ACI SPAN 가이드

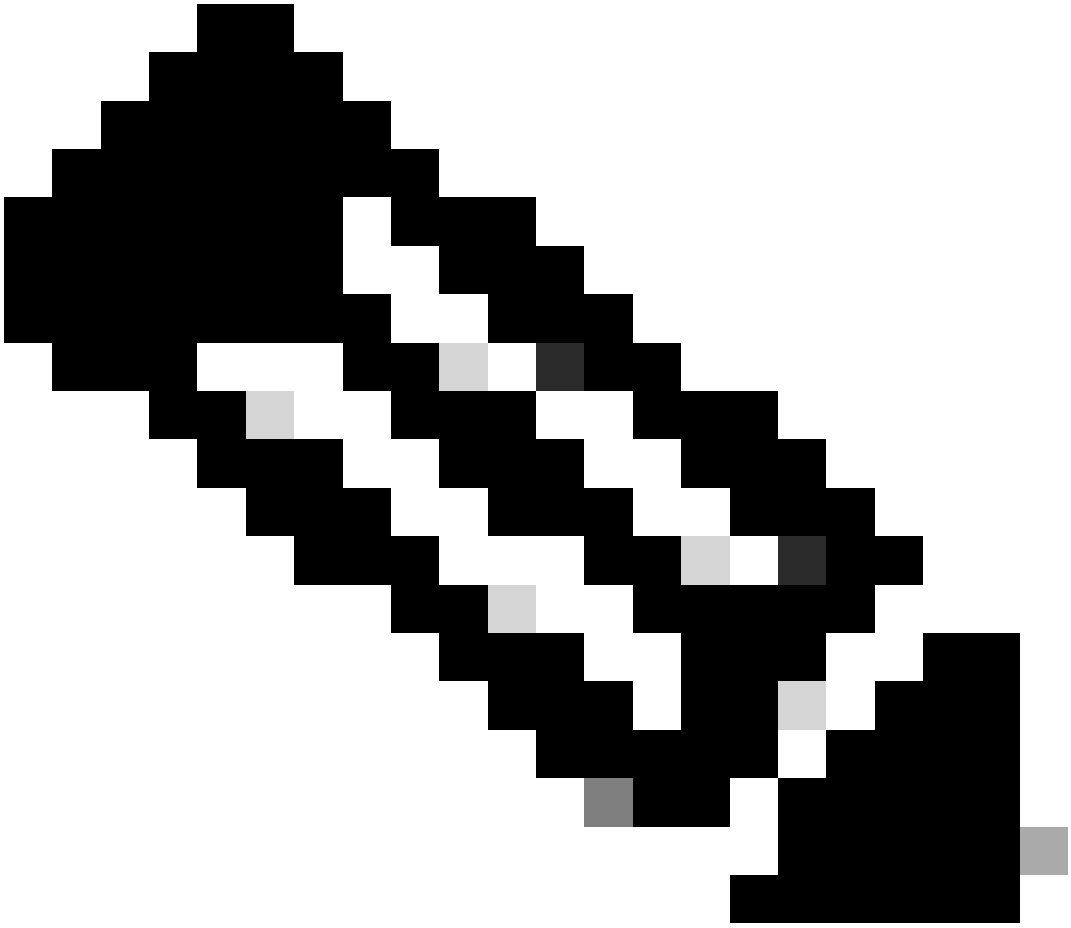
목차

소개

이 문서에서는 Cisco ACI(Application Centric Infrastructure)에서 SPAN(Switched Port Analyzer)을 구성하는 방법에 대해 설명합니다.

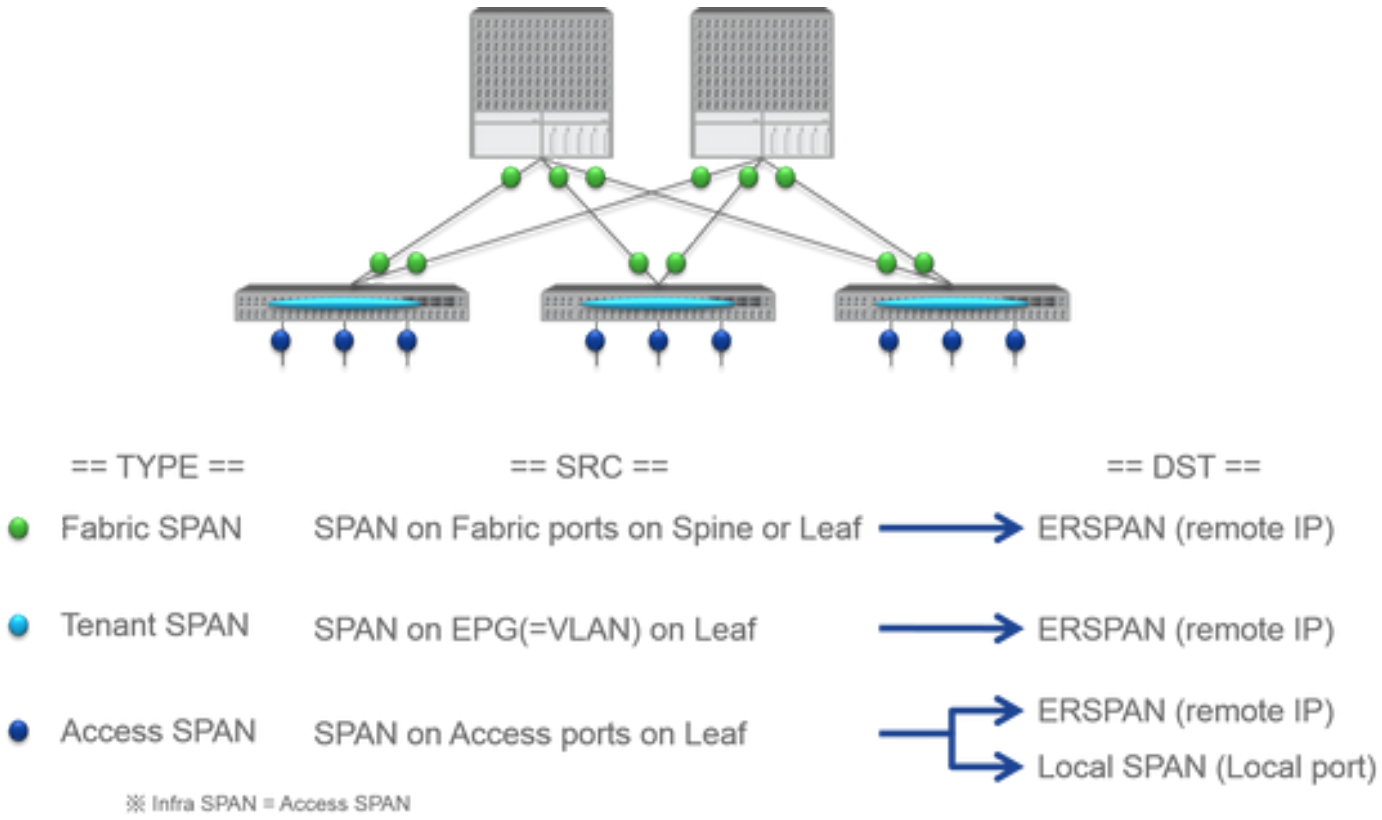
배경 정보

일반적으로 SPAN에는 세 가지 유형이 있습니다. 로컬 SPAN, 원격 SPAN(RSPAN) 및 캡슐화된 원격 SPAN(ERSPAN). 이러한 SPAN의 차이점은 주로 복사 패킷의 대상입니다. Cisco ACI는 로컬 SPAN 및 ERSPAN을 지원합니다.



참고: 이 문서에서는 독자가 로컬 SPAN 및 ERSPAN 차이와 같은 일반적인 SPAN에 대해 이미 잘 알고 있다고 가정합니다.

Cisco ACI의 SPAN 유형



Cisco ACI에는 세 가지 유형의 SPANFabric SPAN, 및Tenant SPAN 이 Access SPAN가 있습니다. 각 SPAN의 차이점은 복제 패킷의 소스입니다.

앞서 언급했듯이

- **Fabric SPAN** 에서 들어오고 나가는 패킷을 캡처하는 **interfaces between Leaf and Spine switches**것입니다.
    - Access SPAN 에서 들어오고 나가는 패킷을 캡처하는 interfaces between Leaf switches and external devices 것입니다.
    - Tenant SPAN 에서 들어오고 나가는 패킷을 캡처하는 EndPoint Group (EPG) on ACI Leaf switches 것입니다.

이 SPAN 이름은 Cisco ACI GUI에서 구성할 위치에 해당합니다.

- 패브릭 SPAN은 Fabric > Fabric Policies
    -

액세스 SPAN은 Fabric > Access Policies

- 테넌트 SPAN이 Tenants > {each tenant}

각 SPAN의 대상에 대해서는 및 를 모두Access SPAN 사용할 수Local SPAN 있는 경우에만 ERSPAN. 나머지 두 SPAN(Fabric 및 Tenant)은 ERSPAN만 가능합니다.

제한 사항 및 지침

Cisco APIC 트러블슈팅 가이드의 제한 및 지침을 검토하십시오. 에 나와 Troubleshooting Tools and Methodology > Using SPAN 있습니다.

설정

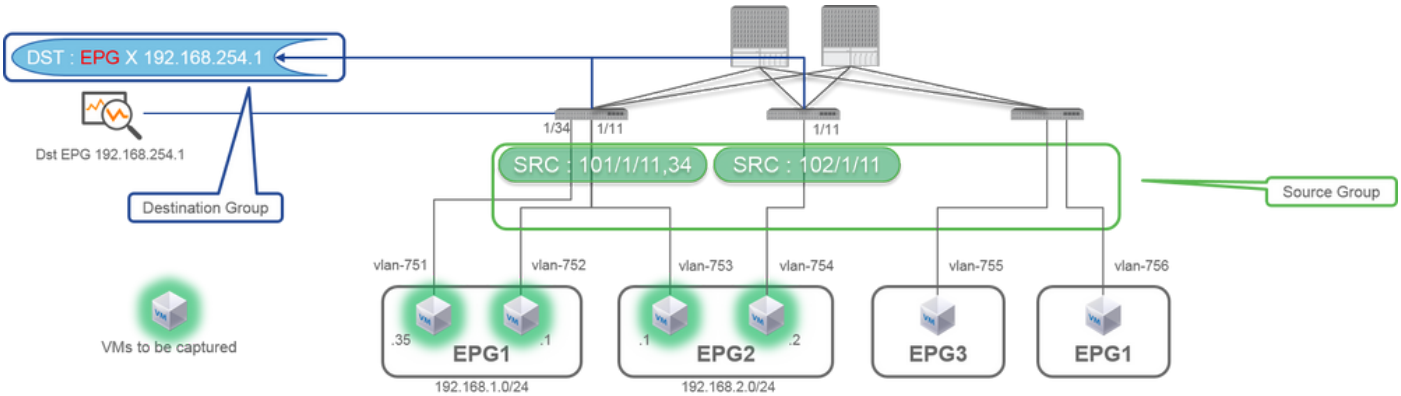
이 섹션에서는 각 SPAN 유형의 컨피그레이션과 관련된 간단한 예를 소개합니다. 이후 섹션에서 span 유형을 선택하는 방법에 대한 구체적인 샘플 사례가 있습니다.

SPAN 컨피그레이션은 Cisco APIC 트러블슈팅 가이드: 트러블슈팅 툴 및 방법론 > SPAN 사용에도 설명되어 있습니다.

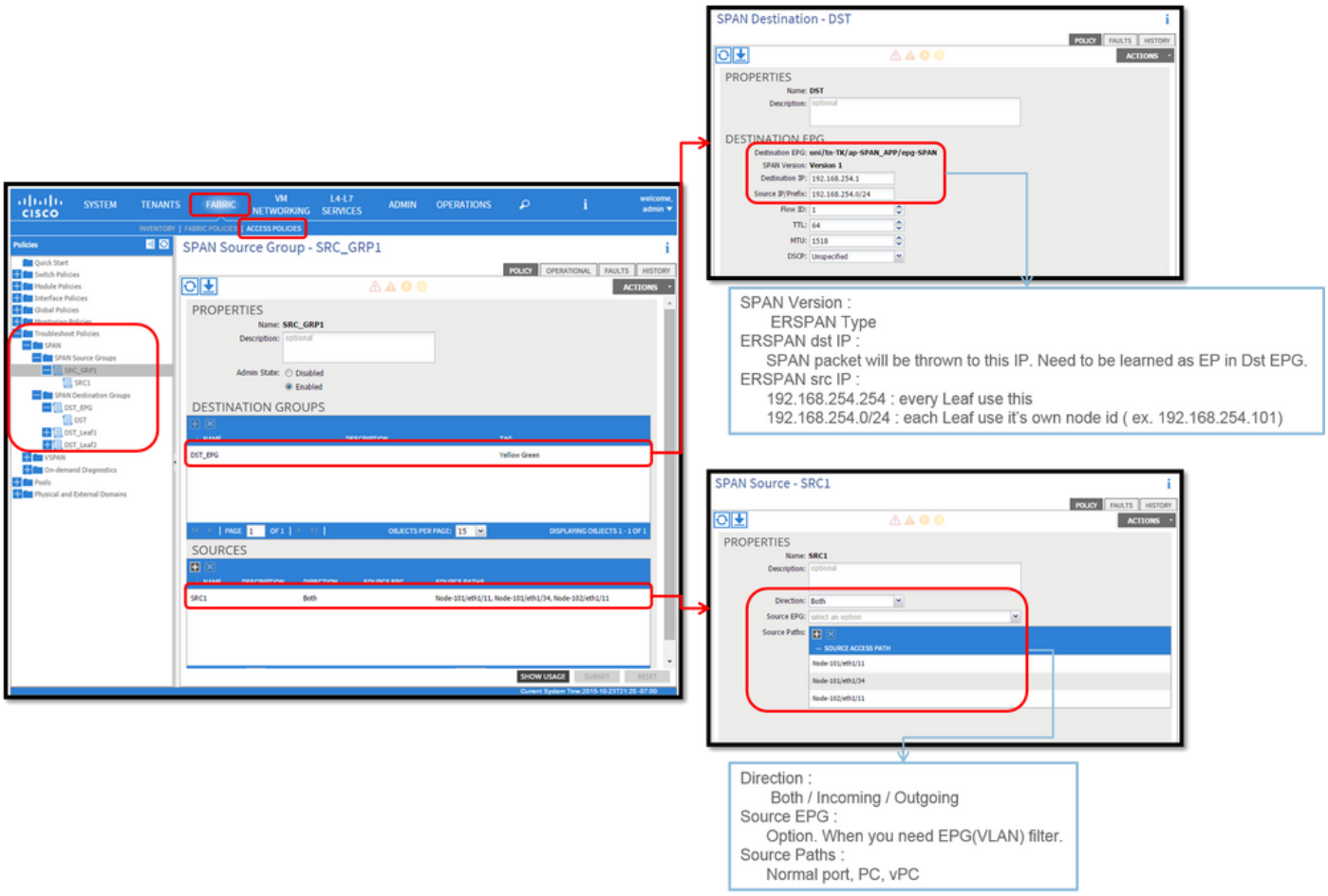
UI가 현재 버전과 다르게 나타날 수 있지만 컨피그레이션 접근 방식은 동일합니다.

액세스 SPAN(ERSPAN)

샘플 토폴로지



컨피그레이션 예시



여기서 각 항목은 다음을 나타냅니다.

로 FABRIC > ACCESS POLICIES > Troubleshoot Policies > SPAN 이동합니다.

- SPAN Source Groups
    - SPAN Destination Groups

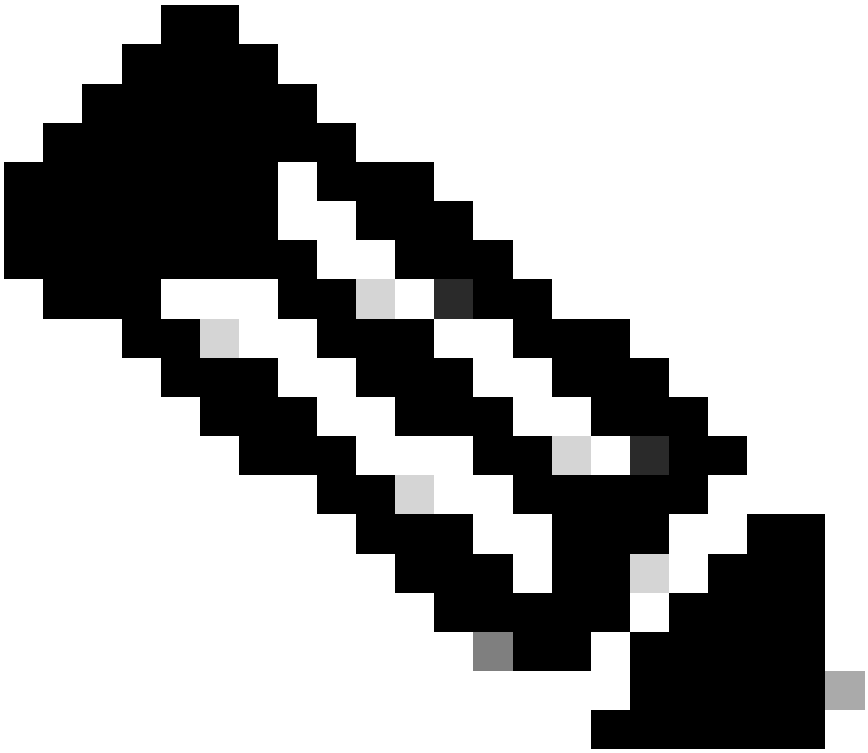
SPAN Source Group 넥타이Destination 및 Sources.

방법:

1. 생성SPAN Source Group(SRC_GRP1)

- (SPAN SourceSRC_GRPSPAN Source Group1)에 (SRC1)을 생성합니다.
- (SRC1)에 대한SPAN Source 이러한 매개변수를 구성합니다.

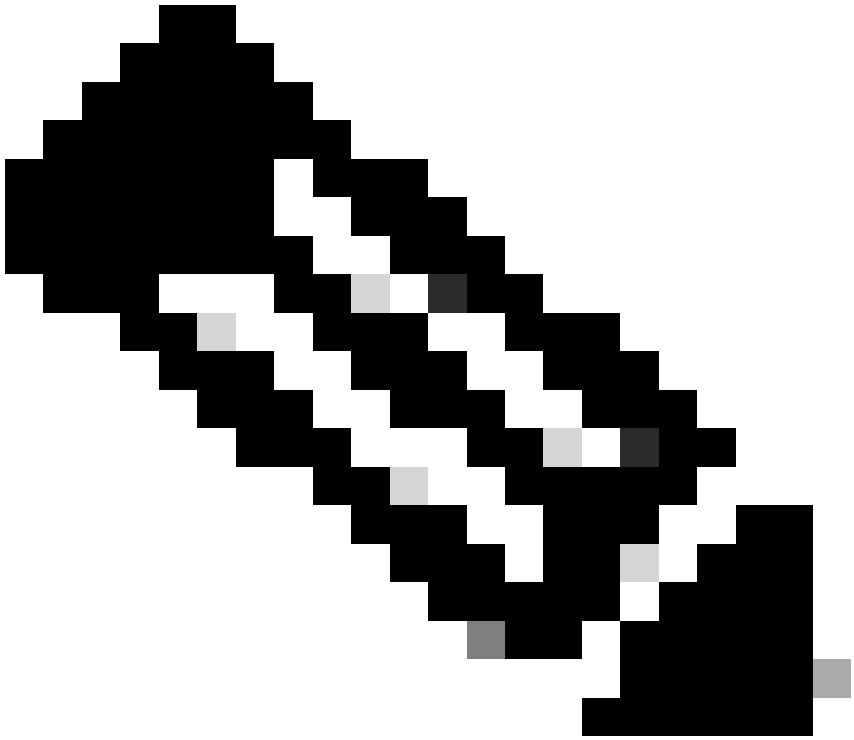
- Direction - Source EPG(옵션)
- 소스 경로(여러 인터페이스일 수 있음)



참고: 각 매개변수에 대한 자세한 내용은 그림을 참조하십시오.

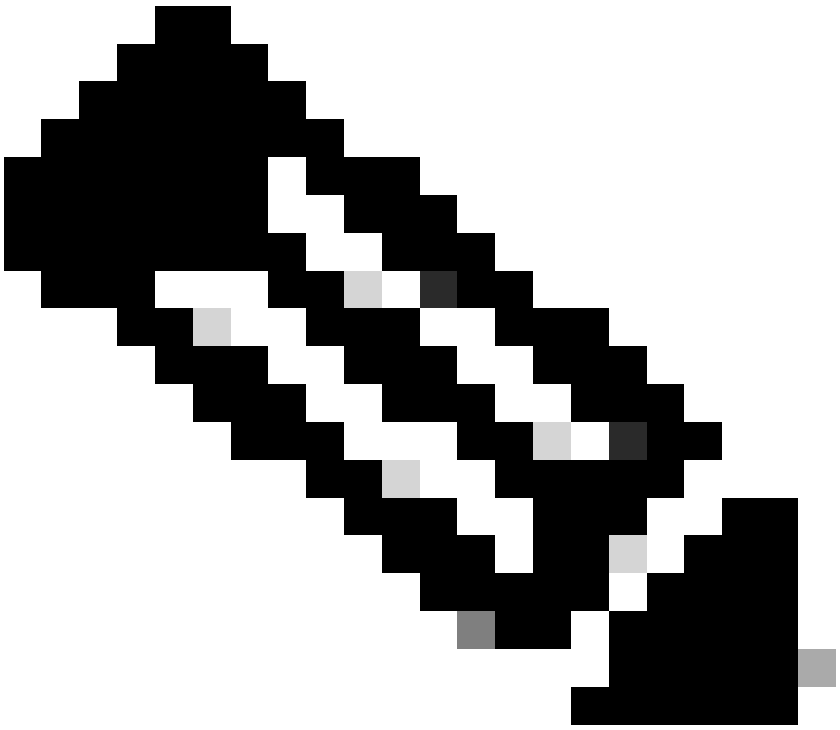
- 생성SPAN Destination Group(DST_EPG).
- DST(생성SPAN Destination)를 클릭합니다.
- DST(SPAN Destination)에 대해 이 매개변수 구성

- 대상 EPG
-대상 IP
- 소스 IP/접두사(임의의 IP일 수 있음) 접두사를 사용하면 소스 노드의 node-id가 정의되지 않은 비트에 사용됩니다. 예를 들어, 접두사: 1.0.0.0/8 on node-101 => src IP 1.0.0.101)
- 다른 매개변수는 기본값으로 둘 수 있습니다.



참고: 각 매개변수에 대한 자세한 내용은 그림을 참조하십시오.

- 가 SPAN Destination Group 적절한 연결에 연결되어 있는지 확인합니다SPAN Source Group.
- 사용Admin State이 설정되었는지 확인합니다.

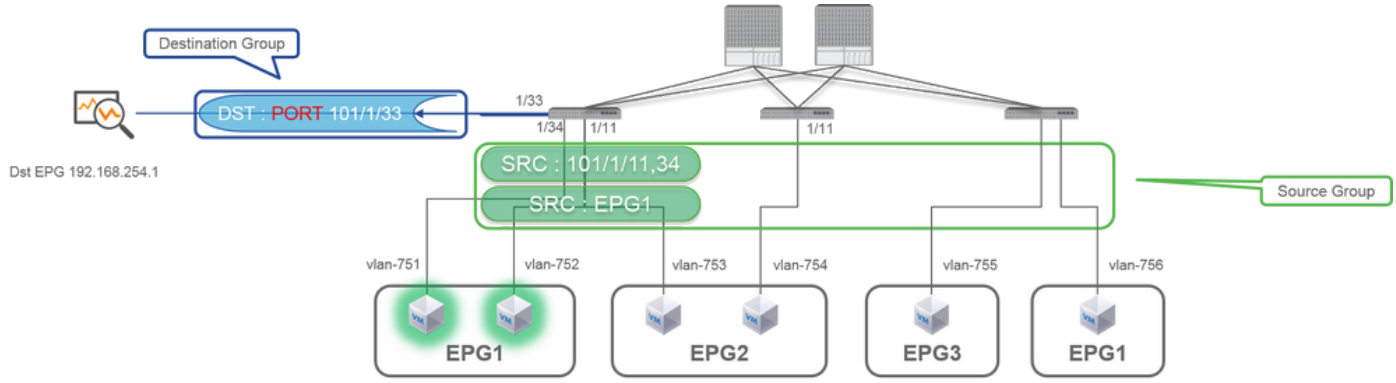


참고: 이 Admin State(관리 상태)에서 Disabled(비활성화됨)를 선택하면 SPAN이 중지됩니다. 나중에 정책을 다시 사용할 경우 모든 정책을 삭제할 필요가 없습니다.

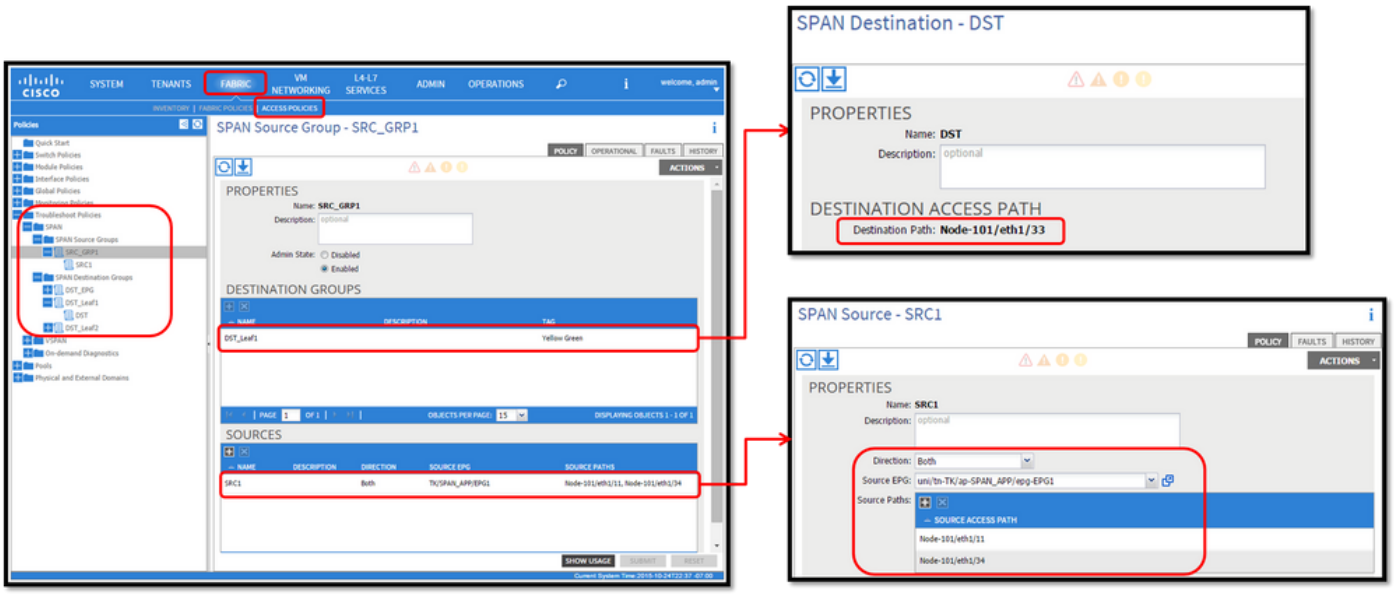
또한 ERSPAN의 대상 IP가 지정된 대상 EPG에서 엔드포인트로 학습되었는지 확인하십시오. 앞서 언급한 예에서 192.168.254.1은 아래에서 학습해야 Tenant TK > Application profile SPAN_APP > EPG SPAN 합니다. 또는 대상 디바이스가 무음 호스트인 경우 이 EPG에서 대상 IP를 고정 엔드포인트로 구성할 수 있습니다.

액세스 SPAN(로컬)

샘플 토폴로지



컨피그레이션 예시



- 여기서 각 항목은 다음을 나타냅니다.

Fabric > ACCESS POLICIES > Troubleshoot Policies > SPAN

- SPAN Source Groups

- SPAN Destination Groups

SPAN Source Group 넥타이Destination 및 Sources.

- 방법:

1. 생성SPAN Source Group(SRC_GRP1)

   - (SPAN SourceSRC_GRPSPAN Source Group1) 아래에 (SRC1) 생성

   - (SRC1)에 대한SPAN Source 다음 매개 변수를 구성합니다.
   -방향
   - 소스 EPG(옵션)
   - 소스 경로(여러 인터페이스일 수 있음)
   각 매개변수에 대한 자세한 내용은 그림을 ※.

   - 만들기(SPAN Destination GroupDST_Leaf1)

   - 만들기(SPAN DestinationDST)

   - DST(SPAN Destination)에 대해 이 매개변수 구성
   - 목적지 인터페이스 및 노드

   - 가 SPAN Destination Group 적절한 연결에 연결되어 있는지 확인합니다SPAN Source Group.

   -

   Enable(Admin State)이 설정되어 있는지 확인합니다.
   ※ Admin State(이 관리 상태)에서 Disabled(비활성화됨)를 선택하면 SPAN이 중지됩니다. 나중에 정책을 다시 사용할 경우 모든 정책을 삭제할 필요가 없습니다.

대상 인터페이스에는 인터페이스 정책 그룹에 의한 컨피그레이션이 필요하지 않습니다. ACI Leaf의 인터페이스에 케이블을 연결할 때 작동합니다.

제한 사항:

- 로컬 SPAN의 경우 대상 인터페이스와 소스 인터페이스가 동일한 Leaf에서 구성되어야 합니다.

- 대상 인터페이스가 UP인 경우 EPG에 있을 필요가 없습니다.

- vPC(virtual Port-Channel) 인터페이스를 소스 포트로 지정한 경우 로컬 SPAN을 사용할 수 없습니다
  하지만, 해결 방법이 있습니다. 1세대 leaf에서 vPC 또는 PC의 멤버인 개별 물리적 포트를 SPAN 소스로 구성할 수 있습니다. 이 로컬 SPAN을 사용하면 vPC 포트의 트래픽에 사용할 수 있습니다.
  그러나 이 옵션은 2세대 리프(CSCvc11053)에서는 사용할 수 없습니다. 대신, "VPC 구성 요소 PC"에서 SPAN에 대한 지원이 2.1(2e), 2.2(2e)의 CSCvc44643을 통해 추가되었고 앞으로 전달되었습니다. 이를 통해 모든 세대 leaf는 vPC의 멤버인 포트 채널을 SPAN 소스로 구성할 수 있습니다. 이렇게 하면 모든 세대의 leaf에서 vPC 포트의 트래픽에 Local SPAN을 사용할 수 있습니다.

- 2세대 leaf에서 포트 채널의 개별 포트를 지정하면 패킷의 하위 집합만 스팬됩니다(CSCvc11053으로 인해).

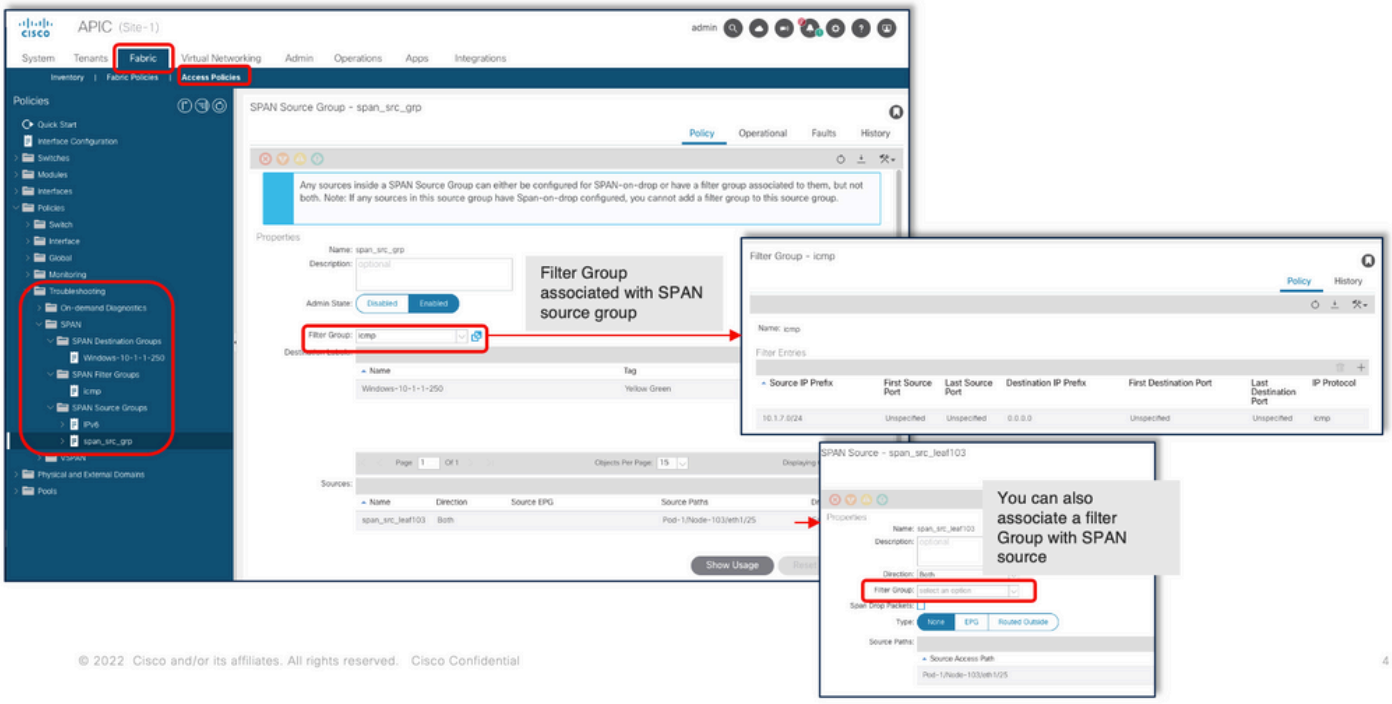
- PC 및 vPC는 로컬 SPAN의 대상 포트로 사용할 수 없습니다. 4.1(1)부터 PC를 로컬 SPAN의 대상 포트로 사용할 수 있습니다.

액세스 SPAN - ACL 필터 사용

액세스 범위 소스에 ACL 필터를 사용할 수 있습니다. 이 기능은 SPAN 소스에서 들어오고 나가는 트래픽의 특정 흐름 또는 흐름을 스패닝할 수 있는 기능을 제공합니다.
사용자는 SPAN 플로우 특정 트래픽의 SPAN이 필요한 경우 소스에 SPAN ACL을 적용할 수 있습니다.
Fabric SPAN 및 Tenant Span 소스 그룹/소스에서는 지원되지 않습니다.
필터 그룹에 필터 항목을 추가할 경우 현재 필터 그룹을 사용하는 모든 소스에 대해 tcam 항목을 추가할 수 있으므로 주의해야 합니다.

필터 그룹은 다음에 연결할 수 있습니다.
-Span Source(스팬 소스): 필터 그룹은 이 스팬 소스 아래에 정의된 모든 인터페이스의 트래픽을 필터링하는 데 사용됩니다.
-Span Source Group(스팬 소스 그룹): 필터 그룹(예: x)은 이 스팬 소스 그룹의 각 스팬 소스 아래에 정의된 모든 인터페이스에서 트래픽을 필터링하는 데 사용됩니다.

이 컨피그레이션 스냅샷에서는 필터 그룹이 Span 소스 그룹에 적용됩니다.

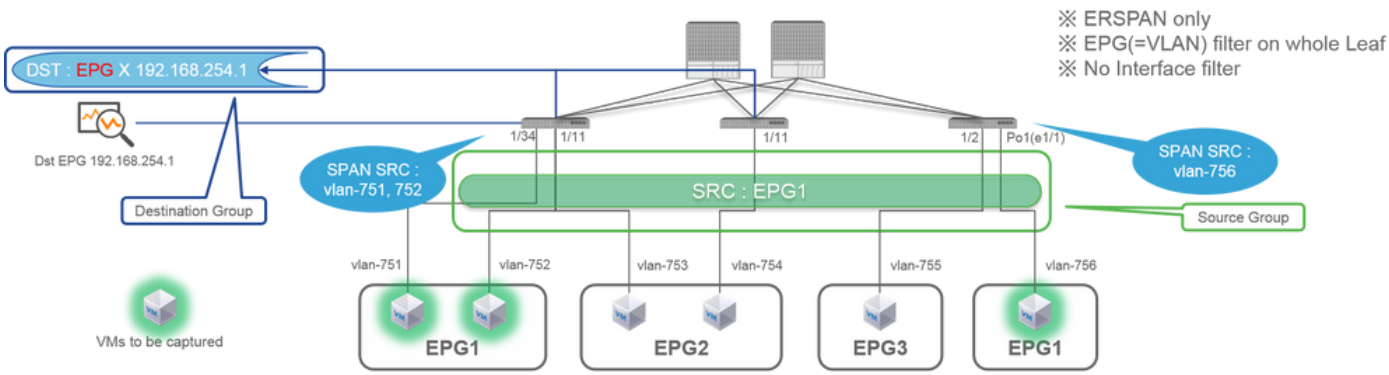


특정 Span Source가 이미 필터 그룹(예: y)과 연결된 경우, 해당 필터 그룹(y)은 이 특정 Span Source 아래의 모든 인터페이스에서 그룹을 필터링하는 데 대신 사용됩니다

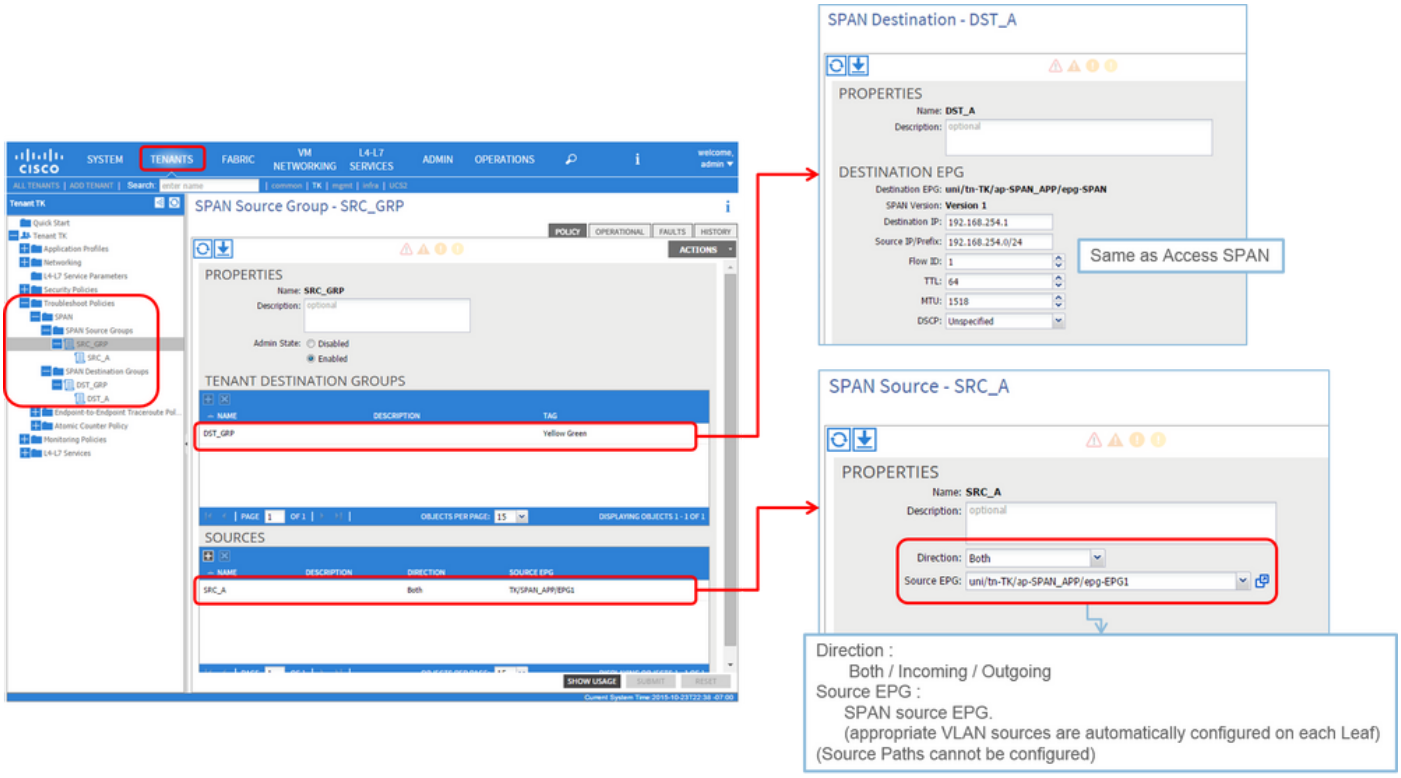
- 소스 그룹에 적용된 필터 그룹이 해당 소스 그룹의 모든 소스에 자동으로 적용됩니다.
- 소스에 적용된 필터 그룹은 해당 소스에만 적용됩니다.
- 필터 그룹이 소스 그룹과 해당 소스 그룹의 소스 모두에 적용되면 소스에 적용된 필터 그룹이 우선적으로 적용됩니다.
- 소스에 적용된 필터 그룹이 삭제되고 상위 소스 그룹에 적용된 필터 그룹이 자동으로 적용됩니다.
- 소스 그룹에 적용된 필터 그룹이 삭제되고 해당 소스 그룹에서 현재 상속되는 모든 소스에서 삭제됩니다.

테넌트 SPAN(ERSPAN)

샘플 토폴로지



컨피그레이션 예시



- 여기서 각 항목은 다음을 나타냅니다.

Tenants > {tenant name} > Troubleshoot Policies > SPAN

- SPAN Source Groups

- SPAN Destination Groups

※ SPAN 소스 그룹 연결 Destination 및 Sources.

- 방법:

1. 생성SPAN Source Group(SRC_GRP)

- (SPAN Source_GRP) 아래에 SPAN Source Group (SRC_A) 생성

- (SRC_A)에 대한SPAN Source 이러한 매개변수 구성
  -방향
  - 소스 EPG

※ 각 매개변수에 대한 자세한 내용은 그림을 참조하십시오.

- 만들기SPAN Destination Group(DST_GRP)

- 만들기SPAN Destination(DST_A)

- (DST_A)에 대한 SPAN Destination다음 매개변수를 구성합니다.
  - 대상 EPG
  -대상 IP
  - 소스 IP/접두사
  - 다른 매개변수는 기본값으로 둘 수 있습니다.

※ 각 매개변수에 대한 자세한 내용은 그림을 참조하십시오.

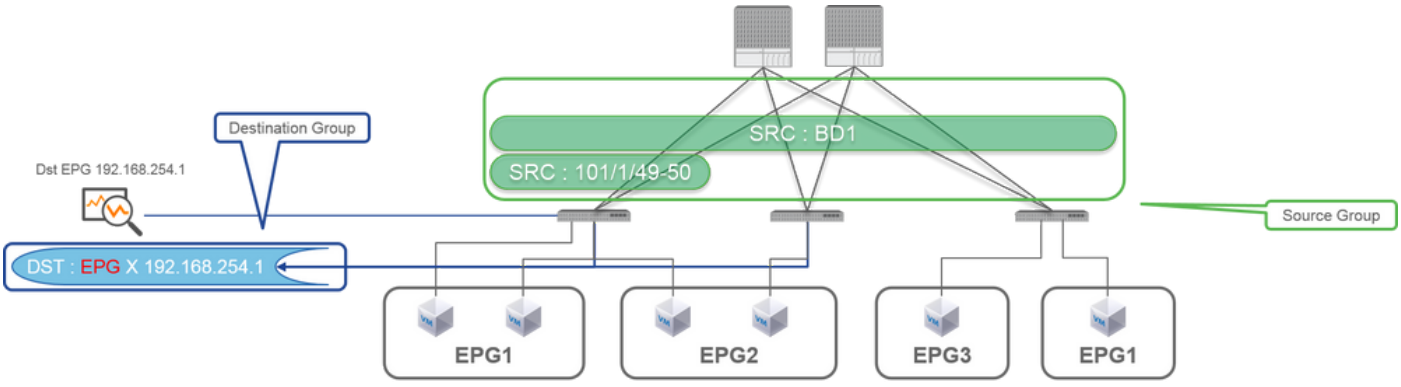
- 해당 SPAN Destination Group 항목에 연결되어 있는지 SPAN Source Group확인합니다.

- Enable(Admin State)이 설정되어 있는지 확인합니다.

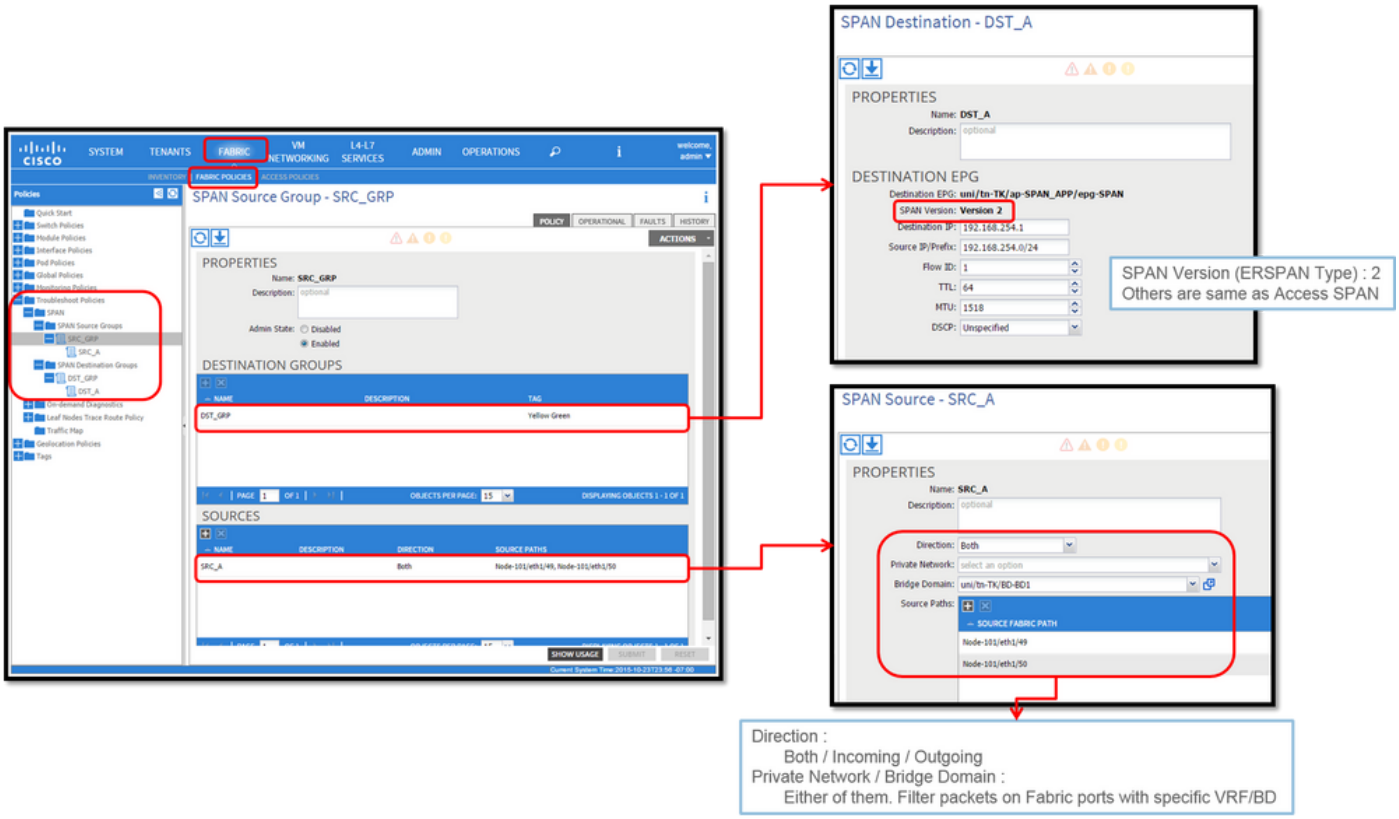
※ Admin State(이 관리 상태)에서 Disabled(비활성화됨)를 선택하면 SPAN이 중지됩니다. 나중에 정책을 다시 사용할 경우 모든 정책을 삭제할 필요가 없습니다.

패브릭 SPAN(ERSPAN)

샘플 토폴로지



컨피그레이션 예시



- 여기서 각 항목은 다음을 나타냅니다.

Fabric > FABRIC POLICIES > Troubleshoot Policies > SPAN

- Fabric

- SPAN Destination Groups

※ SPAN Source GroupDestination 및 Sources

- 방법:

1. 생성SPAN Source Group(SRC_GRP)

- (SPAN Source_GRP) 아래에 SPAN Source Group (SRC_A) 생성

- (SRC_A)에 대한SPAN Source 이러한 매개변수 구성
  -방향
  - 프라이빗 네트워크(옵션)
  - 브리지 도메인(옵션)
  - 소스 경로(여러 인터페이스일 수 있음)

각 매개변수에 대한 자세한 내용은 그림을 ※.

- 만들기SPAN Destination Group(DST_GRP)

- 만들기SPAN Destination(DST_A)

- (DST_A)에 대한SPAN Destination 이러한 매개변수 구성
  - 대상 EPG
  -대상 IP
  - 소스 IP/접두사
  - 다른 매개변수는 기본값으로 둘 수 있습니다.

각 매개변수에 대한 자세한 내용은 그림을 ※.

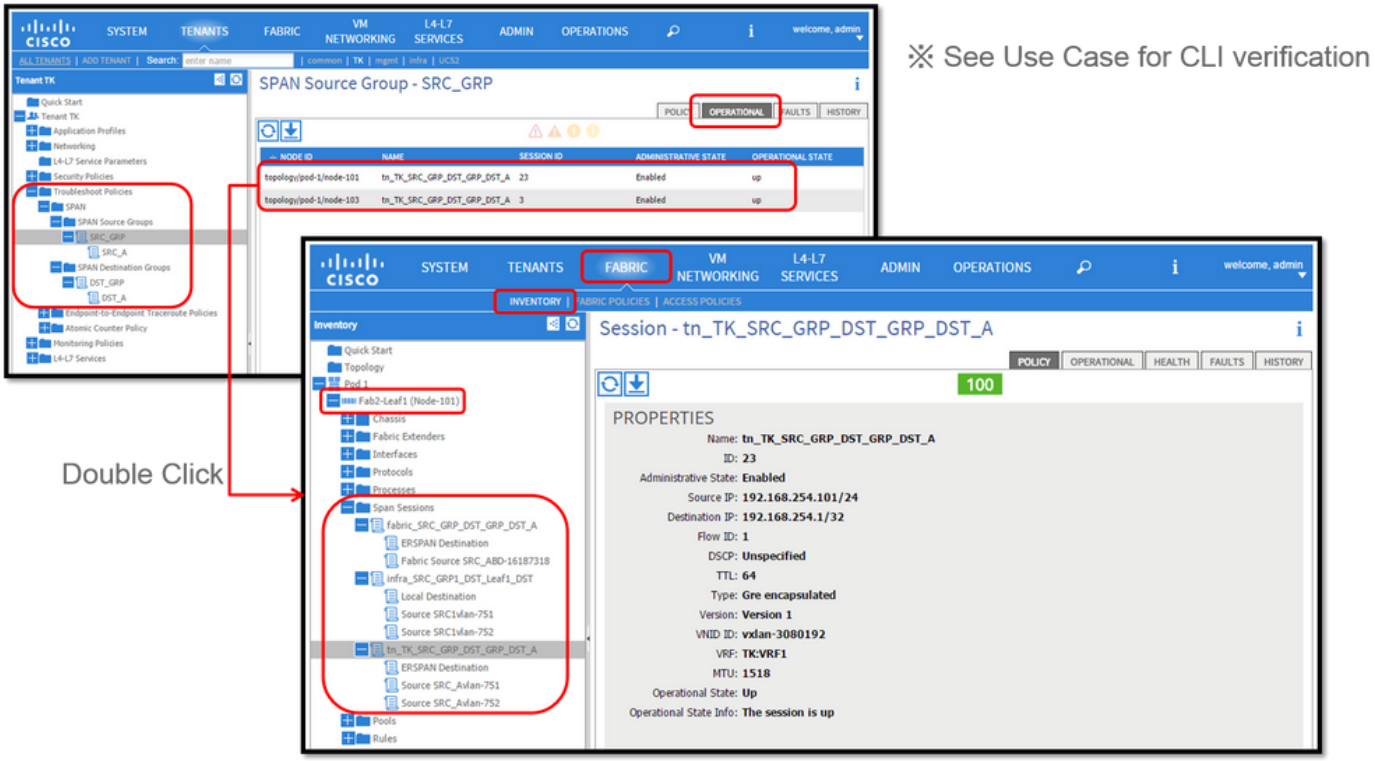
- 해당 SPAN Destination Group 항목에 연결되어 있는지 SPAN Source Group확인합니다.

- 사용Admin State 이 설정되었는지 확인합니다.

※에서 Disabled(비활성화됨)를 선택하면 SPAN이 Admin State중지됩니다. 나중에 정책을 다시 사용할 경우 모든 정책을 삭제할 필요가 없습니다.

나중에 "ERSPAN 버전(유형)" 섹션에 설명되어 있지만 ERSPAN 버전 II가 패브릭 SPAN에 사용되고 버전 I가 테넌트 및 액세스 SPAN에 사용됨을 알 수 있습니다.

GUI 확인



- SPAN 컨피그레이션 정책 확인

1. Fabric > ACCESS POLICIES > Troubleshoot Policies > SPAN > SPAN Source Groups > Operational tab

   - Fabric > FABRIC POLICIES > Troubleshoot Policies > SPAN > SPAN Source Groups > Operational tab
   - Tenants > {tenant name} > Troubleshoot Policies > SPAN > SPAN Source Groups > Operational tab

작동 상태가 켜져 있는지 확인하십시오.

- 노드 자체의 SPAN 세션 확인

1. 또는에서 각 세션을 두 번 SPAN Configuration Policy클릭합니다. Fabric > INVENTORY > Node > Span Sessions > { SPAN session name }

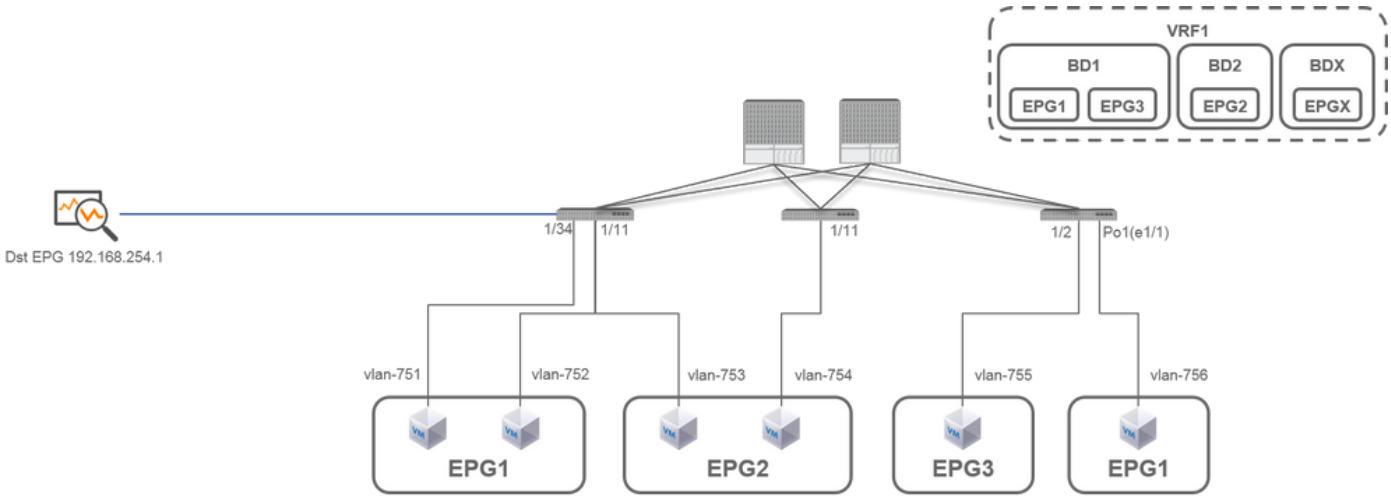
작동 상태가 켜져 있는지 확인하십시오.

SPAN 세션 명명 규칙:

- 패브릭 SPAN: fabric_xxxx

- 액세스 SPAN: infra_xxxx
- 테넌트 SPAN: tn_xxxx

ACI SPAN 유형 선택



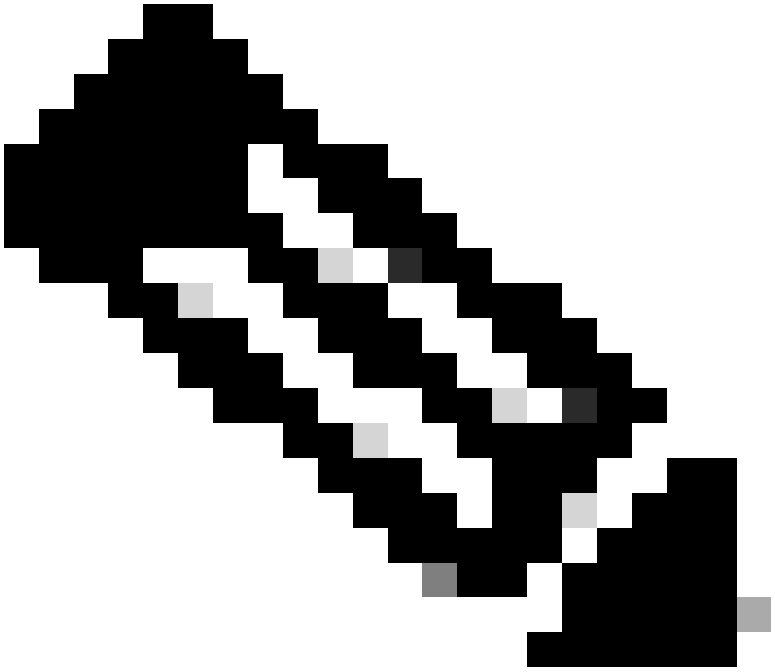
이 섹션에서는 각 ACI SPAN 유형(Access, Tenant, Fabric)에 대한 자세한 시나리오를 설명합니다. 각 시나리오의 기본 토폴로지는 이전 섹션에서 설명합니다.

이러한 시나리오를 이해하면 특정 인터페이스의 패킷만 캡처하거나 인터페이스에 상관없이 특정 EPG의 모든 패킷을 캡처하는 등 요구 사항에 적합한 ACI SPAN 유형을 선택할 수 있습니다.

Cisco ACI에서 SPAN은 및 로source group destination group 구성됩니다. 소스 그룹에는 인터페이스 또는 EPG와 같은 여러 소스 요소가

포함되어 있습니다. 대상 그룹은 로컬 SPAN의 대상 인터페이스 또는 ESPAN의 대상 IP와 같은 대상 정보를 포함합니다.

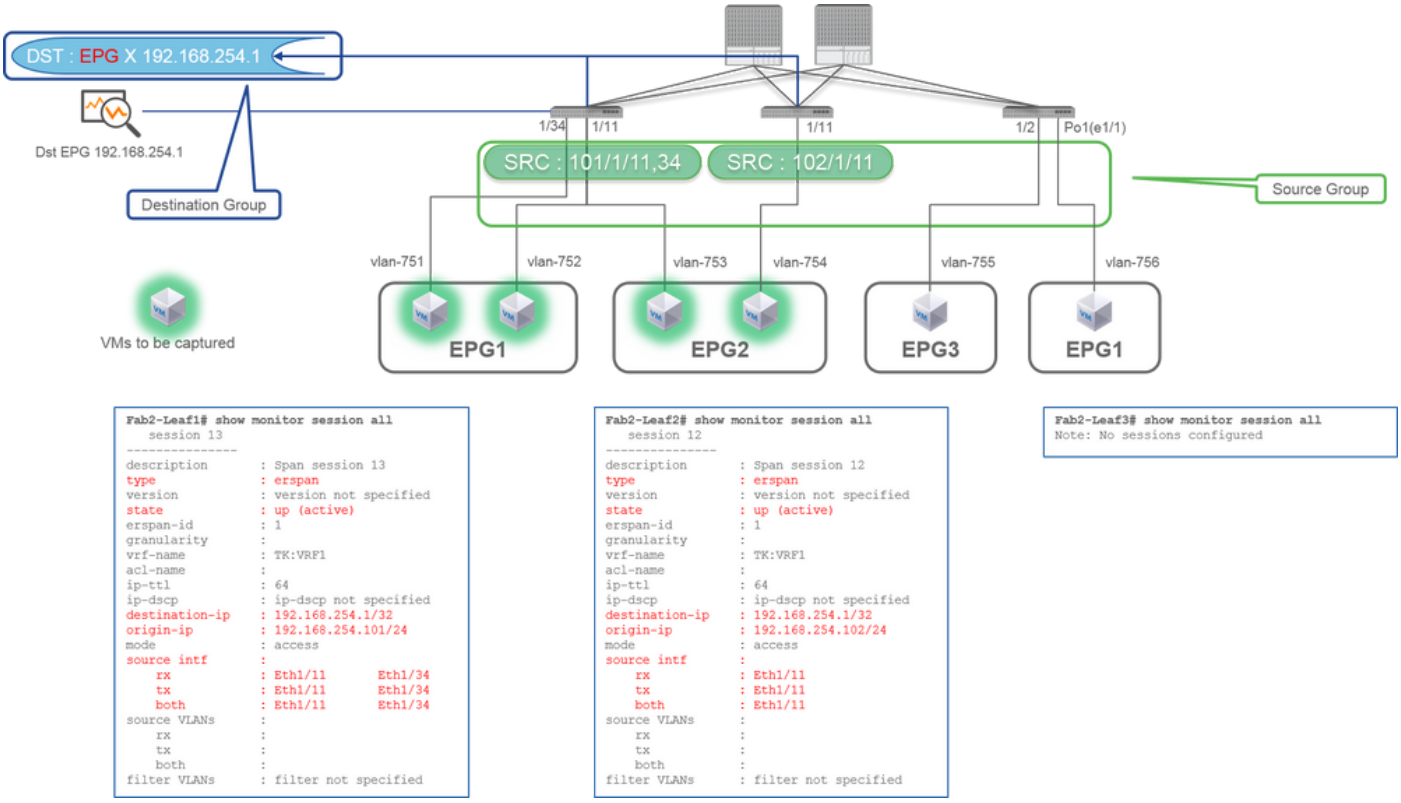
패킷이 캡처된 후 캡처된 패킷을 디코딩하려면 "SPAN 데이터를 읽는 방법" 섹션을 참조하십시오.



참고: 각 토폴로지에서 녹색 표시등으로 강조 표시된 VM에 집중하십시오. 각 시나리오는 강조 표시된 VM에서 패킷을 캡처하는 것입니다.

액세스 SPAN(ERSPAN)

사례 1. Src "Leaf1 e1/11 e1/34 & Leaf2 e1/11" | Dst "192.168.254.1"



- Source Group
  - 리프1 e1/11
  - 리프1 e1/34
  - 리프2 e1/11
- Destination Group
  - EPG X의 192.168.254.1

액세스 SPAN은 단일 SPAN 세션에 대해 여러 인터페이스를 지정할 수 있습니다. EPG와 상관없이 지정된 인터페이스에서 들어오거

나 나가는 모든 패킷을 캡처할 수 있습니다.

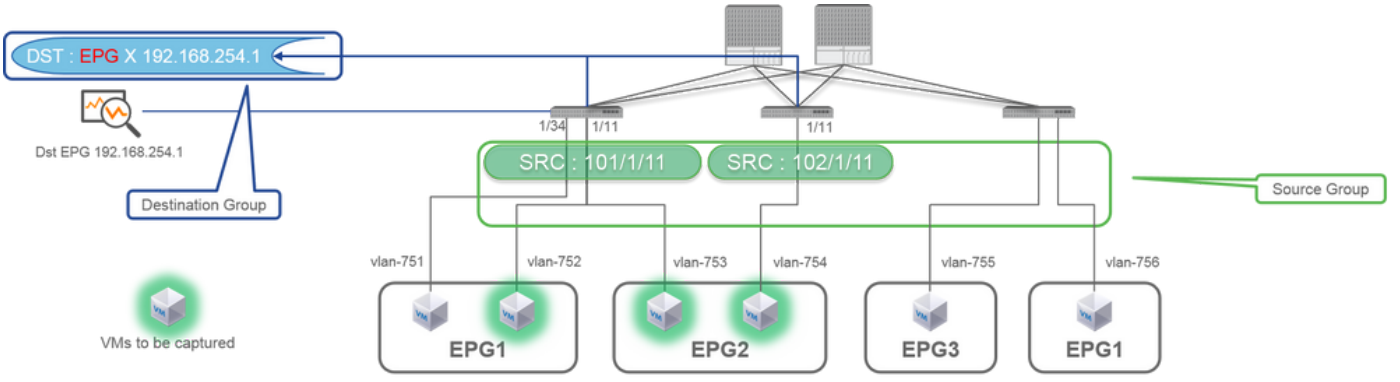
여러 인터페이스가 여러 리프 스위치의 소스 그룹으로 지정된 경우 대상 그룹은 로컬 SPAN이 아니라 ERSPAN이어야 합니다.

이 예에서는 EPG1 및 EPG2의 모든 VM에서 패킷을 복사합니다.

CLI 검사점

- 상태가 "up(active)"인지 확인하십시오.
- "destination-ip"은 ERSPAN의 대상 IP입니다.
  - "origin-ip"은 ERSPAN의 소스 IP입니다.

사례 2. Src "Leaf1 e1/11 & Leaf2 e1/11" | Dst "192.168.254.1"




```
Fab2-Leaf1# show monitor session all
   session 2
---------------
description       : Span session 2
type              : erspan
version           : version not specified
state             : up (active)
erspan-id         : 1
granularity       :
vrf-name          : TK:VRF1
acl-name          :
ip-ttl            : 64
ip-dscp           : ip-dscp not specified
destination-ip    : 192.168.254.1/32
origin-ip         : 192.168.254.101/24
mode              : access
source intf       :
    rx            : Eth1/11
    tx            : Eth1/11
    both          : Eth1/11
source VLANs      :
    rx            :
    tx            :
    both          :
filter VLANs      : filter not specified
```

```
Fab2-Leaf2# show monitor session all
   session 3
---------------
description       : Span session 3
type              : erspan
version           : version not specified
state             : up (active)
erspan-id         : 1
granularity       :
vrf-name          : TK:VRF1
acl-name          :
ip-ttl            : 64
ip-dscp           : ip-dscp not specified
destination-ip    : 192.168.254.1/32
origin-ip         : 192.168.254.102/24
mode              : access
source intf       :
    rx            : Eth1/11
    tx            : Eth1/11
    both          : Eth1/11
source VLANs      :
    rx            :
    tx            :
    both          :
filter VLANs      : filter not specified
```

```
Fab2-Leaf3# show monitor session all
Note: No sessions configured
```

- **소스 그룹**
  - 리프1 e1/11
  - 리프2 e1/11
- **대상 그룹**
  - EPG X의 192.168.254.1

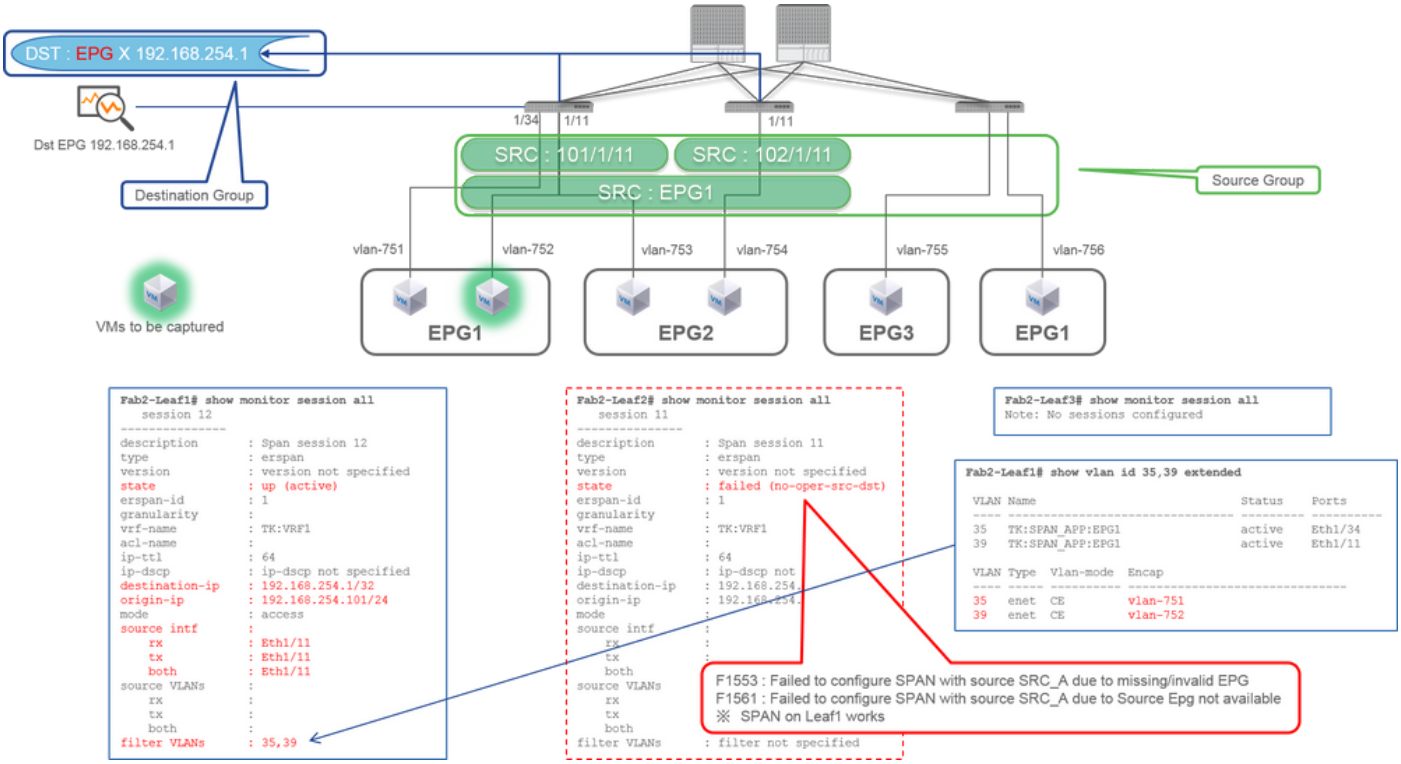
이 예에서는 이전 Case1에서 구성한 SPAN 소스 그룹에서 Leaf1 e1/34가 제거됩니다.

이 예의 핵심은 Access SPAN이 EPG와 상관없이 소스 인터페이스를 지정할 수 있다는 것입니다.

CLI 검사점

- leaf1의 소스 인터페이스가 "Eth1/11 Eth1/34"에서 "Eth1/11"로 변경됩니다.

사례 3. Src "Leaf1 e1/11 & Leaf2 e1/11 & EPG1 filter" | Dst "192.168.254.1"



- **소스 그룹**
  - 리프1 e1/11
  - 리프2 e1/11
  - 필터 EPG1
- **대상 그룹**
  - EPG X의 192.168.254.1

이 예에서는 Access SPAN이 소스 포트에서 특정 EPG를 지정할 수도 있음을 보여 줍니다. 이는 여러 EPG가 단일 인터페이스에서 흐르며 이 인터페이스의 EPG1에 대해서만 트래픽을 캡처해야 하는 경우 유용합니다.

EPG1은 Leaf2에 구축되지 않으므로 Leaf2에 대한 SPAN은 F1553 및 F1561 오류와 함께 실패합니다. 그러나 Leaf1의 SPAN은 여전히 작동합니다.

또한 EPG1은 Leaf1에서 2개의 VLAN(VLAN-751,752)을 사용하므로 Leaf1의 SPAN 세션에 대해 2개의 VLAN 필터가 자동으로 추가됩니다.

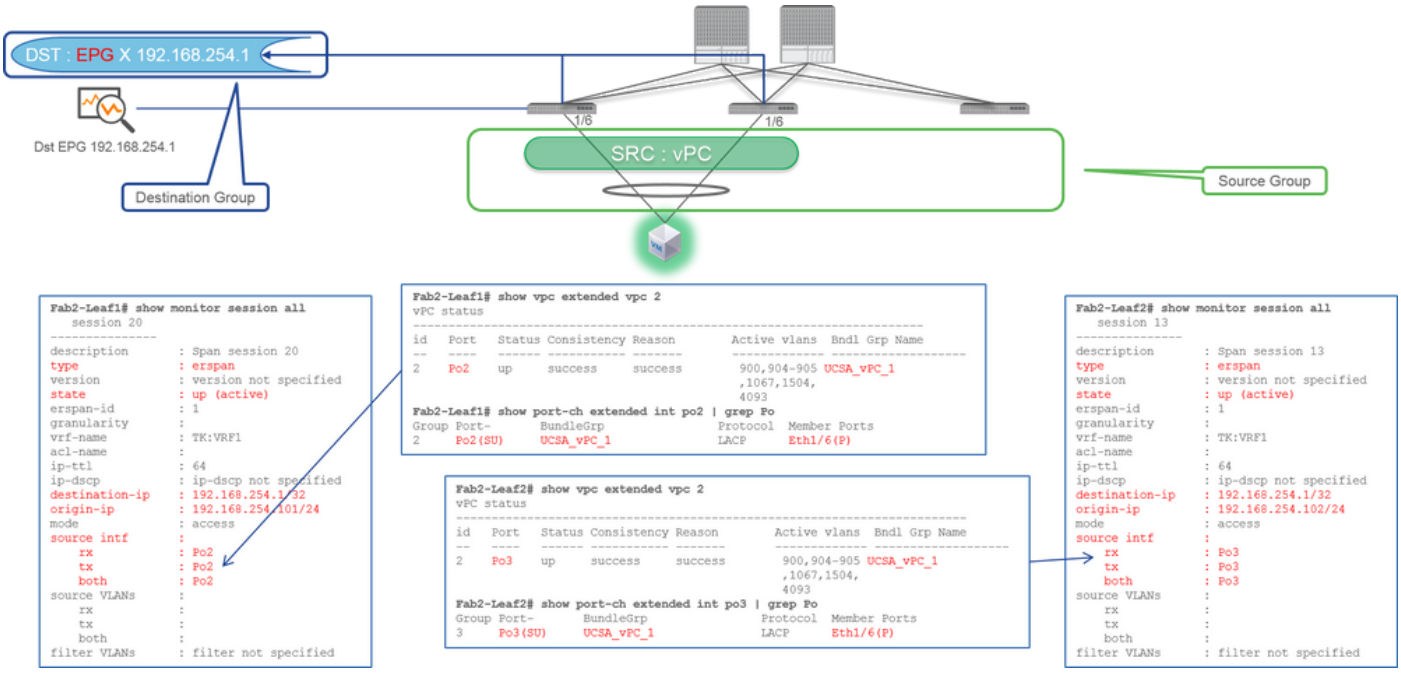
CLI의 VLAN ID(35, 39)는 배선의 실제 ID가 아닌 내부 VLAN, 소위 PI-VLAN(Platform Independent VLAN)이라는 점에 유의하십시오. 그림과 같이 show vlan **extended** 명령은 실제 캡슐화 VLAN ID와 PI-VLAN의 매핑을 보여줍니다.

이 SPAN 세션에서는 EPG2(VLAN-753)가 동일한 인터페이스에서 흐르더라도 Leaf1 e1/11의 EPG1(VLAN-752)에 대해서만 패킷을 캡처할 수 있습니다.

CLI 검사점

- 필터에 사용되는 EPG에 따라 필터 VLAN이 추가됩니다.
- Leaf에 해당 EPG가 없는 경우 해당 Leaf의 SPAN 세션이 실패합니다.

사례 4. Src "Leaf1-Leaf2 vPC" | Dst "192.168.254.1"

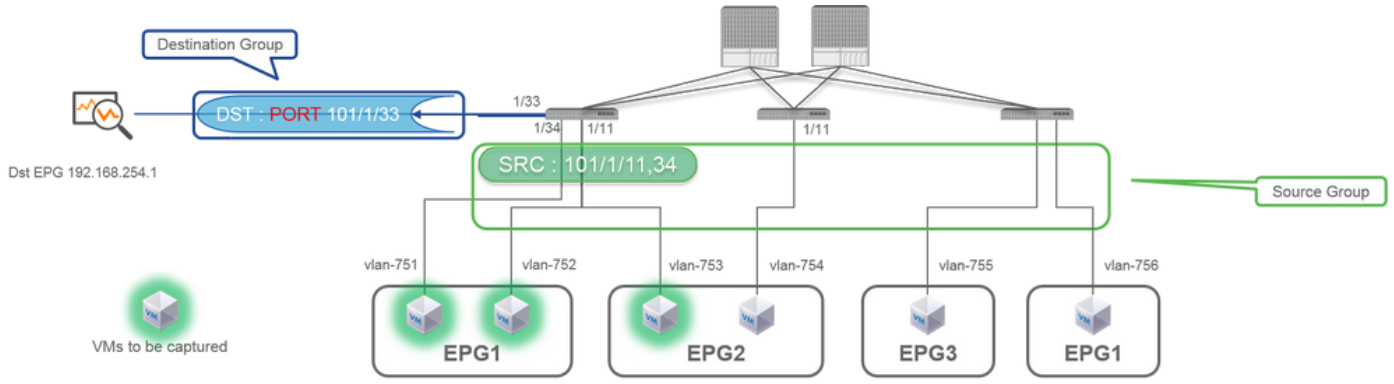


- **소스 그룹**
  - 리프1 - 2e1/11
- **대상 그룹**
  - EPG X의 192.168.254.1

vPC 인터페이스가 소스로 구성된 경우 대상은 인터페이스(Local SPAN)가 아니라 원격 IP(ERSPAN)여야 합니다

액세스 SPAN(로컬 SPAN)

사례 1. Src "Leaf1 e1/11 e1/34" | Dst "Leaf1 e1/33"




```
Fab2-Leaf1# show monitor session all
   session 14
---------------
description       : Span session 14
type              : local
state             : up (active)
mode              : access
source intf       :
    rx            : Eth1/11       Eth1/34
    tx            : Eth1/11       Eth1/34
    both          : Eth1/11       Eth1/34
source VLANs      :
    rx            :
    tx            :
    both          :
filter VLANs      : filter not specified
destination ports : Eth1/33
```

```
Fab2-Leaf2# show monitor session all
Note: No sessions configured
```

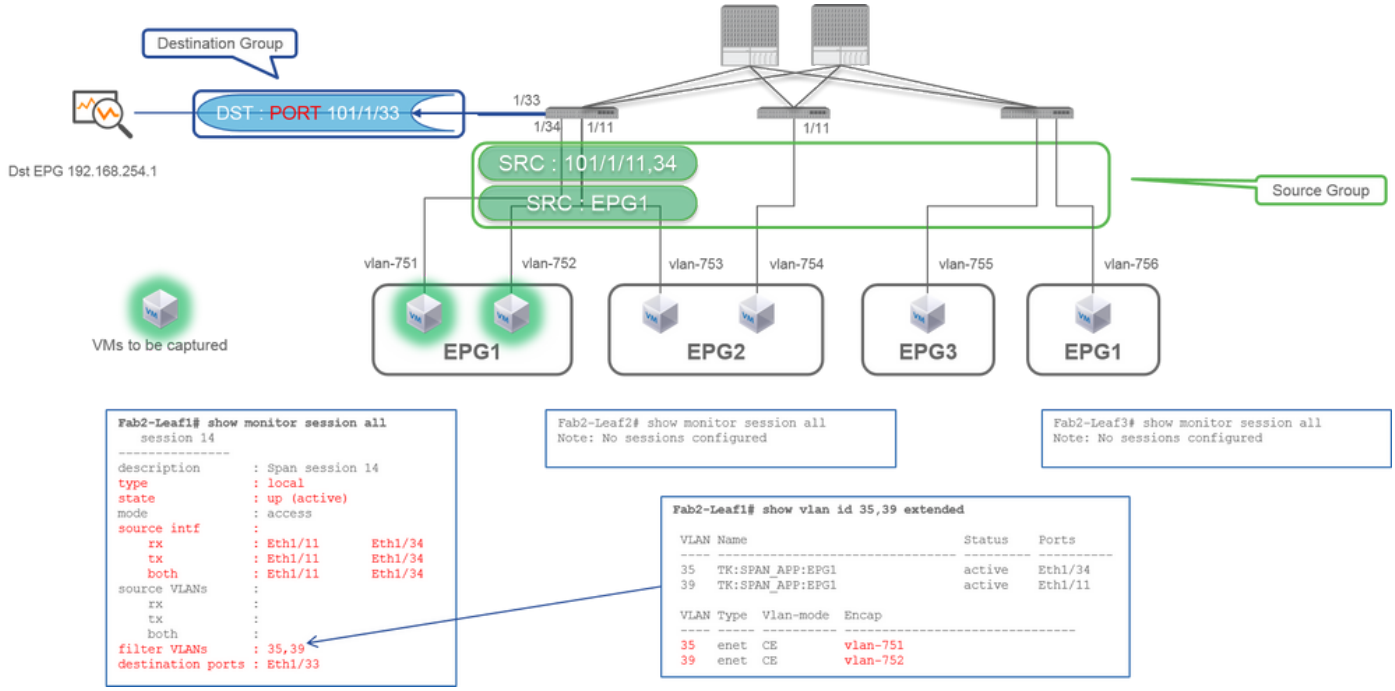
```
Fab2-Leaf3# show monitor session all
Note: No sessions configured
```

- **소스 그룹**
    - 리프1 e1/11
    - 리프1 e1/34
- **대상 그룹**
    - 리프1 e1/33

액세스 SPAN은 로컬 SPAN(즉, 특정 인터페이스를 대상으로 사용)도 사용할 수 있습니다

그러나 이 경우 소스 인터페이스는 대상 인터페이스와 동일한 Leaf에 있어야 합니다.

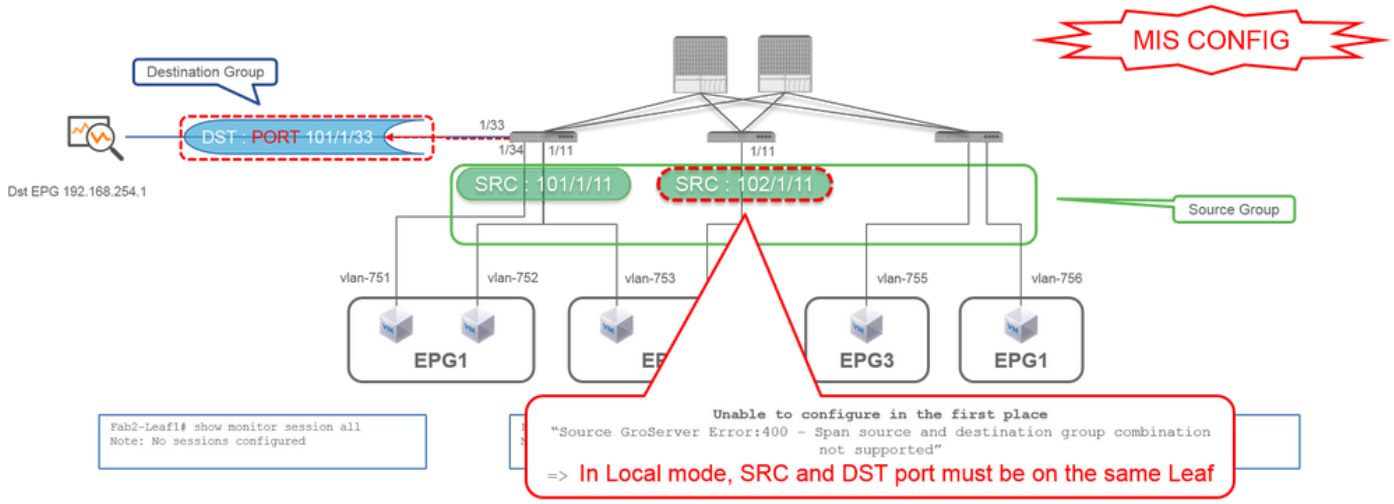
사례 2. Src "Leaf1 e1/11 e1/34 & EPG1 filter | Dst " Leaf1 e1/33"



- **소스 그룹**
  - 리프1 e1/11
  - 리프1 e1/34
  - EPG1 필터
- **대상 그룹**
  - 리프1 e1/33

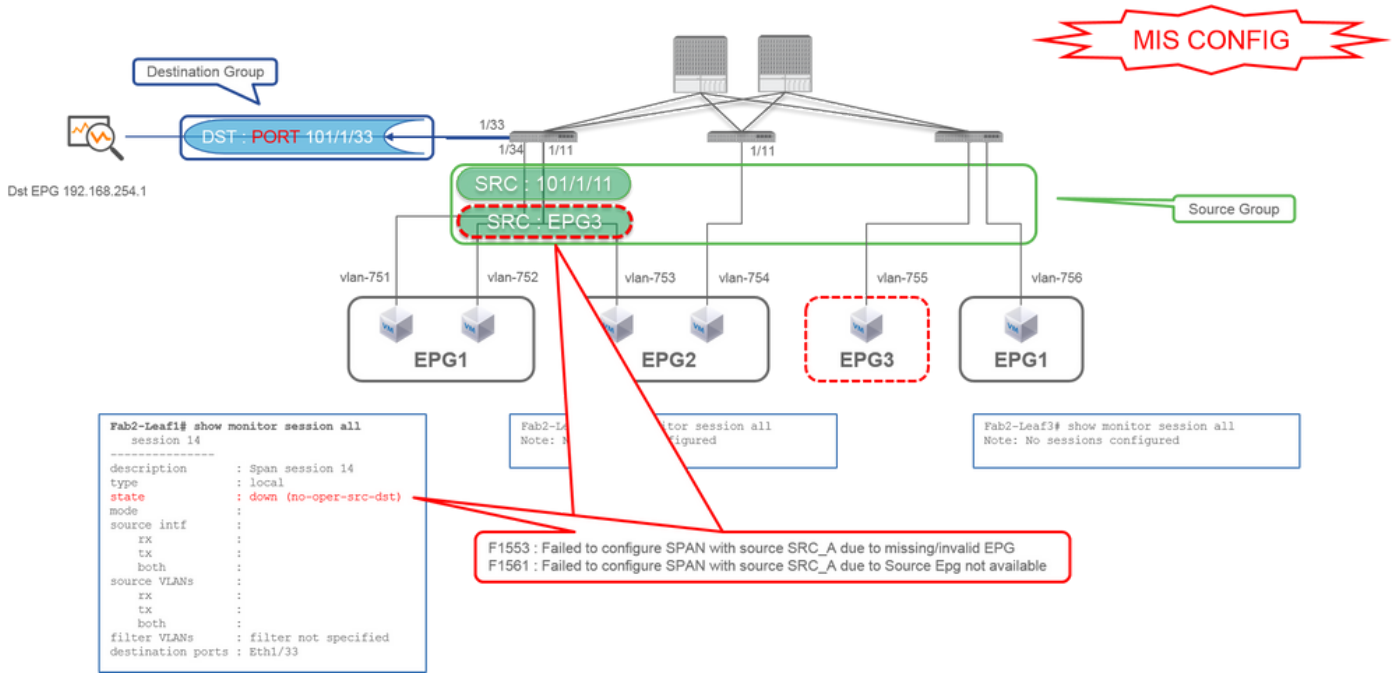
로컬 SPAN을 사용하는 액세스 SPAN에서는 ERSPAN뿐 아니라 EPG 필터도 사용할 수 있습니다.

사례 3. Src "Leaf1 e1/11 & Leaf2 e/11" | Dst "Leaf1 e1/33"(잘못된 경우)



- **소스 그룹**
  - 리프1 e1/11
  - 리프2 e1/11
- **대상 그룹**
  - 리프1 e1/33

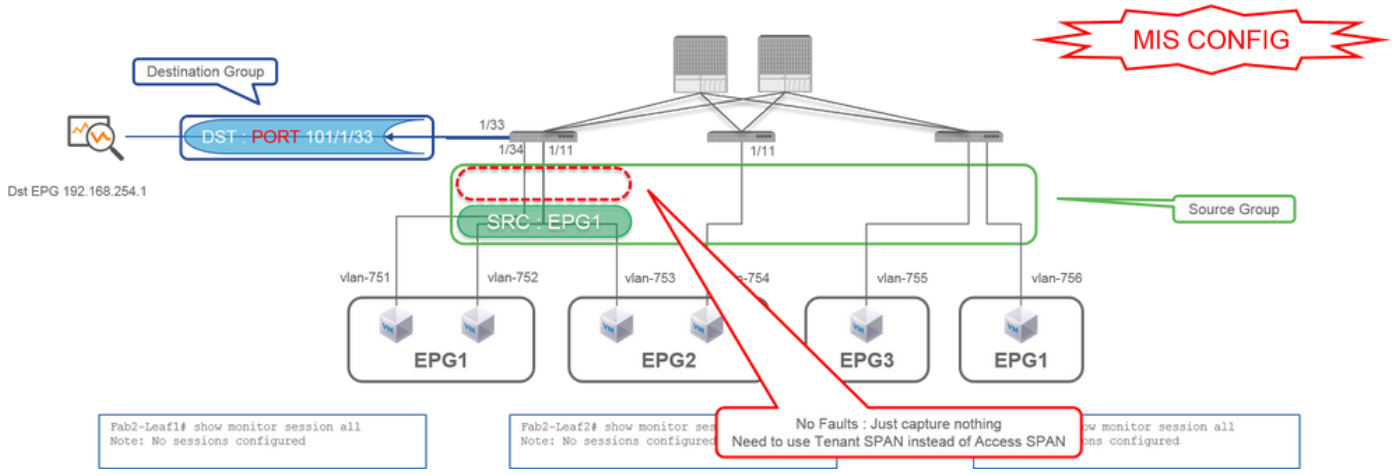
사례 4. Src "Leaf1 e1/11 & EPG3 filter" | Dst "Leaf1 e1/33"(잘못된 경우)



- **소스 그룹**
  - 리프1 e1/11
  - EPG3 필터
- **대상 그룹**
  - 리프1 e1/33

ERSPAN(Access SPAN)의 case 3과 유사하지만, 이 예에서는 EPG3가 Leaf1에 없으므로 Leaf1의 유일한 SPAN 세션이 실패합니다. 따라서 SPAN은 전혀 작동하지 않습니다.

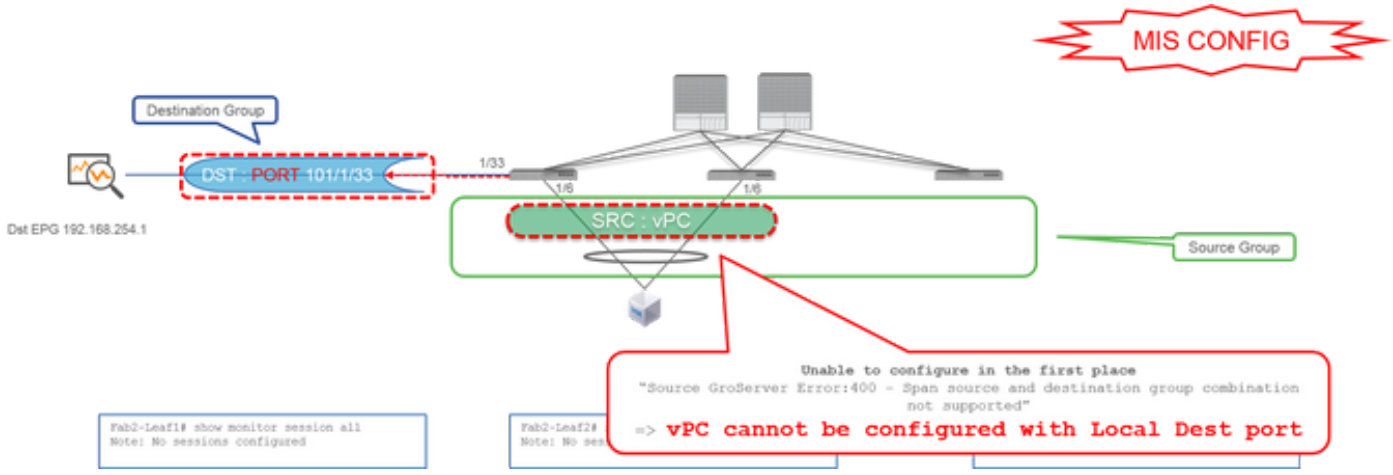
케이스 5: Src "EPG1 filter" | Dst "Leaf1 e1/33"(잘못된 경우)



- **소스 그룹**
  - EPG1 필터
- **대상 그룹**
  - 리프1 e1/33

액세스 SPAN의 EPG 필터는 소스 포트가 구성된 경우에만 작동합니다. EPG를 지정할 유일한 소스인 경우 액세스 SPAN 대신 테넌트 SPAN을 사용해야 합니다.

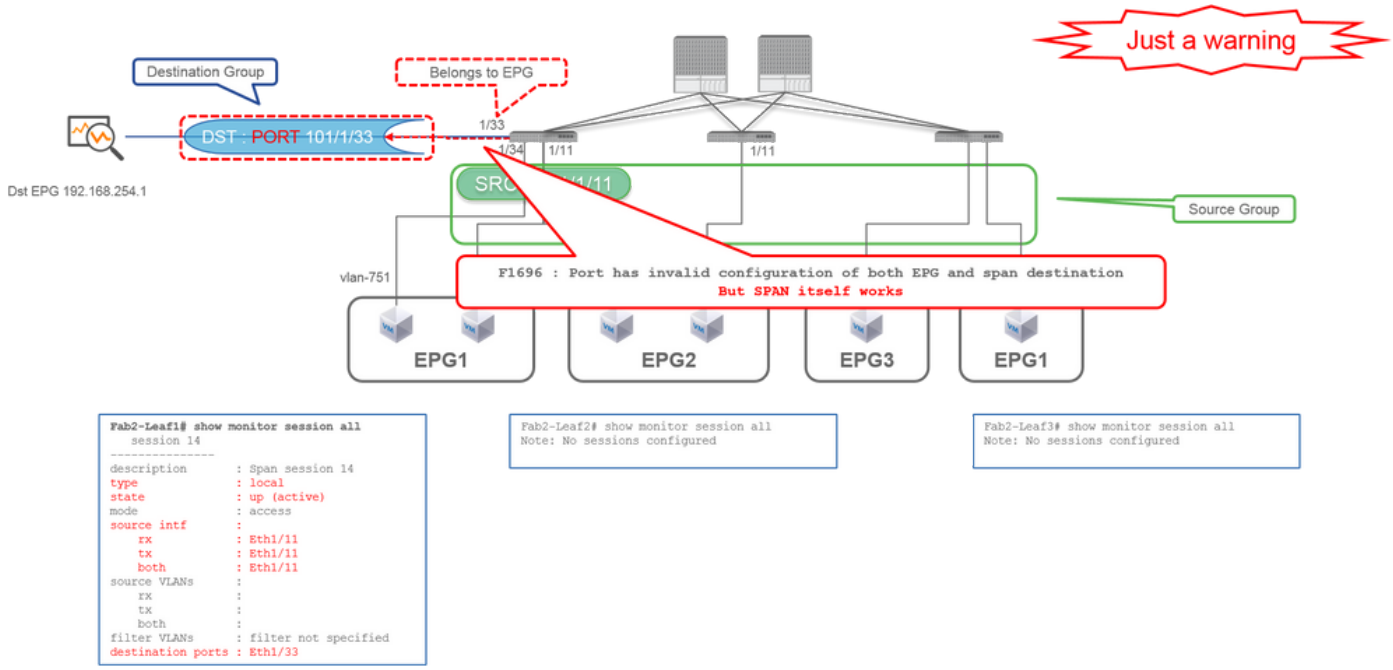
사례 6. Src "Leaf1 - Leaf2 vPC" | Dst "Leaf1 e1/33"(잘못된 경우)



- **소스 그룹**
  - 리프 1-2 vPC
- **대상 그룹**
  - 리프1 e1/33

vPC 인터페이스는 Local SPAN을 사용하여 소스로 구성할 수 없습니다. ERSPAN을 사용하십시오. 액세스 SPAN(ERSPAN)은 case4를 참조하십시오.

사례 7. Src "Leaf1 e1/11 | Dst "Leaf1 e1/33 및 e1/33이 EPG에 속함"(fault와 함께 작동)

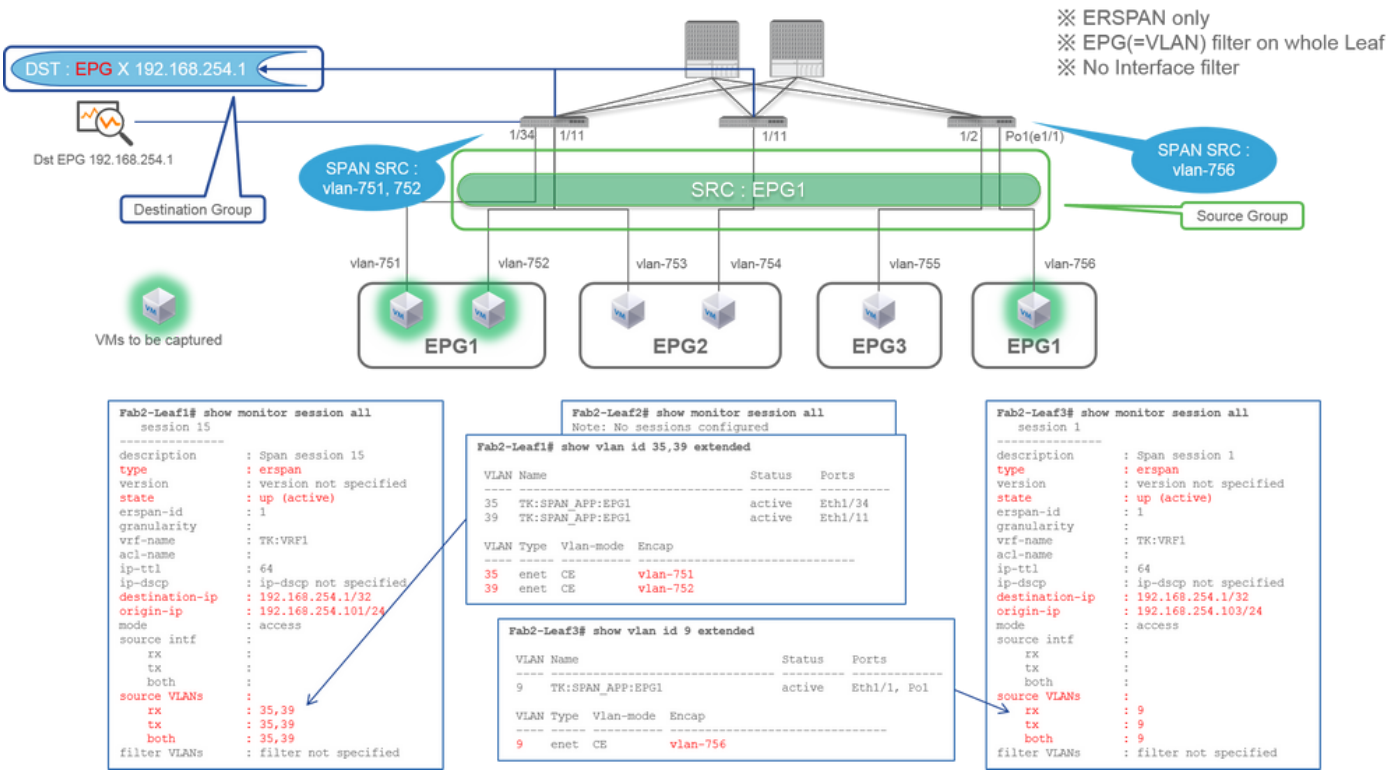


SPAN에 대한 대상 I/F가 이미 EPG에 속한 경우 물리적 I/F 아래에 "F1696: 포트에 EPG 및 SPAN 대상의 잘못된 컨피그레이션이 있습니다."라는 결함이 표시됩니다.

하지만 이 결함에도 SPAN은 문제없이 작동합니다. 이 결함은 동일한 I/F에서 고객의 일반 EPG 트래픽에 영향을 미칠 수 있으므로 SPAN으로 인해 발생하는 추가 트래픽에 대한 경고일 뿐입니다.

테넌트 SPAN(ERSPAN)

사례 1. 소스 "EPG1" | Dst "192.168.254.1"



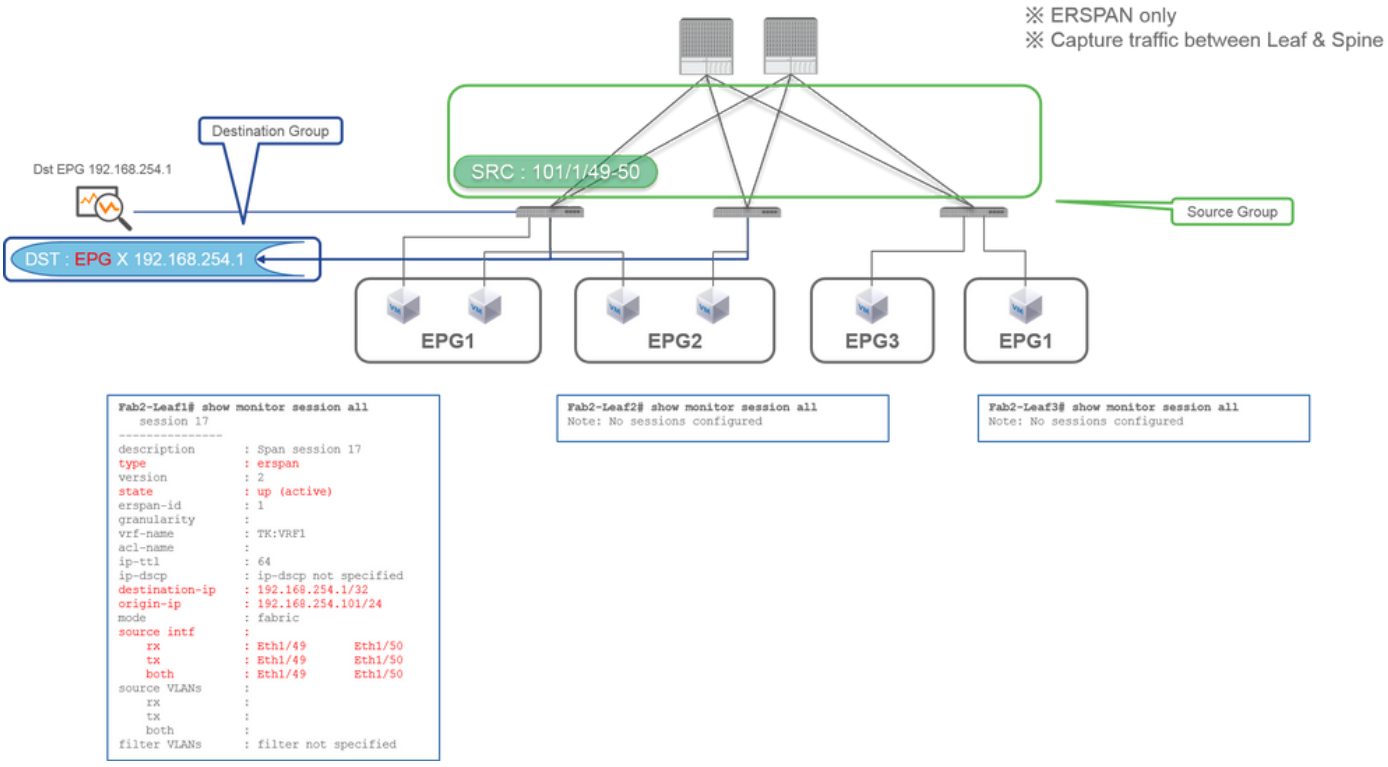
- **소스 그룹**
  - EPG1(필터 없음)
- **대상 그룹**
  - EPG X의 192.168.254.1

테넌트 SPAN은 EPG 자체를 소스로 사용하는 반면 Access SPAN은 필터에 대해서만 EPG를 사용합니다.

테넌트 SPAN의 핵심은 각 개별 포트를 지정할 필요가 없고 ACI가 각 리프 스위치에서 적절한 VLAN을 자동으로 탐지한다는 것입니다. 따라서 특정 EPG에 대한 모든 패킷을 모니터링해야 하고 해당 EPG의 엔드포인트가 리프 스위치 전반의 여러 인터페이스에 속하는 경우 유용합니다.

패브릭 SPAN(ERSPAN)

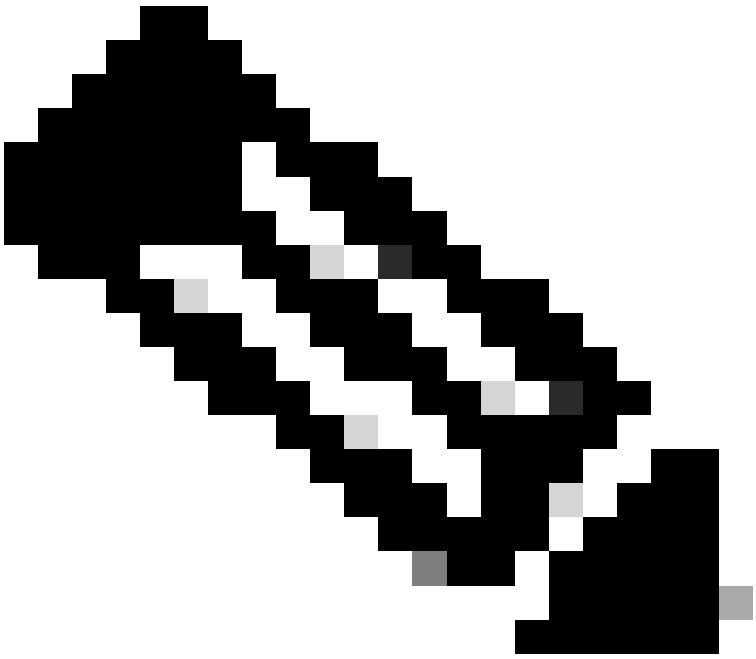
사례 1. Src "Leaf1 e1/49-50" | Dst "192.168.254.1"



- **소스 그룹**
  - 리프1 e1/49-50
- **대상 그룹**
  - EPG X의 192.168.254.1

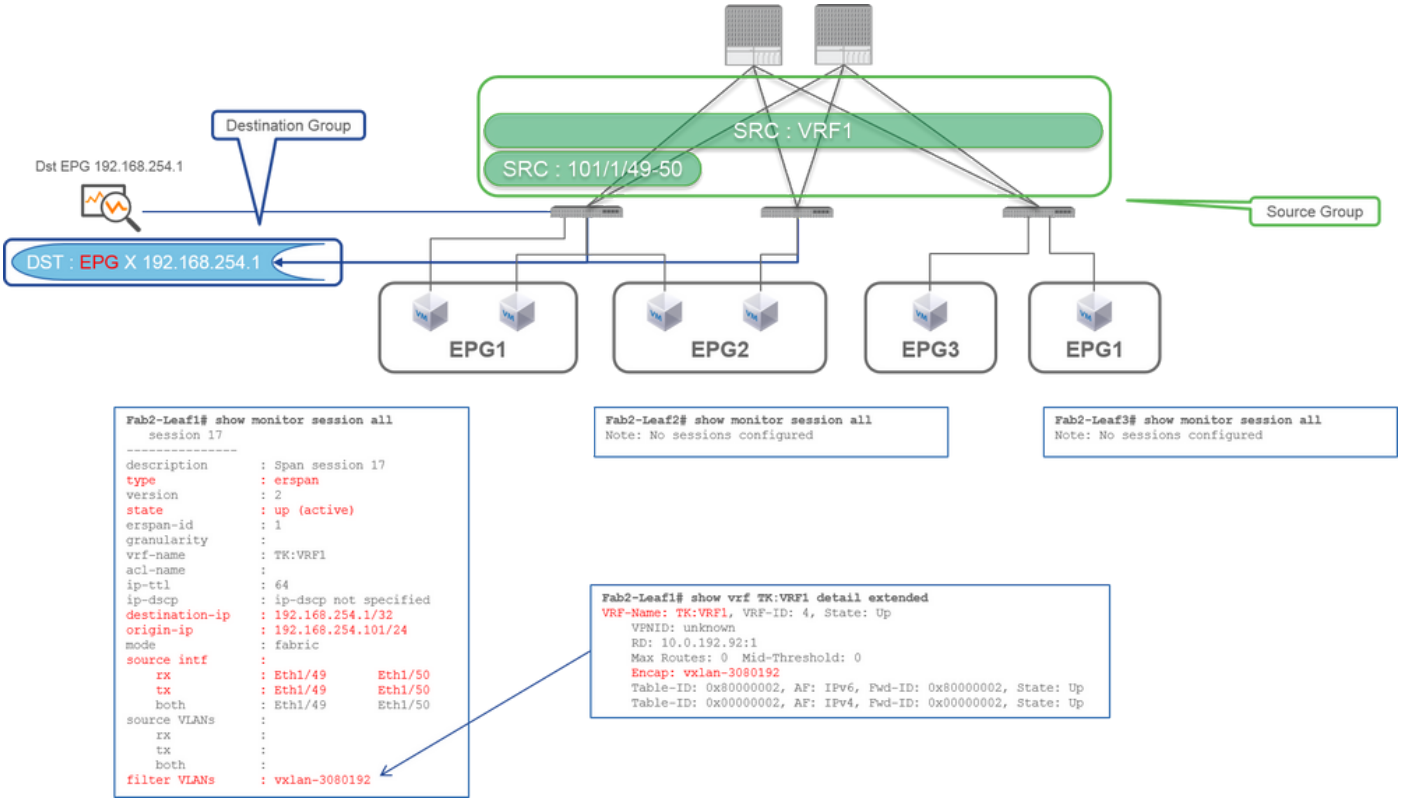
Fabric SPAN은 패브릭 포트를 소스로 지정합니다. 패브릭 포트는 리프 스위치와 스파인 스위치 간의 인터페이스입니다.

이 SPAN은 리프 스위치와 스파인 스위치 간에 패킷을 복사해야 하는 경우 유용합니다. 그러나 리프 스위치와 스파인 스위치 간의 패킷은 iVxLAN 헤더로 캡슐화됩니다. 그래서 그것을 읽으려면 약간의 속임수가 필요하다. "SPAN 데이터 읽기 방법"을 참조하십시오.



참고: iVxLAN 헤더는 ACI Fabric 내부 전용의 향상된 VxLAN 헤더입니다.

사례 2. Src "Leaf1 e1/49-50 & VRF filter" | Dst "192.168.254.1"



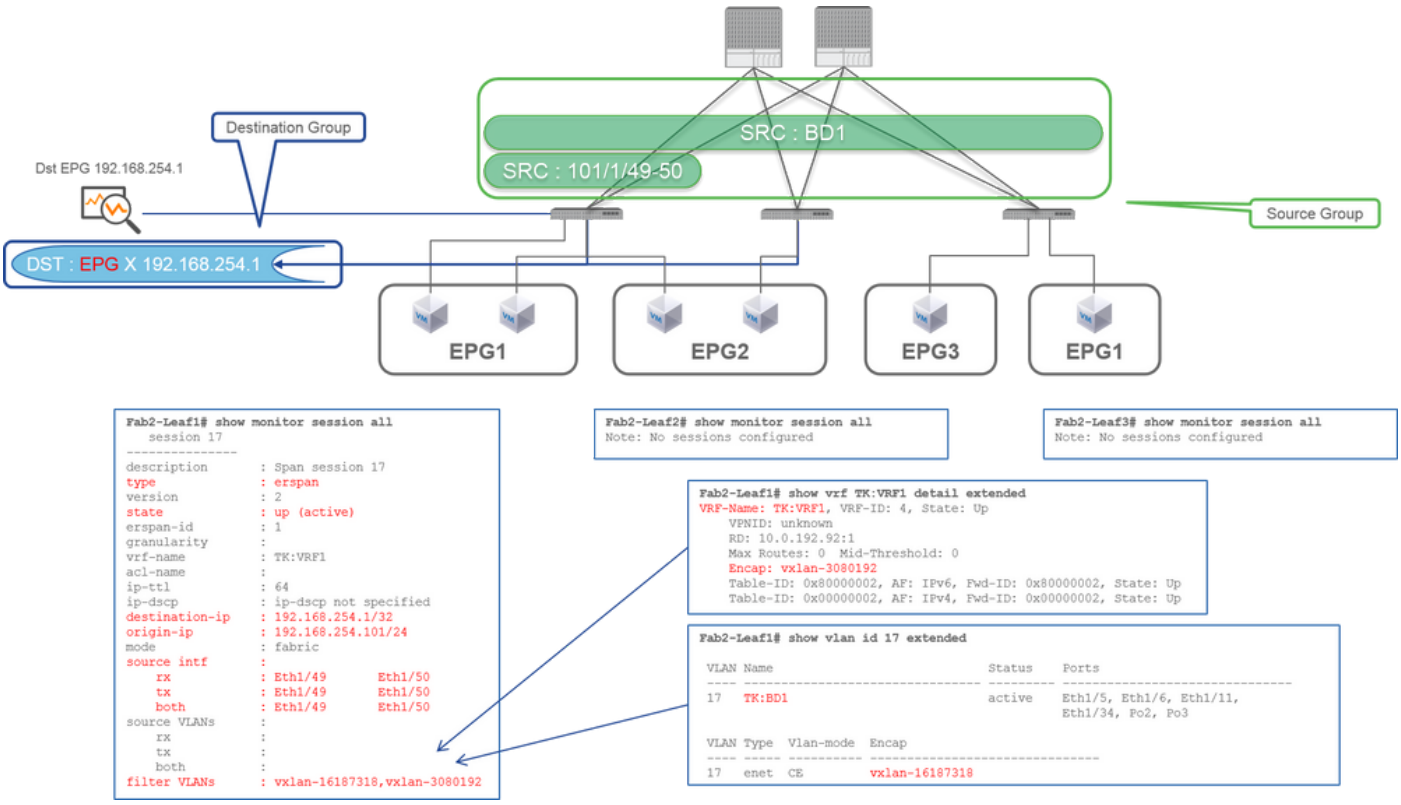
- **소스 그룹**
  - 리프1 e1/49-50
  - VRF 필터
- **대상 그룹**
  - EPG X의 192.168.254.1

Fabric SPAN은 Access SPAN뿐만 아니라 필터도 사용할 수 있습니다. 하지만 필터 종류가 다릅니다. Fabric SPAN은 VRF(Virtual Routing and Forwarding) 또는 BD를 필터로 사용합니다.

Cisco ACI에서는 앞서 설명한 대로 패브릭 포트를 통과하는 패킷이 iVxLAN 헤더로 캡슐화됩니다. 이 iVxLAN 헤더에는 VNID(Virtual Network Identifier)로 VRF 또는 BD 정보가 있습니다. 패킷이 L2(Layer2)로 전달된 경우 iVxLAN VNID는 BD를 나타냅니다. 패킷이 L3(Layer3)으로 전달된 경우 iVxLAN VNID는 VRF를 나타냅니다.

따라서 패브릭 포트에서 라우팅된 트래픽을 캡처해야 하는 경우 VRF를 필터로 사용합니다.

사례 3. Src "Leaf1 e1/49-50 & BD filter" | Dst "192.168.254.1"

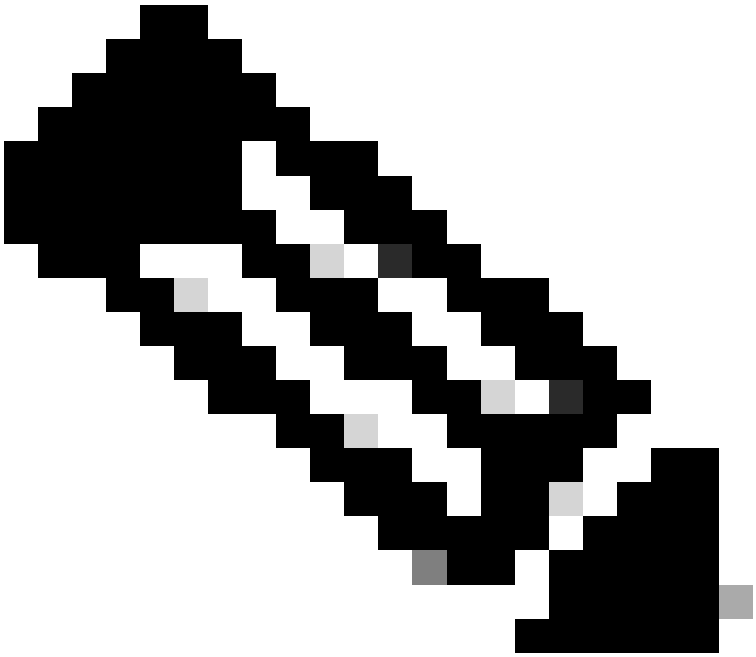


- **소스 그룹**
  - 리프1 e1/49-50
  - BD 필터
- **대상 그룹**

- EPG X의 192.168.254.1

앞의 case 2에서 설명한 바와 같이, Fabric SPAN은 BD를 필터로 사용할 수 있다.

패브릭 포트에서 브리지 트래픽을 캡처해야 하는 경우 BD를 필터로 사용합니다.



참고: BD 또는 VRF의 단일 필터만 한 번에 구성할 수 있습니다.

SPAN 대상 디바이스에는 무엇이 필요합니까?

패킷 캡처 애플리케이션(예: tcpdump, wireshark)을 실행합니다. ERSPAN 대상 세션 등을 구성할 필요는 없습니다.

ERSPAN용

SPAN 패킷이 대상 IP로 전달되므로 ERSPAN에 대한 대상 IP가 있는 인터페이스에서 캡처 툴을 실행해야 합니다.

수신된 패킷은 GRE 헤더로 캡슐화됩니다. ERSPAN GRE 헤더를 디코딩하는 방법에 대해서는 이 섹션 "ERSPAN 데이터 읽기 방법"을 참조하십시오.

로컬 SPAN용

ACI Leaf의 SPAN Destination 인터페이스에 연결하는 인터페이스에서 캡처 툴을 실행해야 합니다.

원시 패킷은 이 인터페이스에서 수신됩니다. ERSPAN 헤더를 처리할 필요는 없습니다.

ERSPAN 데이터 읽기 방법

ERSPAN 버전(유형)

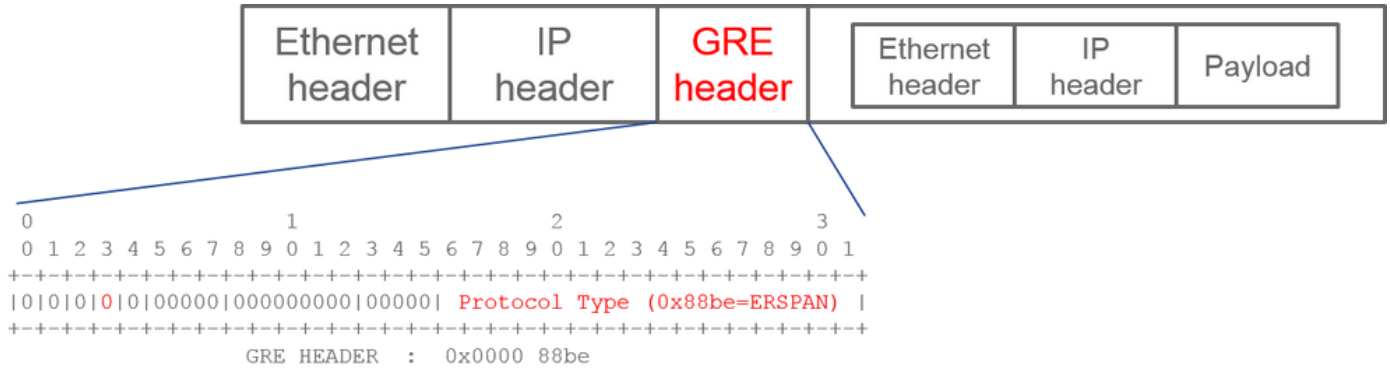
ERSPAN은 복사된 패킷을 캡슐화하여 원격 대상에 전달합니다. 이 캡슐화에는 GRE가 사용됩니다. GRE 헤더의 ERSPAN 프로토콜 유형은 0x88be입니다.

IETF(Internet Engineering Task Force) 문서에서는 ERSPAN 버전이 버전 대신 유형으로 설명됩니다.

ERSPAN에는 세 가지 유형이 있습니다. I, II 및 III. ERSPAN 유형은 이 RFC 초안에 나와 있습니다. 또한 이 GRE RFC1701은 각 ERSPAN 유형을 이해하는 데 도움이 될 수 있습니다.

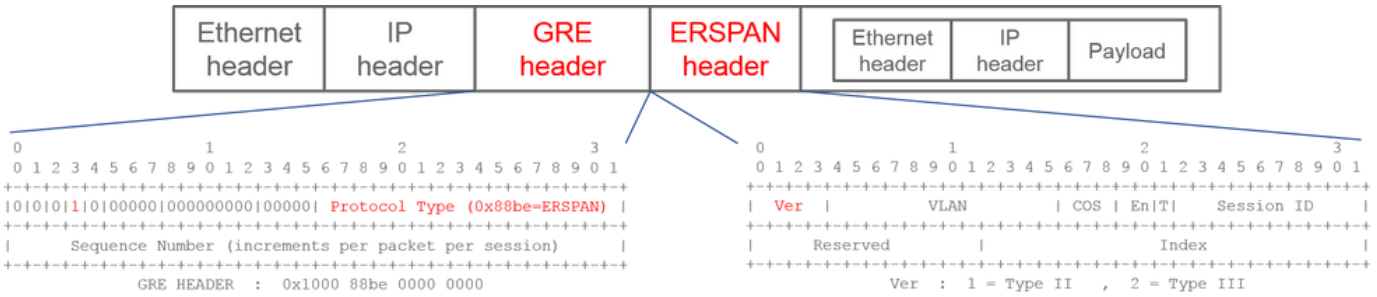
각 유형의 패킷 형식은 다음과 같습니다.

ERSPAN Type I(Broadcom Trident 2에서 사용)



유형 I는 GRE 헤더의 시퀀스 필드를 사용하지 않습니다. ERSPAN 유형이 II 및 III인 경우 GRE 헤더 뒤에 와야 하는 ERSPAN 헤더도 사용하지 않습니다. Broadcom Trident 2는 이 ERSPAN 유형 I만 지원합니다.

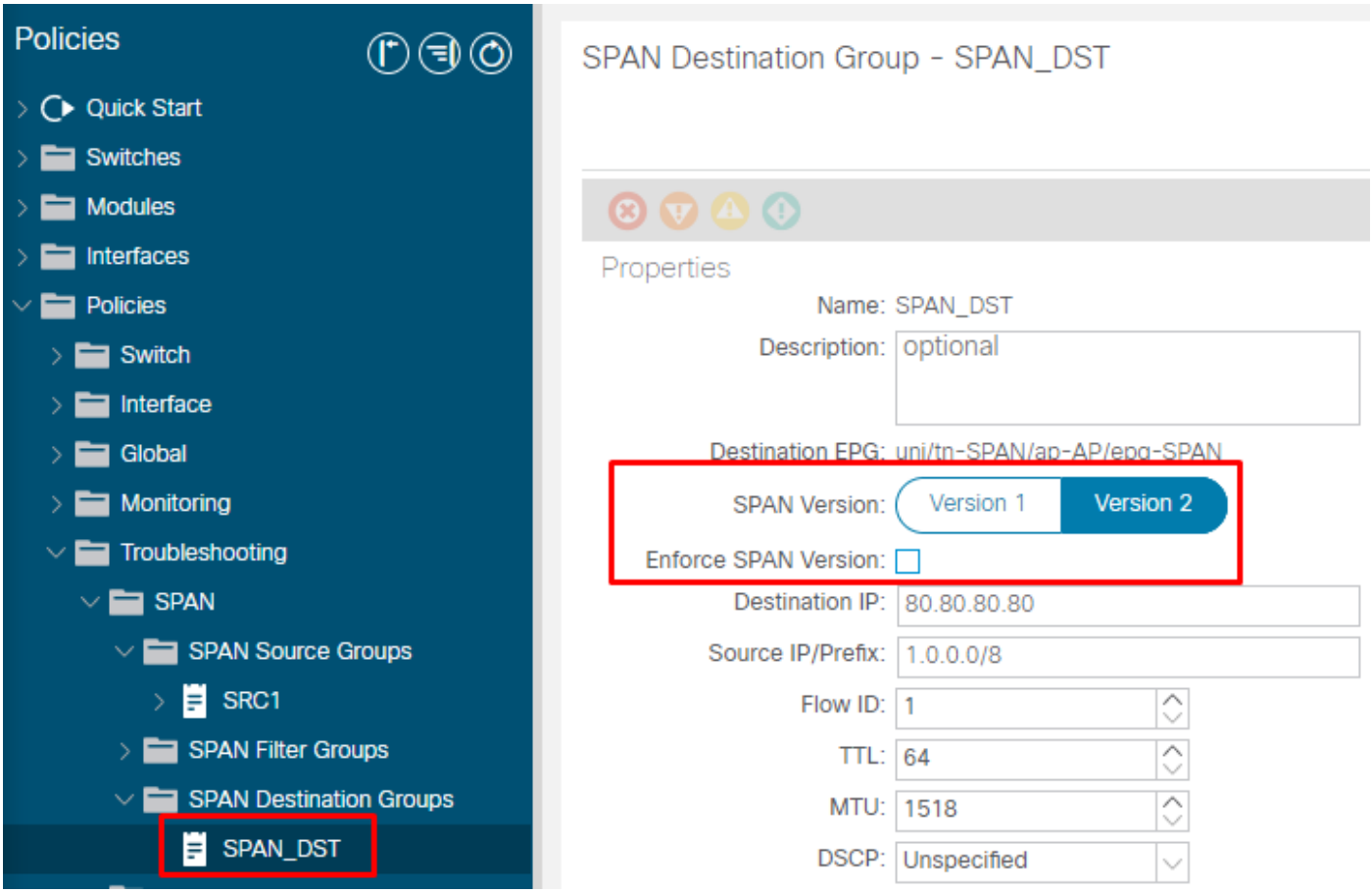
ERSPAN Type II 또는 III



시퀀스 필드가 S 비트에 의해 활성화되는 경우, 이는 ERSPAN 타입 II 또는 III이어야 한다. ERSPAN 헤더의 version 필드는 ERSPAN 유형을 식별합니다. ACI에서 III 유형은 2016년 3월 20일 현재 지원되지 않습니다.

액세스 또는 테넌트 SPAN에 대한 SPAN 소스 그룹에 1세대 및 2세대 노드 모두의 소스가 있는 경우 ERSPAN 대상은 각 세대 노드에서 ERSPAN Type I 및 II 패킷을 모두 수신합니다. 그러나 Wireshark는 한 번에 하나의 ERSPAN 유형만 디코딩할 수 있습니다. 기본적으로 ERSPAN Type II만 디코딩합니다. ERSPAN Type I의 디코딩을 활성화하면 Wireshark는 ERSPAN Type II를 디코딩하지 않습니다. Wireshark에서 ERSPAN Type I를 디코딩하는 방법에 대한 자세한 내용은 뒷부분의 섹션을 참조하십시오.

이러한 유형의 문제를 방지하려면 SPAN 대상 그룹에서 ERSPAN 유형을 구성할 수 있습니다.



- SPAN 버전(버전 1 또는 버전 2): ERSPAN 유형 I 또는 II를 나타냅니다.

- Enforce SPAN Version(SPAN 버전 적용)(선택 또는 선택 취소): 구성된 ERSPAN 유형이 소스 노드 하드웨어에서 지원되지 않는 경우 SPAN 세션이 실패해야 하는지 여부를 결정합니다.

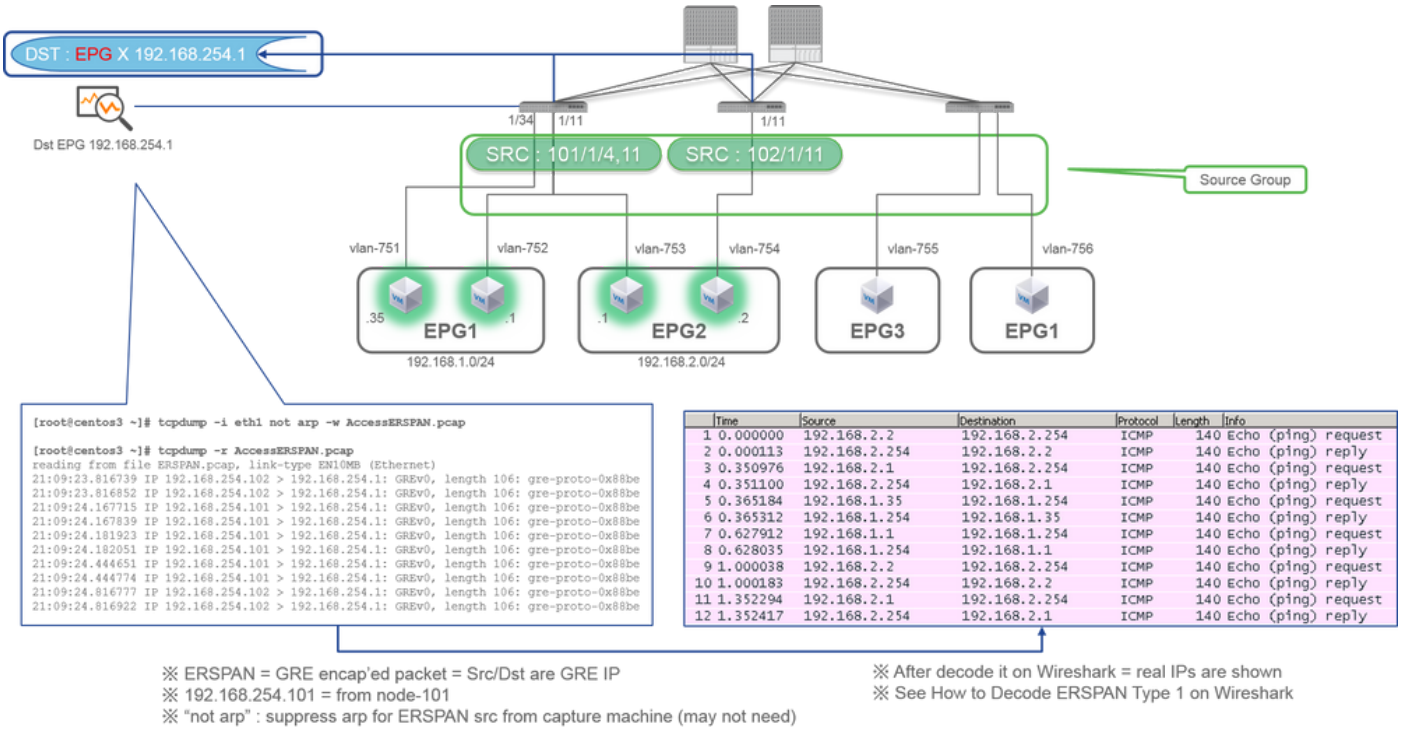
기본적으로 SPAN Version(SPAN 버전)은 Version 2(버전 2)이고 Enforce SPAN Version(SPAN 버전 시행)은 선택 취소되어 있습니다. 이는 소스 노드가 ERSPAN Type II를 지원하는 2세대 이상인 경우 Type II를 사용하여 ERSPAN을 생성함을 의미합니다. 소스 노드가 ERSPAN Type II(Fabric SPAN 제외)를 지원하지 않는 1세대 노드인 경우 SPAN 버전 시행을 선택하지 않았으므로 Type I로 돌아갑니다. 그 결과 ERSPAN 대상이 혼합 유형의 ERSPAN을 수신합니다.

이 표에서는 액세스 및 테넌트 SPAN의 각 조합에 대해 설명합니다.

SPAN 버전	SPAN 버전 적용	1세대 소스 노드	2세대 소스 노드
버전 2	선택 취소됨	유형 I 사용	유형 II 사용
버전 2	선택됨	실패	유형 II 사용
버전 1	선택 취소됨	유형 I 사용	유형 I 사용
버전 1	선택됨	유형 I 사용	유형 I 사용

ERSPAN 데이터 예

테넌트 SPAN/액세스 SPAN(ERSPAN)



패킷은 ERSPAN Type I에 의해 캡슐화되므로 디코딩해야 합니다. 이는 Wireshark를 사용하여 수행할 수 있습니다. "ERSPAN Type 1 디코딩 방법" 섹션을 참조하십시오.

캡처된 패킷의 세부 정보(ERSPAN 유형 I)

```
[root@centos3 ~]# tcpdump -xxr AccessERSPAN.pcap -c 1
reading from file AccessERSPAN.pcap, link-type EN10MB (Ethernet)
21:09:23.816739 IP 192.168.254.102 > 192.168.254.1: GREv0, length 106: gre-proto-0x88be
        0x0000:  0050 56bb 3096 0022 bdf8 19ff 0800 4500
        0x0010:  007e 0000 0000 3d2f ff97 c0a8 fe66 c0a8                ESPAN Ethernet header       : Dst 0050.56bb.3096 , Src 0022.bdf8.19.ff
        0x0020:  fe01 0000 88be 0022 bdf8 19ff 0050 56bb                ERSPAN IP header            : Dst 192.168.254.1  , Src 192.168.254.102
        0x0030:  d6c2 8100 02f2 0800 4500 0054 0000 4000                GRE header (= ERSPAN Type I)  : 0x88be = ERSPAN (S bit off 0x0000)
        0x0040:  4001 b458 c0a8 0202 c0a8 02fe 0800 34cc                Ethernet header             : Dst 0022.bdf8.19ff , Src 0050.56bb.d6c2
        0x0050:  c847 0115 7404 2b56 0000 0000 8da9 0e00                Dot1Q header                : VLAN 754
        0x0060:  0000 0000 1011 1213 1415 1617 1819 1a1b                IP header                   : Dst 192.168.2.254  , Src 192.168.2.2
        0x0070:  1c1d 1e1f 2021 2223 2425 2627 2829 2a2b
        0x0080:  2c2d 2e2f 3031 3233 3435 3637
```

패브릭 SPAN(ERSPAN)

```
[root@centos3 ~]# tcpdump -r FabricERSPAN.pcap
reading from file FabricERSPAN.pcap, link-type EN10MB (Ethernet)
23:25:00.777331 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 54227, length 127: gre-proto-0x88be
23:25:00.777445 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 53328, length 82: gre-proto-0x88be
23:25:00.777567 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 54228, length 187: gre-proto-0x88be
23:25:00.777580 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 53329, length 82: gre-proto-0x88be
23:25:00.778068 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 53330, length 127: gre-proto-0x88be
23:25:00.817915 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 54229, length 82: gre-proto-0x88be
23:25:00.829676 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 54230, length 82: gre-proto-0x88be
23:25:00.829691 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 53331, length 82: gre-proto-0x88be
23:25:00.873953 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 54231, length 82: gre-proto-0x88be
23:25:00.873968 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 53332, length 82: gre-proto-0x88be
```

ERSPAN Type 2 is automatically decoded by Wireshark
※ be noted that this is still iVxLAN header

Filter: ip.addr==10.0.192.92 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
26	0.184754	10.0.192.92	10.0.32.66	UDP	198	Source port: 7248 Destination port: 48879
27	0.184893	10.0.192.95	10.0.192.92	UDP	198	Source port: 25168 Destination port: 48879
32	0.262735	10.0.192.92	10.0.32.65	UDP	160	Source port: 62672 Destination port: 48879
34	0.262855	10.0.192.92	239.255.255.255	UDP	156	Source port: 38745 Destination port: 48879
35	0.262868	10.0.192.92	239.255.255.255	UDP	156	Source port: 38745 Destination port: 48879
38	0.263458	10.0.192.92	225.0.213.250	UDP	160	Source port: 43738 Destination port: 48879
148	0.768367	10.0.0.1	10.0.192.92	TCP	116	56210-12151 [ACK] Seq=1 Ack=1 Win=770 Len=0
149	0.768486	10.0.192.92	10.0.0.1	TCP	116	[TCP ACKed unseen segment] 12151-56210 [ACK]
152	0.856142	10.0.192.92	225.0.213.248	UDP	164	Source port: 45334 Destination port: 48879
175	0.875130	10.0.192.92	10.0.0.1	TCP	116	[TCP Keep-Alive] [TCP ACKed unseen segment]
176	0.875252	10.0.0.1	10.0.192.92	TCP	116	[TCP Previous segment not captured] 56210-12
234	1.185477	10.0.192.92	10.0.32.66	UDP	198	Source port: 7248 Destination port: 48879
235	1.185606	10.0.192.95	10.0.192.92	UDP	198	Source port: 25168 Destination port: 48879
253	1.259119	10.0.192.92	10.0.0.1	TCP	116	57294-12375 [ACK] Seq=1 Ack=1 Win=270 Len=0

Wireshark는 ERSPAN Type II를 자동으로 디코딩합니다. 그러나 여전히 iVxLAN 헤더로 캡슐화됩니다.

기본적으로 Wireshark는 ACI 내부 헤더이므로 iVxLAN 헤더를 인식하지 못합니다. "iVxLAN 헤더를 디코딩하는 방법"을 참조하십시오.

캡처된 패킷의 세부 정보(ERSPAN Type II)

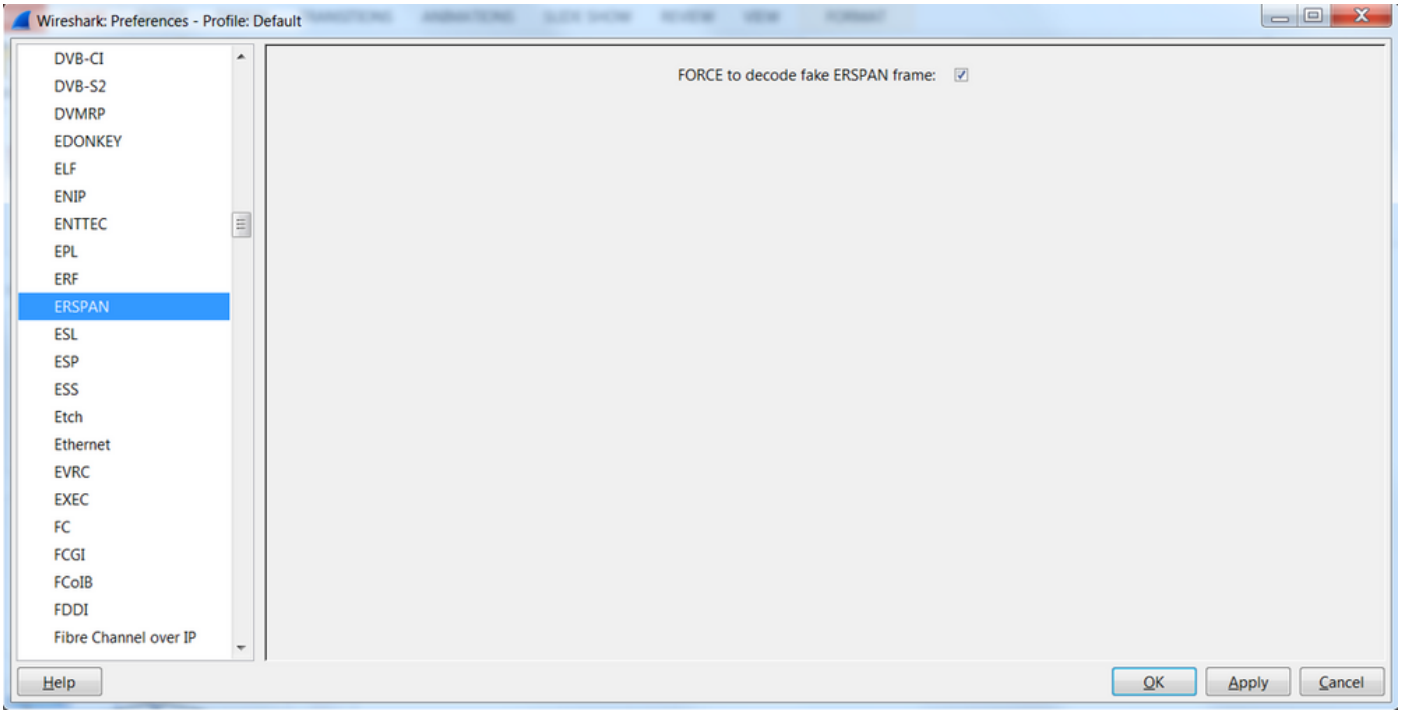
```
[root@centos3 ~]# tcpdump -xxr FabricERSPAN.pcap -c 1
reading from file FabricERSPAN.pcap, link-type EN10MB (Ethernet)
23:25:00.962224 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 53341, length 164: gre-proto-0x88be
        0x0000:  0050 56bb 3096 0022 bdf8 19ff 0800 4500
        0x0010:  00b8 0580 0000 3e2f f8de c0a8 fe65 c0a8
        0x0020:  fe01 1000 88be 0000 d05d 1002 1001 0001
        0x0030:  abcb 000c 0c0c 0c0c 0000 0000 0000 0800
        0x0040:  4500 0086 55aa 0000 1f11 b101 0a00 c05f
        0x0050:  0a00 c05c 6250 beef 0072 0000 c8a0 c007
        0x0060:  fd7f 8200 0050 56bb d95f 0050 56bb d6c2
        0x0070:  0800 4500 0054 799b 0000 4001 7bba c0a8
        0x0080:  0202 c0a8 0201 0000 4f21 b749 0027 3d24
        0x0090:  2b56 0000 0000 c720 0b00 0000 0000 1011
        0x00a0:  1213 1415 1617 1819 1a1b 1c1d 1e1f 2021
        0x00b0:  2223 2425 2627 2829 2a2b 2c2d 2e2f 3031
        0x00c0:  3233 3435 3637

ESPAN Ethernet header          : Dst 0050.56bb.3096 , Src 0022.bdf8.19ff
ERSPAN IP header               : Dst 192.168.254.1  , Src 192.168.254.101
GRE header (= ERSPAN Type II)  : 0x88be = ERSPAN (S bit on 0x1000)
ERSPAN Type II header          : VLAN 2, ERSPAN ID 1
Ethernet header                : Dst 0022.bdf8.19ff , Src 0050.56bb.d6c2
IP header                      : Dst 10.0.192.95    , Src 10.0.192.92
UDP header                     : Dst 0xbeef(48879)  , Src 0x6250(25168)
iVXLAN header                  : sclass 0xc007 , VNID 0xfd7f82
Ethernet header                : Dst 0050.56bb.d95f , Src 0050.56bb.d6c2
IP header                      : Dst 192.168.2.254  , Src 192.168.2.2
```

ERSPAN 유형 I 디코딩 방법

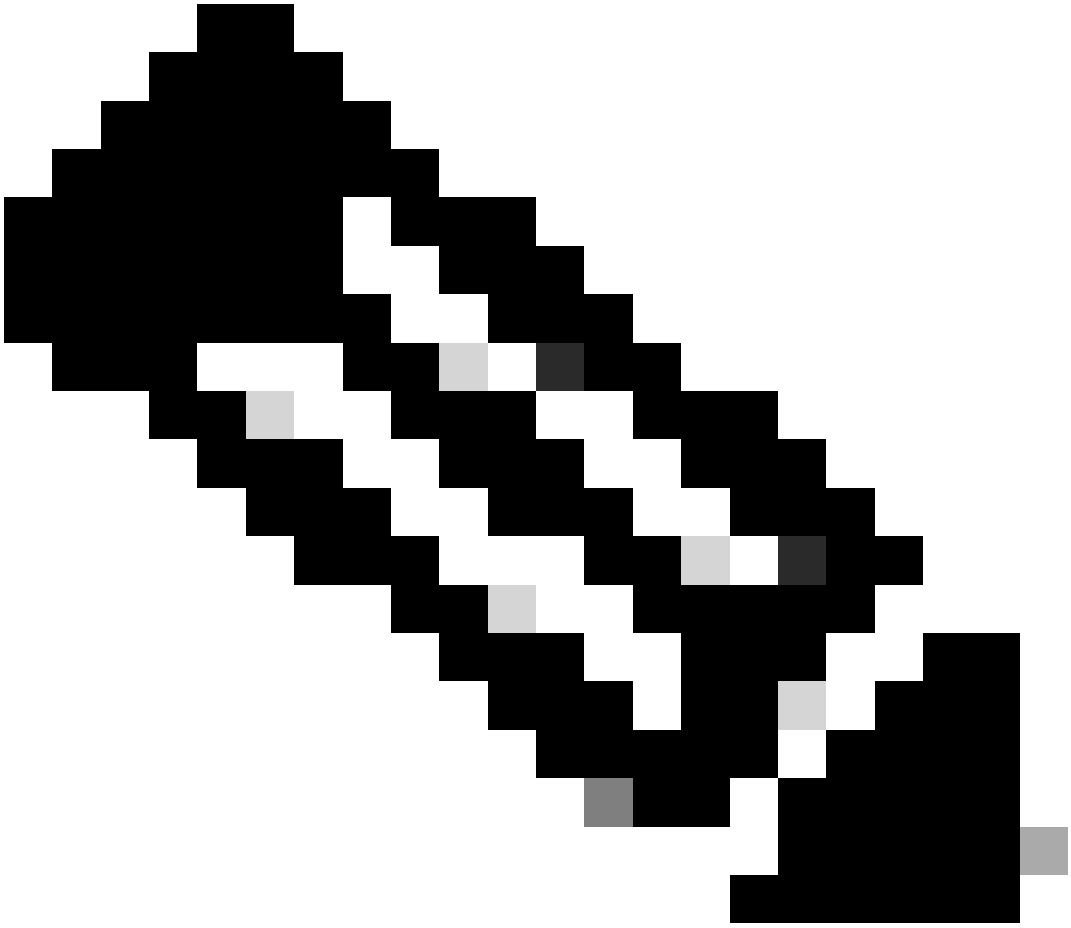
옵션 1. 로 Edit > Preference > Protocols > ERSPAN 이동하고 FORCE를 선택하여 가짜 ERSPAN 프레임을 디코딩합니다.

- Wireshark(GUI)



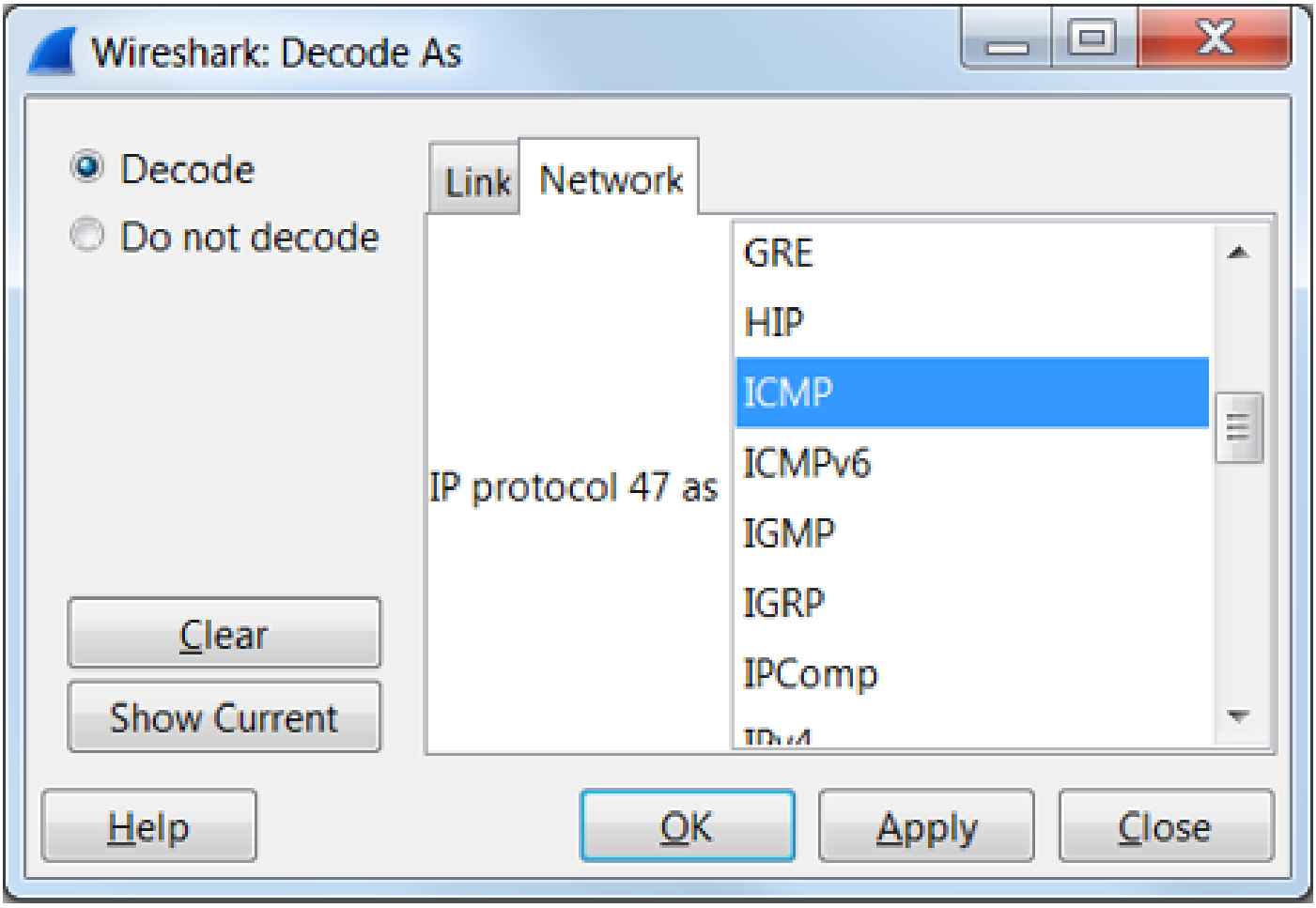
- Tshark(Wireshark CLI 버전):

```
user1@linux# tshark -f 'proto GRE' -nV -i eth0 -o erspan.fake_erspan:true
```

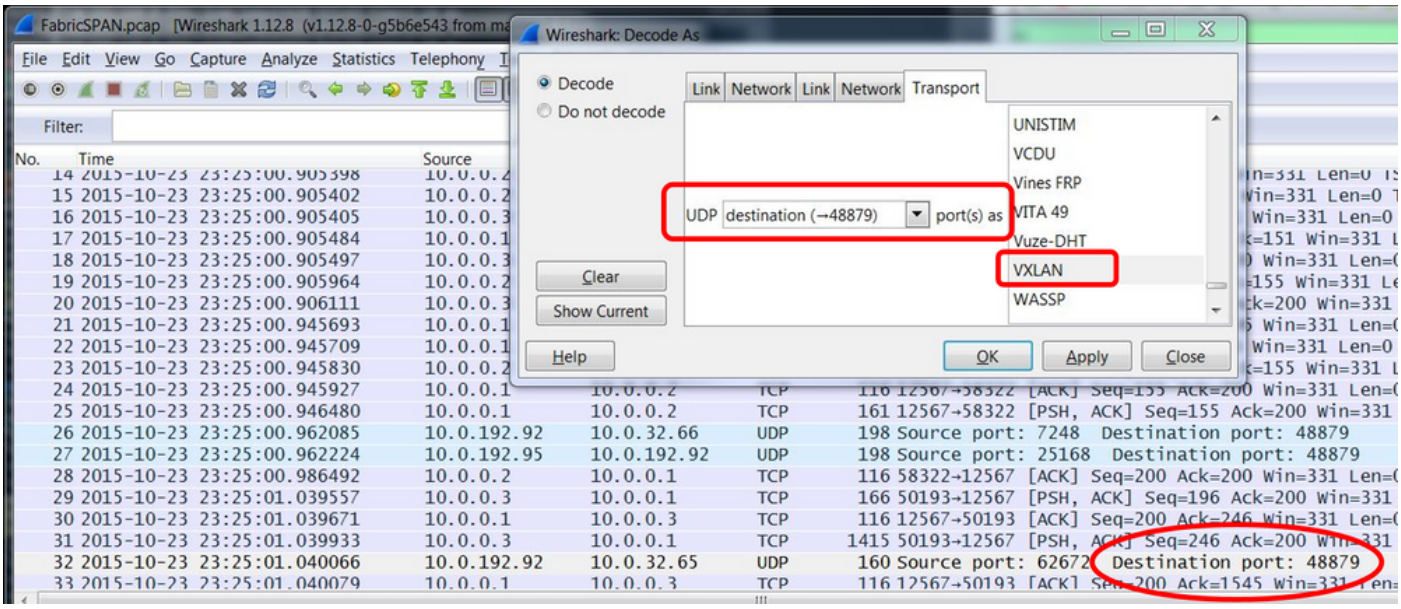


참고: ERSPAN type II 또는 III를 읽을 때 이 옵션을 비활성화하십시오.

옵션 2. 탐색 Decode As > Network > ICMP (if it’s ICMP).



iVxLAN 헤더를 디코딩하는 방법

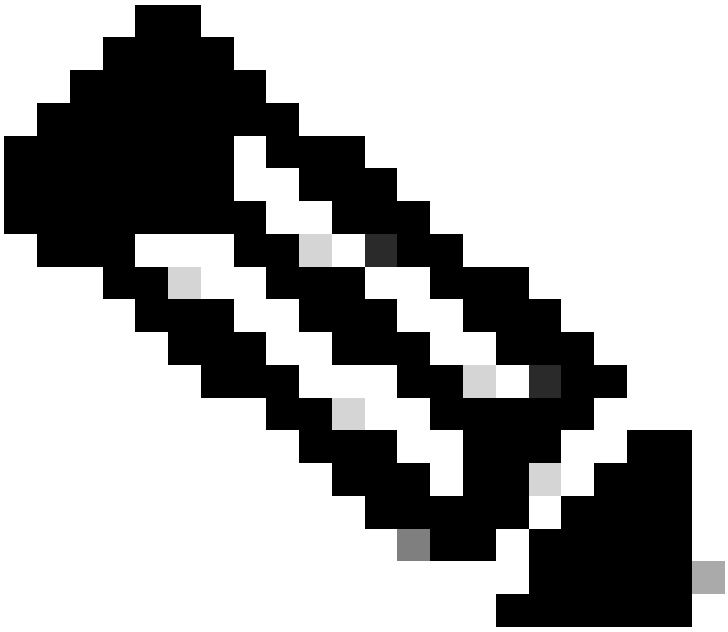


iVxLAN 헤더는 목적지 포트 48879을 사용합니다. 따라서 Wireshark에서 UDP 목적지 포트 48879을 VxLAN으로 구성하는 경우 iVxLAN 헤더와 VxLAN을 디코딩할 수 있습니다.

1. 먼저 iVxLAN 캡슐화 패킷을 선택해야 합니다.

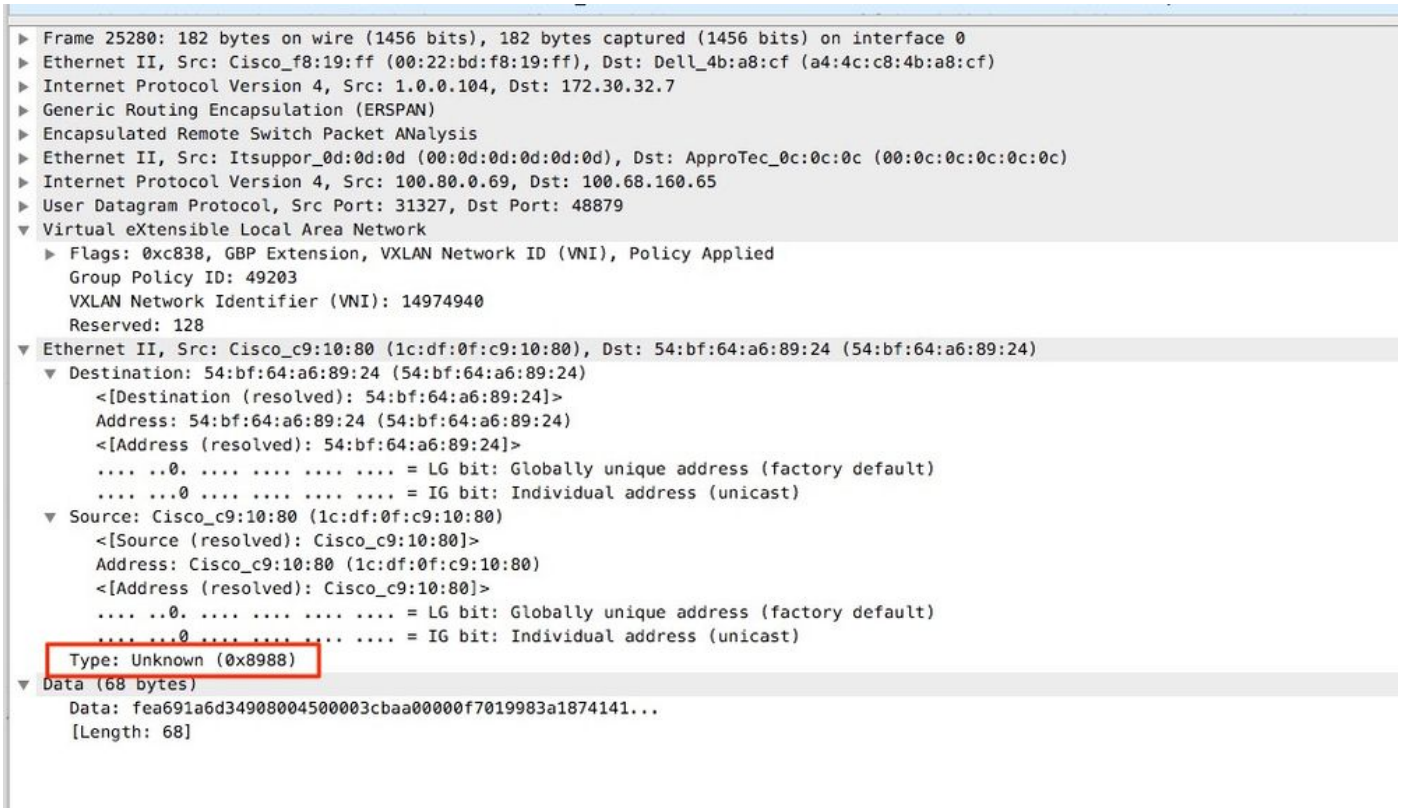
2. 로 Analyze > Decode As > Transport > UDP destination (48879) > VxLAN 이동합니다.

- 그리고 Apply.



참고: 패브릭 포트의 APIC 간에는 통신 패킷이 있습니다. 이러한 패킷은 iVxLAN 헤더로 캡슐화되지 않습니다.

PTP(Precision Time Protocol)를 실행하는 사용자 네트워크에서 erspan 캡처를 수행하는 경우 GRE encap(0x8988) 내의 알 수 없는 이더 타입 때문에 Wireshark가 데이터를 해석하지 않는 경우가 있습니다. 0x8988은 PTP가 활성화될 때 데이터 플레인 패킷에 삽입되는 시간 태그에 대한 이더 타입입니다. 이더 타입 0x8988을 "Cisco ttag"로 디코딩하여 패킷의 세부사항을 공개합니다.


Frame 25280: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on interface 0
Ethernet II, Src: Cisco_f8:19:ff (00:22:bd:f8:19:ff), Dst: Dell_4b:a8:cf (a4:4c:c8:4b:a8:cf)
Internet Protocol Version 4, Src: 1.0.0.104, Dst: 172.30.32.7
Generic Routing Encapsulation (ERSPAN)
Encapsulated Remote Switch Packet ANalysis
Ethernet II, Src: Itsuppor_0d:0d:0d (00:0d:0d:0d:0d:0d), Dst: ApproTec_0c:0c:0c (00:0c:0c:0c:0c:0c)
Internet Protocol Version 4, Src: 100.80.0.69, Dst: 100.68.160.65
User Datagram Protocol, Src Port: 31327, Dst Port: 48879
Virtual eXtensible Local Area Network
Flags: 0xc838, GBP Extension, VXLAN Network ID (VNI), Policy Applied
Group Policy ID: 49203
VXLAN Network Identifier (VNI): 14974940
Reserved: 128
Ethernet II, Src: Cisco_c9:10:80 (1c:df:0f:c9:10:80), Dst: 54:bf:64:a6:89:24 (54:bf:64:a6:89:24)
Destination: 54:bf:64:a6:89:24 (54:bf:64:a6:89:24)
<[Destination (resolved): 54:bf:64:a6:89:24]>
Address: 54:bf:64:a6:89:24 (54:bf:64:a6:89:24)
<[Address (resolved): 54:bf:64:a6:89:24]>
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: Cisco_c9:10:80 (1c:df:0f:c9:10:80)
<[Source (resolved): Cisco_c9:10:80]>
Address: Cisco_c9:10:80 (1c:df:0f:c9:10:80)
<[Address (resolved): Cisco_c9:10:80]>
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: Unknown (0x8988)
Data (68 bytes)
Data: fea691a6d34908004500003cbaa00000f7019983a1874141...
[Length: 68]

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.