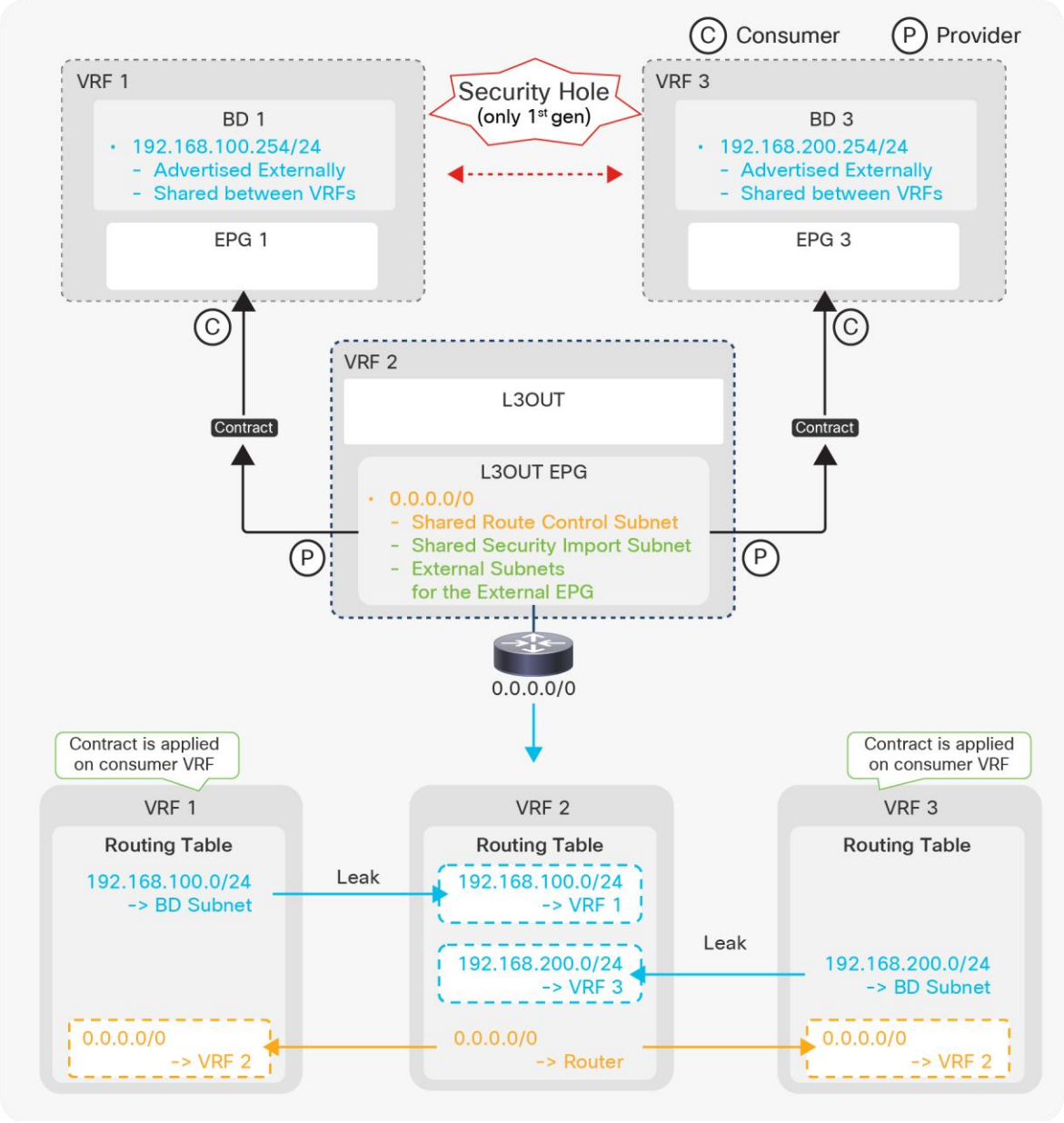

Figure 132.

공유된 L3Out 고급 구성 2(다수의 VRF 와 BD 및 공유된 L3Out)

Figure 132 는 VRF 2 내 한 개의 L3Out 이 VRF 1 과 VRF 3 에서 기본 경로를 EPG 로 공유(유출)하는 구성을 나타냅니다. 이 구성은 유효합니다. VRF 1 과 3 의 EPG 는 Contract 에 기반해 VRF 2 에서 L3Out 뒤의 장치와 통신할 수 있습니다. 그러나 사용자는 1 세대 리프 스위치에서 이 구성에 따른 보안 문제를 인지해야 합니다. 1 세대 리프 스위치가 포함된 이 구성으로 인해 VRF 1 의 EPG 1 과 VRF 3 의 EPG 3 은 VRF 2 를 통해 상호 통신할 수 있습니다. 공유된 서비스(VRF 경로 유출)에서는 공급자 VRF 가 공유한 글로벌 pcTag 를 통해 사용자 VRF 에서 Contract 가 적용됩니다. 이 예시에서는 Contract 가 VRF 1 또는 VRF 3 에 적용됩니다. VRF 1 의 EPG 1 이 192.168.200.1(VRF 3 의 EPG 3)과 통신을 시도할 때, VRF 2 에 의해 유출된 기본 경로에 속하게 되고 기본 경로에 대한 Contract 가 적용됩니다. 따라서 수신 사용자 VRF 1 에서 이 패킷이 허용되며 이후에는 더 많은 Contract 를 적용하지 않고 VRF 3 에 도달하기 위해 각 VRF 의 라우팅 테이블을 따르게 됩니다. 1 세대 리프 스위치에서 일어나는 이러한 문제를 방지하기 위해 VRF 2 의 L3Out 은 다른 VRF 의 서브넷과 중복되지 않는 고유 경로만 유출해야 합니다. 이러한 보안 문제는 2 세대(또는 이후) 리프 스위치에서 해결되었습니다.

고급 구성 3(다수의 VRF 와 L3Out 및 공유된 L3Out)

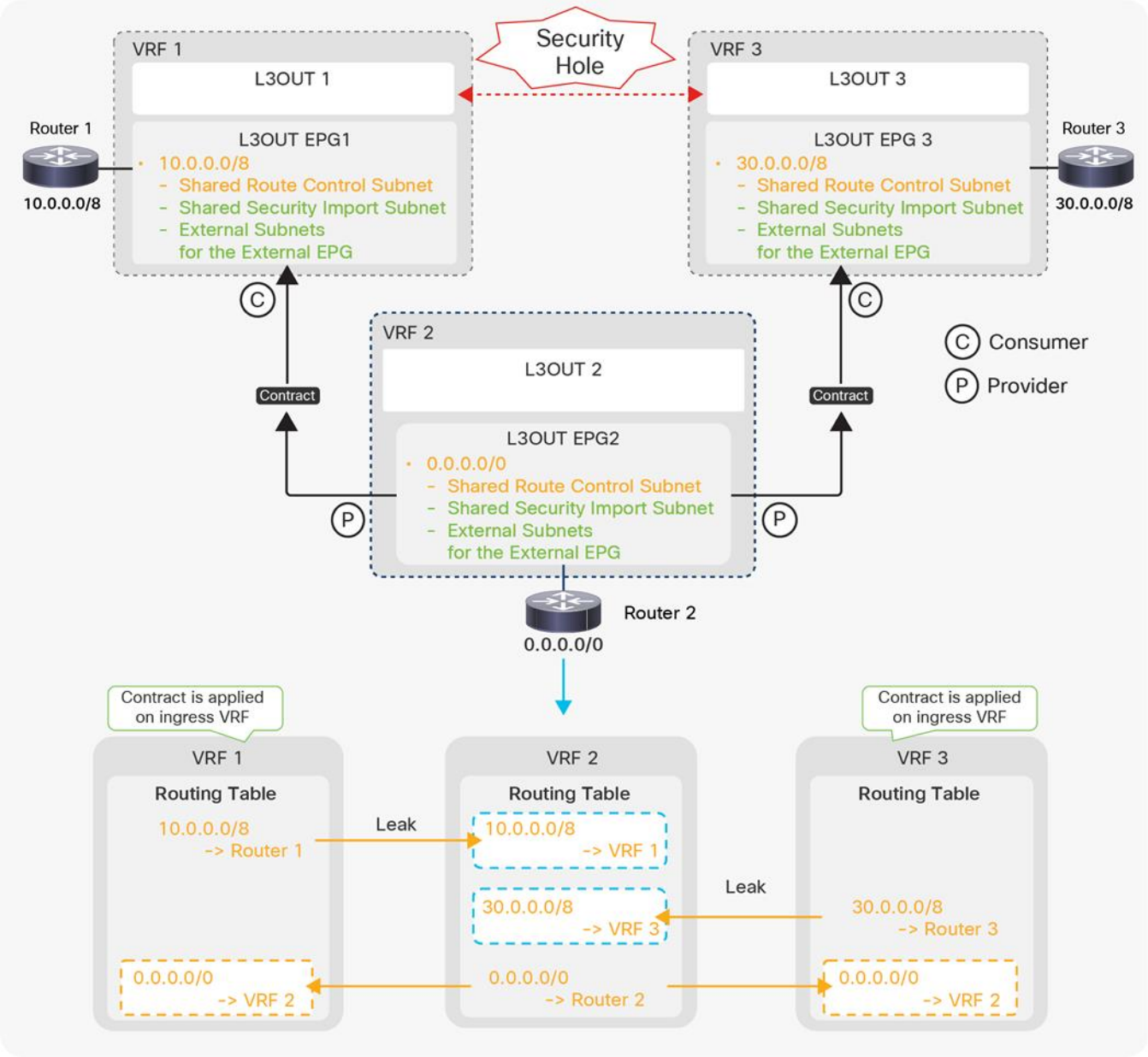

Figure 133.

공유된 L3Out 고급 구성 3(다수의 VRF 와 L3Out 및 공유된 L3Out)

Figure 133 은 VRF 2 내 한 개의 L3Out 이 VRF 1 과 VRF 3 으로 기본 경로를 공유(유출)하는 구성을 나타냅니다. 그 대신 VRF 2 는 VRF 1 과 3 의 L3Out 으로부터 외부 경로(10.0.0.0/8, 30.0.0.0/8)를 수신합니다. 이 구성은 리프의 세대 수와 관계없이 VRF 2 를 통해 L3Out 1(VRF 1)에서 L3Out 3(VRF 3)으로 트래픽을 허용할 수 있습니다. 2 세대 리프 스위치에서 원본 L3Out(VRF)이 중간 VRF 2 와 동일한 보더 리프에 위치한 경우, 트래픽은 VRF 3 로 재전송되지 않고 VRF 2 의 L3Out 2 를 통해 라우터 2 로 송신됩니다. 예를 들어 L3Out 1(VRF 1)과 L3Out 2(VRF 2)가 동일한 보더 리프에 있는 경우 10.0.0.0/8(L3Out 1)에서 30.0.0.0/8(L3Out 3)로 전달된 트래픽은 VRF 3 의 L3Out 3 으로 재전송되지 않고 VRF 2 의 라우터 2 로 송신됩니다. 즉, 세 개의 L3Out 이 모두 동일한 보더 리프에 위치한다면 이러한 보안 문제를 방지할 수 있습니다. 세 개의 L3Out 이 서로 다른 리프 스위치에 배포되는 경우 VRF 2 는 다른 VRF 와 중복되지 않는 고유한 경로만 유출해야 합니다. 이 문제는 다음을 통해 해결됩니다.

CSCvt06173 ACI: 공유된 L3OUt 이 중간 VRF 를 통해 트래픽을 허용

고급 구성 4(의도치 않은 유출 및 공유된 L3Out)

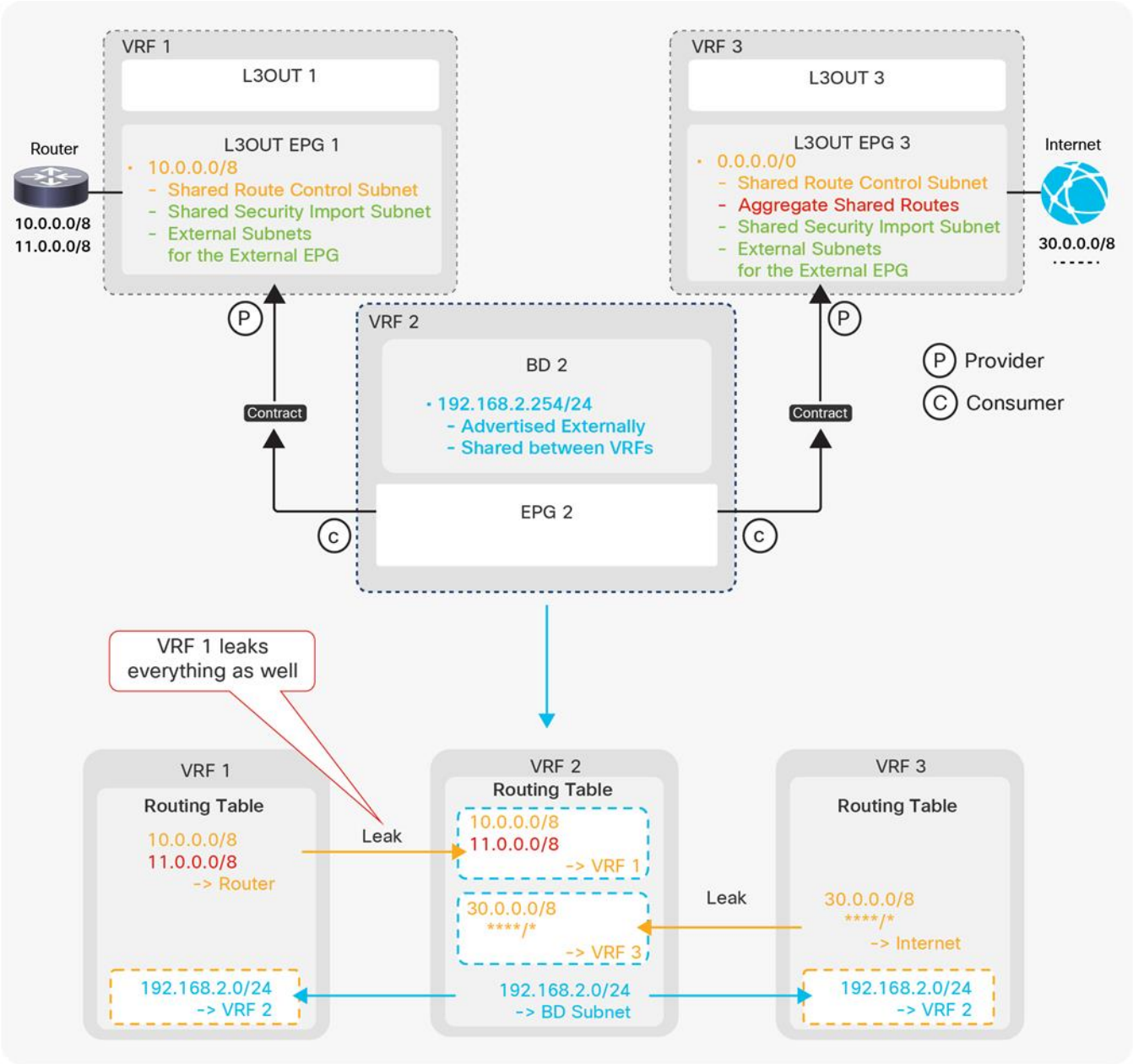

Figure 134.

공유된 L3Out 고급 구성 4(의도치 않은 유출 및 공유된 L3Out)

Figure 134 는 VRF 2 가 다수의 VRF 로부터 (공유 또는 유출된) 경로를 수신하는 구성을 나타냅니다. L3Out 1(VRF 1)이 11.0.0.0/8 없이 10.0.0.0/8 만 유출하고 L3Out 3(VRF 3)이 모든 경로를 VRF 2 에 유출하는 것이 목적입니다. 그러나 이 구성에서는 10.0.0.0/8 뿐만 아니라 L3Out 1(VRF 1)의 모든 경로가 VRF 2 로 유출됩니다. 이는 VRF 2 가 MP-BGP VPNv4 를 통해 다른 VRF 에서 경로를 가져올 때 오직 식별 번호만 확인하기 때문입니다. "인프라 MP-BGP" 섹션에서 언급된 바와 같이 경로 대상(RT)에 의해 식별되는 원본 VRF 는 확인하지 않습니다. 따라서 이 예시에서는 VRF 의 모든 경로가 L3Out 3 의 **공유된 집계 경로**로 인해 VRF 2 로 유출될 수 있습니다(MP-BGP 를 통해 가져옴). 이러한 현상은 L3Out 3 이 집계 옵션이 아닌 11.0.0.0/8 에 대한 **공유된 경로 제어 서브넷**을 통해 구성된 경우에도 발생합니다. 이는 각 VRF 내 공유된 L3Out 구성이 다른 VRF 와 중복되지 않고 고유한 외부 경로만 지정해야 한다는 의미입니다. 이러한 제한 조건은 다음과 같은 개선 기능을 통해 해결됩니다.

CSCvi20535 ACI: 공유된 L3Out 에 대해 공유된 경로 제어 범위를 VRF 가 인식해야 함

L3Out BFD

L3Out 인터페이스의 양방향 전환 탐지(BFD)는 APIC Release 1.2(2)에서 도입되었습니다. 리프 및 스파인 스위치 간 ISIS, OSPF, 스파인 및 IPN 장치 간 고정 경로 등 기타 구성 요소의 BFD 에 대한 자세한 내용은 APIC 계층 3 네트워킹 구성 가이드에서 확인할 수 있습니다.

제한 조건

- L3Out 의 BFD 는 라우팅된 인터페이스, 하위 인터페이스, 그리고 SVI 에서만 지원됩니다. ACI 에는 아직 다중 홉 BFD 가 존재하지 않으므로 루프백 인터페이스에서는 지원되지 않습니다.
- BGP 식별 번호 피어(동적 인접 라우터)에 대한 BFD 는 지원되지 않습니다.
- BFD 하위 인터페이스 최적화는 글로벌 BFD 정책에서는 불가능하며 인터페이스 BFD 정책에서만 활성화될 수 있습니다. BFD 하위 인터페이스 최적화가 한 개의 하위 인터페이스에서 활성화되면 동일한 실제 인터페이스에서 모든 하위 인터페이스에 대해 활성화됩니다.

L3Out 에서 BFD 사용

각 L3Out 에는 사용자 지정이 불필요한 경우 BFD 세션을 설정 및 활성화할 수 있는 선택란이 한 개만 존재합니다. 각 L3Out 라우팅 프로토콜을 다룬 이전 섹션에서 언급한 바와 같이 Figure 135 는 기본적으로 비활성화되어 있는 BFD 를 활성화하는 확인란을 나타냅니다.

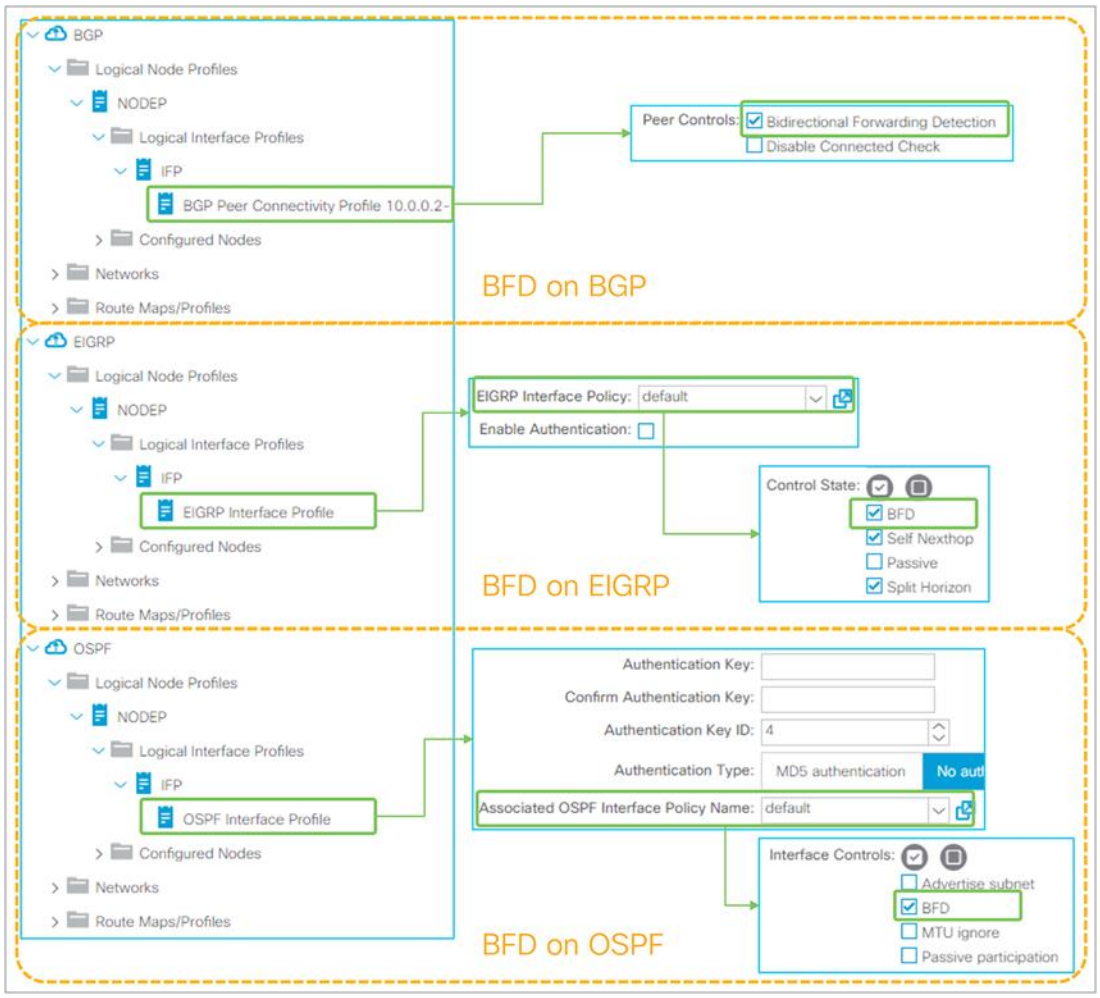

Figure 135.

GUI(APIC Release 3.2) 내 L3Out 라우팅 프로토콜에서 BFD 활성화

BFD 가 사용자 지정 없이 활성화되어 있을 경우 BFD 매개 변수는 "**Fabric > Access Policies > Policies > Switch > BFD > BFD IPv4/v6 > default**"에 위치한 기본 BFD 정책에서 파생됩니다. BFD 매개 변수를 사용자 지정하는 방법은 다음 섹션에 나와 있습니다.

L3Out 에서 BFD 사용자 지정

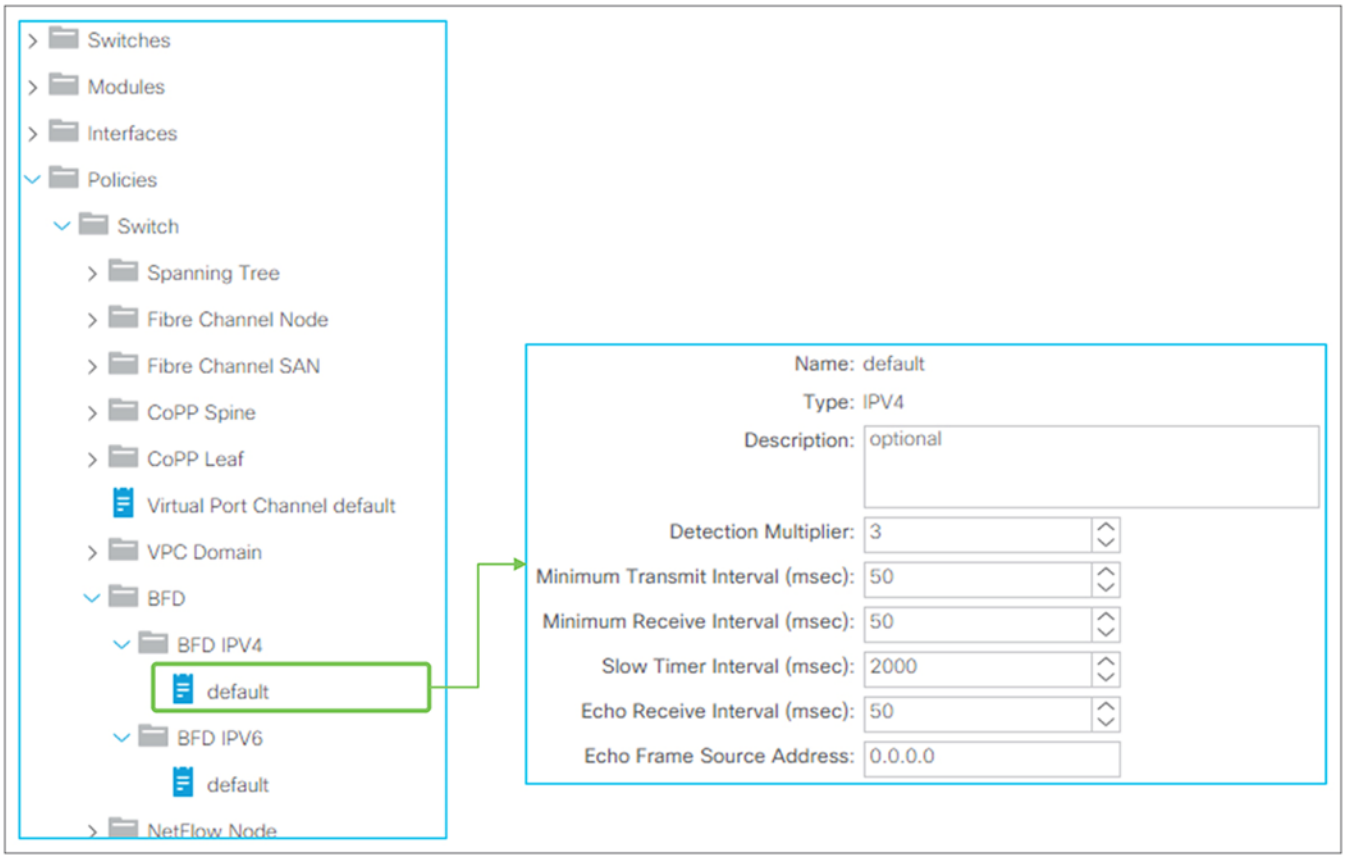

Figure 136.

GUI(APIC Release 3.2) 내 글로벌 BFD 매개 변수

"**Fabric > Access Policies > Policies > Switch > BFD > BFD IPv4/v6 > default**"에 위치한 기본 글로벌 BFD 정책에는 ACI 패브릭 내 모든 스위치에서 사용되는 BFD 매개 변수가 포함됩니다. 사용자는 또한 비 기본 BFD 정책을 생성하여 이를 "**Fabric > Access Policies > Switches**"에 위치한 **스위치 정책 그룹**과 **스위치 프로필**을 통해 특정 스위치에 적용할 수 있습니다.

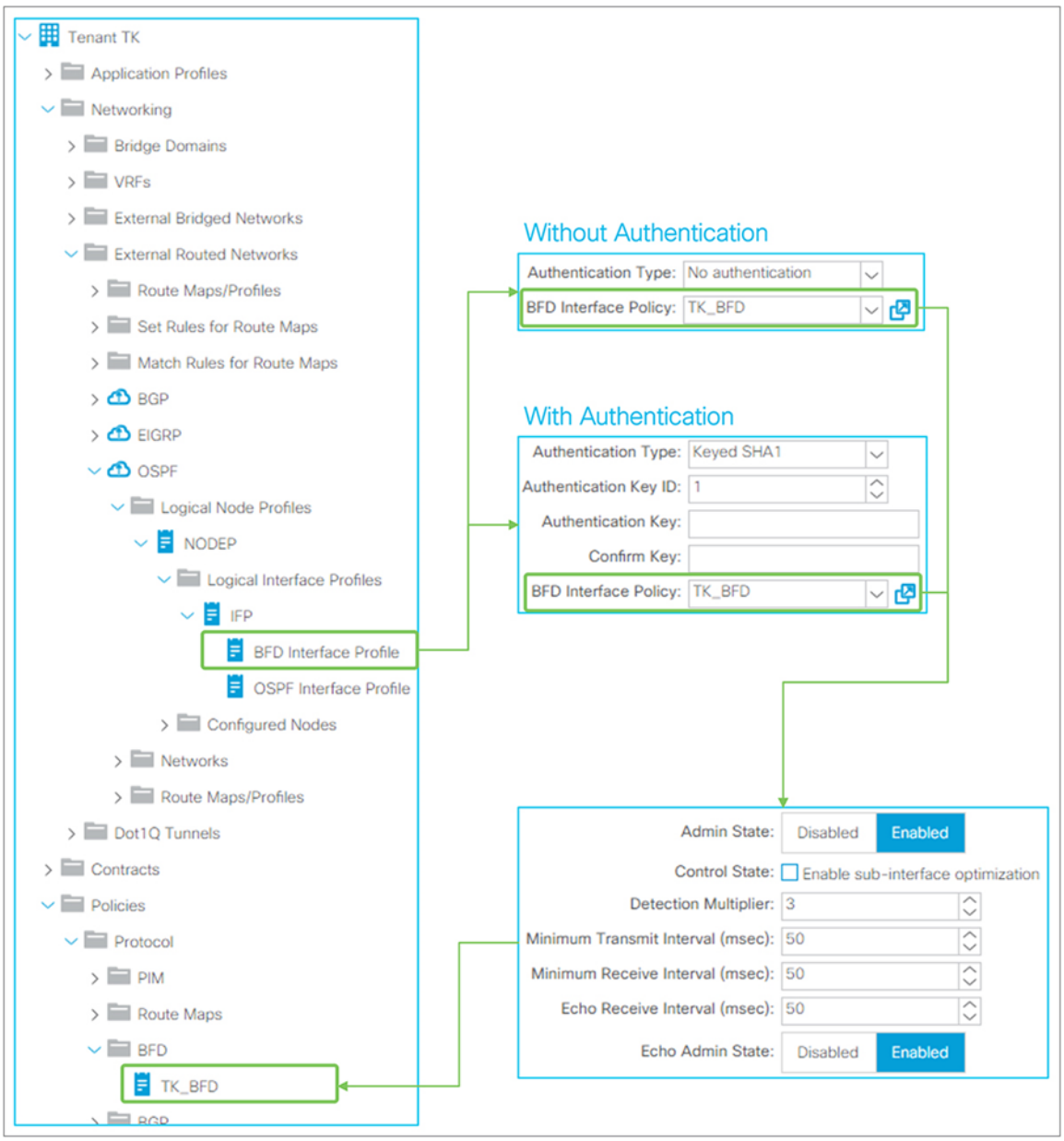

Figure 137.

GUI(APIC Release 3.2) 내 인터페이스 BFD 매개 변수

사용자는 **논리 인터페이스 프로필**의 **BFD 인터페이스 프로필**을 생성함으로써 인터페이스 수준의 BFD 정책을 통해 스위치 수준의 글로벌 BFD 정책에서 BFD 매개 변수를 재정의할 수 있습니다. 인터페이스 수준의 BFD 정책은 **"Tenant > Policies > Protocol > BFD"**에 위치합니다.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

미국에서 인쇄됨 C07-743150-02 07/21