Catalyst 9000 Series 스위치에서 BGP EVPN Protected Overlay Segmentation 구현

목차

소개

이 문서에서는 Catalyst 9000 Series 스위치에서 BGP EVPN VXLAN Protected Overlay Segmentation을 구현하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- BGP EVPN VxLAN 개념
- BGP EVPN 유니캐스트 문제 해결
- BGP EVPN VxLAN 라우팅 정책

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.12.1 이상 버전

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.

배경 정보

고급 기능 설명

보호 세그먼트 기능은 포트가 동일한 VLAN 및 스위치에 있더라도 서로 트래픽을 전달하는 것을 방지하는 보안 조치입니다

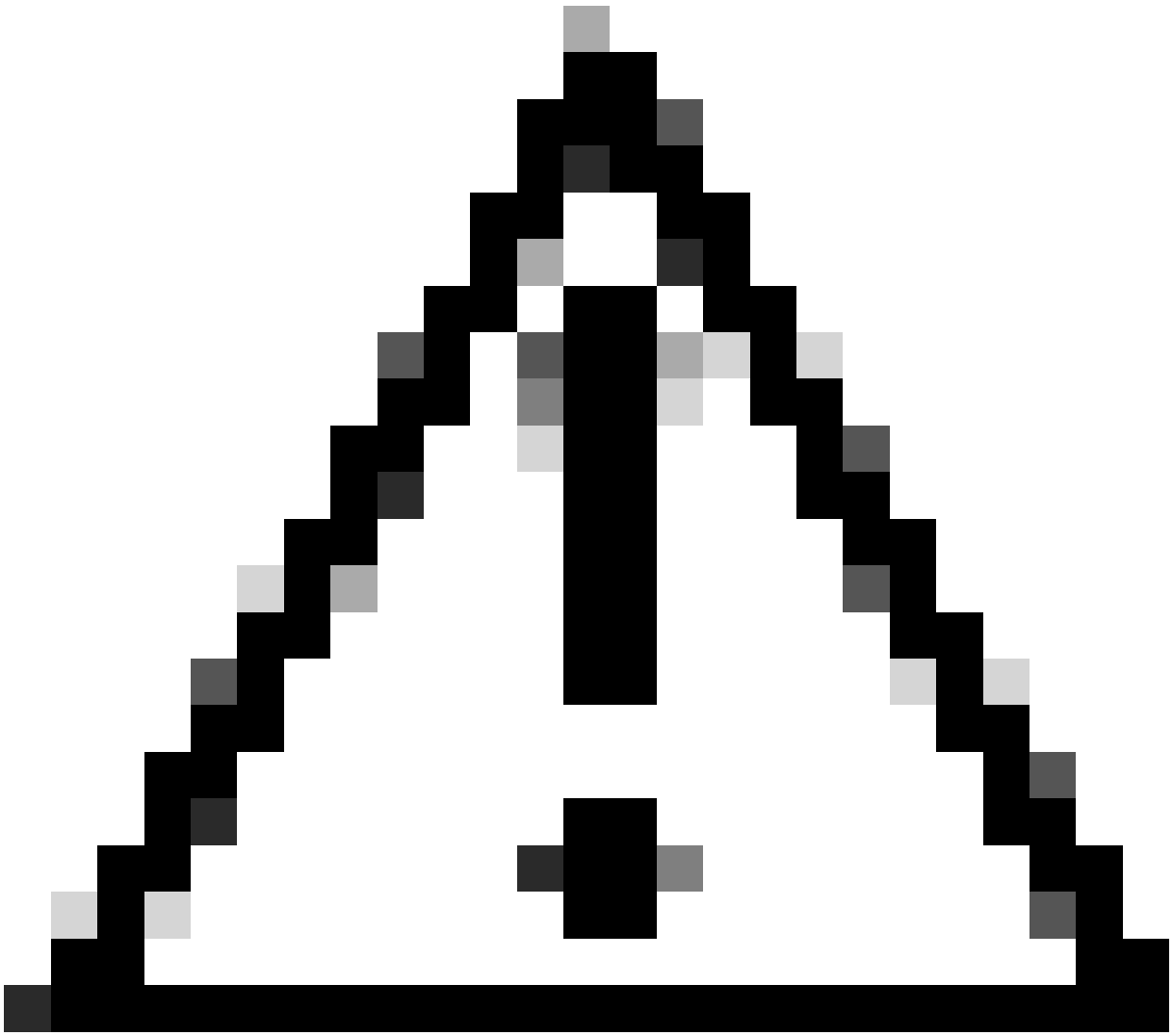
- 이 기능은 'switchport protected' 또는 private Vlan과 유사하지만 EVPN 패브릭의 경우
- 이 설계에서는 모든 트래픽을 CGW로 강제 전송합니다. 여기서 최종 목적지로 전송되기 전에

방화벽에 의해 검사를 받을 수 있습니다.
- 트래픽 흐름은 중앙 집중식 보안 어플라이언스를 사용하여 제어되고 확실하며 검사하기 쉽습니다.

문서 세부 정보

이 문서는 2부 또는 3부의 상호 관련 문서입니다.

- 문서 1: Catalyst 9000 Series 스위치에서 BGP EVPN 라우팅 정책 구현은 오버레이에서 BGP BUM 트래픽을 제어하는 방법을 다루며, 먼저 구성해야 합니다
- 문서 2: 이 문서. 문서 1의 오버레이 설계 및 정책을 기반으로 하는 이 문서에서는 'protected' 키워드의 구현에 대해 설명합니다
- 문서 3:Catalyst 9000 Series Switch에서 BGP EVPN DHCP Layer 2 릴레이 구현에서 L2 전용 VTEP에서 DHCP 릴레이가 작동하는 방식을 다룹니다



주의: 보호된 세그먼트 구성을 구현하기 전에 문서 1의 구성을 구현해야 합니다.

보호된 세그먼트 유형

완전히 고립되어

- 남북 통신만 허용
- 게이트웨이는 'default-gateway advertise' CLI를 사용하여 패브릭에 광고됩니다

대부분 고립

- North to South 통신 허용(이 활용 사례에서는 방화벽 트래픽 정책에 따라 East/West 트래픽 흐름이 허용됨)
- East-to-West 통신 허용(방화벽 트래픽 정책 기반)
- 게이트웨이는 패브릭의 외부에 있으며 'default-gateway advertise' CLI를 사용하여 SVI를 광고하지 않습니다

스위치 동작

- 호스트가 동일한 스위치에 연결되더라도 서로 직접 통신할 수 없습니다(호스트가 동일한 VRF/Vlan/세그먼트에 있는 경우 ARP 요청이 동일한 스위치의 다른 포트로 전송되지 않음).
- L2 VTEP 간 BUM 트래픽이 없음(라우팅 정책 컨피그레이션을 사용하여 필터링된 IMET 접두사)
- 호스트의 모든 패킷은 보더 리프로 릴레이되어 전달됩니다. (이는 호스트 1이 동일한 leaf에서 호스트 2와 통신한다는 것을 의미하며, 트래픽은 CGW에 고정됩니다.)

경로 유형 2 처리

- 액세스 리프는 E-Tree Extended Community 및 리프 플래그가 설정된 로컬 RT2를 광고합니다.
- 액세스 리프는 데이터 평면에 E-Tree Extended Community 및 Leaf 플래그가 설정된 상태로 수신된 원격 RT2를 설치하지 않습니다.
- Access Leaf는 데이터 평면에 서로 다른 RT2를 설치하지 않습니다.
- 액세스 리프 및 CGW(Border Leaf)는 데이터 평면에 서로 RT2를 설치합니다.
- 액세스 리프 또는 경계 리프에 대한 컨피그레이션 변경이 필요하지 않습니다.

설계 요약

- 브로드캐스트(BUM)의 경우 ARP와 같은 브로드캐스트 트래픽을 GCW로 강제 전송하기 위해 RT3 토폴로지는 허브 및 스포크입니다.
- 호스트 이동성을 고려하기 위해 RT2는 BGP 제어 평면에서 풀 메시입니다(호스트가 한 VTEP에서 다른 VTEP로 이동하면 RT2에서 시퀀스 번호가 증가함).
- 데이터 플레인에서는 MAC 주소를 선택적으로 설치합니다.
    - Leaf는 DEF GW 특성이 포함된 로컬 MAC 및 RT2만 설치합니다
    - CGW에는 보호된 KW가 없으며 모든 로컬 MAC 및 원격 RT2를 데이터 평면에 설치합니다.

용어

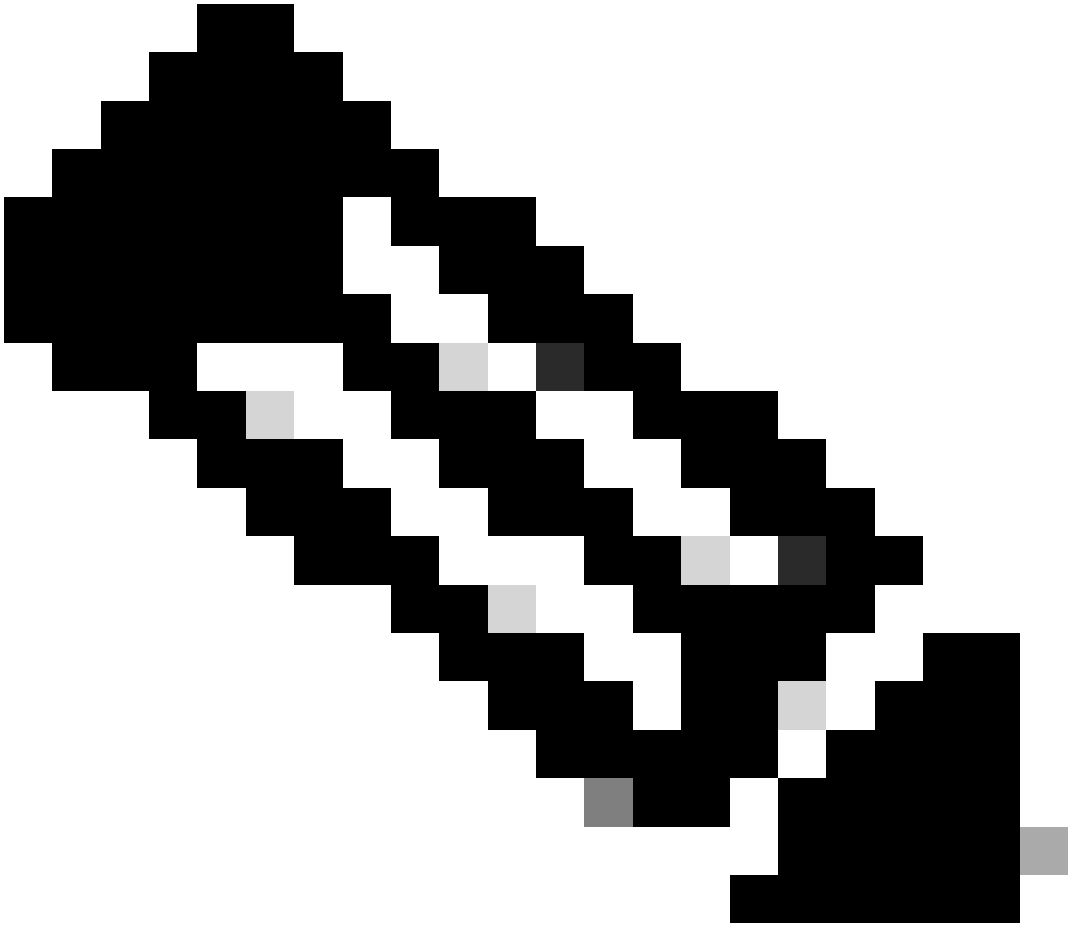
VRF	가상 라우팅 전달	다른 VRF 및 전역 IPv4/IPv6 라우팅 도메인과 구분되는 레이어 3 라우팅 도메인을 정의합니다.
AF	주소군	어떤 유형 접두사 및 라우팅 정보 BGP가 처리되는지 정의합니다.
AS	자동 시스템	단일 엔터티 또는 조직에서 모두 관리, 제어 및 감독하는 네트워크 또는 네트워크 컬렉션에 속하는 인터넷 라우팅 가능 IP 접두사 집합입니다
EVPN	이더넷 가상 사설망	BGP가 레이어 2 MAC 및 레이어 3 IP 정보를 전송할 수 있도록 하는 확장은 EVPN이며, VXLAN 오버레이 네트워크와 관련된 연결 정보를 배포할 프로토콜로 MP-BGP(Multi-Protocol Border Gateway Protocol)를 사용합니다.
VXLAN	가상 확장 LAN(Local Area Network)	VXLAN은 VLAN과 STP의 내재적 한계를 극복하기 위해 설계되었습니다. 이는 VLAN과 동일한 이더넷 레이어 2 네트워크 서비스를 제공하되 더 높은 유연성을 제공하는 IETF 표준[RFC 7348]입니다. 기능적으로 레이어 3 언더레이 네트워크에서 가상 오버레이로 실행되는 MAC-in-UDP 캡슐화 프로토콜입니다.
CGW	중앙 집중식 게이트웨이	게이트웨이 SVI가 각 leaf에 없는 EVPN 구현 대신 모든 라우팅은 비대칭 IRB(Integrated Routing and Bridging)를 사용하여 특정 리프에 의해 수행됩니다
데프 GW	기본 게이트웨이	'l2vpn evpn' 컨피그레이션 섹션 아래에서 "default-gateway advertise enable" 명령을 통해 MAC/IP 접두사에 추가된 BGP 확장 커뮤니티 특성입니다.
IMET(RT3)	포괄적 멀티캐스트 이더넷 태그(경로)	BGP type-3 경로라고도 합니다. 이 경로 유형은 VTEP 간에 BUM(브로드캐스트/알 수 없는 유니캐스트/멀티캐스트) 트래픽을 전달하는 데 EVPN에서 사용됩니다.
RT2	경로 유형 2	호스트 MAC 또는 게이트웨이 MAC-IP를 나타내는 BGP MAC 또는 MAC/IP 접두사
EVPN 관리자	EVPN 관리자	기타 다양한 구성 요소를 위한 중앙 관리 구성 요소(예: SISF에서 학습하고 L2RIB에 신호 전달)

SISF	스위치 통합 보안 기능	EVPN에서 Leaf에 어떤 로컬 호스트가 있는지 학습하는 데 사용되는 비종속적 호스트 추적 테이블
L2RIB	레이어 2 라우팅 정보 베이스	BGP, EVPN Mgr, L2FIB 간의 상호 작용을 관리하는 중간 구성 요소
연방	포워딩 엔진 드라이버	ASIC(하드웨어) 레이어 프로그래밍
매트	Mac 주소 테이블 관리자	IOS MATM: 로컬 주소만 설치하고 FED MATM: 컨트롤 플레인에서 학습한 로컬 및 원격 주소를 설치하고 하드웨어 포워딩 플레인의 일부인 하드웨어 테이블

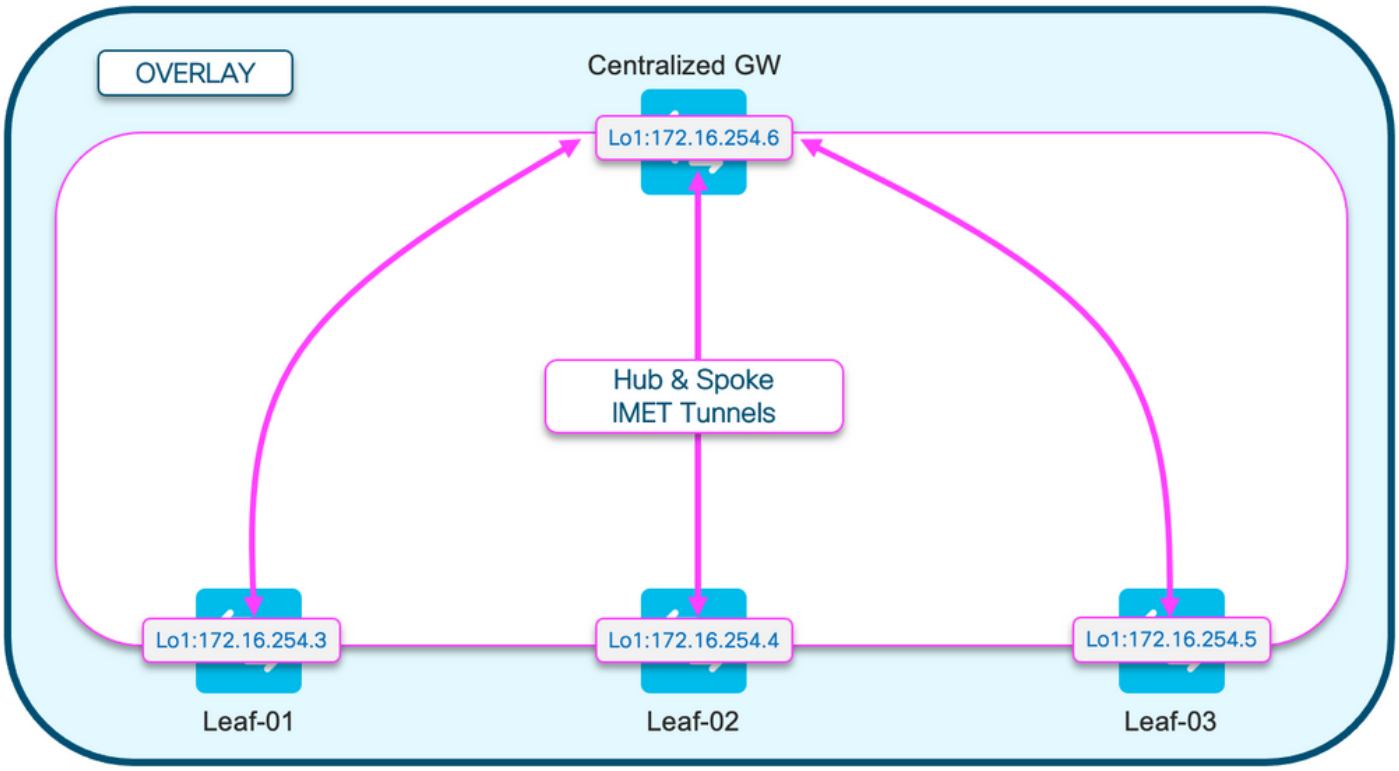
플로우 다이어그램

RT2(Route-Type 2) 다이어그램

이 다이어그램은 유형 2 MAC/MAC-IP 호스트 접두사의 풀 메시 설계를 보여줍니다.

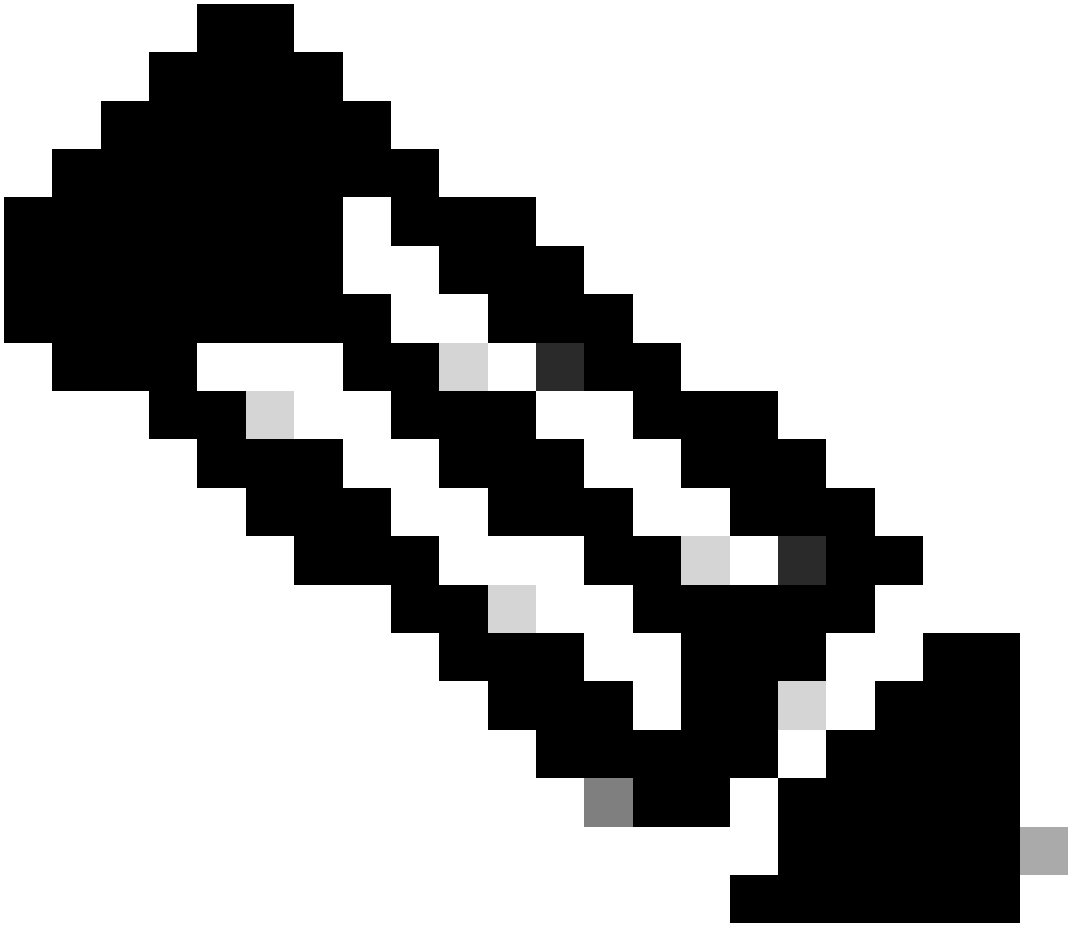


참고: 모빌리티 및 로밍을 지원하려면 풀 메시(full mesh)가 필요합니다.

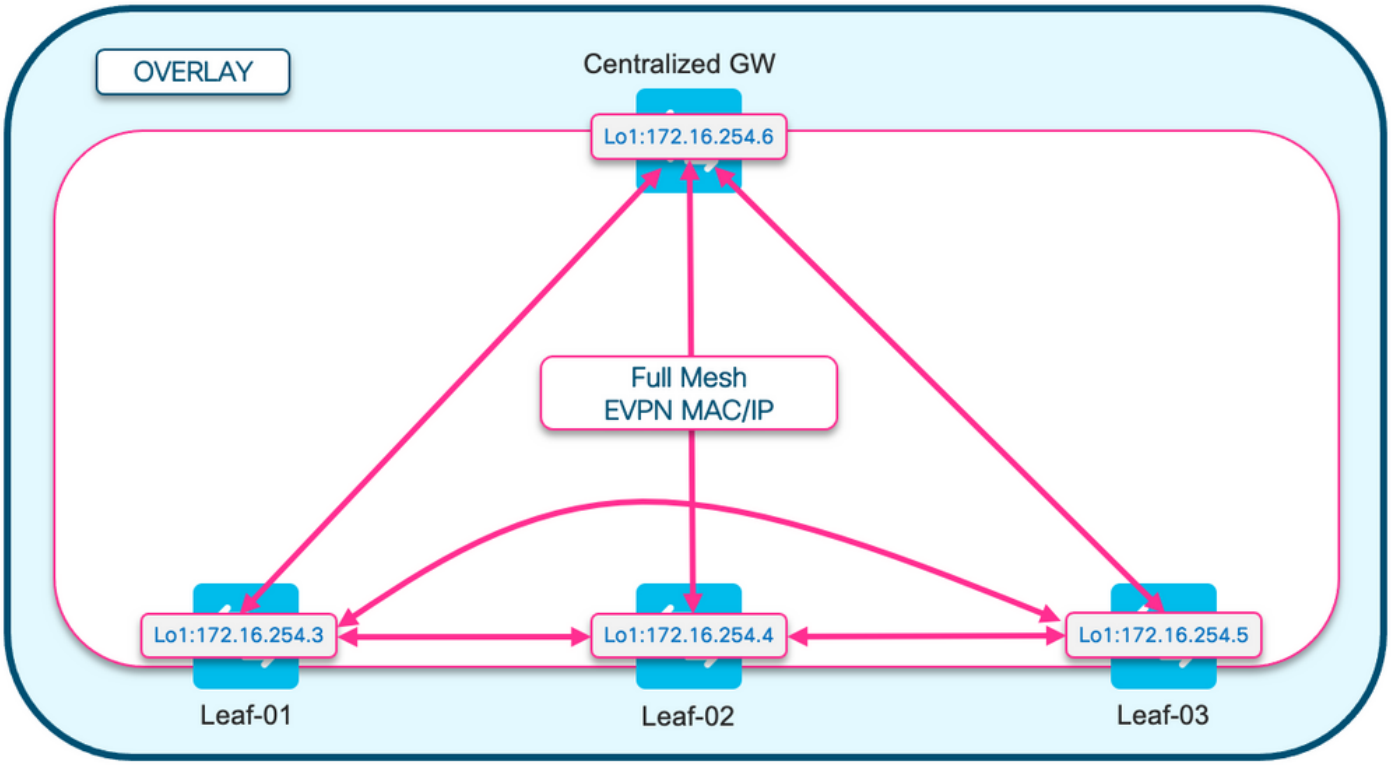


RT3(Route-Type 3) 다이어그램

이 다이어그램은 브로드캐스트 IMET(RT3) 터널의 허브 및 스포크 설계를 보여줍니다

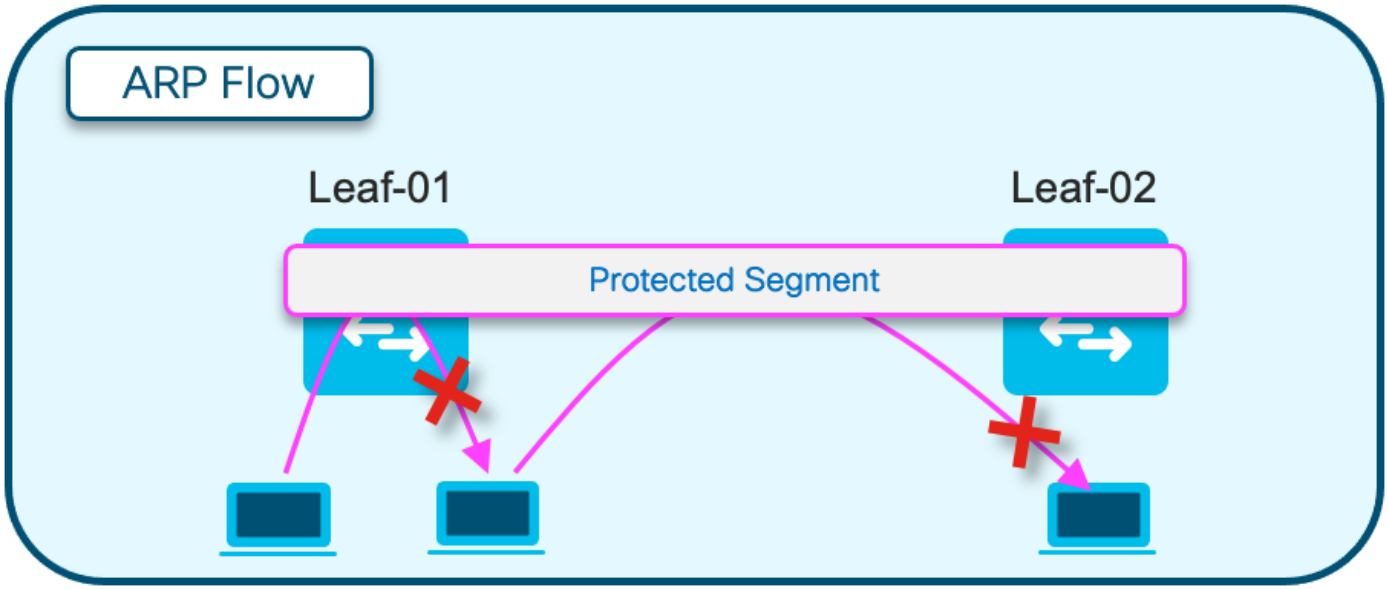


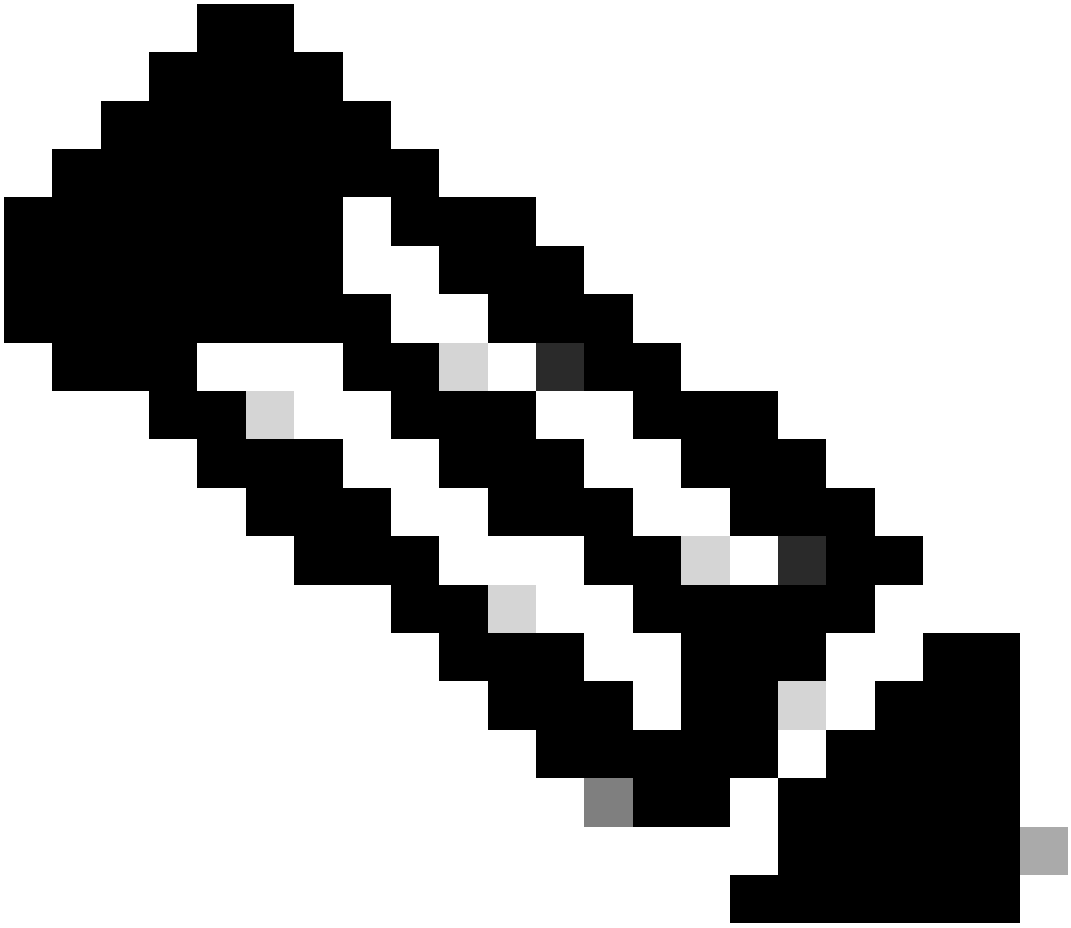
참고: 동일한 세그먼트의 leaf가 서로 직접 브로드캐스트를 보내지 않도록 하려면 허브 및 스포크 브로드캐스트가 필요합니다.



ARP(Address Resolution) 다이어그램

이 다이어그램은 ARP가 동일한 EPVN 세그먼트의 어떤 호스트에도 도달할 수 없음을 보여줍니다. 다른 호스트에 대한 ARP를 호스트하면 CGW만 이 ARP를 얻어 회신합니다



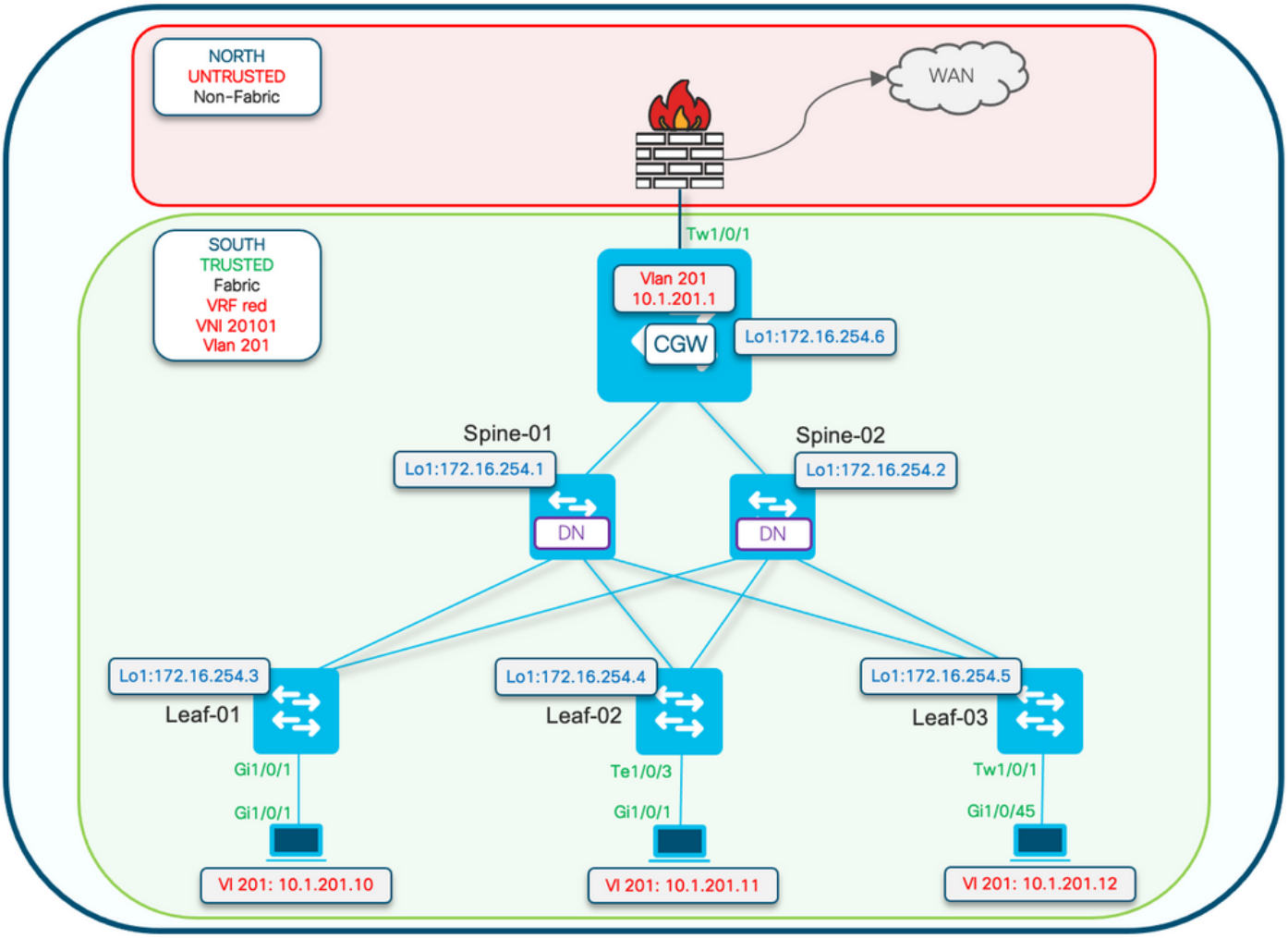


참고: 이 ARP 동작 변경은 'protected' 키워드를 사용하여 인스턴스화됩니다.

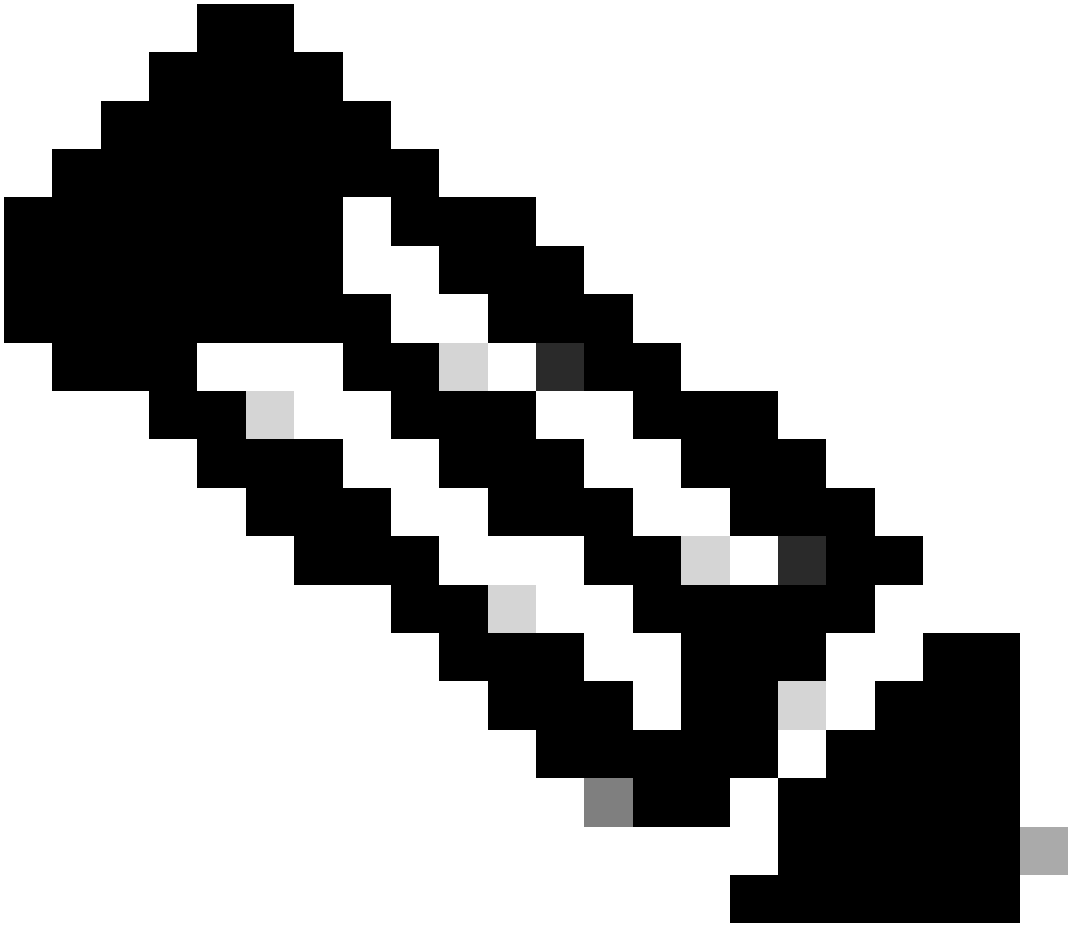
예: 멤버 evpn-instance 202 vni 20201 protected

구성(완전히 격리됨)

네트워크 다이어그램



Protected configuration 키워드는 Leaf 스위치에 적용됩니다. CGW는 프로미스큐어스 (promiscuous) 디바이스이며 모든 mac 주소를 설치합니다.



참고: IMET 접두사의 가져오기/내보내기를 제어하는 라우팅 정책 커뮤니티 목록 및 경로 맵 컨피그레이션은 Implement BGP EVPN Routing Policy on Catalyst 9000 Series Switches에 나와 있습니다. 이 문서에는 보호되는 세그먼트 차이만 표시됩니다.

Leaf-01(기본 EVPN 구성)

<#root>

```
Leaf-01#

show run | sec l2vpn
l2vpn evpn

 replication-type static

 flooding-suppression address-resolution disable  <-- Disables ARP caching so ARP is always sent up to t

 router-id Loopback1
l2vpn evpn

instance 201
```

```
 vlan-based
 encapsulation vxlan

replication-type ingress                          <-- Sets segment to use Unicast replication of BUM traff

 multicast advertise enable
```

<#root>

```
Leaf01#

show run | sec vlan config

vlan configuration 201
 member evpn-instance 201 vni 20101

protected  <-- protected keyword added
```

CGW(기본 구성)

<#root>

```
CGW#

show running-config | beg l2vpn evpn instance 201

l2vpn evpn instance 201 vlan-based
 encapsulation vxlan
 replication-type ingress

 default-gateway advertise enable    <-- adds the BGP attribute EVPN DEF GW:0:0 to the MAC/IP prefix

 multicast advertise enable
```

<#root>

```
CGW#

show running-config | sec vlan config

vlan configuration 201
 member evpn-instance 201 vni 20101
```

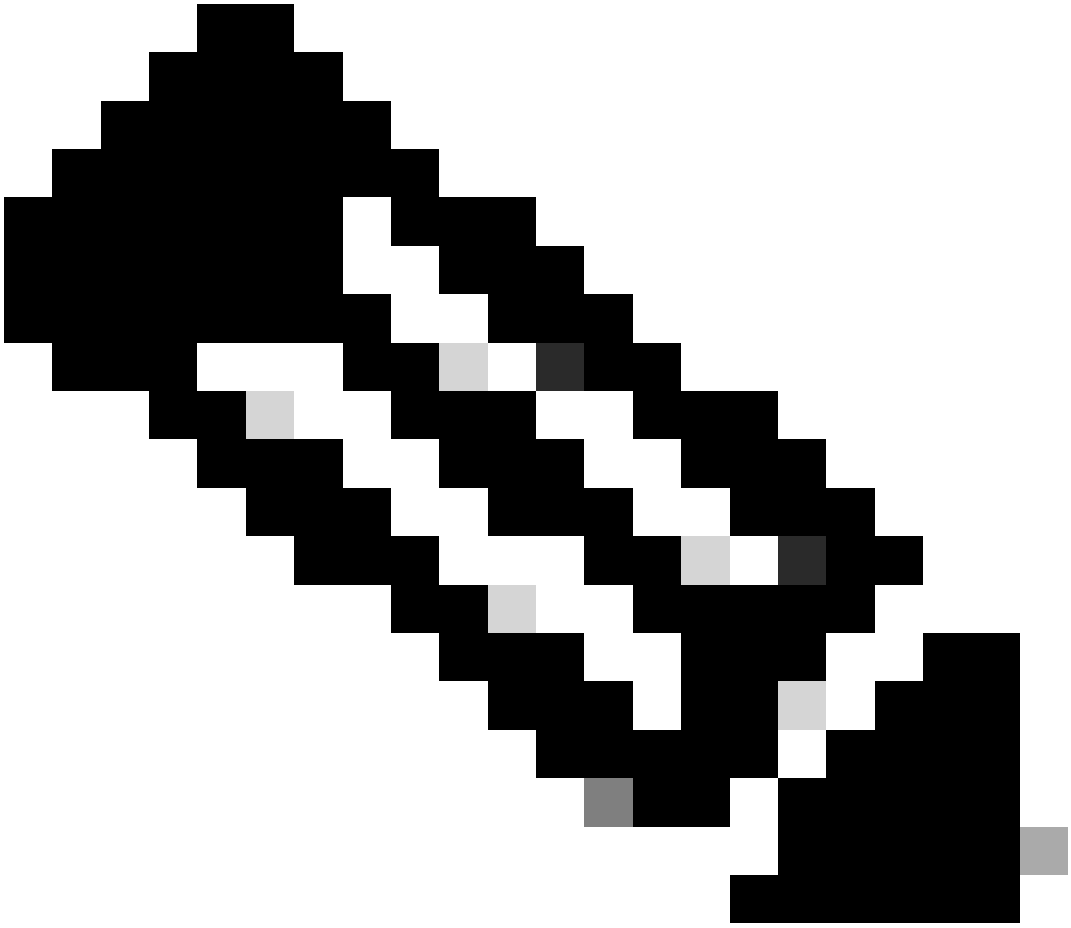
<#root>

```
CGW#

show run int nve 1

Building configuration...

Current configuration : 313 bytes
!
```

```
interface nve1
 no ip address
 source-interface Loopback1
 host-reachability protocol bgp
 member vni 20101 ingress-replication local-routing  <-- 'ingress-replication' (Unicast all BUM traffic)
```

<#root>

```
CGW#
show run interface vlan 201

Building configuration...

Current configuration : 231 bytes
!
interface Vlan201

mac-address 0000.beef.cafe          <-- MAC is static in this example for viewing simplicity. This is no
 vrf forwarding red                  <-- SVI is in VRF red
 ip address 10.1.201.1 255.255.255.0
 no ip redirects
 ip local-proxy-arp                 <-- Sets CGW to Proxy reply even for local subnet ARP requests
 ip pim sparse-mode
 ip route-cache same-interface      <-- This is auto added when local-proxy-arp is configured. However,
 ip igmp version 3
 no autostate
```



참고: CGW에는 BGP 정책이 적용되지 않습니다. CGW는 모든 접두사 유형(RT2, RT5 / RT3)을 수신하고 전송할 수 있습니다.

확인(완전히 격리됨)

EVI 세부 정보

<#root>

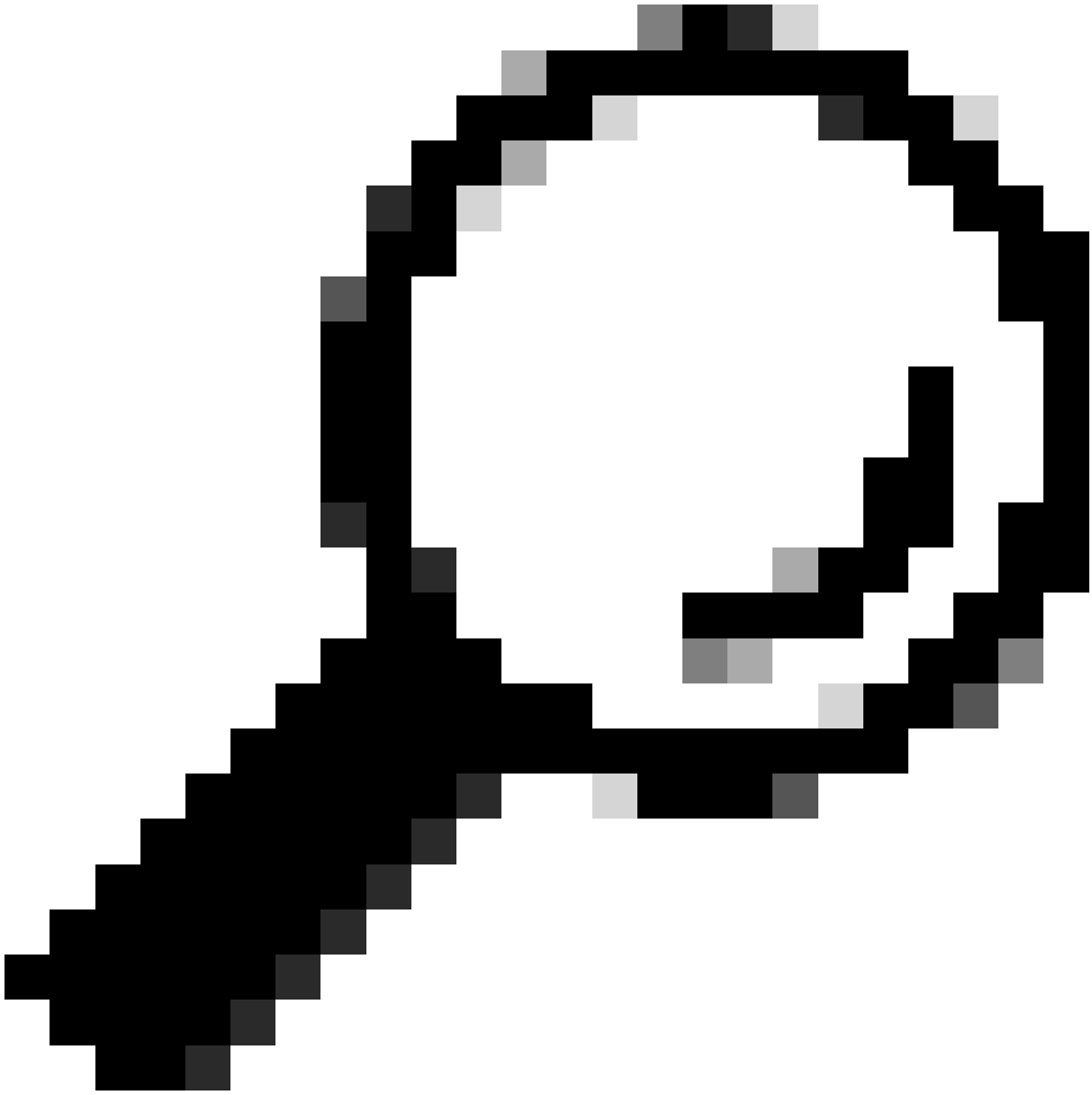
```
Leaf01#

sh l2vpn evpn evi 201 detail

EVPN instance:       201 (VLAN Based)
  RD:                172.16.254.3:201 (auto)
  Import-RTs:        65001:201
  Export-RTs:        65001:201
  Per-EVI Label:     none
  State:             Established
```

```
  Replication Type:  Ingress
  Encapsulation:     vxlan
  IP Local Learn:    Enabled (global)
  Adv. Def. Gateway: Disabled (global)
  Re-originate RT5:  Disabled
  Adv. Multicast:    Enabled
  AR Flood Suppress: Disabled (global)


Vlan:              201
    Protected:       True (local access p2p blocked)  <-- Vlan 201 is in protected mode

<...snip...>
```

로컬 RT2 생성(로컬 호스트에서 RT2)

로컬 호스트 학습에서 RT2 생성에 이르는 구성 요소 종속성 체인을 확인합니다.

- SISF(Leaf에 SVI가 없지만 SISF는 호스트에서 ARP 프레임을 통해 호스트 정보를 계속 가져옵니다.)
- EVPN 관리자
- L2RIB
- BGP

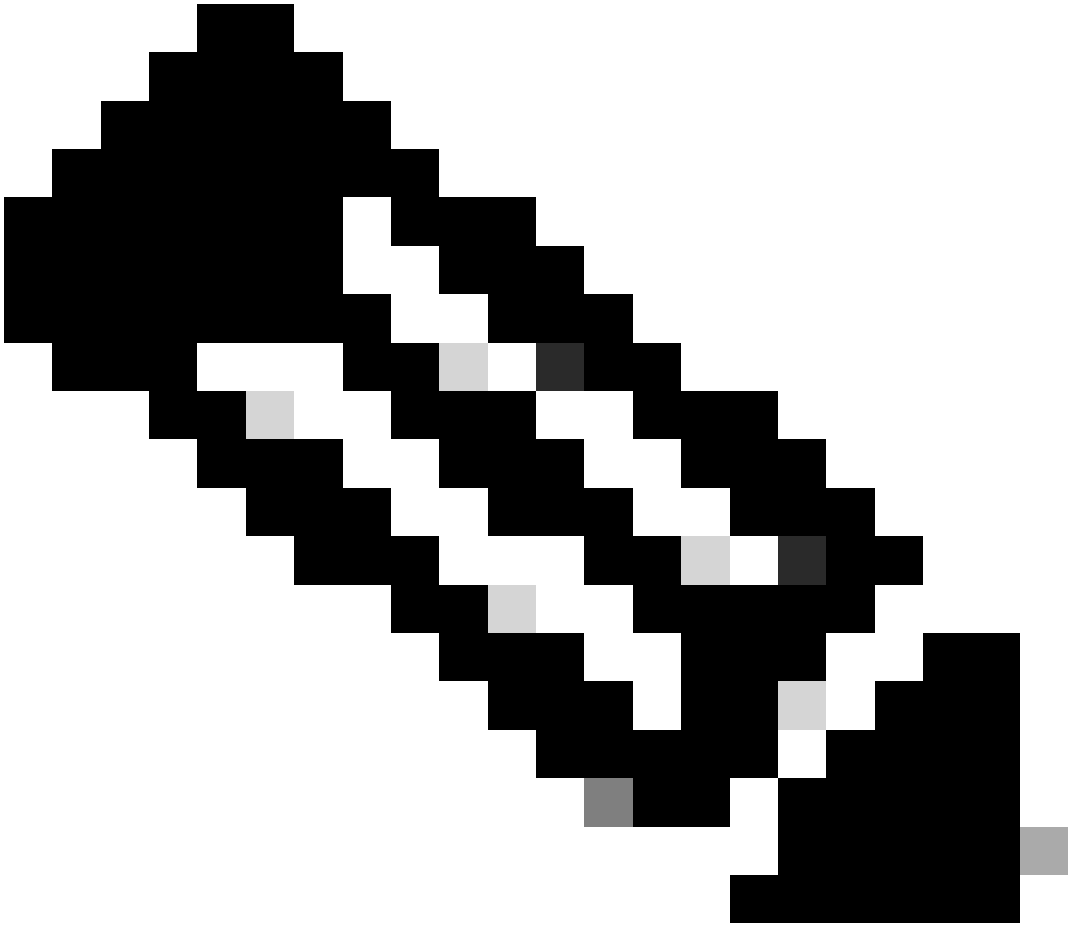


팁: 이전 구성 요소가 전체 종속성 체인 분리를 제대로 프로그래밍하지 않은 경우(예: SISF에 항목이 없으면 BGP에서 RT2를 생성할 수 없음)

SISF

SISF가 DB에서 호스트를 학습했는지 확인(DHCP 또는 ARP에서 학습한 호스트 정보)

- SISF는 IOS-MATM 학습에서 MAC 항목을 학습한 다음 EVPN Mgr로 전송합니다("evpn-sisf-policy" 정책을 통해 MAC에 연결할 수 있어야 함).
- SISF는 로컬 VTEP에서 IP/MAC 바인딩을 수집하고 EVPN 관리자를 사용하여 정보가 BGP를 통해 다른 leaf로 /32 경로로 프로그래밍되도록 합니다.



참고: 이 시나리오에서는 호스트에 고정 IP가 있으므로 SISF는 ARP를 사용하여 호스트 세부 정보를 수집합니다. Mostly Isolated(대부분 격리) 섹션에는 DHCP 및 DHCP 스누핑이 표시됩니다.

<#root>

```
Leaf01#

show device-tracking database vlanid 201

vlanDB has 1 entries for vlan 201, 1 dynamic
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DHC
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


    Network Layer Address                  Link Layer Address     Interface  vlan       prlvl      age

ARP
```

```
 10.1.201.10

0006.f601.cd43


Gi1/0/1

    201        0005       3mn        REACHABLE  86 s

<-- Gleaned from local host ARP Request
```

EVPN 관리자

EVPN Mgr이 로컬 MAC를 학습하여 L2RIB에 설치합니다. EVPN Mgr도 L2RIB에서 원격 MAC를 학습하지만 항목은 MAC 모빌리티 처리에만 사용됩니다

EVPN Mgr이 SISF 항목으로 업데이트되었는지 확인합니다.

```
<#root>

Leaf01#

show l2vpn evpn mac evi 201

MAC Address    EVI   VLAN  ESI                       Ether Tag  Next Hop(s)
-------------- ----- ----- ------------------------- ---------- ---------------

0006.f601.cd43 201   201

0000.0000.0000.0000.0000 0

         Gi1/0/1:201    <-- MAC in VLan 201 local interface Gi1/0/1:service instance 201

<...snip...>
```

L2RIB

- L2RIB는 EVPN Mgr에서 로컬 MAC를 학습하여 BGP 및 L2FIB에 전송합니다.
- L2RIB는 EVPN Mgr 및 L2FIB를 업데이트하기 위해 BGP에서 원격 MAC를 학습하는 역할도 담당합니다.
- L2RIB를 사용하려면 다른 구성 요소를 올바르게 업데이트하기 위해 로컬 및 원격 둘 다 필요합니다.
- L2RIB 구성 요소는 업데이트해야 하는 방향/구성 요소에 따라 로컬 및 원격 MAC 학습 사이에 위치합니다.

EVPN Mgr의 로컬 MAC으로 L2RIB가 업데이트되었는지 확인합니다.

```
<#root>

Leaf01#
```

show l2route evpn mac topology 201 <-- View the overall topology for this segment

EVI ETag

Prod

Mac Address Next Hop(s) Seq Number

----- ---------- ----- -------------- ---------- ----------

201 0

BGP

0000.beef.cafe V:20101 172.16.254.6 0

<-- produced by BGP who updated L2RIB (remote learn)

201 0

L2VPN

0006.f601.cd43 Gi1/0/1:201 0

<-- produced by EVPN Mgr who updated L2RIB (local learn)

Leaf01#

show l2route evpn mac mac-address 0006.f601.cd43 detail

EVPN Instance: 201

Ethernet Tag: 0

Producer Name: L2VPN <-- Produced by local

MAC Address: 0006.f601.cd43 <-- Host MAC Address

Num of MAC IP Route(s): 1
Sequence Number: 0
ESI: 0000.0000.0000.0000.0000
Flags: B()

Next Hop(s): Gi1/0/1:201 (E-LEAF) <-- Port:Instance and info about the Role (Leaf)

BGP

BGP가 L2RIB에 의해 업데이트되었는지 확인합니다.

<#root>

Leaf01#

show bgp l2vpn evpn route-type 2 0 0006.f601.cd43 *

BGP routing table entry for [2][172.16.254.3:201][0][48][0006F601CD43][0][*]/20, version 268232
Paths: (1 available, best #1,

table evi_201

)

<-- In the totally isolated evi context

```
  Advertised to update-groups:
     2
  Refresh Epoch 1
  Local


 0.0.0.0 (via default) from 0.0.0.0

 (172.16.255.3)
```

<-- from 0.0.0.0 indicates local

```
      Origin incomplete, localpref 100, weight 32768, valid, sourced,
```

local

```
, best
```

<-- also indicates local

```
      EVPN ESI: 00000000000000000000, Label1 20101
      Extended Community: RT:65001:201 ENCAP:8
```

EVPN E-Tree:flag:1

```
,label:0
```

<-- EVPN e-Tree attribute with Leaf flag = 1 (added to indicate this is a host address)

```
      Local irb vxlan vtep:
        vrf:not found, l3-vni:0
        local router mac:0000.0000.0000
        core-irb interface:(not found)


 vtep-ip:172.16.254.3                                                    <-- Local VTEP Loopback

      rx pathid: 0, tx pathid: 0x0
      Updated on Sep 14 2023 20:16:17 UTC
```

원격 RT2 학습(기본 게이트웨이 RT2)

BGP

BGP가 CGW RT2 접두사를 학습했는지 확인합니다.

<#root>

```
Leaf01#
```

show bgp l2vpn evpn route-type 2 0 0000.beef.cafe 10.1.201.1

```
BGP routing table entry for [2][172.16.254.3:201][0][48][0000BEEFCAFE][32][10.1.201.1]/24, version 1141
Paths: (1 available, best #1,
```

table evi_201

```
)
```

<-- EVI context is 201

```
  Flag: 0x100
  Not advertised to any peer
  Refresh Epoch 2
  Local, imported path from [2][172.16.254.6:201][0][48][0000BEEFCAFE][32][10.1.201.1]/24 (global)
    172.16.254.6 (metric 3) (via default) from 172.16.255.1 (172.16.255.1)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      EVPN ESI: 00000000000000000000,

Label1 20101                <-- Correct segment identifier

      Extended Community: RT:65001:201 ENCAP:8

EVPN DEF GW:0:0    <-- Default gateway attribute is added via the 'default gateway advertise CLI'

      Originator: 172.16.255.6, Cluster list: 172.16.255.1
      rx pathid: 0, tx pathid: 0x0
      Updated on Sep 1 2023 15:27:45 UTC
```

L2RIB

BGP 업데이트 L2RIB 확인

- L2RIB는 EVPN Mgr에서 로컬 MAC를 학습하여 BGP 및 L2FIB에 전송합니다. L2RIB는 EVPN Mgr 및 L2FIB를 업데이트하기 위해 BGP에서 원격 MAC를 학습하는 역할도 담당합니다.
- L2RIB를 사용하려면 다른 구성 요소를 올바르게 업데이트하기 위해 로컬 및 원격 둘 다 필요합니다.
- L2RIB 구성 요소는 업데이트해야 할 방향과 구성 요소에 따라 로컬 및 원격 MAC 학습 사이에 위치합니다.

<#root>

```
Leaf01#

show l2route evpn default-gateway host-ip 10.1.201.1

  EVI       ETag  Prod    Mac Address                                Host IP
----- ---------- ----- -------------- ---------------------------------------- -------------------------


201

          0

BGP


0000.beef.cafe


10.1.201.1

                              V:20101 172.16.254.6

<-- L2RIB has the MAC-IP of the Gateway programmed
```

L2FIB

L2FIB에서 확인

- 하드웨어에서 프로그래밍하기 위해 MAC으로 FED를 업데이트하는 구성 요소입니다.
- L2FIB가 FED-MATM에 설치한 원격 MAC 항목은 IOS-MATM에 대해 펀팅되지 않습니다. (IOS-MATM은 로컬 MAC만 표시하는 반면 FED-MATM은 로컬 및 원격 MAC을 모두 표시합니다.)
- L2FIB 출력에는 원격 MAC만 표시됩니다(로컬 MAC 프로그래밍은 담당하지 않음).

<#root>

```
Leaf01#

show l2fib bridge-domain 201 address unicast 0000.beef.cafe


MAC Address                  :

0000.beef.cafe                                        <-- CGW MAC

Reference Count              : 1
Epoch                        : 0

Producer                     : BGP                                                    <-- Learned fro

Flags                        : Static
Adjacency                    :

VXLAN_UC

  PL:2973(1) T:VXLAN_UC [MAC]20101:

172.16.254.6  <-- CGW Loopback IP

PD Adjacency                 : VXLAN_UC  PL:2973(1) T:VXLAN_UC [MAC]20101:172.16.254.6
Packets                      : 6979
Bytes                        : 0
```

연방

FED MATM에서 확인

- 'protected 키워드'로 구성된 Leaf의 하드웨어 레벨에서 CGW 기본 게이트웨이 MAC 및 로컬 호스트 MAC만 볼 수 있습니다.
- 스위치는 설치할 수 있는 원격 MAC을 확인하기 위해 DEF GW 특성의 RT2 접두사를 확인합니다.

<#root>

```
Leaf01#

show platform software fed switch active matm macTable vlan 201

VLAN   MAC
```

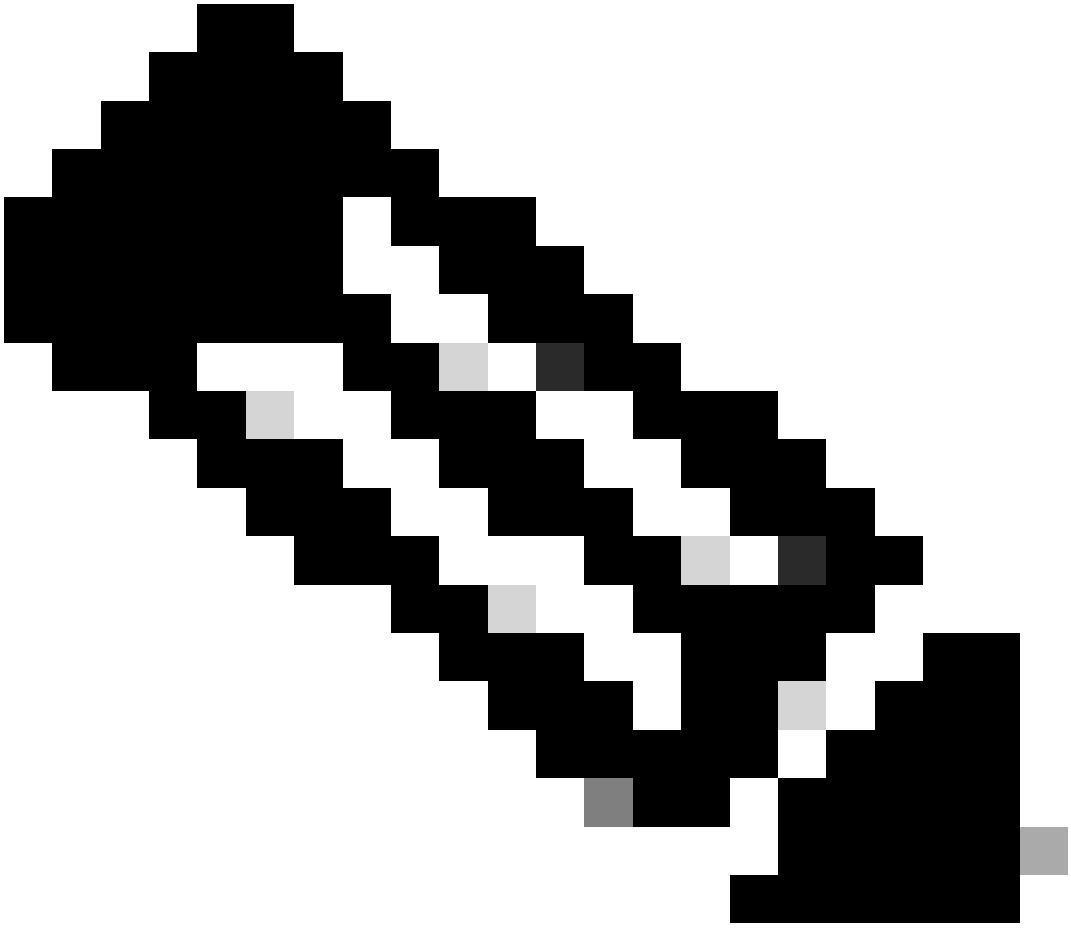
```
Type
  Seq#    EC_Bi  Flags  machandle           siHandle            riHandle            diHandle
Con
-------------------------------------------------------------------------------------------------
201    0000.beef.cafe


0x5000001
       0      0     64  0x7a199d182498      0x7a199d183578
0x71e059173e08
      0x0                          0       82
VTEP 172.16.254.6
 adj_id 9
No
<-- Only remote MAC installed in Fed is the Default Gateway (0x5000001 type) Conn = No (meaning not dire
201    0006.f601.cd01
0x1
    2458      0      0  0x7a199d1a2248      0x7a199d19eef8      0x0                 0x7a199c6f7cd8
201    0006.f601.cd43        0x1    8131      0      0  0x7a199d195a98      0x7a199d19eef8      0x0
<-- Two local MAC addresses (0x1 type) Conn = Yes (directly connected)


Total Mac number of addresses:: 5
Summary:
Total number of secure addresses:: 0
Total number of drop addresses:: 0
Total number of lisp local addresses:: 0
Total number of lisp remote addresses:: 3
*a_time=aging_time(secs)  *e_time=total_elapsed_time(secs)
Type:
MAT_DYNAMIC_ADDR           0x1
  MAT_STATIC_ADDR            0x2  MAT_CPU_ADDR               0x4  MAT_DISCARD_ADDR           0x8
MAT_ALL_VLANS             0x10  MAT_NO_FORWARD            0x20  MAT_IPMULT_ADDR           0x40  MAT_RESV
MAT_DO_NOT_AGE           0x100  MAT_SECURE_ADDR          0x200  MAT_NO_PORT              0x400  MAT_DROP
MAT_DUP_ADDR            0x1000  MAT_NULL_DESTINATION    0x2000  MAT_DOT1X_ADDR          0x4000  MAT_ROUT
MAT_WIRELESS_ADDR      0x10000  MAT_SECURE_CFG_ADDR    0x20000  MAT_OPQ_DATA_PRESENT   0x40000  MAT_WIRE
MAT_DLR_ADDR          0x100000  MAT_MRP_ADDR          0x200000  MAT_MSRP_ADDR         0x400000  MAT_LISP
MAT_LISP_REMOTE_ADDR 0x1000000
  MAT_VPLS_ADDR        0x2000000
MAT_LISP_GW_ADDR     0x4000000
<-- the addition of these values = 0x5000001
MAT_LISP_REMOTE_ADDR 0x1000000
MAT_LISP_GW_ADDR 0x4000000
MAT_DYNAMIC_ADDR 0x1
```

데이터 플레인 인접성

FED 항목을 확인한 후 마지막 단계로 재작성 인덱스(RI)를 해결할 수 있습니다

<#root>

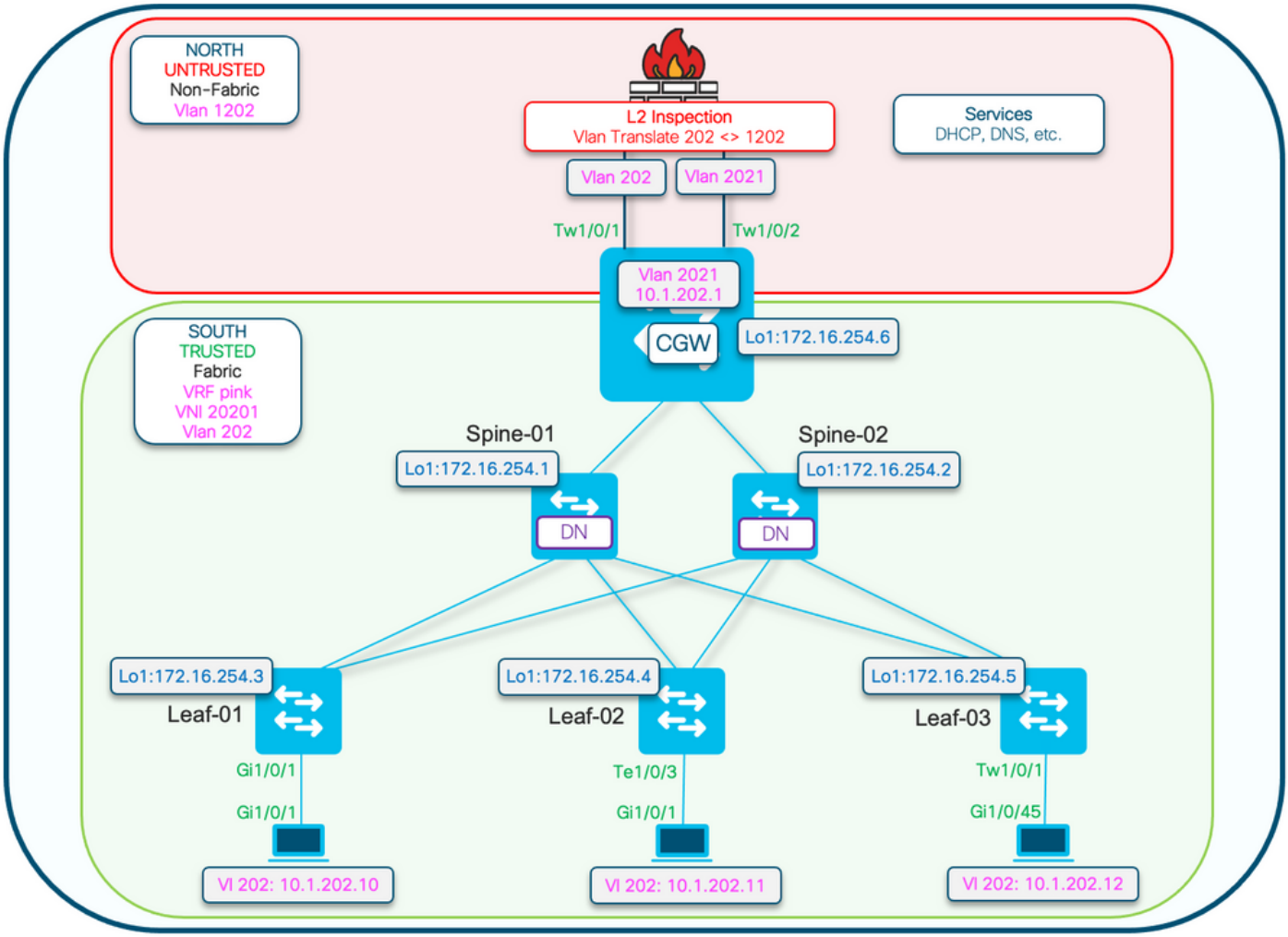
```
Leaf01#

sh platform hardware fed switch active fwd-asic abstraction print-resource-handle 0x71e059173e08 0
<-- 0x71e059173e08 is taken from previous FED command riHandle for the CGW MAC

Handle:0x71e059173e08 Res-Type:ASIC_RSC_RI Res-Switch-Num:255 Asic-Num:255 Feature-ID:AL_FID_L2_WIRELESS
priv_ri/priv_si Handle: 0x71e05917b8d8Hardware Indices/Handles: index0:0x38  mtu_index/l3u_ri_index0:0x0
Features sharing this resource:58 (1)]


Brief Resource Information (ASIC_INSTANCE# 0)
---------------------------------------
ASIC#:0 RI:56 Rewrite_type:AL_RRM_REWRITE_LVX_IPV4_L2_PAYLOAD_ENCAP_EPG(116) Mapped_rii:LVX_L3_ENCAP_L2_

 Src IP:     172.16.254.3      <-- source tunnel IP
 Dst IP:     172.16.254.6      <-- dest tunnel IP

 iVxlan dstMac:     0x9db:0x00:0x00
 iVxlan srcMac:     0x00:0x00:0x00
 IPv4 TTL:     0
 iid present:     0

 lisp iid:     20101            <-- Segment 20101

 lisp flags:     0

 dst Port:     4789             <-- VxLAN

 update only l3if:     0
 is Sgt:     0
 is TTL Prop:     0
 L3if LE:     53 (0)
 Port LE:     281 (0)
 Vlan LE:     8 (0)
```

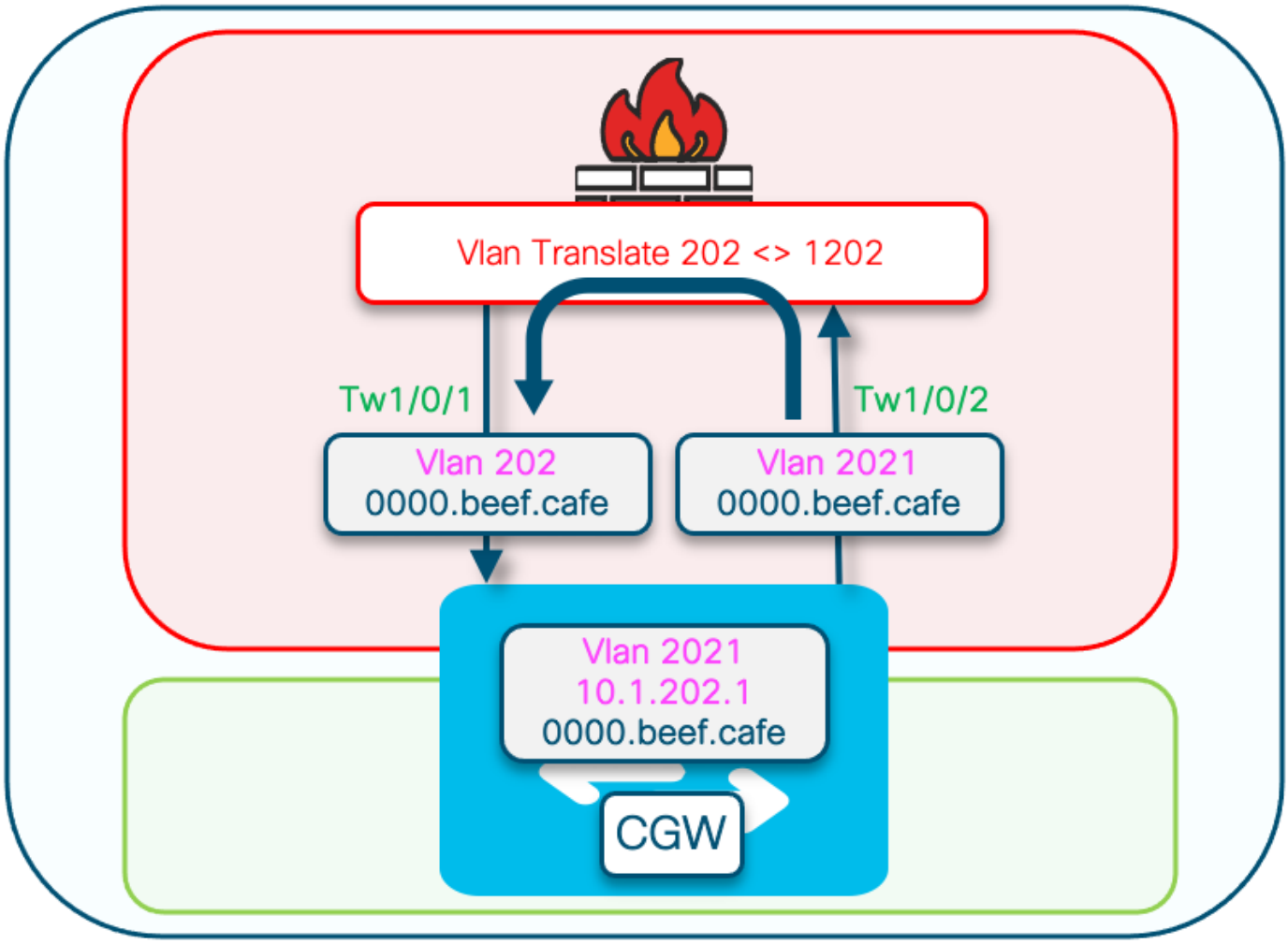


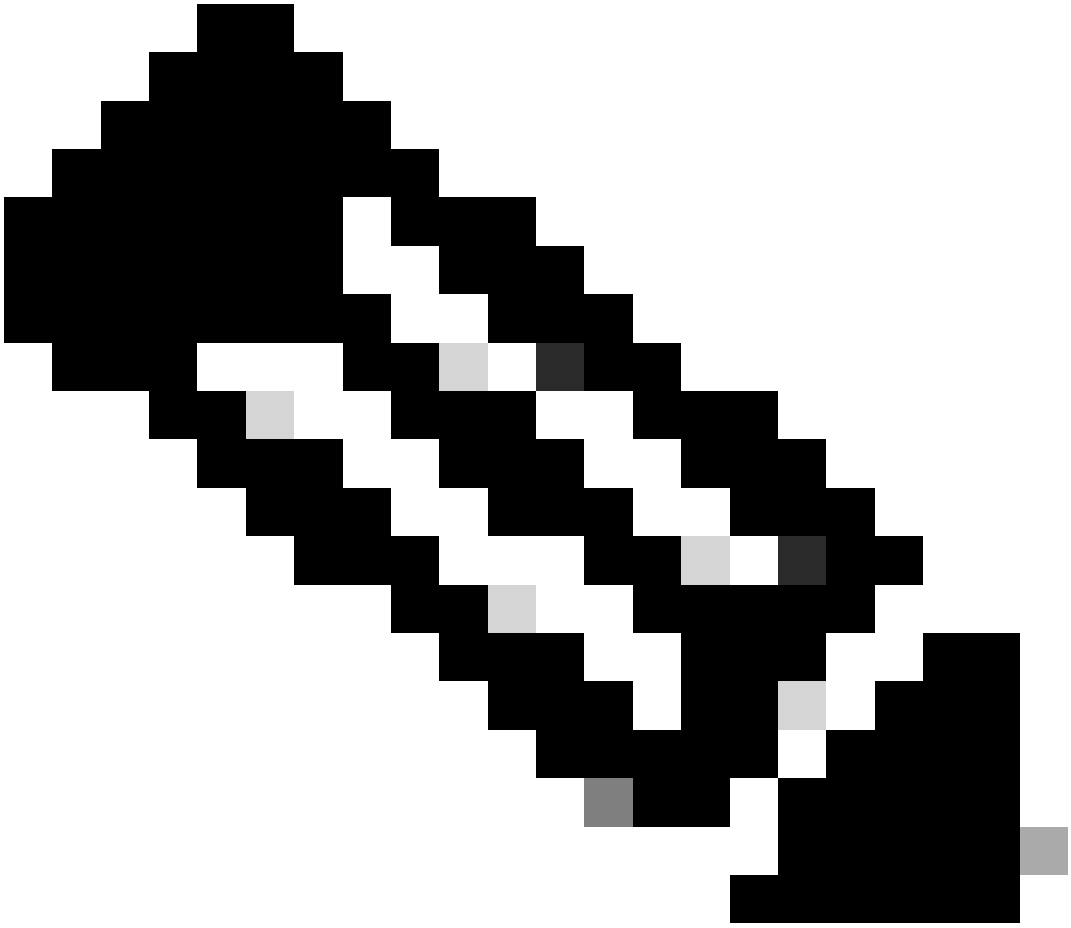
참고: 이 명령을 FED 명령과 연결하여 하나의 결과로 만드는 'show platform software fed switch active matm macTable vlan 201 detail'을 사용할 수도 있습니다

구성(부분적으로 격리)

네트워크 다이어그램


NORTH
UNTRUSTED
Non-Fabric
Vlan 1202
L2 Inspection
Vlan Translate 202 <> 1202
Services
DHCP, DNS, etc.
Vlan 202
Vlan 2021
Tw1/0/1
Tw1/0/2
Vlan 2021
10.1.202.1
CGW
Lo1:172.16.254.6
SOUTH
TRUSTED
Fabric
VRF pink
VNI 20201
Vlan 202
Spine-01
Lo1:172.16.254.1
DN
Spine-02
Lo1:172.16.254.2
DN
Lo1:172.16.254.3
Leaf-01
Lo1:172.16.254.4
Leaf-02
Lo1:172.16.254.5
Leaf-03
Gi1/0/1
Gi1/0/1
Te1/0/3
Gi1/0/1
Tw1/0/1
Gi1/0/45
Vl 202: 10.1.202.10
Vl 202: 10.1.202.11
Vl 202: 10.1.202.12


Vlan Translate 202 <> 1202
Tw1/0/1
Tw1/0/2
Vlan 202
0000.beef.cafe
Vlan 2021
0000.beef.cafe
Vlan 2021
10.1.202.1
0000.beef.cafe
CGW



참고: 이 섹션에서는 완전히 격리된 세그먼트와의 차이점만 다룹니다.

- DEF GW 특성으로 GCW 게이트웨이 MAC IP를 표시하는 라우팅 정책
- MAC 플랩을 방지하는 데 필요한 맞춤형 디바이스 추적 정책
- GW MAC IP에 대한 정적 장치 추적 바인딩

Leaf-01(기본 EVPN 구성)

<#root>

```
Leaf-01#

show run | sec l2vpn
l2vpn evpn

 replication-type static

 flooding-suppression address-resolution disable  <-- Disables ARP caching so ARP is always sent up to t

 router-id Loopback1
```

```
l2vpn evpn
instance 202
 vlan-based
 encapsulation vxlan

replication-type ingress
 multicast advertise enable
```

<#root>

```
Leaf01#
show run | sec vlan config

vlan configuration 202
 member evpn-instance 202 vni 20201
protected <-- protected keyword added
```

CGW(기본 구성)

nve에서 복제 모드 설정

<#root>

```
CGW#
show run int nve 1

Building configuration...

Current configuration : 313 bytes
!
interface nve1
 no ip address
 source-interface Loopback1
 host-reachability protocol bgp
 member vni 20201 ingress-replication local-routing <-- 'ingress-replication' (Unicast all BUM traffic)
end
```

외부 게이트웨이 SVI 구성

<#root>

```
CGW#
show run interface vlan 2021
```

```
Building configuration...

Current configuration : 231 bytes
!
interface Vlan2021

mac-address 0000.beef.cafe          <-- MAC is static in this example for viewing simplicity. This is no

 vrf forwarding pink                  <-- SVI is in VRF pink

 ip address 10.1.202.1 255.255.255.0
 no ip redirects

 ip local-proxy-arp                 <-- Sets CGW to Proxy reply even for local subnet ARP requests

 ip pim sparse-mode

 ip route-cache same-interface      <-- This is auto added when local-proxy-arp is configured. However,

 ip igmp version 3
 no autostate
end
```

청소가 비활성화된 정책 생성

<#root>

```
device-tracking policy dt-no-glean

 <-- Configure device tracking policy to prevent MAC-IP flapping

 security-level glean
 no protocol ndp
 no protocol dhcp6
 no protocol arp
 no protocol dhcp4
```

externalgatewayevi/vlans에 연결

<#root>

```
CGW#

show running-config | sec vlan config

vlan configuration 202
 member evpn-instance 202 vni 20201

 device-tracking attach-policy dt-no-glean <-- apply the new device tracking policy to the vlan configur
```

외부 게이트웨이 mac-ip용 디바이스 추적 테이블에 고정 항목 추가

<#root>

```
device-tracking binding vlan 202 10.1.202.1 interface TwentyFiveGigE1/0/1 0000.beef.cafe
```

```
<-- All static entries in device tracking table should be for external gateway mac-ip's.
 If there is any other static entry in device tracking table, match ip/ipv6 configurations in route map
```

RT2 MAC-IP 접두사를 일치시키고 기본 게이트웨이 확장 커뮤니티를 설정하기 위한 BGP 경로 맵을 만듭니다.

<#root>

```
route-map CGW_DEF_GW permit 10
```

```
match evpn route-type 2-mac-ip <-- match RT2 type MAC-IP
```

```
 set extcommunity default-gw <-- Set Default-gateway (DEF GW 0:0) extended community
```

```
route-map CGW_DEF_GW permit 20
```

BGP 경로 리플렉터 네이버에 경로 지도 적용

<#root>

```
CGW#
```

```
sh run | s r bgp
```

```
address-family l2vpn evpn
 neighbor 172.16.255.1 activate
 neighbor 172.16.255.1 send-community both
 neighbor 172.16.255.1
```

```
route-map CGW_DEF_GW out <-- Sets the DEF GW Community when it advertises MAC-IP type RT2 to the RR
```

```
 neighbor 172.16.255.2 activate
 neighbor 172.16.255.2 send-community both
 neighbor 172.16.255.2
```

```
route-map CGW_DEF_GW out <-- Sets the DEF GW Community when it advertises MAC-IP type RT2 to the RR
```

확인(부분적으로 격리)

EVI 세부 정보

<#root>

```
Leaf01#

show l2vpn evpn evi 202 detail

EVPN instance:       202 (VLAN Based)
  RD:                172.16.254.3:202 (auto)
  Import-RTs:        65001:202
  Export-RTs:        65001:202
  Per-EVI Label:     none
  State:             Established
  Replication Type:  Ingress
  Encapsulation:     vxlan
  IP Local Learn:    Enabled (global)
  Adv. Def. Gateway: Enabled (global)
  Re-originate RT5:  Disabled
  Adv. Multicast:    Enabled

  Vlan:              202
    Protected:       True (local access p2p blocked)  <-- Vlan 202 is in protected mode

<...snip...>
```

로컬 RT2 생성(로컬 호스트에서 RT2)

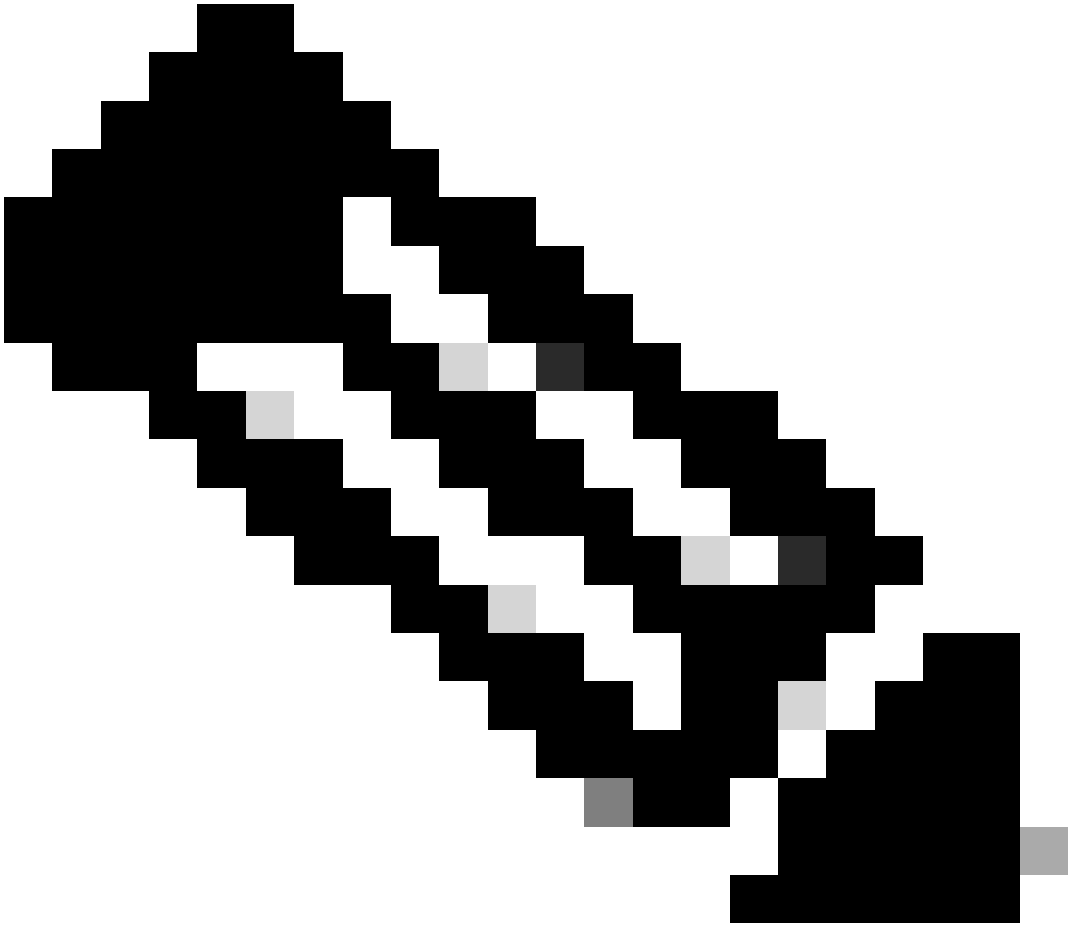
이전에 완전히 격리된 예에서 다룬 내용

원격 RT2 학습(기본 게이트웨이 RT2)

완전히 격리된 상태의 차이점 설명

CGW 기본 게이트웨이 접두사(리프)

하드웨어에 설치할 수 있도록 접두사에 적절한 속성이 있는지 확인합니다



참고: 이는 DHCP L2 릴레이가 작동하는 데 중요합니다

<#root>

Leaf01#

show bgp l2vpn evpn route-type 2 0 0000.beef.cafe 10.1.202.1

BGP routing table entry for [2][172.16.254.3:202][0][48][0000BEEFCAFE][32][10.1.202.1]/24, version 1846
Paths: (1 available, best #1,

table evi_202

)

<-- the EVI context of 202 which matches the Vlan/EVI we are concerned about

  Not advertised to any peer
  Refresh Epoch 2
  Local, imported path from [2][172.16.254.6:202][0][48][0000BEEFCAFE][32][10.1.202.1]/24 (global)
    172.16.254.6 (metric 3) (via default) from 172.16.255.1 (172.16.255.1)
      Origin incomplete, metric 0, localpref 100, valid, internal, best

```
      EVPN ESI: 00000000000000000000,
Label1 20201              <-- Correct Segment ID
      Extended Community: RT:65001:202 ENCAP:8
EVPN DEF GW:0:0  <-- prefix has the Default GW attribute added
      Originator: 172.16.255.6, Cluster list: 172.16.255.1
      rx pathid: 0, tx pathid: 0x0
      Updated on Sep 7 2023 19:56:43 UTC
```

FED MATM(리프)

<#root>

```
F241.03.23-9300-Leaf01#
show platform software fed active matm macTable vlan 202 mac 0000.beef.cafe
VLAN   MAC                  Type  Seq#    EC_Bi  Flags  machandle           siHandle            riHandl
-------------------------------------------------------------------------------------------------------
202    0000.beef.cafe
  0x5000001       0      0     64  0x71e058da7858      0x71e05916c0d8      0x71e059171678      0x0
VTEP 172.16.254.6
 adj_id 651
No
<-- MAC of Default GW is installed in FED
```

SISF(CGW)

<#root>

```
CGW#
sh device-tracking database vlanid 202
vlanDB has 1 entries for vlan 202, 0 dynamic
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DH
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned

    Network Layer Address                  Link Layer Address     Interface  vlan       prlvl      ag
S   10.1.202.1                             0000.beef.cafe         Twe1/0/1   202        0100       13
```

IOS MATM(CGW)

<#root>

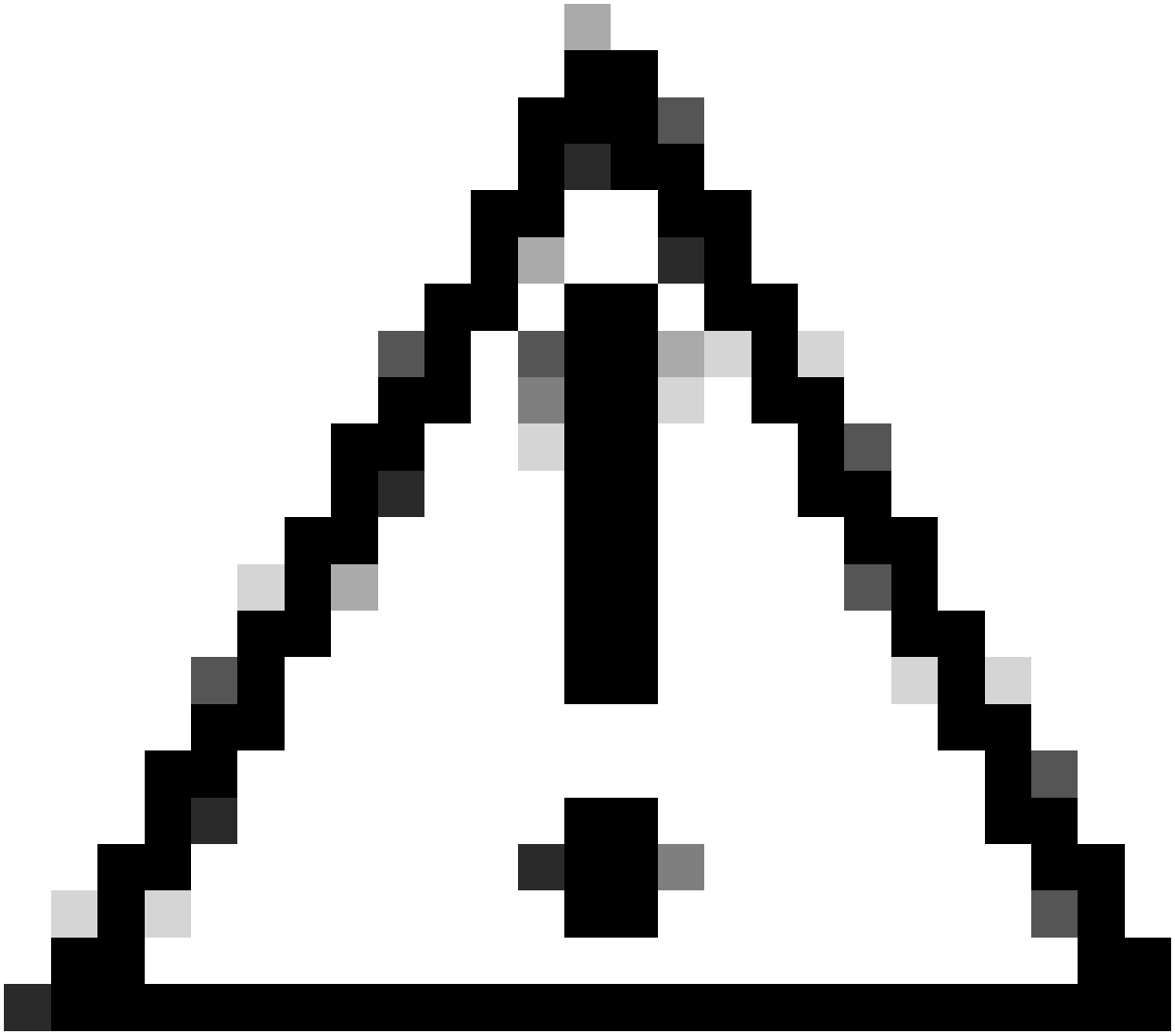
```
CGW#

show mac address-table address 0000.beef.cafe

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 201    0000.beef.cafe    STATIC      Vl201

2021    0000.beef.cafe    STATIC      Vl2021   <-- The Vlan 2021 SVI MAC advertised out Tw1/0/1

 202    0000.beef.cafe    DYNAMIC     Twe1/0/1 <-- The Vlan 2021 SVI MAC learned dynamically after passi
```

문제 해결

ARP(Address Resolution)

ARP 문제를 격리하기 위한 일반적인 단계

- IMET 터널이 준비되었는지 확인합니다.
- CGW 업링크에서 캡처하여 Leaf에서 캡슐화된 ARP 수신 확인
- 업링크에서 ARP가 엔드캡에 도달하는 것이 보이지 않는 경우.
  - Leaf 및 CGW 모두에서 IMET 터널이 준비되었는지 확인합니다.
  - 리프 업링크에서 캡처하여 ARP가 캡슐화되어 전송되는지 확인
  - 중간 경로 문제 해결
- ARP가 보더 IMET 터널 캡처에 도착했지만 VRF ARP 테이블에 프로그래밍되지 않은 경우
  - CPU/CoPP 펀트 경로 문제를 해결하여 ARP가 CPU에 펑트되었는지 확인합니다.
  - IP 주소/클라이언트 정보가 정확한지 확인합니다.
  - VRF에서 ARP를 디버깅하여 ARP 프로세스에 영향을 미칠 수 있는 사항 확인
- 호스트에 next hop/dest mac으로 설치된 CGW MAC 확인
- CGW에 실제 호스트 MAC과 함께 두 ARP 항목이 모두 있는지 확인
- 방화벽 정책이 이 유형의 트래픽을 허용하는지 확인



주의: 디버그를 활성화할 때 주의하십시오!

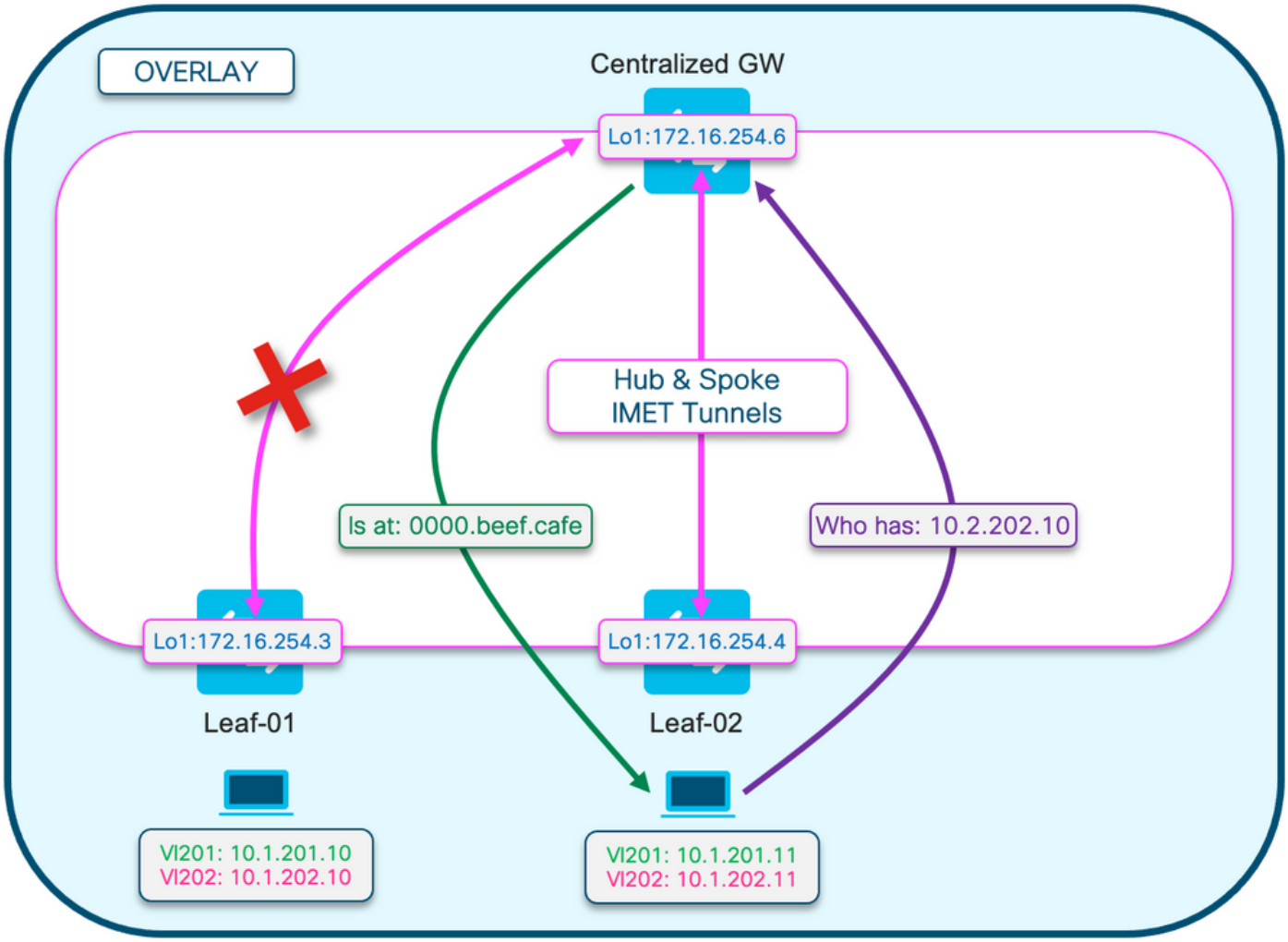
플러딩 억제를 비활성화했는지 확인합니다.

<#root>

```
Leaf-01#

show run | sec l2vpn
l2vpn evpn

 replication-type static

 flooding-suppression address-resolution disable <-- This CLI prevents a VTEP from trying to unicast oth
```

호스트 오프 Leaf-02가 호스트 오프 Leaf-01에 대한 ARP를 확인하는 경우 ARP 요청이 Leaf-01로 직접 브로드캐스트되지 않습니다

- 대신 ARP는 Leaf-02에 프로그래밍된 유일한 BUM 터널을 CGW로 전달합니다
- CGW는 이를 Leaf-01로 전달하지 않고 대신 자체 MAC으로 응답합니다
- 그러면 모든 통신이 CGW로 전달된 다음 호스트 간에 라우팅됩니다
- CGW는 동일한 로컬 서브넷에 있는 경우에도 패킷을 라우팅합니다



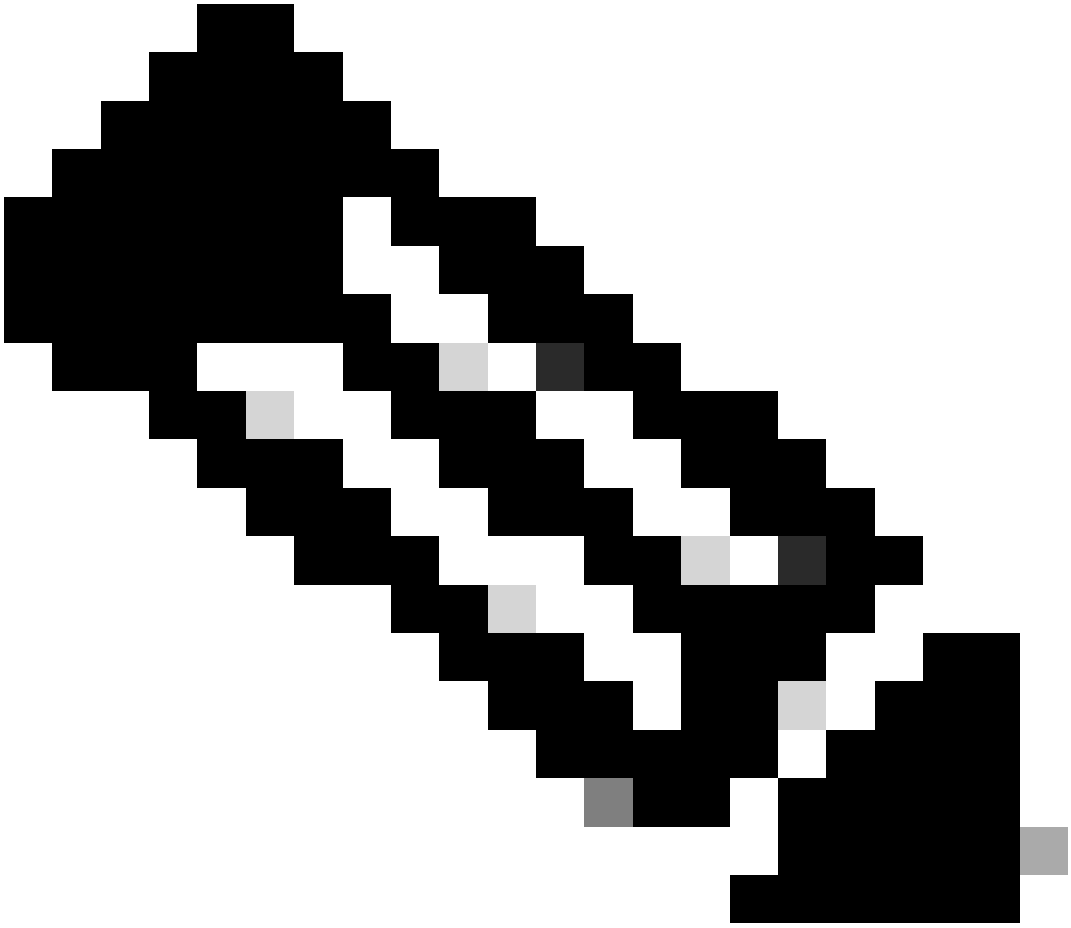
이 다이어그램은 이 섹션에서 설명하는 ARP 해결 프로세스의 흐름을 시각화하는 데 도움이 됩니다
.

ARP 요청은 보라색으로 표시됩니다

- 이 ARP 요청은 Leaf-01에서 호스트 10.1.202.10의 MAC 주소를 확인하기 위한 것입니다
- 보라색 선은 CGW에서 종료되며 Leaf-01에 도달하지 않습니다

ARP 회신은 녹색으로 표시됩니다

- 회신에는 VLAN 202용 CGW SVI의 MAC이 포함되어 있습니다
- 녹색 선은 실제 호스트가 아니라 CGW에서 옵니다



참고: 빨간색 X는 이 통신에 Leaf-01에 트래픽을 보내지 않았음을 나타냅니다.

각 호스트에서 ARP 항목을 관찰합니다

<#root>

```
Leaf02-HOST#

sh ip arp 10.1.202.10

Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.202.10             1

0000.beef.cafe

  ARPA   Vlan202

<-- MAC address for Leaf01 host is CGW MAC


Leaf01-HOST#
```

sh ip arp 10.1.202.11

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.202.11             7
```

0000.beef.cafe

```
  ARPA   Vlan202
```

<-- MAC address for Leaf02 host is CGW MAC

RT2 접두사가 학습되는지 CGW에서 관찰합니다. 이는 CGW가 패킷을 라우팅하는 데 필요합니다

<#root>

CGW#

sh bgp l2vpn evpn route-type 2 0 0006.f617.eec4 * <-- Leaf02 actual MAC

BGP routing table entry for [2][172.16.254.6:202][0][48][0006F617EEC4][0][*]/20, version 235458
Paths: (1 available, best #1,

table evi_202

)
  Not advertised to any peer
  Refresh Epoch 2
  Local, imported path from [2][172.16.254.4:202][0][48][0006F617EEC4][0][*]/20 (global)
    172.16.254.4 (metric 3) (via default) from 172.16.255.1 (172.16.255.1)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      EVPN ESI: 00000000000000000000,

Label1 20201 <-- correct segment identifier

      Extended Community: RT:65001:202 ENCAP:8

EVPN E-Tree:flag:1

,label:0

<-- prefix contains the Leaf flag indicating this is a normal host

      Originator: 172.16.255.4, Cluster list: 172.16.255.1
      rx pathid: 0, tx pathid: 0x0
      Updated on Apr 9 2025 17:11:22 UTC

CGW#

sh bgp l2vpn evpn route-type 2 0 0006.f601.cd44 * <-- Leaf01 actual MAC

BGP routing table entry for [2][172.16.254.6:202][0][48][0006F601CD44][0][*]/20, version 235521
Paths: (1 available, best #1,

table evi_202)

  Not advertised to any peer
  Refresh Epoch 2
  Local, imported path from [2][172.16.254.3:202][0][48][0006F601CD44][0][*]/20 (global)
    172.16.254.3 (metric 3) (via default) from 172.16.255.1 (172.16.255.1)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      EVPN ESI: 00000000000000000000,

```
Label1 20201                          <-- correct segment identifier

      Extended Community: RT:65001:202 ENCAP:8

EVPN E-Tree:flag:1

,label:0

<-- prefix contains the Leaf flag indicating this is a normal host


      Originator: 172.16.255.3, Cluster list: 172.16.255.1
      rx pathid: 0, tx pathid: 0x0
      Updated on Apr 9 2025 17:17:06 UTC
```

업링크에서 ARP 교환을 캡처하여 양방향 통신을 확인합니다.

- 패브릭 업링크에서 EPC(Embedded Packet Capture)를 사용할 수 있습니다
- 이 시나리오에서는 Leaf01 업링크의 EPC를 보여줍니다. 필요한 경우 CGW에서 동일한 프로세스를 반복합니다

EPC 구성

```
<#root>

Leaf01#

monitor capture 1 interface range te 1/1/2 , te 1/1/4 both match any buffer size 100


<-- both Uplinks toward fabric included
```

캡처 시작

```
<#root>

Leaf01#

monitor capture 1 start
```

ping을 시작하여 ARP 요청을 트리거합니다(이 경우 ping은 Leaf01 호스트 10.1.201.10에서 Leaf02 호스트 10.1.201.11로).

```
<#root>

Leaf01-HOST#

ping vrf red 10.1.201.11
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.201.11, timeout is 2 seconds:
...!!
Success rate is 40 percent (2/5), round-trip min/avg/max = 1/1/1 ms
```

캡처 중지 및 ARP 프레임 확인

<#root>

Leaf01#

mon cap 1 stop

F241.03.23-9300-Leaf01#

show mon cap 1 buff br | i ARP

11

8.153510 00:06:f6:01:cd:42 -> ff:ff:ff:ff:ff:ff ARP 110

Who has 10.1.201.11? Tell 10.1.201.10 <-- .10 requests .11 MAC (this is Frame 11)

12 8.154030 00:00:be:ef:ca:fe -> 00:06:f6:01:cd:42 ARP 110 10.1.201.11

is at 00:00:be:ef:ca:fe <-- CGW replies with its MAC

캡처 패킷을 자세히 봅니다. 패키지에 대한 추가 정보를 보려면 EPC의 detail 옵션을 사용하십시오

- 이 출력은 간결성을 위해 여러 곳에서 잘립니다

<#root>

Leaf01#

show mon cap 1 buffer detailed | beg Frame 11 <-- begin detail result from Frame 11 (ARP Request)

Frame 11: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface /tmp/epc_ws/wif_to_t

Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)

```
    Destination: 00:00:00:00:00:00 (00:00:00:00:00:00)
        Address: 00:00:00:00:00:00 (00:00:00:00:00:00)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: 00:00:00:00:00:00 (00:00:00:00:00:00)
        Address: 00:00:00:00:00:00 (00:00:00:00:00:00)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

Internet Protocol Version 4, Src: 172.16.254.3, Dst: 172.16.254.6 <--- Outer tunnel IP header

Source: 172.16.254.3
Destination: 172.16.254.6
User Datagram Protocol, Src Port: 65483,

Dst Port: 4789 <-- VXLAN Dest port

Virtual eXtensible Local Area Network
VXLAN Network Identifier

(VNI): 20101 <-- Verify the VNI for the segment you are investigating

Reserved: 0

Ethernet II, Src: 00:06:f6:01:cd:42 (00:06:f6:01:cd:42), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff) <--

Type: ARP (0x0806)

Trailer: 00000000000000000000000000000000000000
Address Resolution Protocol (

request

)

<-- is an ARP request

Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)

Sender MAC address: 00:06:f6:01:cd:42 (00:06:f6:01:cd:42) <-- Sending host
Sender IP address: 10.1.201.10
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00) <-- Trying to resolve MAC for host
Target IP address: 10.1.201.11

Frame 12:

110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface /tmp/epc_ws/wif_to_ts_pipe, i

<-- ARP reply

Ethernet II,

Src: dc:77:4c:8a:6d:7f

(dc:77:4c:8a:6d:7f),

Dst: 68:2c:7b:f8:87:48

(68:2c:7b:f8:87:48)

<-- Underlay MACs

Internet Protocol Version 4, Src: 172.16.254.6, Dst: 172.16.254.3

```
User Datagram Protocol, Src Port: 65410, Dst Port: 4789
Virtual eXtensible Local Area Network
    VXLAN Network Identifier (VNI): 20101
    Reserved: 0
Ethernet II,
```

Src: 00:00:be:ef:ca:fe

(00:00:be:ef:ca:fe),

Dst: 00:06:f6:01:cd:42

(00:06:f6:01:cd:42)

<-- Start of payload

Type: ARP

(0x0806)

```
    Trailer: 000000000000000000000000000000000000
Address Resolution Protocol (
```

reply

)

<-- is an ARP reply

```
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
```

Sender MAC address: 00:00:be:ef:ca:fe (00:00:be:ef:ca:fe) <-- Reply is that of the CGW MAC due to loc

```
    Sender IP address: 10.1.201.11
    Target MAC address: 00:06:f6:01:cd:42 (00:06:f6:01:cd:42)
    Target IP address: 10.1.201.10
```

CGW RT2 게이트웨이 접두사

게이트웨이 접두사 누락

부분 격리 세그먼트에 대한 이전 섹션에서 언급한 것처럼 MAC는 패브릭 Vlan에서 학습해야 합니다

- 이 문제는 게이트웨이로 향하는 트래픽이 MAC 에이징 타이머보다 오래 없을 경우 나타날 수 있습니다.
- CGW 게이트웨이 접두사가 없는 경우 MAC가 있는지 확인해야 합니다

<#root>

CGW#

show bgp l2vpn evpn route-type 2 0 0000.beef.cafe 10.1.202.1

```
% Network not in table <-- RT2 not generated on CGW


CGW#

show mac address-table address 0000.beef.cafe

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 201    0000.beef.cafe    STATIC      Vl201
2021    0000.beef.cafe    STATIC      Vl2021

<-- MAC is not learned in Fabric Vlan 202

Total Mac Addresses for this criterion: 2
```

게이트웨이 접두사 누락 교정

대부분의 프로덕션 네트워크에는 항상 일부 트래픽이 있을 수 있습니다. 그러나 이 문제가 발생하는 경우 다음 옵션 중 하나를 사용하여 문제를 해결할 수 있습니다.

- 'mac address-table static 000.beef.cafe vlan 202 interface TwentyFiveGigE1/0/1'과 같은 고정 MAC 항목을 추가합니다.
- 'mac address-table aging-time <seconds>'으로 MAC 에이징 타이머를 늘립니다. (이 경우 모든 MAC 주소의 에이징 시간이 늘어나므로 고정 MAC 옵션이 기본 설정됨)

DEF GW 속성이 없습니다.

Partially Isolated Segments(부분적으로 격리된 세그먼트)에는 이 특성을 추가할 수 있는 여러 추가 컨피그레이션이 있습니다.

DEF GW 속성 교정 누락

다음 세부 정보를 확인합니다.

- 17.12.1 이상을 실행하고 있습니다.
- SISF(Device-Tracking) CLI가 컨피그레이션에 있습니다
- route-map match & set 명령이 구성되고 route-map이 BGP 인접 디바이스에 적용됩니다
- BGP 광고를 새로 고쳤습니다(접두사를 새 특성으로 다시 광고하려면 BGP를 지워야 함).

무선 로밍

로밍이 잦으면 BGP가 너무 자주 업데이트될 수 있습니다. 스위치에서 MAC을 소유하고 RT2 업데이트를 전송한다고 선언하기 전에 시간 간격당 로밍을 늘려야 합니다

- 호스트가 서로 다른 스위치에 있는 두 AP 사이를 이동할 때 발생합니다.
- 로밍 기본 제한은 180초당 5입니다.

```
Leaf01#

sh run | sec l2vpn

l2vpn evpn
 replication-type static
 flooding-suppression address-resolution disable

 ip duplication limit 10 time 180          <--- You can adjust this default in the global l2vpn sectior
 mac duplication limit 10 time 180


Leaf01#

sh l2vpn evpn summary

L2VPN EVPN
  EVPN Instances (excluding point-to-point): 4
    VLAN Based:   4
  Vlans: 4
  BGP: ASN 65001, address-family l2vpn evpn configured
  Router ID: 172.16.254.3
  Global Replication Type: Static
  ARP/ND Flooding Suppression: Disabled
  Connectivity to Core: UP

  MAC Duplication: seconds 180 limit 10

  MAC Addresses: 13
    Local:     6
    Remote:    7

    Duplicate: 0
  IP Duplication: seconds 180 limit 10

  IP Addresses: 7
    Local:     4
    Remote:    3

    Duplicate: 0

<...snip...>
```

TAC를 위해 수집할 명령

이 설명서에서 문제를 해결하지 못한 경우 표시된 명령 목록을 수집하여 TAC 서비스 요청에 첨부하십시오.

수집할 최소 정보

(다시 로드/복구 작업 전에 데이터를 수집하는 데 걸리는 시간 제한)

- 기술 이벤트 표시
- Show tech
- Tech sisf 표시

수집할 세부 정보

(더 완전한 데이터를 수집할 시간이 있는 경우 이 옵션을 사용하는 것이 좋습니다.)

- show tech
- 기술 이벤트 표시
- show tech platform evpn_vxlan switch <number>
- show tech 플랫폼
- 기술 리소스 표시
- show tech sisf
- show tech isis
- show tech bgp
- show monitor event-trace evpn event all
- show monitor event-trace evpn 오류 모두
- 플랫폼 소프트웨어 추적 아카이브 요청

관련 정보

- Catalyst 9000 Series 스위치에 BGP EVPN 라우팅 정책 구현
- DHCP Layer 2 Relay(제공 예정)

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.