ACI에서 PBR 문제 해결

목차

소개

이 문서에서는 단일 포드 패브릭에서 PBR(Policy-Based Redirect)을 사용하여 ACI(Application Centric Infrastructure) 환경을 트러블슈팅하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에서는 다음과 같은 주제에 대해 일반적으로 알고 있는 것이 좋습니다.

- ACI 개념: 액세스 정책, 엔드포인트 학습, 계약 및 L3out

사용되는 구성 요소

이 트러블슈팅 연습은 2세대 Nexus 스위치 N9K-C93180YC-EX 및 N9K-C93240YC-FX2를 사용하여 ACI 버전 6.0(8f)에서 수행되었습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

약어

- BD: 브리지 도메인

- EPG: 엔드포인트 그룹
- 클래스 ID: EPG를 식별하는 태그
- PBR 노드: PBR 대상에 사용되는 L4-L7 디바이스
- 소비자 커넥터: 소비자측과 대면하는 PBR 노드 인터페이스
- 공급자 커넥터: 제공자측을 향하는 PBR 노드 인터페이스

PBR 기록

버전	주요 기능
2.0(1m)	• 서비스 그래프는 PBR 기능을 제공합니다.
3.x 이전	• 멀티 노드 PBR(policy-based redirect) 지원 • PBR 복원력 해싱
3.2(x)	• 단일 노드 방화벽 PBR은 멀티 사이트 환경에서 지원됩니다.
4.0(x)	• 다중 사이트 환경에서 2노드 방화벽 PBR이 지원됩니다.
4.2(1)	• 이제 대기 PBR 노드를 생성하기 위한 백업 정책이 지원됩니다.
4.2(3)	• Filter-from-contract 옵션은 GUI를 사용하여 서비스 그래프 템플릿에서 사용할 수 있습니다.
5.0(1)	• L3Out은 서비스 노드의 모든 공급자 측에서 지원됩니다. • 액티브-액티브 구축/ECMP 경로는 레이어 1/레이어 2 PBR 디바이스에서 지원됩니다.
5.2(1)	• 이제 PBR 대상이 L3Out에 있을 수 있습니다. • HTTP URI를 사용하여 서비스 노드를 추적할 수 있습니다. • 서비스 그래프 관리 및 하이브리드 모드는 더 이상 지원되지 않습니다. • 동적 PBR 노드 mac 주소가 지원됩니다.
6.0(1)	• 가중치 기반 PBR(Symmetric Policy-Based Redirect)

설계 고려 사항

- PBR은 물리적 및 가상 어플라이언스 모두에서 작동합니다
- PBR은 L3Out EPG와 EPG 사이, EPG 사이 및 L3Out EPG 사이에 사용될 수 있습니다. L2Out EPG가 계약의 일부인 경우 PBR은 지원되지 않습니다

- PBR은 Cisco ACI Multi-Pod, Multi-Site 및 Remote Leaf 환경에서 지원됩니다.
- Cisco ACI 패브릭은 서버 및 PBR 노드의 게이트웨이여야 합니다
- L4-L7 디바이스는 go-to 모드(라우팅된 모드)에서 구축되어야 합니다
- PBR 노드는 FEX 스위치에서 지원되지 않습니다.
- PBR 노드에 전용 브리지 도메인이 필요합니다.
- 이제 PBR 노드의 동적 MAC 주소가 상태 그룹을 사용하여 지원됩니다.
- PBR 노드 브리지 도메인에서 GARP 기반 탐지를 활성화하는 것이 좋습니다
- ARP, 이더넷 트래픽 및 기타 비IP 트래픽을 포함하는 공통 기본 필터는 PBR에 사용할 수 없습니다
- PBR 노드는 VRF 인스턴스 간에 또는 VRF 인스턴스 중 하나에 있을 수 있습니다. 이 토폴로지의 경우 PBR 노드는 세 번째 VRF에 있을 수 없으며, 소비자 또는 공급자 VRF에서 구성해야 합니다

배경 정보

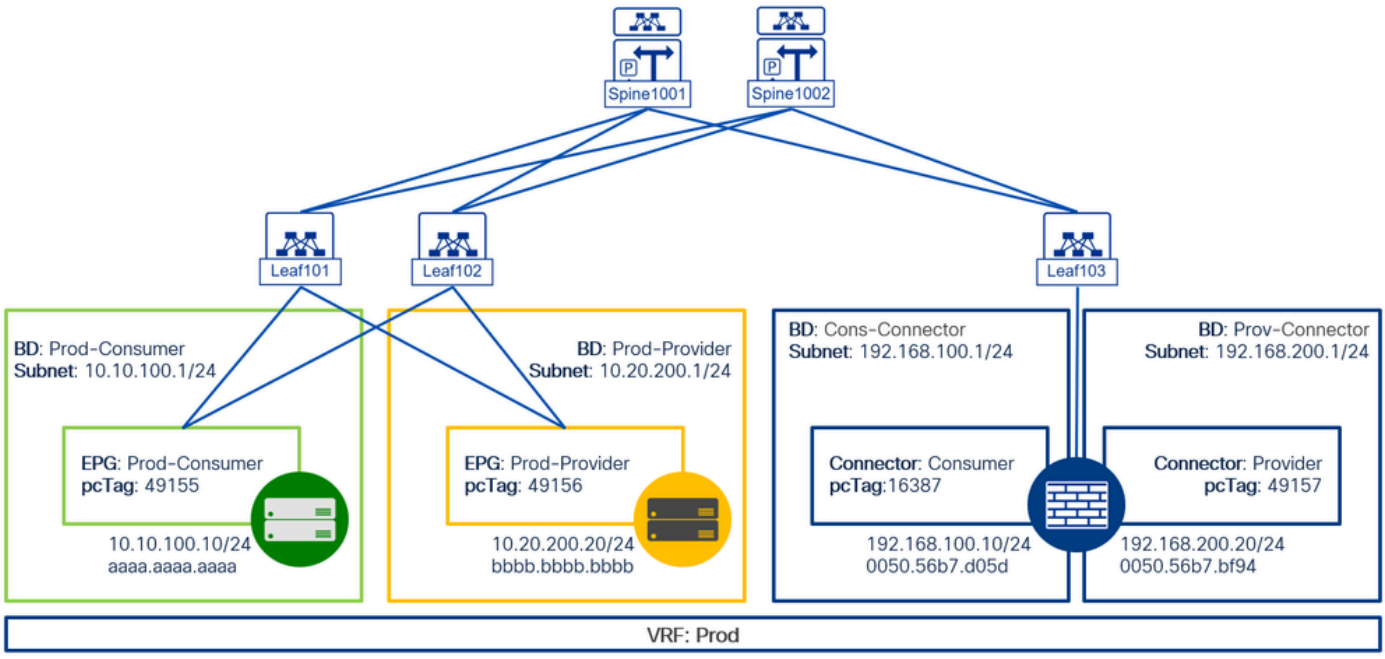
ELAM과 Ftriage에 대한 자세한 설명은 세션 BRKDCN-3900b의 CiscoLive 온디맨드 라이브러리에서 확인할 수 있습니다.

또한 모든 컨피그레이션 지침은 Cisco Application Centric Infrastructure Policy-Based Redirect Service Graph Design 백서에서 확인할 수 있습니다.

시나리오: 단일 포드 패브릭의 단일 VRF

네트워크 다이어그램

물리적 토폴로지:



문제 해결

1단계: 결함

컨피그레이션 또는 정책 상호 작용에 문제가 있을 경우 ACI에서 결함이 생성됩니다. 장애 발생 시 PBR 렌더링 프로세스에 대한 특정 장애가 식별되었습니다.

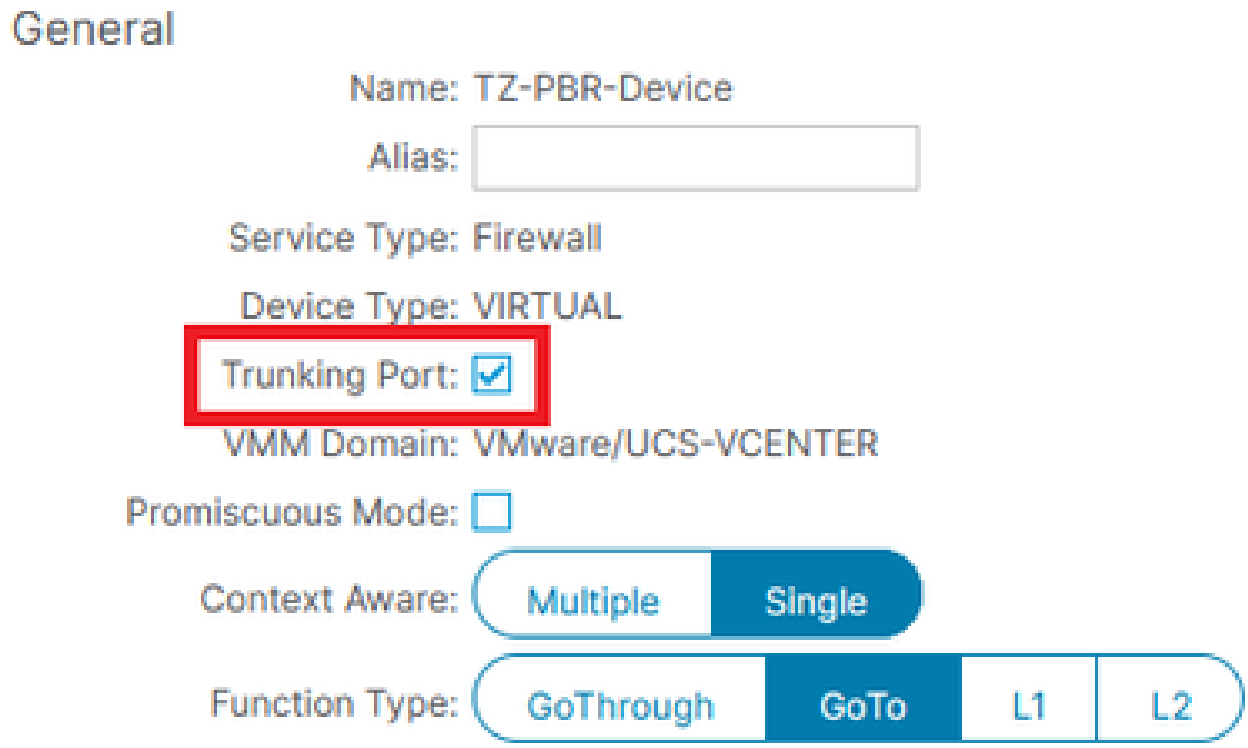
F1690: 다음 이유로 인해 구성이 유효하지 않습니다.

- ID 할당 실패

  이 결함은 서비스 노드에 대해 캡슐화된 VLAN을 사용할 수 없음을 나타냅니다. 예를 들어 논리적 디바이스에서 사용하는 VMM(Virtual Machine Manager) 도메인과 연결된 VLAN 풀에서 사용 가능한 동적 VLAN이 없을 수 있습니다.

  해결 방법: 논리 장치가 사용하는 도메인 내에서 VLAN 풀을 확인합니다. 논리 장치 인터페이스가 물리적 도메인 내에 있는 경우 캡슐화된 VLAN 구성도 검사합니다. 이러한 설정은 Tenant(테넌트) > Services(서비스) > L4-L7 > Devices and Fabric(디바이스 및 패브릭) > Access Policies(액세스 정책) > Pools(풀) > VLAN에서 찾을 수 있습니다.

  반대로, 논리적 디바이스 인터페이스가 가상 도메인 내에 있고 트렁크 인터페이스를 통해 ESXi 호스트에 연결하는 경우 트렁킹 포트 옵션이 활성화되었는지 확인합니다.

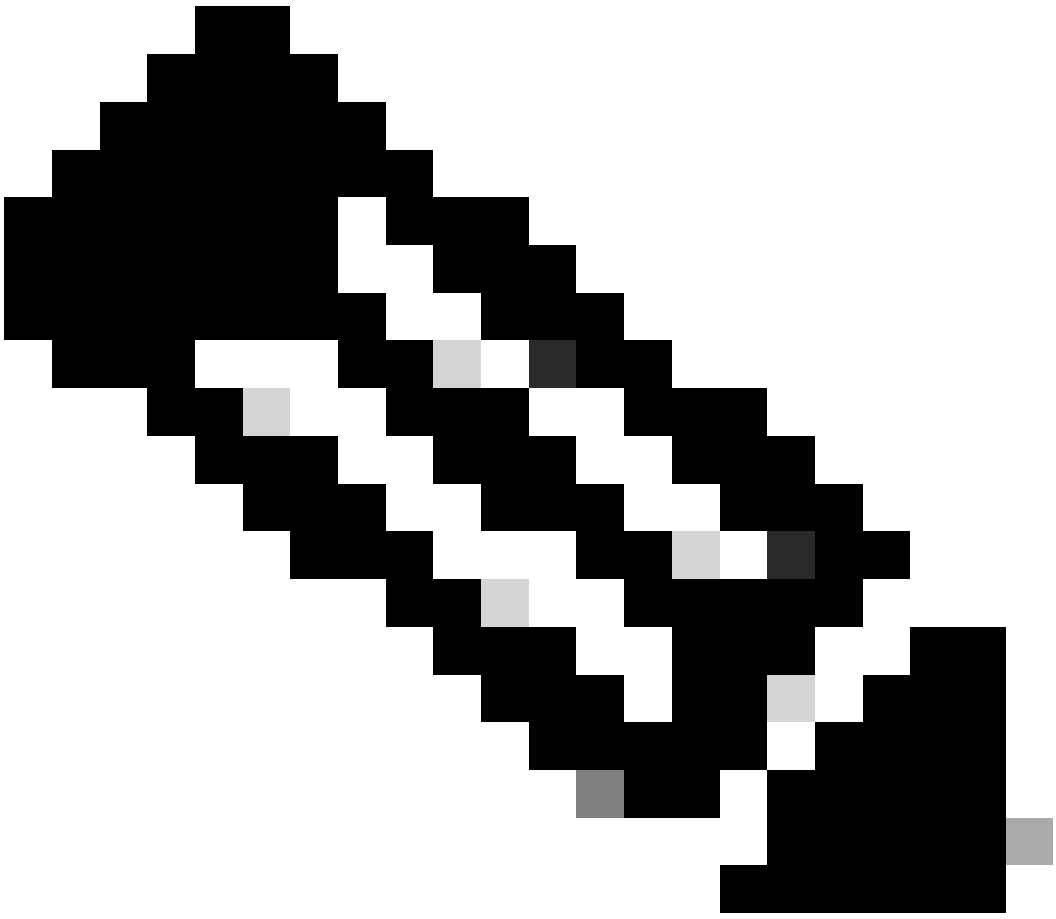


- LDev에 대한 디바이스 컨텍스트를 찾을 수 없습니다.

  이 결함은 논리 디바이스가 서비스 그래프 렌더링에 대해 위치할 수 없음을 나타냅니다. 예를 들어 서비스 그래프와 연결된 계약과 일치하는 디바이스 선택 정책이 없을 수 있습니다.

  해결 방법: 디바이스 선택 정책이 정의되었는지 확인합니다. Device Selection Policy(디바이스 선택 정책)는 계약 이름, 서비스 그래프 이름, 서비스 그래프 내의 노드 이름을 기반으로 서비스

디바이스 및 해당 커넥터에 대한 선택 기준을 지정합니다. 이는 Tenant(테넌트) > Services(서비스) > L4-L7 > Device Selection Policy(디바이스 선택 정책)에서 찾을 수 있습니다.

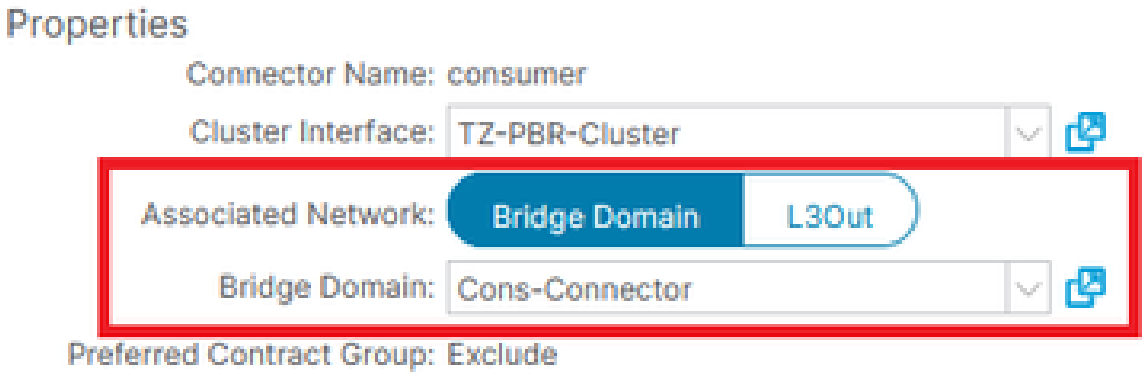


참고: 서비스 그래프 템플릿을 구축할 때 ACI는 소스 EPG에 대한 브리지 도메인을 미리 선택합니다. PBR 소비자 커넥터에 대해 이 브리지 도메인을 변경해야 합니다. 공급자 커넥터에도 마찬가지입니다.

- BD를 찾을 수 없음

  이 결함은 서비스 노드의 BD(Bridge Domain)를 찾을 수 없음을 나타냅니다. 예를 들어, BD는 Device Selection Policy(디바이스 선택 정책)에 지정되어 있지 않습니다.

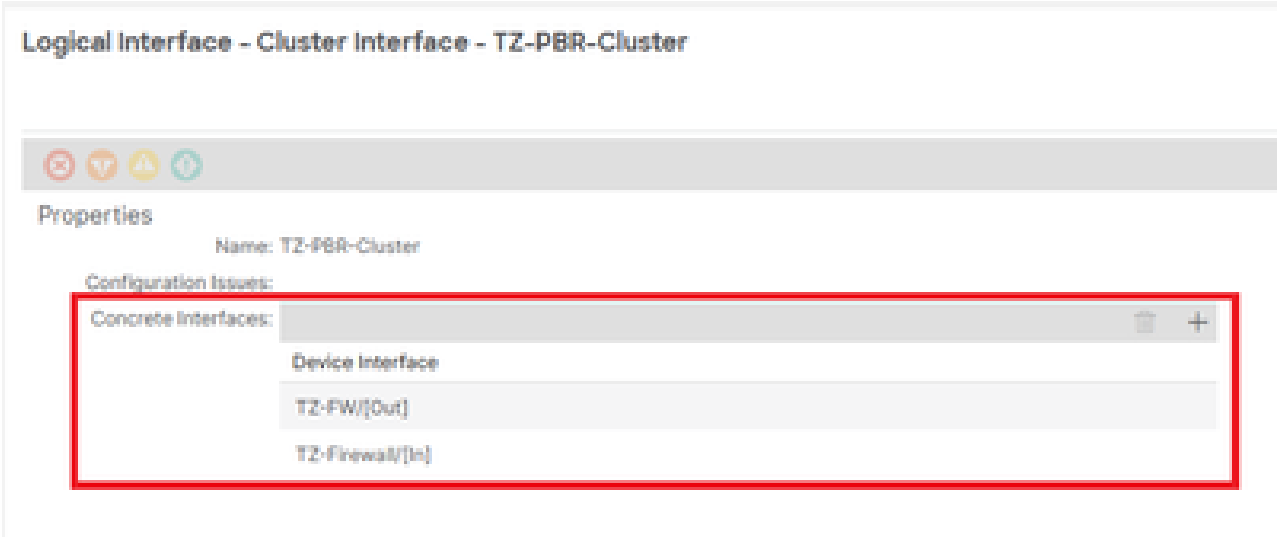
  해결 방법: BD가 장치 선택 정책에 지정되어 있고 커넥터 이름이 올바른지 확인하십시오. 이 컨피그레이션은 Tenant(테넌트) > Services(서비스) > L4-L7 > Devices Selection Policy(디바이스 선택 정책) > [Contract + SG] > [Consumer(소비자) 아래에 있습니다 | 공급자].



- LIf는 CIf와 관계가 없으며 LIf는 유효하지 않은 CIf를 갖습니다
- 클러스터 인터페이스를 찾을 수 없습니다.

  이러한 결함은 디바이스가 클러스터 인터페이스와 관계가 없음을 나타냅니다.

  해결 방법: 레이어 4 ~ 레이어 7(L4-L7) 디바이스 컨피그레이션에 지정된 콘크리트 인터페이스 선택기가 포함되어 있는지 확인합니다. 이 컨피그레이션은 Tenant(테넌트) > Services(서비스) > L4-L7 > Devices(디바이스) > [Device] > Cluster Interfaces(클러스터 인터페이스)에 있습니다.

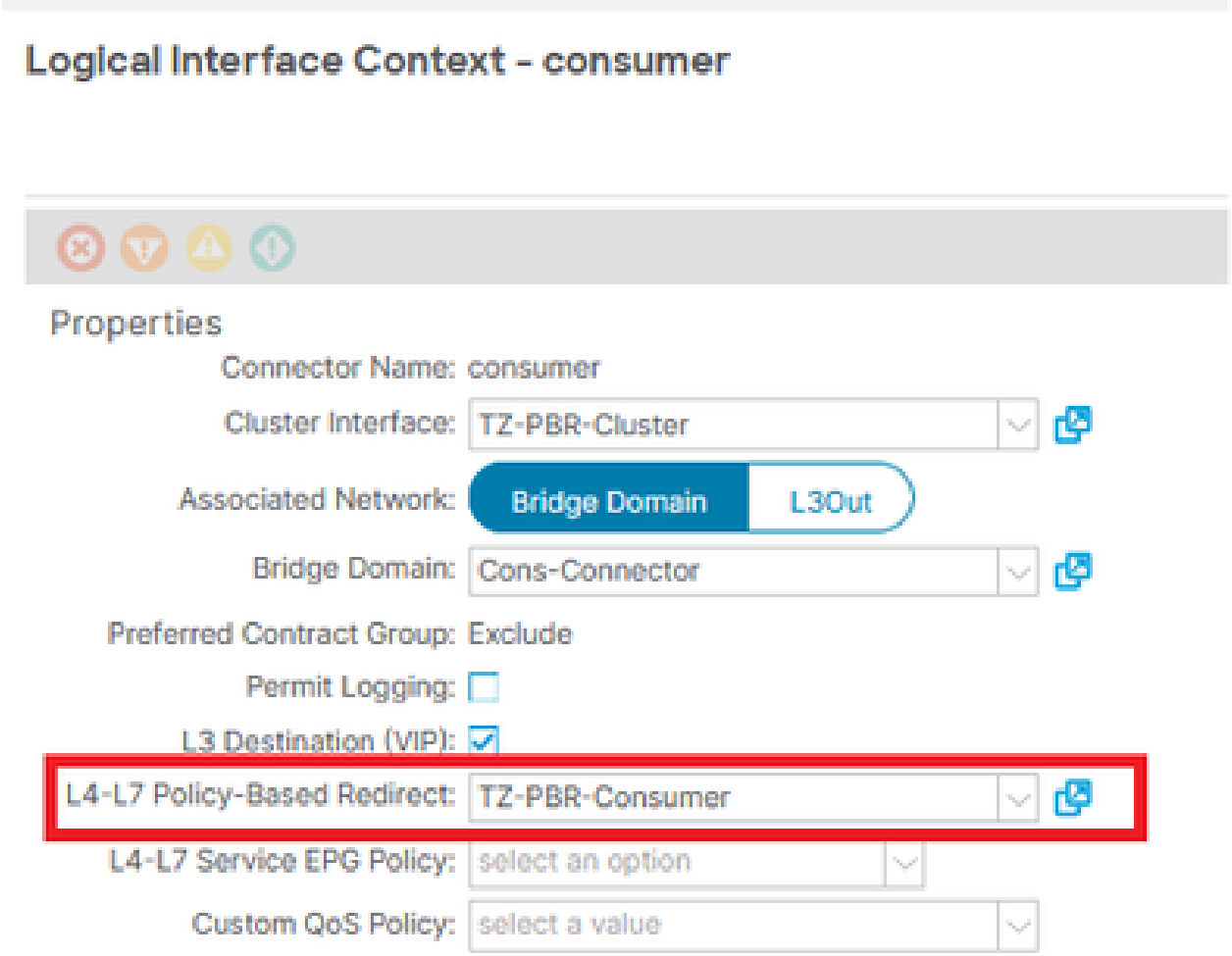


- 잘못된 서비스 리디렉션 정책

  이 결함은 서비스 그래프 내의 서비스 함수에서 리디렉션이 활성화되었음에도 불구하고

PBR 정책이 적용되지 않았음을 나타냅니다.

해결 방법: PBR 정책이 Device Selection Policy(디바이스 선택 정책) 설정 내에 구성되어 있는지 확인합니다. 이 컨피그레이션은 Tenant(테넌트) > Services(서비스) > L4-L7 > Devices Selection Policy(디바이스 선택 정책) > [Contract + SG] > [Consumer(소비자) 아래에 있습니다 | 공급자].



F0759: graph-rendering-failure - "Service graph for tenant < tenant >를 인스턴스화할 수 없습니다. 함수 노드 < node > 컨피그레이션이 잘못되었습니다."

함수 노드 이름의 잘못된 컨피그레이션으로 인해 지정된 테넌트에 대한 서비스 그래프를 인스턴스화할 수 없습니다.

이 오류는 앞서 언급한 조건과 관련된 컨피그레이션 문제가 있음을 나타냅니다.

또한 초기 구축 과정에서 이 결함이 일시적으로 발생하여 신속하게 해결될 수 있습니다. 이는 ACI가 모든 정책을 구축하기 위해 겪는 렌더링 프로세스로 인해 발생합니다.

해결 방법: 보고된 추가 결함을 조사하고 그에 따라 해결합니다.

F0764: configuration-failed - "L4-L7 Devices configuration < device > for tenant < tenant > is invalid."

PBR 디바이스 정책의 잘못된 컨피그레이션으로 인해 지정된 테넌트에 대한 서비스 그래프를

인스턴스화할 수 없습니다.

이 오류는 앞서 언급한 조건과 관련된 컨피그레이션 문제가 있음을 나타냅니다.

해결 방법: 보고된 추가 결함을 조사하고 그에 따라 해결합니다.

F0772: configuration-failed - "LIf configuration < cluster > for L4-L7 Devices < device > for tenant < tenant > is invalid."

PBR 디바이스 클러스터 인터페이스 선택의 잘못된 컨피그레이션으로 인해 지정된 테넌트에 대한 서비스 그래프를 인스턴스화할 수 없습니다.

이 오류는 앞서 언급한 조건과 관련된 컨피그레이션 문제가 있음을 나타냅니다.

해결 방법: 보고된 추가 결함을 조사하고 그에 따라 해결합니다.

2단계: 소스 및 대상 엔드포인트 학습

소스 및 대상 엔드포인트가 패브릭 내에서 인식되는지 확인합니다. 이 경우 기본 컨피그레이션이 필요합니다.

- VRF(Virtual Routing and Forwarding) 객체
- 유니캐스트 라우팅이 활성화된 BD(브리지 도메인) 개체입니다. IP 데이터 플레인 학습을 활성화하는 것이 모범 사례로 간주되지만, 필수 사항은 아닙니다.
- EPG(Endpoint Group) 객체. 가상 및 물리적 도메인에 모두 적용 가능합니다.
- 액세스 정책: 액세스 정책 컨피그레이션 체인이 완료되었으며 EPG에 결함이 보고되지 않았는지 확인합니다.

올바른 EPG 및 인터페이스에 대한 엔드포인트 학습을 확인하려면 엔드포인트가 학습된 경우(컴퓨팅 leaf라고도 함)에서 다음 명령을 실행합니다.

<#root>

show system internal epm endpoint [ip | mac] [x.x.x.x | eeee.eeee.eeee]

<#root>

Leaf101#

show system internal epm endpoint ip 10.10.100.10

MAC :

aaaa.aaaa.aaaa

::: Num IPs : 1

IP# 0 : 10.10.100.10

```
 ::: IP# 0 flags : ::: l3-sw-hit: No
Vlan id : 57 ::: Vlan vnid : 10865 :::
```

VRF name : TZ:Prod

```
BD vnid : 16056291 ::: VRF vnid : 2162692
Phy If : 0x16000008 ::: Tunnel If : 0
Interface :
```

port-channel9

```
Flags : 0x80004c05 :::
```

sclass : 49155

```
 ::: Ref count : 5
EP Create Timestamp : 02/18/2025 15:00:18.767228
EP Update Timestamp : 02/18/2025 15:04:57.908343
EP Flags : local|VPC|IP|MAC|sclass|timer|

::::


Leaf101#
```

이 명령을 사용하면 엔드포인트가 분류된 EPG와 연결된 sclass(pcTag)를 식별하고 인터페이스, VRF 범위 및 MAC 주소 정보를 검색할 수 있습니다.

소스 또는 대상 엔드포인트의 위치를 모르는 경우 APIC에서 항상 다음 명령을 수행할 수 있습니다.

<#root>

show endpoint [ip | mac] [x.x.x.x | eeee.eeee.eeee]

<#root>

```
APIC#
```

show endpoint ip 10.10.100.10

```
Legends:
(P):Primary VLAN
(S):Secondary VLAN


Dynamic Endpoints:
Tenant : TZ
Application : TZ
AEPg : Prod-Consumer

End Point MAC     IP Address                                Source       Node       Interface
----------------- ----------------------------------------- ------------ ---------- --------------------
```

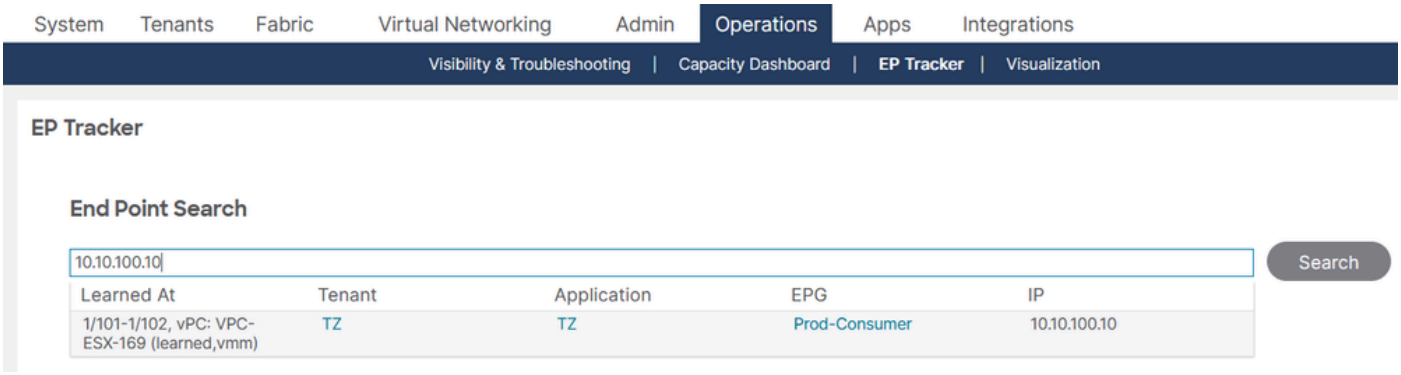
AA:AA:AA:AA:AA:AA 10.10.100.10

```
                              learned,vmm
101 102    vpc VPC-ESX-169

                vlan-2673       not-applicable    2025-02-18T15:16:40.

Total Dynamic Endpoints: 1
Total Static Endpoints: 0
APIC#
```

GUI에서 엔드포인트 모니터링 및 관리를 위해 Operations(운영) > EP Tracker(EP 추적기)로 이동하여 EP 추적기 기능에 액세스할 수 있습니다.



소스 및 대상 엔드포인트에서 수집한 정보를 바탕으로 이제 PBR 정책 구축에 집중할 수 있습니다.

3단계: 계약 리디렉션

PBR은 Service Graph 프레임워크 내에 통합됩니다. 따라서 계약에 따라 소스 스위치와 대상 스위치 모두에 서비스 그래프 템플릿을 구축하고 구성해야 합니다. 이전 단계에서 수집한 pcTags 정보를 활용하여 이 명령을 실행하여 EPG(Endpoint Group)가 서비스 그래프 그룹으로 리디렉션되고 있는지 확인할 수 있습니다.

<#root>

```
show zoning-rule scope [ vrf_scope ]
```

조닝 (zoning) 규칙에서는 다음 사항을 고려해야 합니다.

1. 연결된 리디렉션 그룹이 있는 대상 EPG에 대한 소스 EPG
2. 소스 PBR-노드 섀도우 EPG - 소스 EPG
3. 연결된 리디렉션 그룹이 있는 소스 EPG로의 대상 EPG. 이 그룹은 이전 컨피그레이션과 동일하거나 다를 수 있습니다.
4. 대상 EPG에 대한 대상 PBR-노드 섀도우 EPG

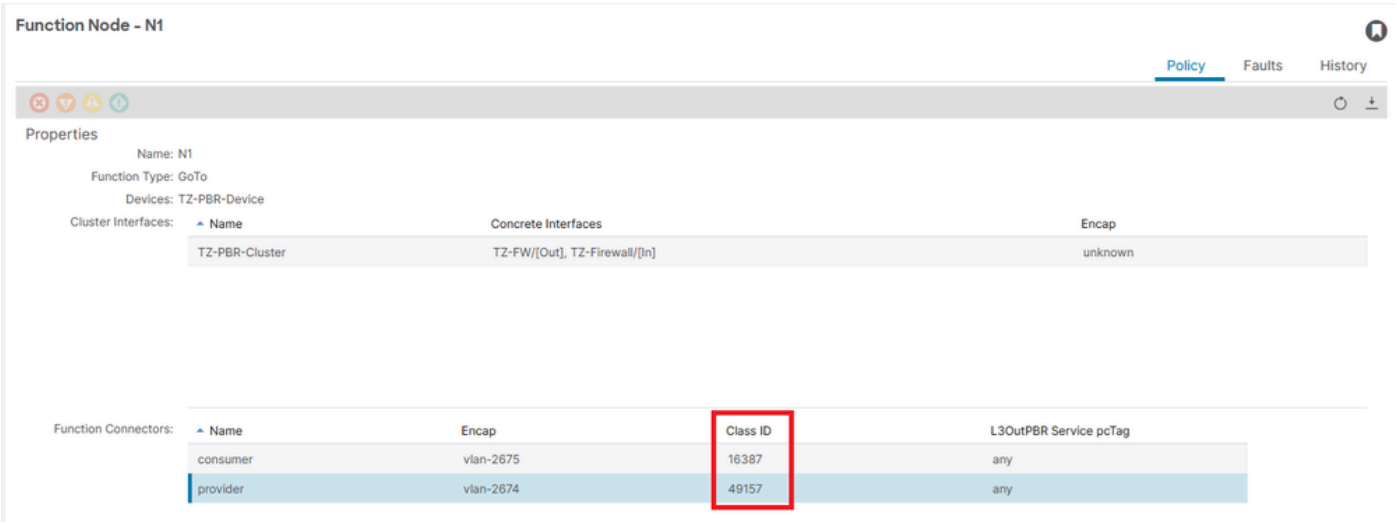
<#root>

```
Leaf101#

show zoning-rule scope 2162692
```

```
+---------+--------+--------+----------+---------------+---------+---------+------+------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |       Dir     |  operSt |  Scope  | Name |      Action      |
+---------+--------+--------+----------+---------------+---------+---------+------+------------------+
|   4565  |  49155 |  49156 |  default |     bi-dir    | enabled | 2162692 |      | redir(destgrp-8) |
|   4565  |  49156 |  49155 |  default | uni-dir-ignore | enabled | 2162692 |      | redir(destgrp-9) |
|   4973  |  16387 |  49155 |  default |     uni-dir   | enabled | 2162692 |      |      permit      |
|   4564  |  49157 |  49156 |  default |     uni-dir   | enabled | 2162692 |      |      permit      |
+---------+--------+--------+----------+---------------+---------+---------+------+------------------+
Leaf101#
```

PBR(Policy-Based Routing) 구축 프로세스 중에 생성된 섀도우 EPG의 pcTag를 확인하려면 Tenants > [TENANT_NAME] > Services > L4-L7 > Deployed Graph Instance > [SG_NAME] > Function Node - N1로 이동합니다.



- Contract 파서

스크립트는 영역 지정 규칙, 필터, 통계 및 EPG 이름의 상관관계를 분석합니다. ACI 리프 또는 APIC에서 직접 이 스크립트를 안전하게 실행할 수 있습니다. APIC에서 실행할 경우 모든 리프 스위치에서 구체적인 객체를 수집합니다. 대규모 정책 구축에 몇 분 정도 걸릴 수 있습니다.

ACI 버전 3.2부터 contract_parser는 이미지 내에 번들로 제공되며 leaf에서 사용할 수 있습니다. iBash 셸에서 contract_parser.py를 입력하기만 하면 됩니다.

<#root>

```
Leaf101#
```

contract_parser.py --sepg 49155

```
Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4] [flags][contract:{str}] [hi

[7:4999] [vrf:TZ:Prod] log,
```

redir

```
 ip tn-TZ/ap-TZ/epg-
```

Prod-Consumer(49155)

tn-TZ/ap-TZ/epg-

Prod-Provideer(49156)

[contract:uni/tn-TZ/brc-

TZ-PBR-Contract

] [

hit=81

]

destgrp-8

vrf:TZ:Prod ip:

192.168.100.10

mac:

00:50:56:B7:D0:5D

bd:uni/tn-TZ/

BD-Cons-Connector

Leaf101#

이 명령은 계약 작업, 소스 및 대상 EPG, 사용 중인 계약 이름, 적중 횟수 등의 세부 정보를 제공합니다.

4단계: 리디렉션 그룹

조닝 규칙에 적용된 계약에 따라 리디렉션 그룹을 식별한 다음 단계는 리디렉션 대상 디바이스의 IP 및 MAC 주소를 확인하는 것입니다. 이를 위해 다음 명령을 실행합니다.

<#root>

show service redir info group [destgrp_ID]

<#root>

Leaf101#

show service redir info group 8

```
========================================================================================================
LEGEND
TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest | TRA: Tr
========================================================================================================
GrpID Name      destination                          HG-name         BAC W   operSt  operStQual   TL  T
===== ====      ===========                          ============== === === ======= ============ === ==
```

```
8     destgrp-8 dest-[
192.168.100.10
]-[vxlan-
2162692
] Not attached   N   1
enabled
 no-oper-grp  0   0   sym no  no
Leaf101#
Leaf101# show service redir info group 9
================================================================================================================
LEGEND
TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest | TRA: Tra
================================================================================================================
GrpID Name      destination                          HG-name        BAC W   operSt  operStQual   TL  TH
===== ====      ===========                          ============== === === ======= ============ === ==
9     destgrp-9 dest-[
192.168.200.20
]-[vxlan-
2162692
] Not attached   N   1
enabled
 no-oper-grp  0   0   sym no  no
Leaf101#
```

이 명령을 사용하면 리디렉션 그룹의 운영 상태(OperSt), L4-L7 PBR 섹션에 구성된 IP 주소, PBR-노드 브리지 도메인과 연결된 VRF의 VNID를 확인할 수 있습니다. 이제 구성된 MAC 주소를 결정해야 합니다.

<#root>

show service redir info destinations ip [PBR-node IP] vnid [VRF_VNID]

<#root>

```
Leaf101#
show service redir info destination ip 192.168.100.10 vnid 2162692

================================================================================================================
LEGEND
TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest | TRA: Tra
================================================================================================================
Name                                bdVnid         vMac              vrf     operSt  operStQual   HG-n
====                                ======         ====              ====    =====   ==========   ====
dest-[
```

192.168.100.10

]-[vxlan-

2162692

] vxlan-

15826939

00:50:56:B7:D0:5D

TZ:Prod

enabled

no-oper-dest Not attached
Leaf101#
Leaf101# show service redir info destination ip 192.168.200.20 vnid 2162692
==========
LEGEND
TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest | TRA: Tra
==========
Name bdVnid vMac vrf operSt operStQual HG-
==== ====== ==== ==== ===== ========= ===
dest-[

192.168.200.20

]-[vxlan-

2162692

] vxlan-

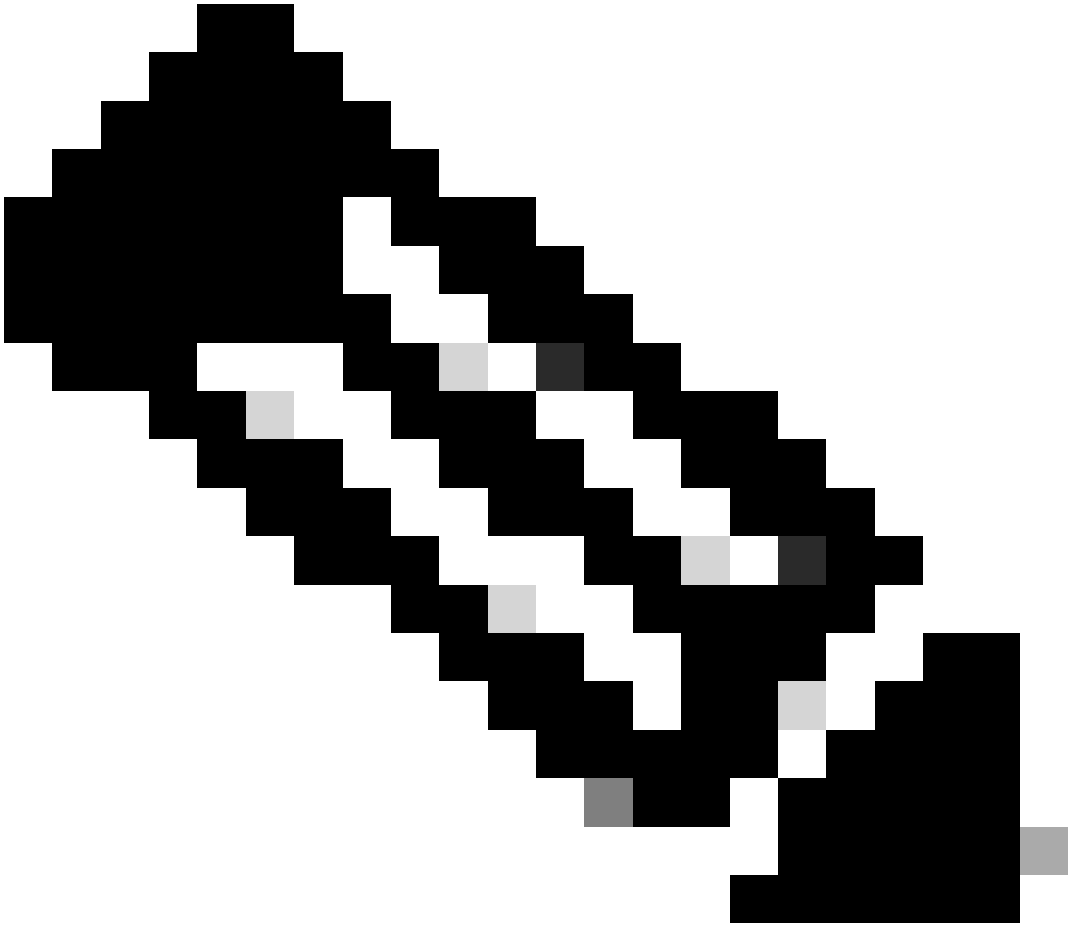
16646036 00:50:56:B7:BF:94

TZ:Prod

enabled

no-oper-dest Not attached
Leaf101#

앞서 언급한 세부사항 외에도 이 명령은 VRF 이름, BD VNID 및 PBR-node의 구성된 MAC 주소를 비롯한 유용한 정보를 제공합니다.



참고: 이 단계에서 IP 주소와 MAC 주소가 모두 사용자 구성됩니다. 즉, L4-L7 정책 기반 라우팅 정의 중에 입력 오류가 발생할 수 있습니다.

5단계: PBR-node가 트래픽을 수신하지 않습니다.

PBR 전달에서 자주 발생하는 문제는 PBR 노드에 도달하는 트래픽이 없다는 것입니다. 이 문제의 빈번한 원인은 L4-L7 정책 기반 라우팅 컨피그레이션에서 잘못 지정된 MAC 주소입니다.

L4-L7 정책 기반 라우팅에 구성된 MAC 주소의 정확성을 확인하려면 2단계에서 이전에 사용한 명령을 실행합니다. 이 명령은 서비스 리프로 지정된 리프 스위치에서 실행할 수 있으며, 여기서 노드를 학습해야 합니다.

<#root>

```
show system internal epm endpoint [ ip | mac ] [ x.x.x.x | eeee.eeee.eeee ]
```

<#root>

Leaf103#

show system internal epm endpoint ip 192.168.100.10

MAC :

0050.56b7.d05d

::: Num IPs : 1
IP# 0 :

192.168.100.10

::: IP# 0 flags : ::: l3-sw-hit: Yes ::: flags2 :

dp-lrn-dis

Vlan id : 71 ::: Vlan vnid : 10867 ::: VRF name : TZ:Prod
BD vnid : 15826939 ::: VRF vnid :

2162692

Phy If : 0x16000008 ::: Tunnel If : 0
Interface : port-channel19
Flags : 0x80004c25 ::: sclass : 16387 ::: Ref count : 5
EP Create Timestamp : 02/19/2025 12:07:44.065032
EP Update Timestamp : 02/19/2025 15:27:03.400086
EP Flags : local|vPC|peer-aged|IP|MAC|sclass|timer|

::::

Leaf103#

.....

Leaf103#

show system internal epm endpoint ip 192.168.200.20

MAC :

0050.56b7.bf94

::: Num IPs : 1
IP# 0 :

192.168.200.20

::: IP# 0 flags : ::: l3-sw-hit: Yes ::: flags2 :

dp-lrn-dis

Vlan id : 60 ::: Vlan vnid : 10866 ::: VRF name : TZ:Prod
BD vnid : 16646036 ::: VRF vnid :

2162692

```
Phy If : 0x16000008 ::: Tunnel If : 0
Interface : port-channel19
Flags : 0x80004c25 ::: sclass : 49157 ::: Ref count : 5
EP Create Timestamp : 02/19/2025 13:51:03.377942
EP Update Timestamp : 02/19/2025 15:28:34.151877
EP Flags : local|vPC|peer-aged|IP|MAC|sclass|timer|

::::


Leaf103#
```

EPM 테이블에 기록된 MAC 주소가 서비스 리디렉션 그룹에 구성된 주소와 일치하는지 확인합니다. PBR 노드 대상에 대한 적절한 트래픽 라우팅을 보장하려면 사소한 입력 오류라도 수정해야 합니다.

6단계: 트래픽 흐름.

- 부패

ELAM 프로세스의 구성 및 해석을 엔드 투 엔드로 자동화하도록 설계된 APIC용 CLI 툴입니다. 이 도구를 사용하면 특정 흐름 및 흐름이 시작되는 리프 스위치를 지정할 수 있습니다. 각 노드에서 ELAM을 순차적으로 실행하여 플로우의 포워딩 경로를 분석합니다. 이 툴은 패킷 경로를 쉽게 식별할 수 없는 복잡한 토폴로지에서 특히 유용합니다.

<#root>

```
APIC #
```

ftriage -user admin route -sip 10.10.100.10 -dip 10.20.200.20 -ii LEAF:101,102

```
Starting ftriage
```

Log file name for the current run is: ftlog_2025-02-25-10-26-05-108.txt

```
2025-02-25 10:26:05,116 INFO /controller/bin/ftriage -user admin route -sip 10.10.100.10 -dip 10.20.200
Request password info for username: admin
Password:
2025-02-25 10:26:31,759 INFO ftriage: main:2505 Invoking ftriage with username: admin
2025-02-25 10:26:34,188 INFO ftriage: main:1546 Enable Async parellel ELAM with 2 nodes
2025-02-25 10:26:57,927 INFO ftriage: fcls:2510
```

LEAF101

```
: Valid ELAM for asic:0 slice:0 srcid:64 pktid:1913
2025-02-25 10:26:59,120 INFO ftriage: fcls:2863
```

LEAF101

```
: Signal ELAM found for Async lookup
2025-02-25 10:27:00,620 INFO ftriage: main:1317 L3 packet
```

Seen on LEAF101

```
 Ingress:
```

Eth1/45 (Po9)

Egress: Eth1/52 Vnid: 2673
2025-02-25 10:27:00,632 INFO ftriage: main:1372 LEAF101: Incoming Packet captured with [

SIP:10.10.100.10, DIP:10.20.200.20

]
...
2025-02-25 10:27:08,665 INFO ftriage: main:480 Ingress

BD(s) TZ:Prod-Consumer

2025-02-25 10:27:08,666 INFO ftriage: main:491 Ingress

Ctx: TZ:Prod Vnid: 2162692

...
2025-02-25 10:27:45,337 INFO ftriage: pktrec:367 LEAF101:

traffic is redirected

...
2025-02-25 10:28:10,701 INFO ftriage: unicast:1550 LEAF101:

traffic is redirected

to vnid:15826939

mac:00:50:56:B7:D0:5D

via tenant:TZ

graph:TZ-PBR-SG

contract:

TZ-PBR-Contract

...
2025-02-25 10:28:20,339 INFO ftriage: main:975

Found peer-node SPINE1001

and IF: Eth1/1 in candidate list
...
2025-02-25 10:28:39,471 INFO ftriage: main:1366

SPINE1001

: Incoming Packet captured with Outer [SIP:10.2.200.64, DIP:10.2.64.97] .... Inner [

SIP:10.10.100.10, DIP:10.20.200.20

]
2025-02-25 10:28:39,472 INFO ftriage: main:1408

SPINE1001

: Outgoing packet's Vnid:

15826939

2025-02-25 10:28:58,469 INFO ftriage: fib:524

SPINE1001: Proxy in spine

```
...
2025-02-25 10:29:07,898 INFO ftriage: main:975
Found peer-node LEAF103
. and IF: Eth1/50 in candidate list
...
2025-02-25 10:29:35,331 INFO ftriage: main:1366
LEAF103
: Incoming Packet captured with Outer [SIP:10.2.200.64, DIP:10.2.200.64] .... Inner [
SIP:10.10.100.10, DIP:10.20.200.20
]
...
2025-02-25 10:29:50,277 INFO ftriage: ep:128 LEAF103: pbr traffic with dmac:
00:50:56:B7:D0:5D

2025-02-25 10:30:07,374 INFO ftriage: main:800 Computed egress encap string
vlan-2676

2025-02-25 10:30:13,326 INFO ftriage: main:535 Egress
Ctx TZ:Prod

2025-02-25 10:30:13,326 INFO ftriage: main:536 Egress BD(s):
TZ:Cons-Connector

...
2025-02-25 10:30:18,812 INFO ftriage: misc:908 LEAF103: caller unicast:581
EP if(Po19)
 same as egr if(Po19)
2025-02-25 10:30:18,812 INFO ftriage: misc:910 LEAF103: L3 packet caller unicast:668 getting
bridged
 in SUG
2025-02-25 10:30:18,813 INFO ftriage: main:1822 dbg_sub_nexthop function returned values on node LEAF10
2025-02-25 10:30:19,378 INFO ftriage: acigraph:794 : Ftriage Completed with hunch: matching service dev
APIC #
```

- ELAM:

ELAM(Embedded Logic Analyzer Module)은 사용자가 하드웨어에서 특정 조건을 설정하여 해당 조건을 충족하는 초기 패킷 또는 프레임을 캡처할 수 있도록 하는 진단 도구입니다. 캡처에 성공하면 ELAM 상태가 트리거됨으로 표시됩니다. 트리거되면 ELAM이 비활성화되어 데이터 덤프를 수집할 수 있습니다. 그러면 해당 패킷 또는 프레임에 대해 스위치의 ASIC에서 실행한 수많은 포워딩 결정을 쉽게 분석할 수 있습니다. ELAM은 ASIC 레벨에서 작동하므로 스위치의 CPU 또는 기타 리소스에 영향을 주지 않습니다.

명령 구문의 구조. 이 구조는 Troubleshoot ACI Intra-Fabric Forwarding Tools에서 수집되었습니다

```
vsh_lc                                          [This command enters the line card shell where ELAMs are r
debug platform internal <asic> elam asic 0      [refer to the ASICs table]
```

트리거할 조건 설정

```
trigger reset                                                   [ensures no existing triggers are running]
trigger init in-select <number> out-select <number>             [determines what information about a packet is
set outer/inner                                                 [sets conditions]
start                                                           [starts the trigger]
status                                                          [checks if a packet is captured]
```

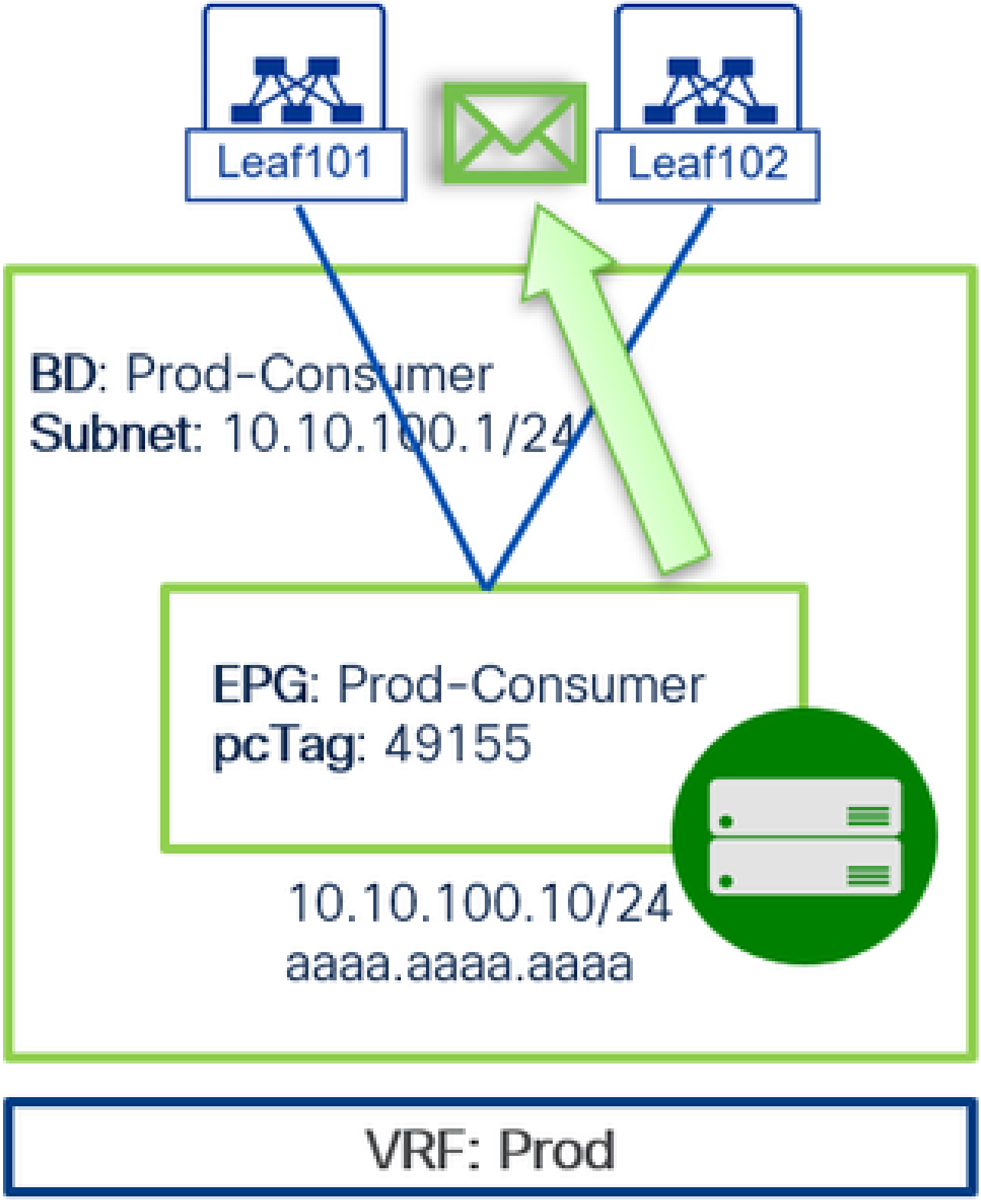
패킷 분석을 포함하는 덤프를 생성합니다.

```
ereport             [display detailed forwarding decision for the packet]
```

- 트래픽 흐름

문제가 되는 모든 디바이스의 트래픽 흐름을 이해하는 것이 중요합니다. Ftriage 툴은 이 흐름을 매우 잘 요약합니다. 그러나 세부적인 단계별 검증을 수행하고 패킷 수신 프로세스에 대한 심층적인 통찰력을 얻기 위해 네트워크 토폴로지 내의 각 지점에서 ELAM(Embedded Logic Analyzer Module)을 실행할 수 있습니다.

1. 소스 서버가 학습된 컴퓨팅 리프에서 인그레스 트래픽이 발생합니다. 이 시나리오에서는 소스가 vPC 인터페이스 뒤에 배치되므로 vPC 피어에서 ELAM을 구성해야 합니다. 이는 해싱 알고리즘이 선택한 물리적 인터페이스가 불확정이기 때문에 필요합니다.



<#root>

LEAF101#

vsh_lc

module-1#

debug platform internal tah elam asic 0

```
module-1(DBG-elam)#
trigger reset

module-1(DBG-elam)#
trigger init in-select 6 out-select 1

module-1(DBG-elam-insel6)#
reset

module-1(DBG-elam-insel6)#
set outer ipv4 src_ip 10.10.100.10 dst_ip 10.20.200.20

module-1(DBG-elam-insel6)#
start

module-1(DBG-elam-insel6)#
status

ELAM STATUS
===========
Asic 0 Slice 0 Status
Triggered

Asic 0 Slice 1 Status Armed

module-1(DBG-elam-insel6)#
 ereport

================================================================================================================
Trigger/Basic Information
================================================================================================================
...
Incoming Interface : 0x40( 0x40 )


>>> Eth1/45


...

----------------------------------------------------------------------------------------------------------------
Outer L2 Header
----------------------------------------------------------------------------------------------------------------
Destination MAC : 0022.BDF8.19FF >>> Bridge-domain MAC address


Source MAC : AAAA.AAAA.AAAA
```

802.1Q tag is valid : yes(0x1)
CoS : 0(0x0)

Access Encap VLAN : 2673

(0xA71)

Outer L3 Header

L3 Type : IPv4
IP Version : 4
DSCP : 0
IP Packet Length : 84 (= IP header(28 bytes) + IP payload)
Don't Fragment Bit : set
TTL : 64
IP Protocol Number : ICMP
IP CheckSum : 6465(0x1941)

Destination IP : 10.20.200.20

Source IP : 10.10.100.10

Contract Lookup Key

IP Protocol : ICMP(0x1)
L4 Src Port : 2048(0x800)
L4 Dst Port : 7345(0x1CB1)

sclass (src pcTag) : 49155(0xC003) >>> Prod-Consumer

EPG

dclass (dst pcTag) : 49156(0xC004)

>>> Prod-Provider EPG

src pcTag is from local table : yes

>>> EPGs are known locally

derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet : no
If yes, Contract is not applied here because it is flooded

Sideband Information

---

ovector : 176(0xB0) >>> Eth1/52

```
Ovec in "show plat int hal l2 port gpd"

Opcode : OPCODE_UC


----------------------------------------------------------------------------------------------------
sug_luc_latch_results_vec.luc3_0.

service_redir: 0x1 >>> Service Redir 0x1 = PBR was applied


----------------------------------------------------------------------------------------------------
```

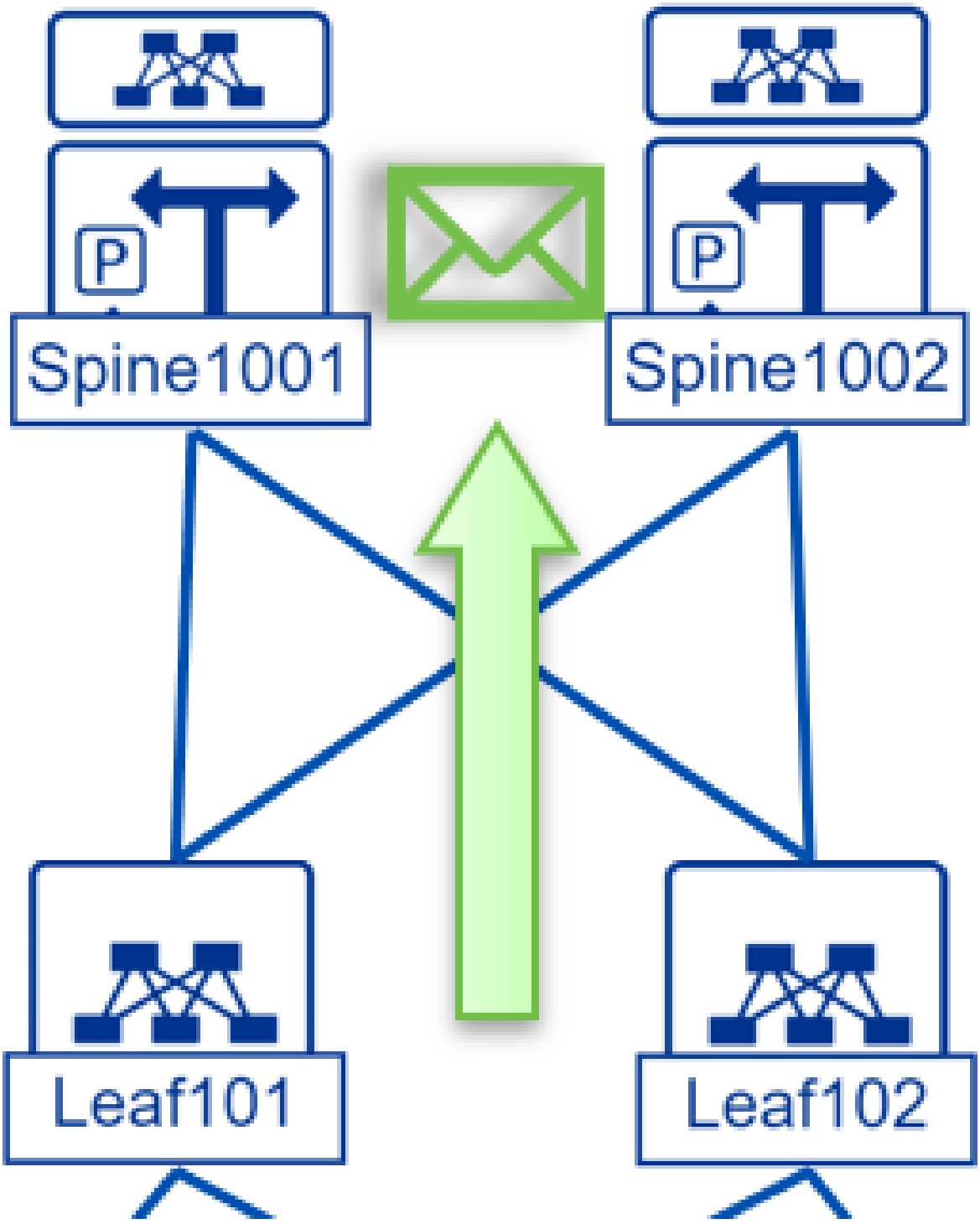
제공된 정보에 따르면 service_redir 옵션이 활성화되었으므로 패킷이 PBR(Policy-Based Routing)을 통해 리디렉션되고 있음이 분명합니다. 또한 sclass 및 dclass 값을 검색합니다. 이 특정 시나리오에서 스위치는 dclass를 인식합니다. 그러나 대상 끝점이 EPM 테이블에 없는 경우 dclass 값은 기본적으로 1입니다.

또한 인그레스 인터페이스는 SRCID에 의해 결정되며 이그레스 인터페이스는 벡터 값에 의해 식별됩니다. 다음 값은 vsh_lc 레벨에서 이 명령을 실행하여 전면 포트로 변환할 수 있습니다.

<#root>

```
show platform internal hal l2 port gpd
```

2. 흐름의 후속 단계에서는 대상 MAC 주소를 PBR 노드에 매핑하기 위해 스파인 스위치에 연결합니다. 트래픽이 VXLAN 헤더에 캡슐화되므로 스파인 또는 원격 리프에 ELAM을 실행하려면 in-select 14를 사용하여 캡슐화를 올바르게 디코딩해야 합니다.



<#root>

SPINE1001#

vsh_lc

module-1#

debug platform internal roc elam asic 0

```
module-1(DBG-elam)#
trigger reset

module-1(DBG-elam)#
trigger init in-select 14 out-selec 0

module-1(DBG-elam-insel14)#
reset

module-1(DBG-elam-insel14)#
set inner ipv4 src_ip 10.10.100.10 dst_ip 10.20.200.20

module-1(DBG-elam-insel14)#
start

module-1(DBG-elam-insel14)#
status

ELAM STATUS
===========
Asic 0 Slice 0 Status Armed
Asic 0 Slice 1 Status Armed
Asic 0 Slice 2 Status Triggered

Asic 0 Slice 3 Status Armed

module-1(DBG-elam-insel14)#
ereport



================================================================================================================
Trigger/Basic Information
================================================================================================================
Incoming Interface :
0x48( 0x48 )  >>> Eth1/1

( Slice Source ID(Ss) in "show plat int hal l2 port gpd" )
Packet from vPC peer LEAF : yes
Packet from tunnel (remote leaf/avs) : yes

----------------------------------------------------------------------------------------------------------------
Outer L2 Header
----------------------------------------------------------------------------------------------------------------
Destination MAC : 000D.0D0D.0D0D
Source MAC : 000C.0C0C.0C0C

----------------------------------------------------------------------------------------------------------------
Inner L2 Header
```

Inner Destination MAC : 0050.56B7.D05D >>> Firewall MAC

Source MAC : AAAA.AAAA.AAAA

Outer L3 Header

L3 Type : IPv4
DSCP : 0
Don't Fragment Bit : 0x0
TTL : 32
IP Protocol Number : UDP
Destination IP : 10.2.64.97
Source IP : 10.2.200.64

Inner L3 Header

L3 Type : IPv4
DSCP : 0
Don't Fragment Bit : 0x1
TTL : 63
IP Protocol Number : ICMP

Destination IP : 10.20.200.20

Source IP : 10.10.100.10

Outer L4 Header

L4 Type : iVxLAN
Don't Learn Bit : 1
Src Policy Applied Bit : 1
Dst Policy Applied Bit : 1

sclass (src pcTag) : 0xc003 >>> pcTag 49155 (Prod-Consumer)

VRF or BD VNID : 15826939(0xF17FFB) >>> BD: Prod-Consumer

Sideband Information

Opcode : OPCODE_UC

---

bky_elam_out_sidebnd_no_spare_vec.

ovector_idx: 0x1F0 >>> Eth1/10

이전 출력에서 대상 MAC 주소가 방화벽의 MAC 주소로 재작성되는 것이 분명합니다. 그런 다음 COOP 조회를 수행하여 MAC의 목적지 게시자를 확인한 다음 패킷을 스위치의 해당 인터페이스로 전달합니다.

브리지 도메인 VNID 및 방화벽의 MAC 주소를 사용하여 이 명령을 실행하여 스파인에서 이 조회를 시뮬레이션할 수 있습니다.

<#root>

SPINE1001#

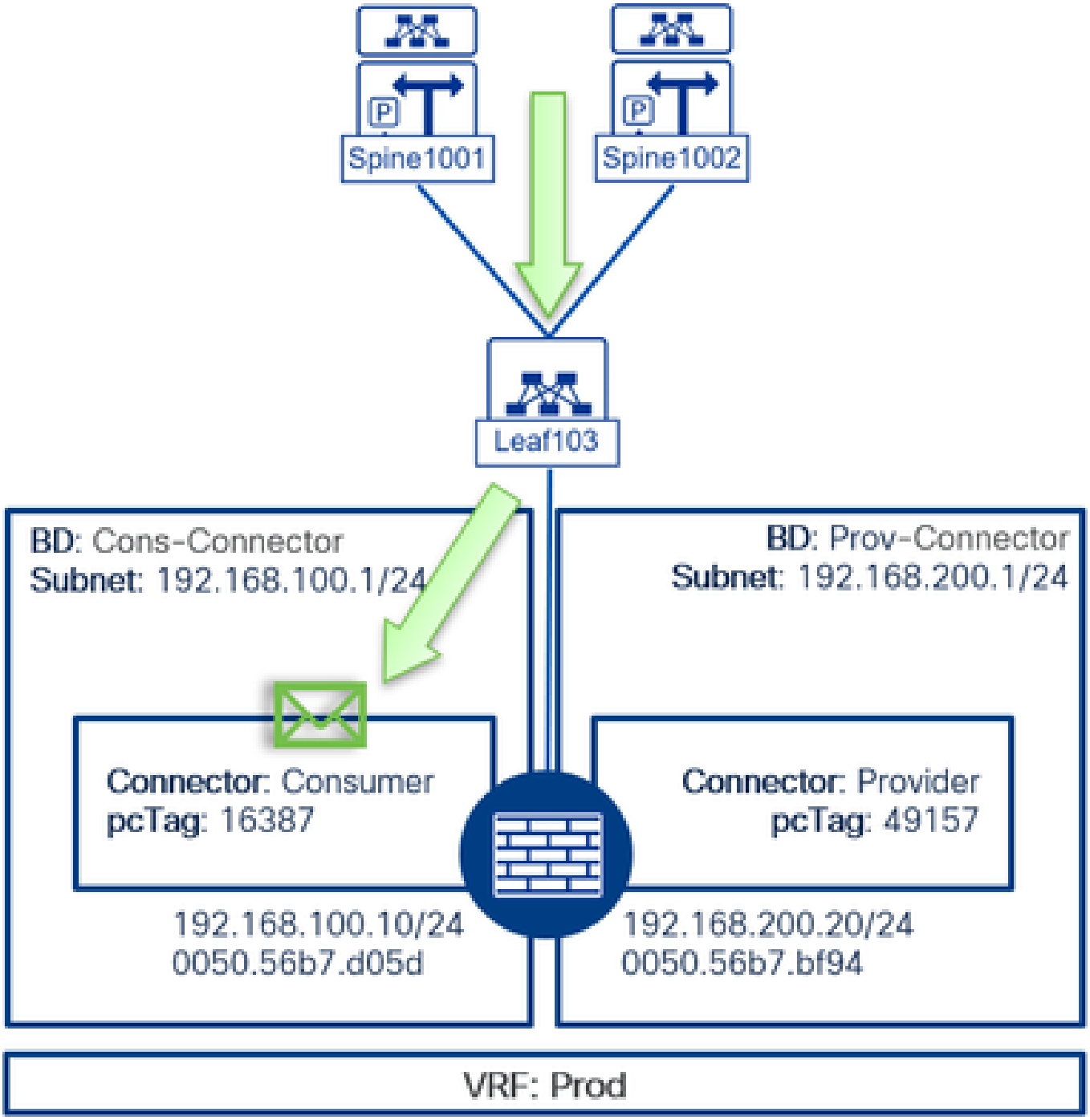
show coop internal info repo ep key 15826939 0050.56B7.D05D | egrep "Tunnel|EP" | head -n 3

EP bd vnid : 15826939
EP mac : 00:50:56:B7:D0:5D

Tunnel nh : 10.2.200.66

SPINE1001#

3. 트래픽은 방화벽의 MAC 주소가 인식되어 PBR 노드로 전달되는 서비스 leaf에 도달합니다.



<#root>

MXS2-LF101#

vsh_lc

module-1#

debug platform internal tah elam asic 0

module-1(DBG-elam)#

trigger reset

```
module-1(DBG-elam)#
trigger init in-select 14 out-select 1

module-1(DBG-elam-insel14)#
reset

module-1(DBG-elam-insel14)#
set inner ipv4 src_ip 10.10.100.10 dst_ip 10.20.200.20

module-1(DBG-elam-insel14)#
start

module-1(DBG-elam-insel14)#
status


ELAM STATUS
===========
Asic 0 Slice 0 Status Armed
Asic 0 Slice 1 Status Triggered


module-1(DBG-elam-insel14)#
ereport


================================================================================================================
Trigger/Basic Information
================================================================================================================
Incoming Interface : 0x0( 0x0 ) >>> Eth1/17

( Slice Source ID(Ss) in "show plat int hal l2 port gpd" )
Packet from vPC peer LEAF : yes
Packet from tunnel (remote leaf/avs) : yes

----------------------------------------------------------------------------------------------------------------
Outer L2 Header
----------------------------------------------------------------------------------------------------------------
Destination MAC : 000D.0D0D.0D0D
Source MAC : 000C.0C0C.0C0C

----------------------------------------------------------------------------------------------------------------
Inner L2 Header
----------------------------------------------------------------------------------------------------------------
Inner
Destination MAC : 0050.56B7.D05D >>> Firewall MAC

Source MAC : AAAA.AAAA.AAAA
```

```
------------------------------------------------------------------------------------------------------------
Outer L3 Header
------------------------------------------------------------------------------------------------------------
L3 Type : IPv4
DSCP : 0
Don't Fragment Bit : 0x0
TTL : 32
IP Protocol Number : UDP
Destination IP : 10.2.200.66
Source IP : 10.2.200.64

------------------------------------------------------------------------------------------------------------
Inner L3 Header
------------------------------------------------------------------------------------------------------------
L3 Type : IPv4
DSCP : 0
Don't Fragment Bit : 0x1
TTL : 63
IP Protocol Number : ICMP
```

Destination IP : 10.20.200.20

Source IP : 10.10.100.10

```
------------------------------------------------------------------------------------------------------------
Outer L4 Header
------------------------------------------------------------------------------------------------------------
L4 Type : iVxLAN
Don't Learn Bit : 1
Src Policy Applied Bit : 1
Dst Policy Applied Bit : 1
```

sclass (src pcTag) : 0xc003 >>> pcTag 49155 (Prod-Consumer)

VRF or BD VNID : 15826939(0xF17FFB) >>> BD: Prod-Consumer

```
------------------------------------------------------------------------------------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------------------
IP Protocol : ICMP( 0x1 )
L4 Src Port : 2048( 0x800 )
L4 Dst Port : 50664( 0xC5E8 )
```

sclass (src pcTag) : 49155(0xC003) >>> Prod-Consumer EPG

dclass (dst pcTag) : 16387(0x4003) >>> Consumer connector EPG

```
src pcTag is from local table : no
derived from group-id in iVxLAN header of incoming packet
Unknown Unicast / Flood Packet : no
If yes, Contract is not applied here because it is flooded

------------------------------------------------------------------------------------------------------------
Sideband Information
```

---

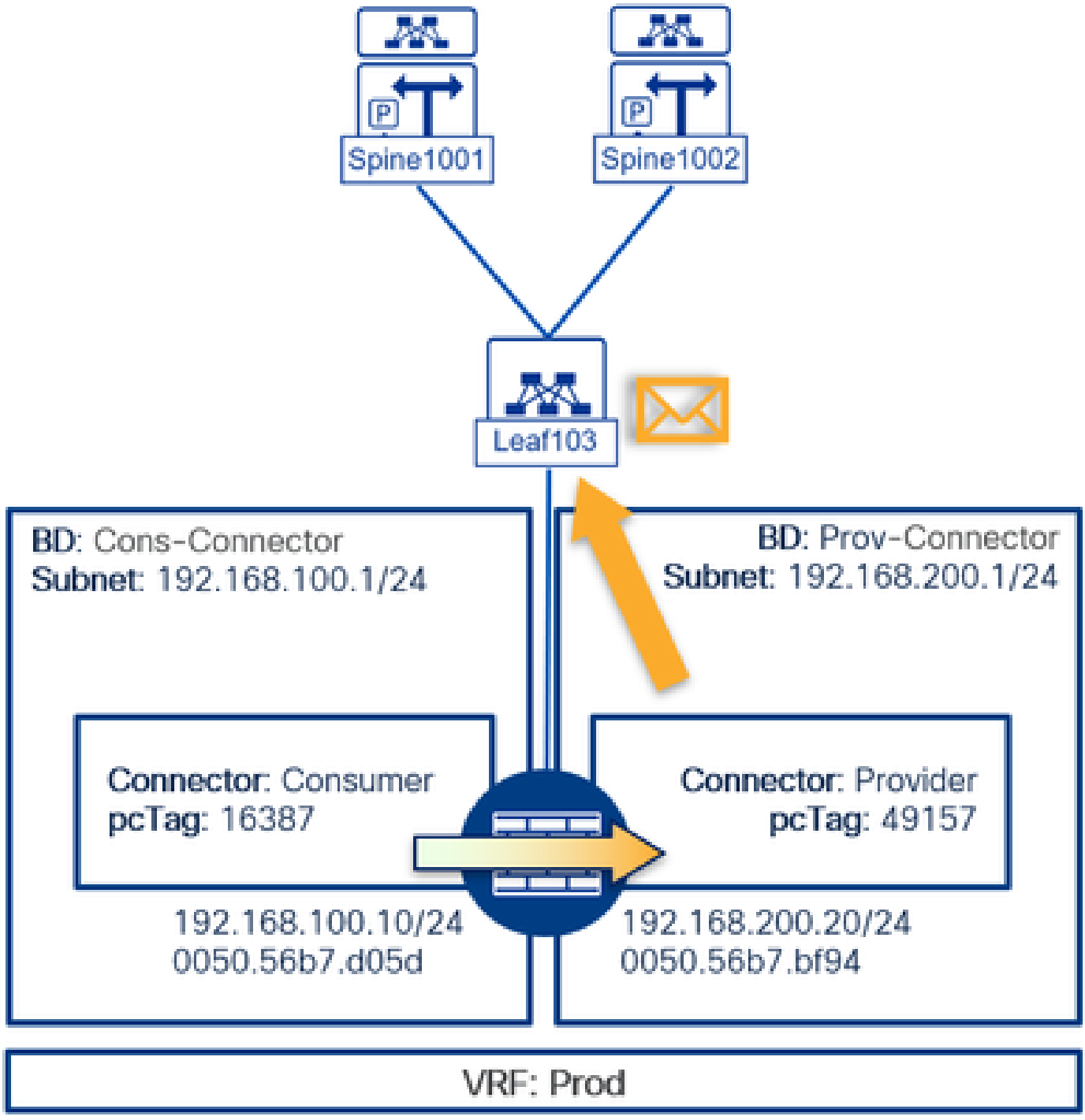
ovector

:

64(0x40) >>> Eth1/45

```
Ovec in "show plat int hal l2 port gpd"
Opcode : OPCODE_UC
```

4. PBR 노드에서 반환하는 패커의 경우, 먼저 이 패커는 자체 실사를 수행하고 VRF, 인터페이스 또는 VLAN을 변경해야 합니다. 그런 다음 패킷은 사업자 커넥터의 ACI로 다시 전달됩니다.



<#root>

LEAF103#

vsh_lc

module-1#

debug platform internal tah elam asic 0

module-1(DBG-elam)#

trigger reset

module-1(DBG-elam)#

trigger init in-select 6 out-select 1

module-1(DBG-elam-insel6)#

reset

module-1(DBG-elam-insel6)#

set outer ipv4 src_ip 10.10.100.10 dst_ip 10.20.200.20

module-1(DBG-elam-insel6)#

set outer l2 src_mac 0050.56b7.bf94

module-1(DBG-elam-insel6)#

start

module-1(DBG-elam-insel6)#

stat

ELAM STATUS
==========

Asic 0 Slice 0 Status Triggered

Asic 0 Slice 1 Status Armed

module-1(DBG-elam-insel6)#

ereport

==
Trigger/Basic Information
==
...

Incoming Interface : 0x40(0x40)

>>> Eth1/45

...

Outer L2 Header

Destination MAC : 0022.BDF8.19FF

Source MAC : 0050.56B7.BF94

802.1Q tag is valid : yes(0x1)
CoS : 0(0x0)

Access Encap VLAN : 2006(0x7D6)

Outer L3 Header

L3 Type : IPv4
IP Version : 4
DSCP : 0
IP Packet Length : 84 (= IP header(28 bytes) + IP payload)
Don't Fragment Bit : set
TTL : 62
IP Protocol Number : ICMP
IP CheckSum : 46178(0xB462)

Destination IP : 10.20.200.20

Source IP : 10.10.100.10

Contract Lookup Key

IP Protocol : ICMP(0x1)
L4 Src Port : 2048(0x800)
L4 Dst Port : 37489(0x9271)

sclass (src pcTag) : 49157(0xC005) >>> Provider connector EPG

dclass (dst pcTag) : 49156(0xC004)

>>> Prod-Provider EPG

src pcTag is from local table : yes
derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet : no
If yes, Contract is not applied here because it is flooded

```
Sideband Information
------------------------------------------------------------------------------------------------------------------

ovector : 176( 0xB0 )  >>> Eth1/52


Ovec in "show plat int hal l2 port gpd"
Opcode : OPCODE_UC

------------------------------------------------------------------------------------------------------------------
sug_luc_latch_results_vec.luc3_0.

service_redir: 0x0


------------------------------------------------------------------------------------------------------------------
```

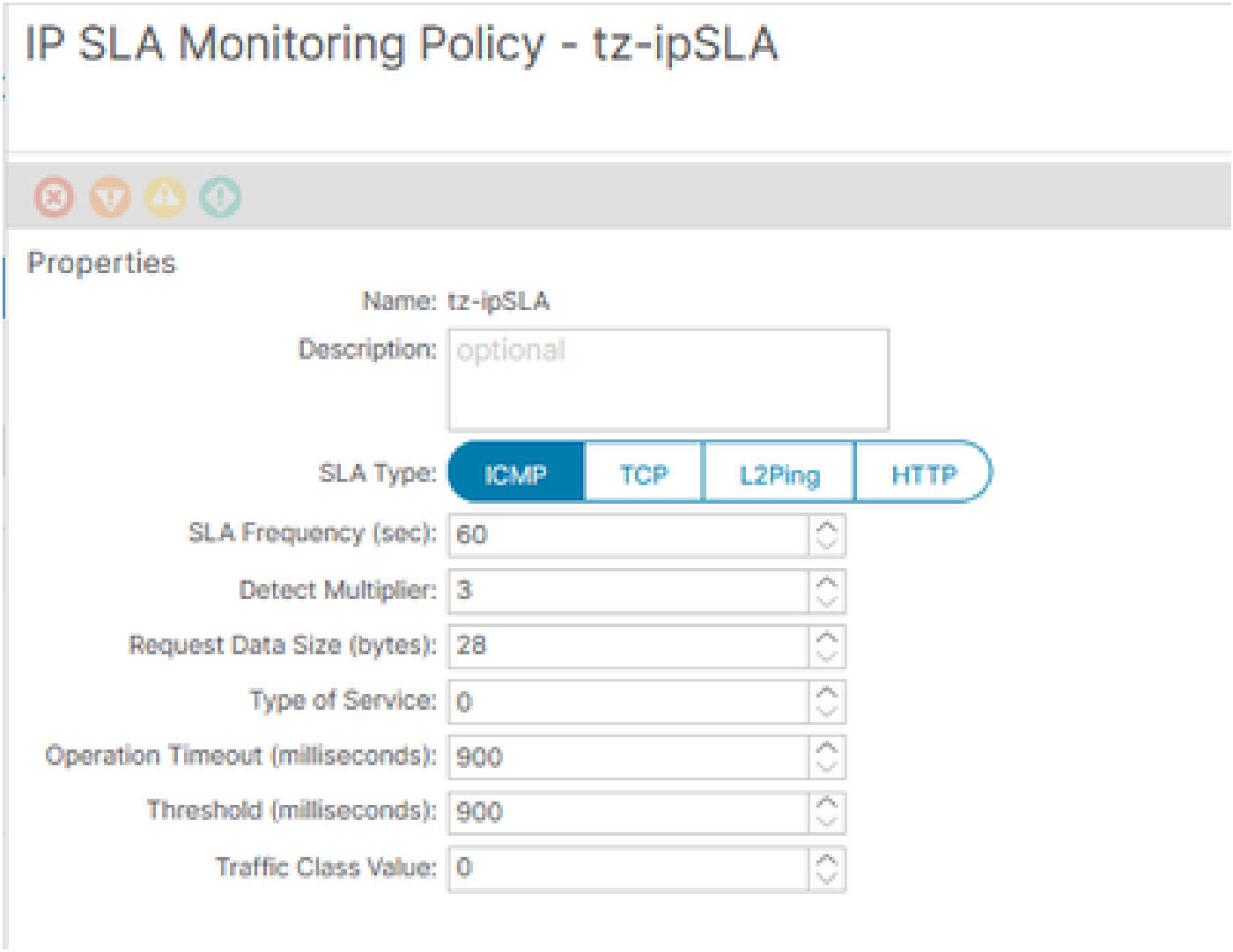
5. 나머지 네트워크 트래픽은 지금까지 설명한 설정된 단계를 준수하며, 여기서 패킷은 coop 조회를 기반으로 최종 서버 대상을 결정하기 위해 스파인 스위치로 돌아갑니다. 그런 다음 패킷은 로컬 학습 플래그가 있는 컴퓨팅 리프 스위치로 전달되어 이 정보를 스파인의 COOP 테이블에 전달합니다. 2단계와 3단계의 ELAM 실행은 최종 목적지를 향하는 패킷 배포에 일관됩니다. 정확한 전달을 위해 이러한 목적지 EPG pcTag 및 이그레스(egress) 인터페이스를 검증해야 합니다.

IP SLA

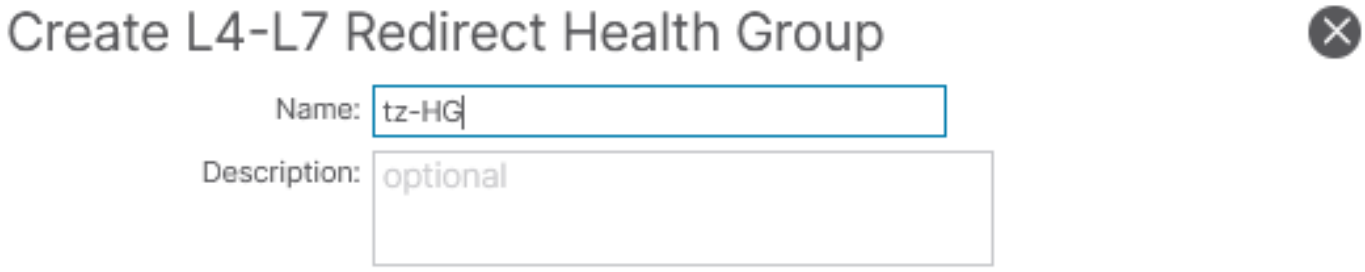
IP SLA는 네트워크 경로의 운영 상태 및 성능을 평가하는 데 사용됩니다. 또한 실시간 네트워크 상태를 기반으로 정의된 정책에 따라 트래픽이 효율적으로 라우팅되도록 합니다. ACI에서 PBR은 IP SLA를 활용하여 정보에 근거한 라우팅 결정을 내립니다. IP SLA 메트릭이 경로가 수행 중임을 나타낼 경우 PBR은 필요한 성능 기준을 충족하는 대체 경로를 통해 트래픽을 다시 라우팅할 수 있습니다.

버전 5.2(1)부터 IP SLA에 대한 동적 MAC 추적을 활성화할 수 있습니다. 이 기능은 PBR-노드가 장애 조치되어 동일한 IP 주소의 MAC 주소를 변경하는 경우에 유용합니다. 고정 구축에서는 PBR-노드가 MAC 주소를 변경할 때마다 정책 기반 리디렉션 정책을 변경해야 트래픽을 계속 전송할 수 있습니다. IP SLA를 사용하면 이 정책에 사용된 MAC 주소가 프로브 응답으로 릴레이됩니다. PBR 노드가 정상적인지 여부를 확인하기 위해 여러 프로브를 사용할 수 있습니다. 이 글을 쓰는 순간 다음과 같은 정보가 포함됩니다. ICMP, TCP, L2Ping 및 HTTP입니다.

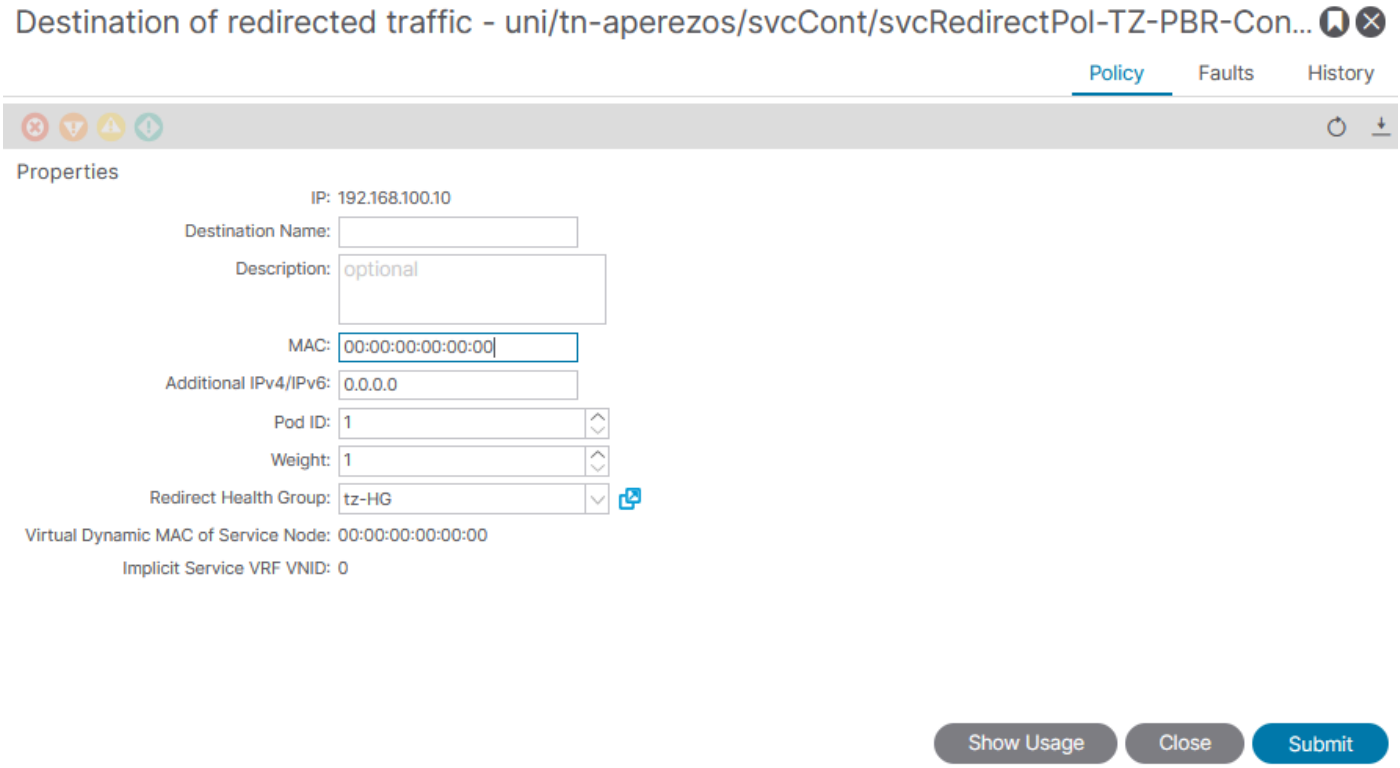
IP SLA 정책의 일반 컨피그레이션은 다음과 같아야 합니다.



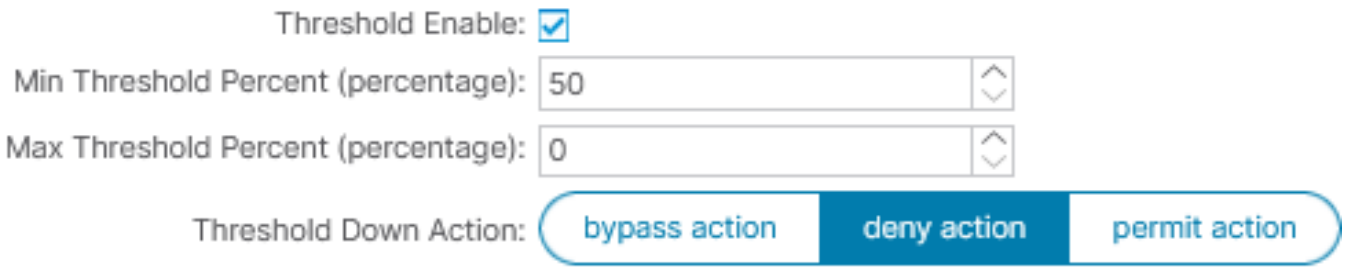
IP SLA 정책은 상태 그룹을 통해 PBR 노드 IP에 매핑해야 합니다.



MAC 주소를 동적으로 검색하는 IP SLA가 사용되는 경우 이 필드는 비워둘 수 없지만 모두 0으로 설정됩니다.



상태 그룹이 L4-L7 정책 기반 리디렉션 정책의 L3 대상을 통해 PBR 노드 IP와 연결되면 임계값을 설정하여 연결할 수 없을 때 IP SLA 동작을 정의합니다. 리디렉션을 유지하는 데 필요한 최소 활성 L3 대상 수를 지정합니다. 라이브 PBR 노드 수가 임계값 백분율에 속하거나 이를 초과할 경우, 전체 그룹이 선택한 임계값 감소 작업의 영향을 받아 재배포가 중지됩니다. 이 접근 방식은 트래픽 흐름에 영향을 주지 않고 트러블슈팅 중에 PBR-노드를 우회하도록 지원합니다.



상태 그룹은 단일 L4-L7 정책 기반 리디렉션 정책 또는 여러 L4-L7 정책 기반 리디렉션 정책의 L3 대상에 정의된 모든 IP를 바인딩하므로 동일한 상태 그룹 정책이 사용됩니다.

```
Leaf101# show service redir info health-group aperezos::tz-HG
==========================================================================================================
LEGEND
TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest | TRA: Tr
==========================================================================================================
HG-Name HG-OperSt HG-Dest HG-Dest-OperSt
======= ========== ======= ==============
aperezos::tz-HG enabled dest-[192.168.100.10]-[vxlan-2162692]] up
                        dest-[192.168.200.20]-[vxlan-2162692]] up
Leaf1011#
```

관련 정보

- Cisco Application Centric Infrastructure 정책 기반 리디렉션 서비스 그래프 설계 백서
- ACI Layer 4-7 PBR(Policy-Based Redirect) 심층 분석 및 팁(Cisco Live Presentation)
- Multipod PBR의 IP SLA 문제 해결

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.