ACI에서 L3Out 서브넷 분류 문제 해결

목차

소개

이 문서에서는 Cisco ACI의 L3Out EPG 내에서 외부 서브넷의 분류에 대해 설명합니다.

약어

- BD: 브리지 도메인
- EPG: 엔드포인트 그룹
- ExEPG: 외부 엔드포인트 그룹
- RIB: 라우팅 정보 베이스
- VRF: 가상 라우팅 및 포워딩
- 클래스 ID: EPG를 식별하는 태그

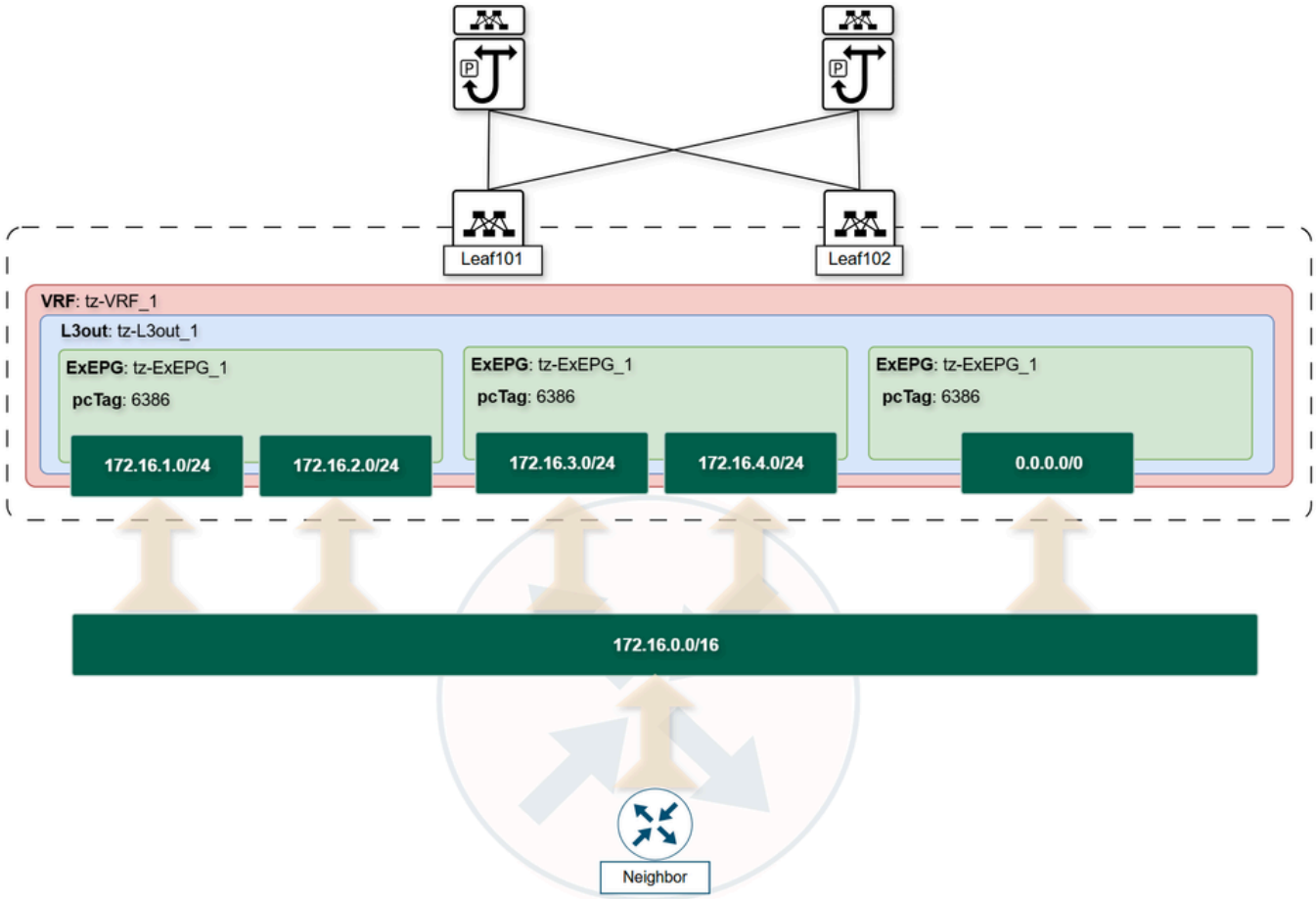
외부 EPG 분류

Cisco ACI의 외부 EPG는 L3Out을 통해 연결된 외부 라우팅 네트워크를 나타냅니다. 일반 EPG가 엔드포인트를 분류하는 방식과 마찬가지로, 외부 EPG는 VRF별로 외부 서브넷을 분류합니다. 즉, 각 서브넷은 VRF 컨텍스트 내에서 고유해야 합니다.

일반적인 오해는 외부 EPG 서브넷에 동적 라우팅 프로토콜을 통해 허용되는 접두사만 포함된다는 것입니다. 그러나 L3Out이 생성되면 수신 광고를 필터링하는 기본 경로 맵이 있습니다. 따라서 동적 라우팅 프로토콜에서 광고하는 모든 접두사는 기본적으로 수락됩니다. ExEPG에서 서브넷을 정의하는 주된 목적은 계약 시행 및 정책 적용을 위해 ExEPG에 포함된 서브넷에 고유한 pcTag를 할당하는 것입니다.

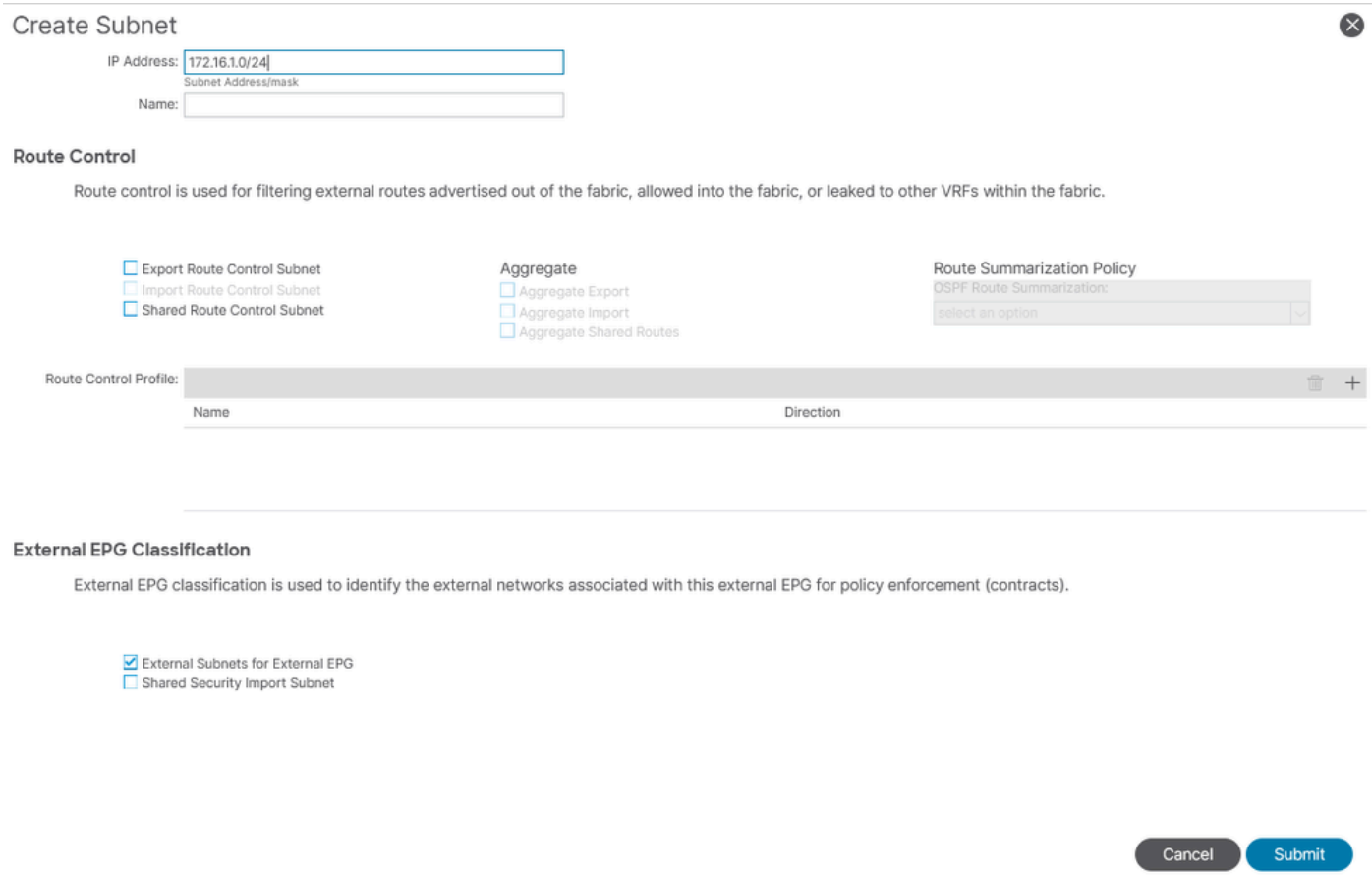
이러한 분류는 세분화된 정책 제어를 가능하게 합니다. 예를 들어, 단일 외부 인접 디바이스는 수퍼넷을 ACI에 광고할 수 있으며, 그런 다음 이를 여러 ExEPG로 분할할 수 있습니다. 이를 통해 특정 내부 EPG가 지정된 외부 서브넷과만 통신하도록 허용하거나, 최종 목적지에 도달하기 전에 특정 접두사를 목적지로 하는 트래픽을 PBR-노드로 리디렉션하는 것과 같이 서로 다른 계약 작업을 고유한 서브넷에 적용할 수 있습니다.

이 다이어그램은 Cisco ACI가 외부 EPG를 기반으로 외부 서브넷을 분류하는 방식을 보여줍니다. 이를 통해 정밀한 트래픽 세그멘테이션 및 계약 적용이 가능합니다.



외부 EPG 서브넷 플래그

ACI의 ExEPG 내에서 외부 접두사를 분류하고 관리하기 위해 ExEPG에서 서브넷 접두사를 생성할 때 특정 서브넷 플래그가 구성됩니다. 이 섹션에서는 각 플래그 및 해당 용도에 대해 자세히 설명합니다.



- 외부 EPG를 위한 외부 서브넷:
  이 플래그는 서브넷이 ACI 패브릭 외부에 있으며 어떤 브리지 도메인 또는 EPG 내에서도 구성되지 않음을 나타냅니다. 접두사가 라우팅 네이버에 의해 광고되거나 RIB에 정적으로 주입되는 경우에만 사용해야 합니다. 이 플래그는 기본적으로 활성화되어 있습니다.

- 경로 제어 서브넷 내보내기:
  이 플래그는 서브넷이 ACI에서 동적 라우팅 프로토콜을 통해 라우팅 네이버로 광고되도록 지정합니다. 외부 EPG용 외부 서브넷 플래그와 동시에 활성화해서는 안 됩니다. 이렇게 하면 레이어 3 라우팅 루프가 발생할 수 있습니다. ACI는 서브넷을 외부로 분류하고 다시 광고하기 때문에 라우팅 프로토콜의 루프 회피 메커니즘에도 불구하고 라우팅 불일치를 초래할 수 있습니다.

- 공유 경로 제어 서브넷:
  이 플래그는 여러 VRF에서 서브넷 접두사를 공유하여 컨텍스트 간에 경로 유출을 활성화할 때 설정됩니다.

- 공유 보안 가져오기 서브넷:
  공유 경로 제어 서브넷 플래그와 함께 사용하면 여러 VRF에서 외부 서브넷에 대한 보안 pcTag를 공유할 수 있으므로 일관된 정책을 적용할 수 있습니다.

- 경로 제어 서브넷 가져오기:
  이 플래그를 사용하면 라우팅 네이버에서 수신된 접두사를 세부적으로 제어할 수 있습니다. 기본적으로 ACI는 모든 수신 경로 광고를 수락합니다. 이 플래그를 활성화하려면 경로 제어 시행을 활성화하여 들어오는 접두사를 필터링해야 합니다.

- 집계 섹션:
  Quad-0(0.0.0.0/0) 서브넷에만 적용할 수 있으며, 이 섹션에서는 집계 내보내기 또는 가져오기를 위해 RIB의 모든 접두사를 요약합니다. 서브넷이 다른 VRF로 유출되면 라우팅 테이블을 최적화하기 위해 종합 공유 경로로 요약됩니다.

확인 및 문제 해결 명령

라우팅

먼저 경로가 Border Leaf 스위치에 있는 VRF의 라우팅 테이블에 있어야 합니다. 예를 들어 이 명령은 VRF tz:tz-VRF_1의 BGP 경로를 보여줍니다.

```
<#root>

Leaf101#

show ip route bgp vrf tz:tz-VRF_1


IP Route Table for VRF "tz:tz-VRF_1"


'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>


172.16.1.0/24

, ubest/mbest: 1/0

*via 10.10.1.2

%tz:tz-VRF_1, [20/0], 00:00:04, bgp-65002, external, tag 65003
Leaf101#
```

그러면 경로가 VRF 라우팅 테이블에 설치되고 전달 결정에 사용할 수 있음을 확인합니다.

분류

경로가 라우팅 테이블에 있으면 분류는 정책을 기반으로 트래픽 처리 방법을 결정합니다. ACI에서는 분류가 ExEPG 및 관련 서브넷에 연결됩니다.

ExEPG에서 서브넷 분류를 검증하기 위해 외부 EPG 인스턴스를 나타내는 l3extInstP 클래스에 대해 APIC를 쿼리할 수 있습니다. 해당 하위 클래스 l3extSubnet은 해당 ExEPG에 구성된 서브넷을 나열합니다. 예를 들면 다음과 같습니다.

```
<#root>

moquery -c l3extInstP -f 'l3ext.InstP.dn*"[ tenant name ].*[ l3out name ]"' -x rsp-subtree=children rsp-
```

<#root>

APIC#

moquery -c l3extInstP -f 'l3ext.InstP.dn*"tz.*l3out"' -x rsp-subtree=children rsp-subtree-class=l3extSub

Total Objects shown: 1

l3ext.InstP

name : tz-ExEPG_1

!-- cut for brevity --!
configSt : applied
descr :
dn : uni/tn-tz/out-l3out/instP-tz-ExEPG_1
!-- cut for brevity --!
floodOnEncap : disabled
isSharedSrvMsiteEPg : no
lcOwn : local
matchT : AtleastOne
mcast : no
modTs : 2025-09-10T00:36:49.239+00:00
monPolDn : uni/tn-common/monepg-default
nameAlias :
pcEnfPref : unenforced

pcTag : 32771

pcTagAllocSrc : idmanager
prefGrMemb : exclude
prio : unspecified
rn : instP-tz-ExEPG_1
scope : 3047430
status : modified
targetDscp : unspecified
triggerSt : triggerable
txId : 1152921504612318828
uid : 15374
userdom : :all:

l3ext.Subnet

ip : 172.16.1.0/24

!-- cut for brevity --!
dn : uni/tn-tz/out-l3out/instP-tz-ExEPG_1/extsubnet-[172.16.1.0/24]
extMngdBy :
lcOwn : local
modTs : 2025-09-10T01:05:13.249+00:00
monPolDn : uni/tn-common/monepg-default
!-- cut for brevity --!
rn : extsubnet-[172.16.1.0/24]

scope : import-security

status :
uid : 15374

```
userdom : :all:

APIC#
```

l3extSubnet 클래스에 대해 어떤 출력도 반환되지 않으면 외부 EPG에 서브넷이 구성되어 있지 않음을 나타냅니다. 서브넷을 구성하지 않으면 ACI에서 pcTag를 수신 트래픽 서브넷에 연결할 수 없으므로 라우팅 테이블에 경로가 있더라도 트래픽이 삭제됩니다.

주목해야 할 또 다른 중요한 측면은 서브넷의 범위입니다. 이는 해당 서브넷에 대해 설정된 플래그를 나타냅니다.

- 가져오기 보안

서브넷에 외부 EPG용 외부 서브넷이 플래그되었습니다.

- 내보내기-rtctrl

서브넷에 Export Route Control 플래그가 지정되었습니다.

- import-rtctrl

서브넷에 Import Route Control 플래그가 지정되었습니다.

- 공동 보안

서브넷에 공유 보안 가져오기 서브넷이 플래그가 지정되었습니다.

- 공유 rtctrl

서브넷에 공유 경로 제어 플래그가 지정되었습니다.

라우팅 프로토콜 및 제어 평면 프로세스는 언급된 인접 디바이스로부터 접두사를 수신할 때 라우팅 테이블을 업데이트하며, 이 접두사는 HAL L3 포워딩 테이블에 프로그래밍됩니다. HAL L3 경로는 리프 스위치의 하드웨어 포워딩 테이블(ASIC)에 프로그래밍된 실제 레이어 3 경로를 나타냅니다. 이러한 경로는 라우팅 프로토콜 및 라우팅 테이블 계산에서 파생되며 전달 결정에 사용됩니다.

<#root>

```
<-- When the prefix is not configured under the External EPG, a classification of 0xf is seen -->
Leaf101#

vsh_lc -c 'show platform internal hal l3 routes vrf tz:tz-VRF_1' | egrep "Prefix/Len|172.16.1.0" | cut -

VRF |   Prefix/Len  | RT|CLSS| Flags

4675| 172.16.1.0/ 24| UC| f|spi,dpi

Leaf101#

<-- When the prefix is configured under the External EPG, a classification of the pcTag in hexadecimal
Leaf101#
```

```
vsh_lc -c 'show platform internal hal l3 routes vrf tz:tz-VRF_1' | egrep "Prefix/Len|172.16.1.0" | cut -

VRF |   Prefix/Len  | RT|CLSS| Flags
4675| 172.16.1.0/ 24| UC|8003|spi,dpi

Leaf101#

Leaf101#

vsh_lc -c '

dec 0x8003'

32771
Leaf101#
```

그런 다음 ExEPG에서 외부 EPG용 외부 서브넷을 사용하여 서브넷을 구성하면 정책 관리자(policy-mgr)라는 내부 프로세스가 접두사-pcTag 매핑 테이블을 이 서브넷 항목 및 연결된 pcTag로 업데이트합니다. Policy Manager는 패브릭 중앙 집중식 정책 오케스트레이션 엔진 역할을 하면서 상위 레벨 정책 정의를 ACI 패브릭 전체에서 실행 가능한 컨피그레이션으로 변환합니다. 이렇게 하면 구성된 외부 서브넷을 기반으로 트래픽 분류 및 전달 결정에 올바른 pcTag를 적용하여 일관성 있고 안전한 애플리케이션 연결 및 네트워크 동작을 보장합니다.

```
<#root>

Leaf101#

vsh -c 'show system internal policy-mgr prefix' | egrep "tz:tz-VRF_1"

3047430 36 0x80000024 Up tz:tz-VRF_1 ::/0 15 True True False False
3047430 36 0x24 Up tz:tz-VRF_1 0.0.0.0/0 15 True True False False
3047430 36 0x24 Up tz:tz-VRF_1 172.16.1.0/24 32771 True True False False

Leaf101#
```

이는 접두사 172.16.1.0/24이 네이버에서 ACI 보더 리프 스위치에 알려지고 있으며 ACI에서 pcTag 아래의 접두사를 분류했음을 32771

계약

영역 지정 규칙은 패브릭 내 EPG(ExEPG 포함) 간에 계약 정책을 시행하는 기본 프로세스입니다. 외부 EPG의 VRF VNID(범위) 및 pcTag를 사용하여 소스 EPG와 대상 EPG 간에 적용된 통신 규칙을 정의하고 검증할 수 있습니다. 기본적으로 zoning-rule은 상위 레벨 계약 관계를 리프 스위치에 프로그래밍된 특정 시행 가능한 규칙으로 변환합니다.

패브릭에서 계약이 설치되는 위치는 고려해야 할 중요한 부분입니다. 기본적으로 VRF는 Policy

Control Enforcement Direction이 ingress로 설정된 상태로 구성됩니다. 이 설정은 지정된 계약에 대한 영역 지정 규칙이 소스 엔드포인트가 있는 리프 스위치에 설치되도록 결정합니다.

이 연습에서는 트래픽이 L3Out에서 들어오고, 영역 지정 규칙이 해당 L3Out에 연결되는 경계 leaf에 설치됩니다. 이 leaf는 패브릭에 들어오는 트래픽의 소스 leaf 역할을 합니다.

<#root>

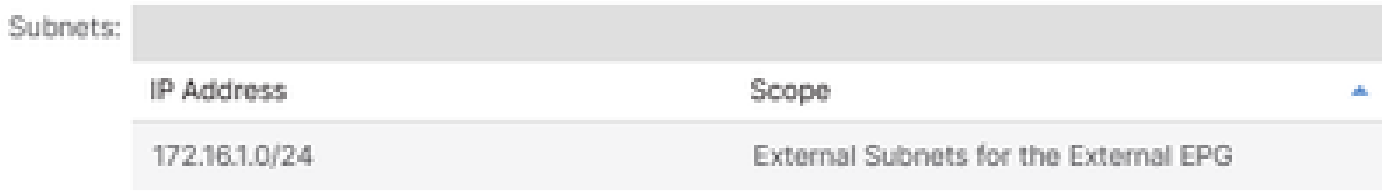
```
Leaf101#
```

show zoning-rule scope 3047430 | egrep "Rule|---|32771"

```
+---------+--------+--------+----------+----------------+---------+---------+--------------------+------
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       | operSt  |  Scope  |        Name        |
+---------+--------+--------+----------+----------------+---------+---------+--------------------+------
|  4441   | 49153  | 32771  |     5    |     bi-dir     | enabled | 3047430 |     tz:Contract    |
|  4500   | 32771  | 49153  |     5    | uni-dir-ignore | enabled | 3047430 |     tz:Contract    |
+---------+--------+--------+----------+----------------+---------+---------+--------------------+------
Leaf101#
```

통과 경로

트랜짓 라우팅은 패브릭이 하나의 L3Out에서 다른 L3Out으로 학습된 외부 경로를 광고함으로써 트랜짓 네트워크의 역할을 할 수 있게 합니다. 트랜짓 라우팅을 올바르게 구성하려면 외부 EPG에 대한 외부 서브넷이 수신 서브넷에 표시되어야 합니다.



동시에 이 서브넷을 다른 외부 피어에 광고하는 L3Out의 경우 해당 서브넷에서 경로 제어 서브넷 내보내기 플래그가 활성화되어 있어야 합니다. 이 플래그를 사용하면 서브넷을 재배포하고 해당 L3Out에 구성된 라우팅 프로토콜을 통해 패브릭 외부로 알릴 수 있습니다.

Subnets:

IP Address	Scope
172.16.1.0/24	Export Route Control Subnet

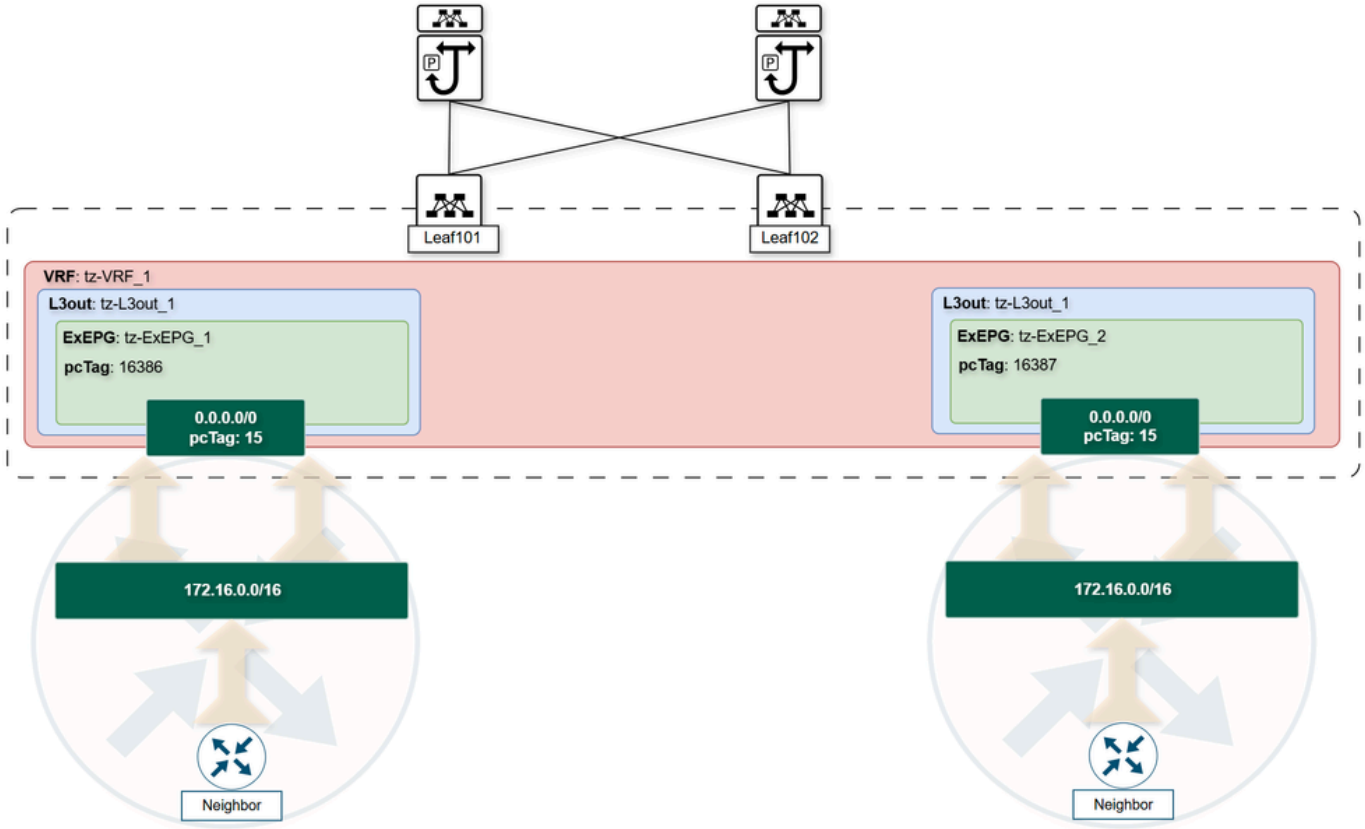
마지막으로, 경로를 배포하는 프로세스를 완료하려면 수신자와 내보내는 L3out 간의 계약이 구성되어야 합니다.

서브넷 외부 EPG 분류의 일반적인 문제

pcTag 15

이전에는 이 문서에서 ExEPG 서브넷이 정책 시행을 위해 올바른 pcTag에서 서브넷을 분류하는 데 도움이 된다고 설명했습니다. 이 분류의 중요한 예외는 외부 EPG 플래그로 외부 서브넷을 구성한 경우 쿼드 0 서브넷(0.0.0.0/0)입니다. 이 서브넷에는 항상 예약된 pcTag 15가 할당되어 VRF 내의 모든 외부 트래픽에 대해 와일드카드 역할을 합니다.

이 다이어그램은 동일한 VRF 내의 여러 ExEPG에서 외부 EPG를 위한 외부 서브넷을 사용하여 쿼드-0을 구성하는 문제를 나타냅니다.



- Quad-0 서브넷은 종종 기본 경로로 오인됩니다. 동적 라우팅 네이버가 ACI L3Out에 기본 경로만 광고하는 경우처럼 이것이 때때로 사실이지만, ACI에서 쿼드-0 서브넷의 역할은 catch-all 분류로 더 넓습니다.

- 일반적으로 쿼드-0 서브넷으로 여러 ExEPG를 구성하여 네이버에서 광고하는 모든 접두사를 수락합니다. 폭넓은 허용이 목표이지만, 동일한 VRF 내에서 quad-0을 사용하는 여러 ExEPG가 구성된 경우 예기치 않은 비대칭 라우팅이 발생할 수 있습니다. 동일한 VRF 내의 여러 ExEPG가 외부 서브넷으로 quad-0을 사용하여 구성된 경우 ACI는 특정 대상 서브넷에 사용할 L3Out을 확정적으로 선택할 수 없습니다. 대신 임의로 L3Out 하나를 선택합니다.
- 이러한 동작으로 인해 비대칭 라우팅, 트래픽 간헐적 또는 무작위로 선택된 L3Out에 통신을 허용하는 데 필요한 계약이 없는 경우 트래픽이 중단될 수 있습니다.

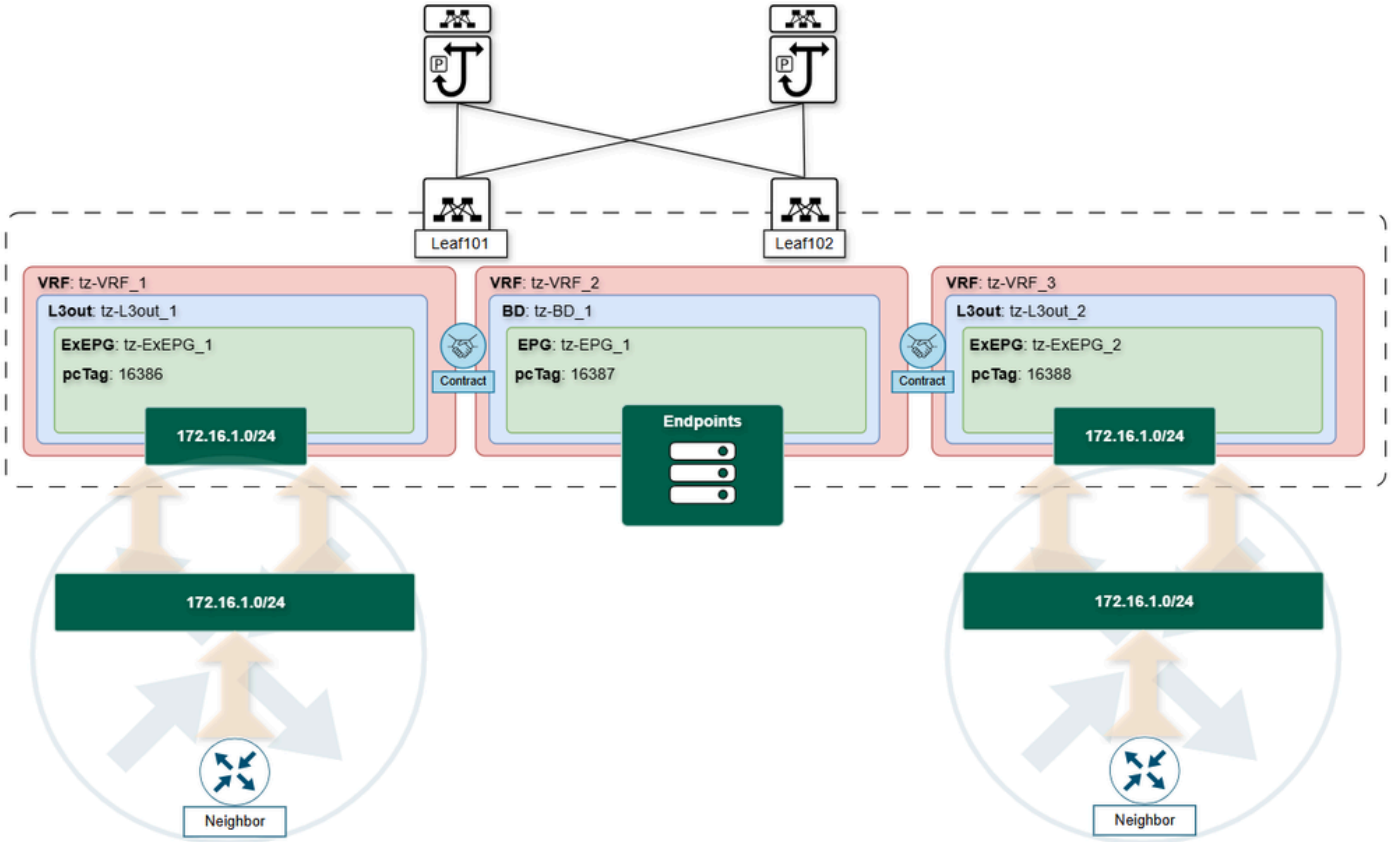
겹치는 서브넷

서로 다른 ExEPG에 동일한 서브넷을 구성하는 것은 허용되지 않습니다. 이렇게 하면 결함 "F0467: Prefix Entry Already Used in Another EPG"(다른 EPG에서 접두사 항목이 이미 사용됨)로 인해 VRF 내에서 서브넷이 중복되지 않습니다.

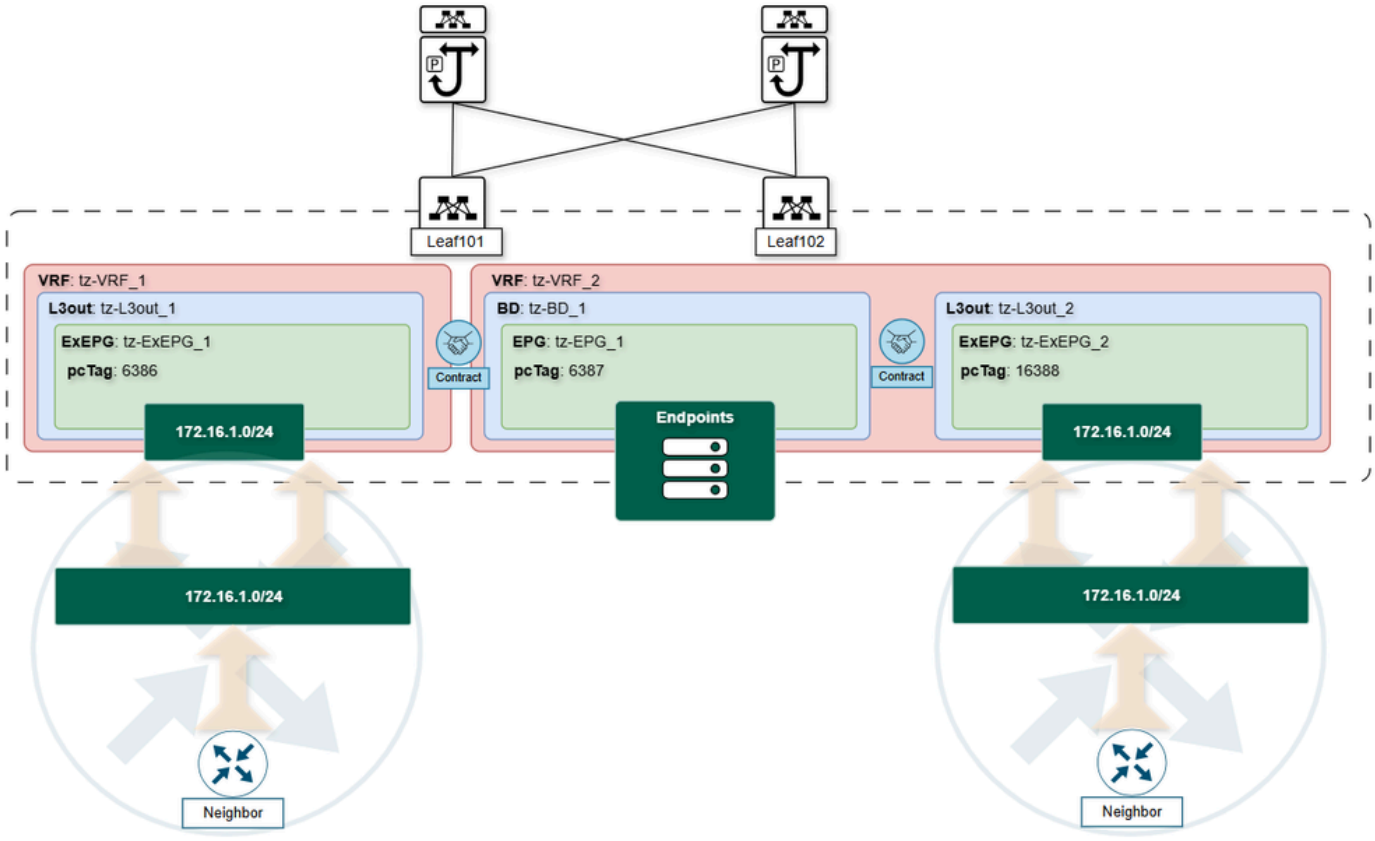
그러나 각 VRF가 독립적인 라우팅 테이블 컨텍스트를 유지하기 때문에 서로 다른 VRF에 걸쳐 중첩된 서브넷이 존재할 수 있습니다. 이렇게 분리하면 서로 다른 VRF에 속하는 ExEPG에서 동일한 서브넷을 구성할 수 있습니다. 그럼에도 불구하고 이러한 중첩된 서브넷과 관련된 VRF 경로 유출을 수행할 경우, RIB(라우팅 정보)와 pcTag(서브넷 분류)의 충돌로 인해 비대칭 포워딩 결정을 내릴 수 있으므로 주의가 필요합니다.

주요 시나리오는 다음과 같습니다.

- 두 VRF에서 세 번째 VRF로 누수 경로 지정:
  두 VRF가 동일한 서브넷을 세 번째 VRF로 유출하면 수신 VRF는 APIC의 공유 정책에 따라 수신한 첫 번째 서브넷을 설치합니다. 이 VRF를 처리하는 리프 스위치가 재부팅되거나 라우팅 선택이 변경되면 라우팅 테이블이 다른 L3Out으로 업데이트되어 일관성 없는 포워딩 동작이 발생할 수 있습니다.



- 유출된 서브넷과 중첩되는 로컬-VRF L3Out ExEPG:
  경로 유출이 사용되는 설계에서 로컬 L3Out ExEPG가 유출된 서브넷과 동일한 서브넷으로 구성된 경우 로컬 라우팅 엔트리는 항상 유출된 경로보다 우선합니다.



이러한 상황에서는 라우팅 테이블 자체가 아닌 분류 및 포워딩 결정 레이어에서 비대칭 포워딩 문제가 발생한다는 점을 강조합니다. 서브넷 분류는 정책 시행을 위해 서브넷을 특정 L3Out 및 ExEPG와 연결하지만 라우팅 테이블은 다른 L3Out 대상을 가리킬 수 있습니다. 이러한 불일치로 인해 트래픽이 일관성 없이 전달될 수 있으며, 이로 인해 잠재적 연결 문제 또는 정책 시행 공백이 발생할 수 있습니다.

경로 제어 기본 동작 변경 가져오기

기본적으로 ACI는 네이버의 모든 수신 경로 광고를 수락합니다. 허용되는 접두사를 제어하려면 Route Control Enforcement를 활성화해야 합니다. L3Out 루트 개체의 인바운드:

Tenants(테넌트) > [tenant name] > Networking(네트워킹) > L3outs > [L3out name]으로 이동합니다.

이 작업은 선택한 라우팅 프로토콜 아래에 경로 맵을 생성합니다.

<#root>

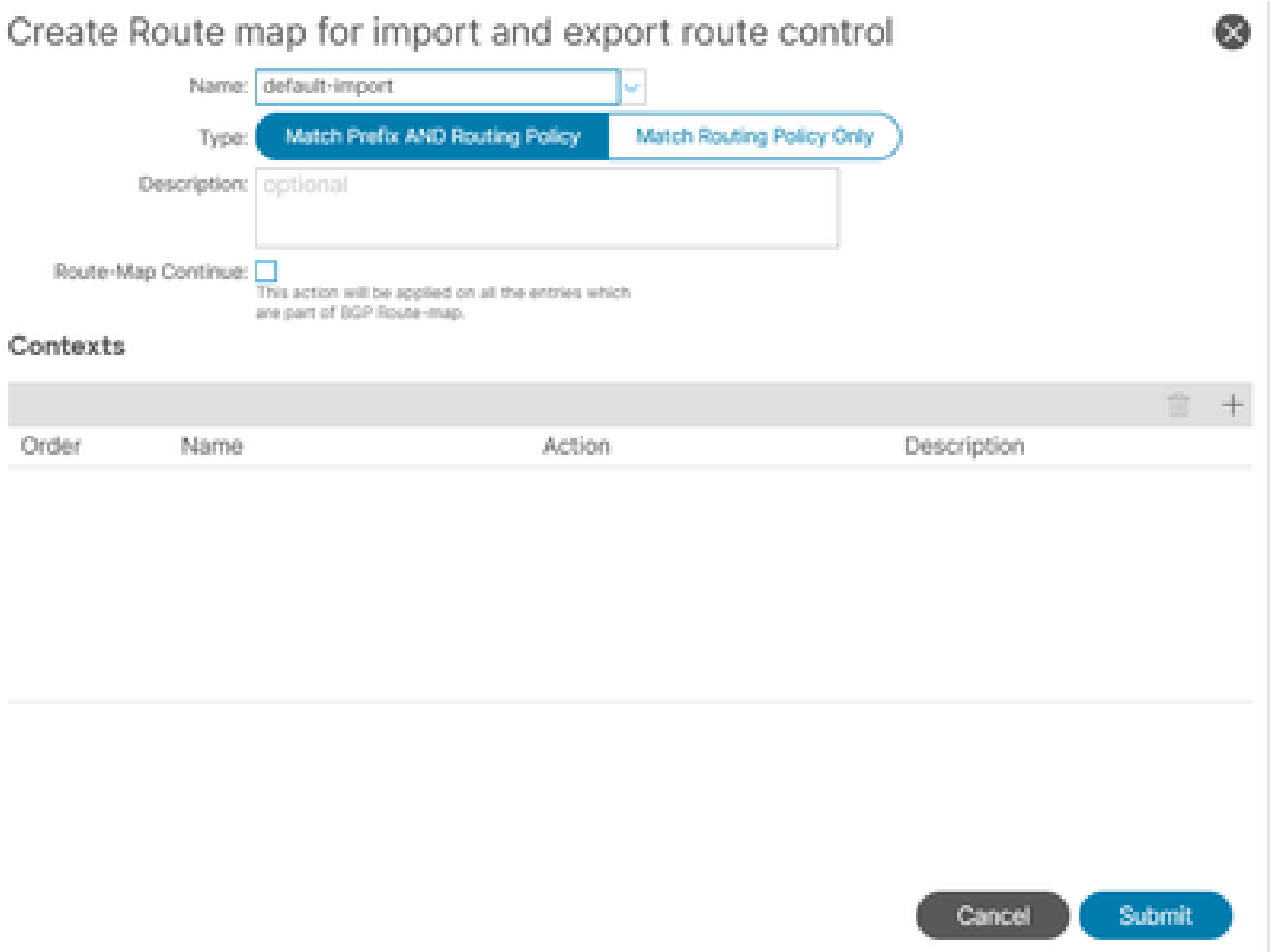
```
Border Leaf#
show ip bgp neighbors vrf tz:tz-VRF1 | egrep route-map

Outbound route-map configured is exp-l3out-ExEPG-peer-2981888, handle obtained
Inbound route-map configured is imp-l3out-ExEPG-peer-2981888, handle obtained


Border Leaf#
show route-map imp-l3out-ExEPG-peer-2981888

route-map imp-l3out-ExEPG-peer-2981888,
permit
, sequence 15801
Match clauses:
ip address prefix-lists: IPv4-peer49155-2981888-exc-ext-inferred-import-dst

ipv6 address prefix-lists: IPv6-deny-all
Set clauses:

Border Leaf#
show ip prefix-list IPv4-peer49155-2981888-exc-ext-inferred-import-dst
```

```
ip prefix-list IPv4-peer49155-2981888-exc-ext-inferred-import-dst: 1 entries
seq 1 permit 172.16.1.0/24
Border Leaf#
```

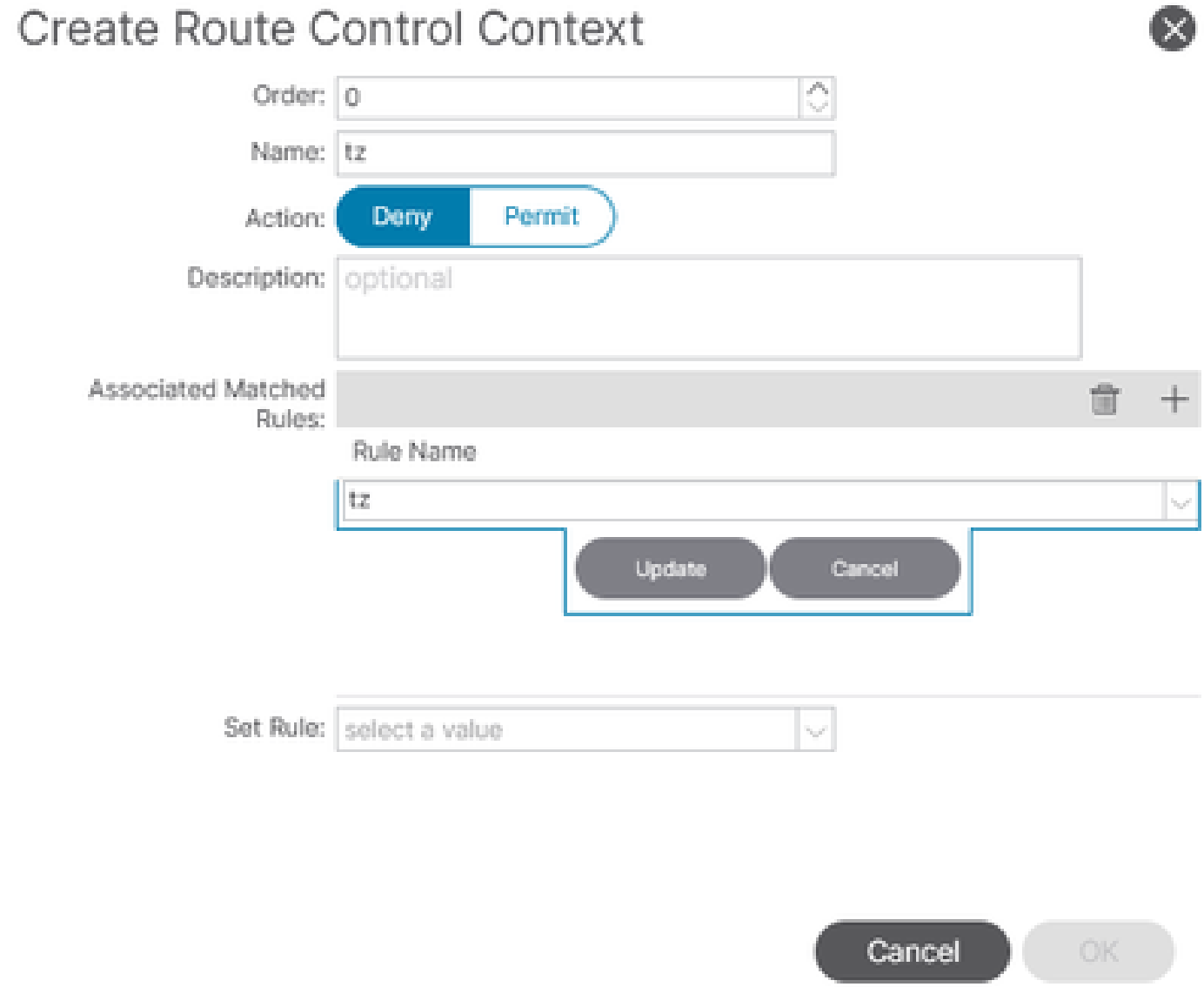
기본적으로 이 가져오기 경로 맵은 모든 들어오는 접두사를 허용합니다. 이 동작을 수정하려면

Tenants(테넌트) > [tenant name] > Networking(네트워킹) > L3outs(L3out) > [L3out name] > Route map for import and export route control(경로 맵)으로 이동합니다.

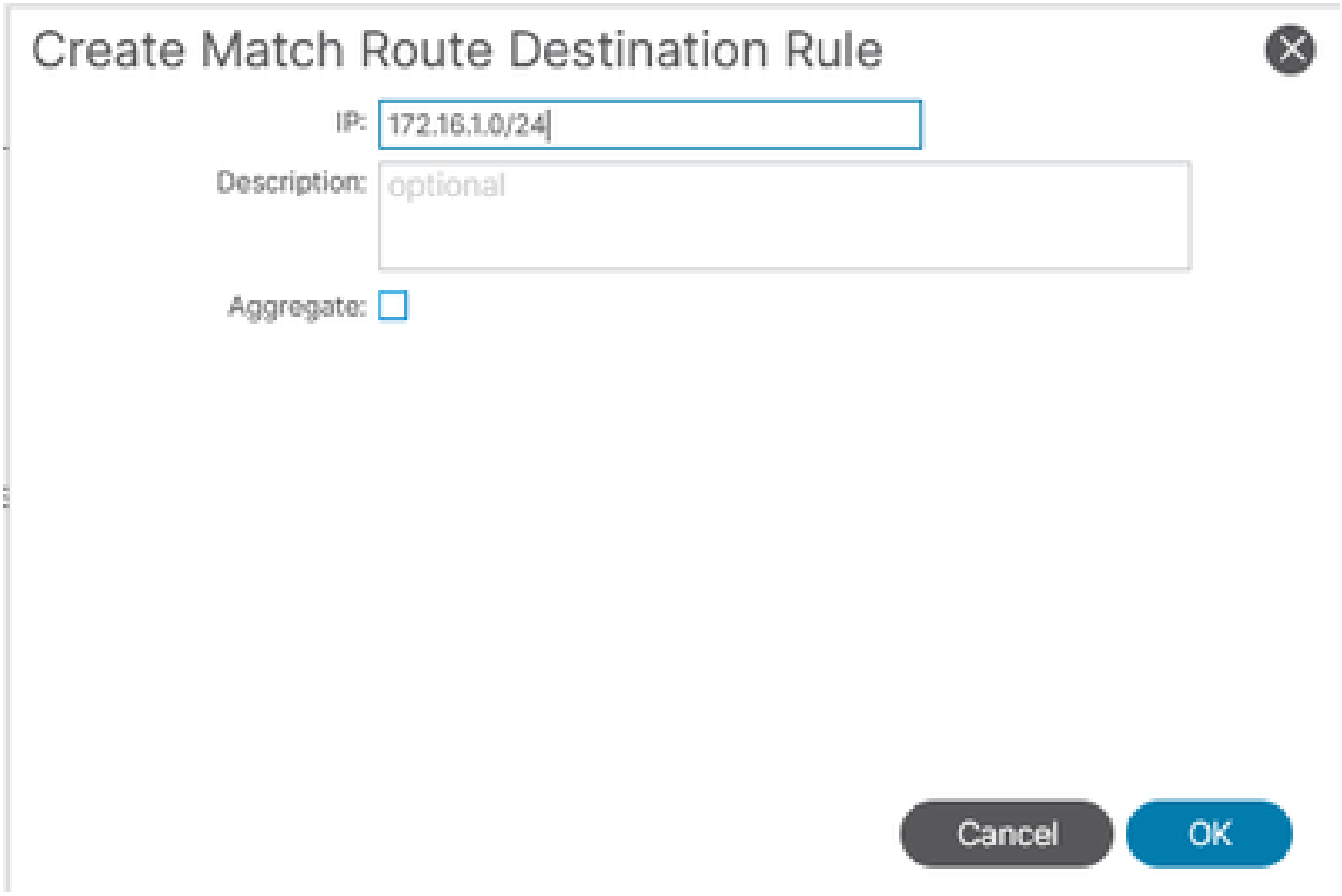
기본 가져오기 경로 맵을 선택하거나 오른쪽 상단에 있는 기어 아이콘을 사용하여 새 경로 맵을 만듭니다.



Context(컨텍스트) 섹션에서 새 Associated Matched Rule(연결된 일치 규칙)을 생성합니다.



Match Rules 섹션에서 Match Prefix로 스크롤하여 제어할 특정 서브넷을 추가합니다.



정책을 제출하면 경로 맵 가져오기 작업이 그에 따라 변경되어 원하는 접두사 필터링을 적용합니다 .

<#root>

```
Border Leaf#

show route-map imp-l3out-ExEPG-peer-2981888


route-map imp-l3out-ExEPG-peer-2981888,

deny

, sequence 8001
Match clauses:
ip address prefix-lists: IPv4-peer49155-2981888-exc-ext-in-default-import2tzOtz-dst
ipv6 address prefix-lists: IPv6-deny-all
Set clauses:

Border Leaf#
```

이 번역에 관하여

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