레이어 2 전용 VLAN에서 DHCP 문제 해결 - 유선

목차

소개

이 문서에서는 SDA(SD-Access) 패브릭의 레이어 2 전용 네트워크에서 유선 엔드포인트에 대한 DHCP 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- IP(인터넷 프로토콜) 포워딩

- LISP(Locator/ID Separation Protocol)
- PIM(Protocol Independent Multicast) 스파스 모드

하드웨어 및 소프트웨어 요구 사항

- Catalyst 9000 시리즈 스위치
- Catalyst Center 버전 2.3.7.9
- Cisco IOS® XE 17.12 이상

제한 사항

- 링크를 비활성화하는 FlexLink+ 또는 EEM 스크립트와 같은 강력한 루프 방지 메커니즘이 제대로 구성되지 않는 한, 하나의 L2 경계에서만 고유한 VLAN/VNI를 동시에 전달할 수 있습니다.

L2 전용 개요

개요

일반적인 SD-Access 구축에서 L2/L3 경계는 FE(Fabric Edge)에 있습니다. 여기서 FE는 SVI 형식으로 클라이언트의 게이트웨이를 호스팅합니다. 이를 "Anycast Gateway"라고 합니다. L3 VNI(라우팅됨)는 서브넷 간 트래픽에 대해 설정되고, L2 VNI(스위칭됨)는 서브넷 내 트래픽을 관리합니다. 모든 FE에서 일관된 컨피그레이션을 통해 원활한 클라이언트 로밍이 가능합니다. 전달이 최적화되었습니다. 서브넷 내(L2) 트래픽은 FE 간에 직접 브리지되며 서브넷 간(L3) 트래픽은 FE 간에 또는 FE와 경계 노드 간에 라우팅됩니다.

패브릭 외부에서 엄격한 네트워크 진입점이 필요한 SDA 패브릭의 엔드포인트의 경우, SDA 패브릭은 에지에서 외부 게이트웨이로의 L2 채널을 제공해야 합니다.

이 개념은 레이어 2 액세스 네트워크가 레이어 3 라우터에 연결되는 기존 이더넷 캠퍼스 구축과 유사합니다. VLAN 내 트래픽은 L2 네트워크 내에 남아 있는 반면, VLAN 간 트래픽은 L3 디바이스에서 라우팅되며 L2 네트워크의 다른 VLAN으로 돌아가는 경우가 많습니다.

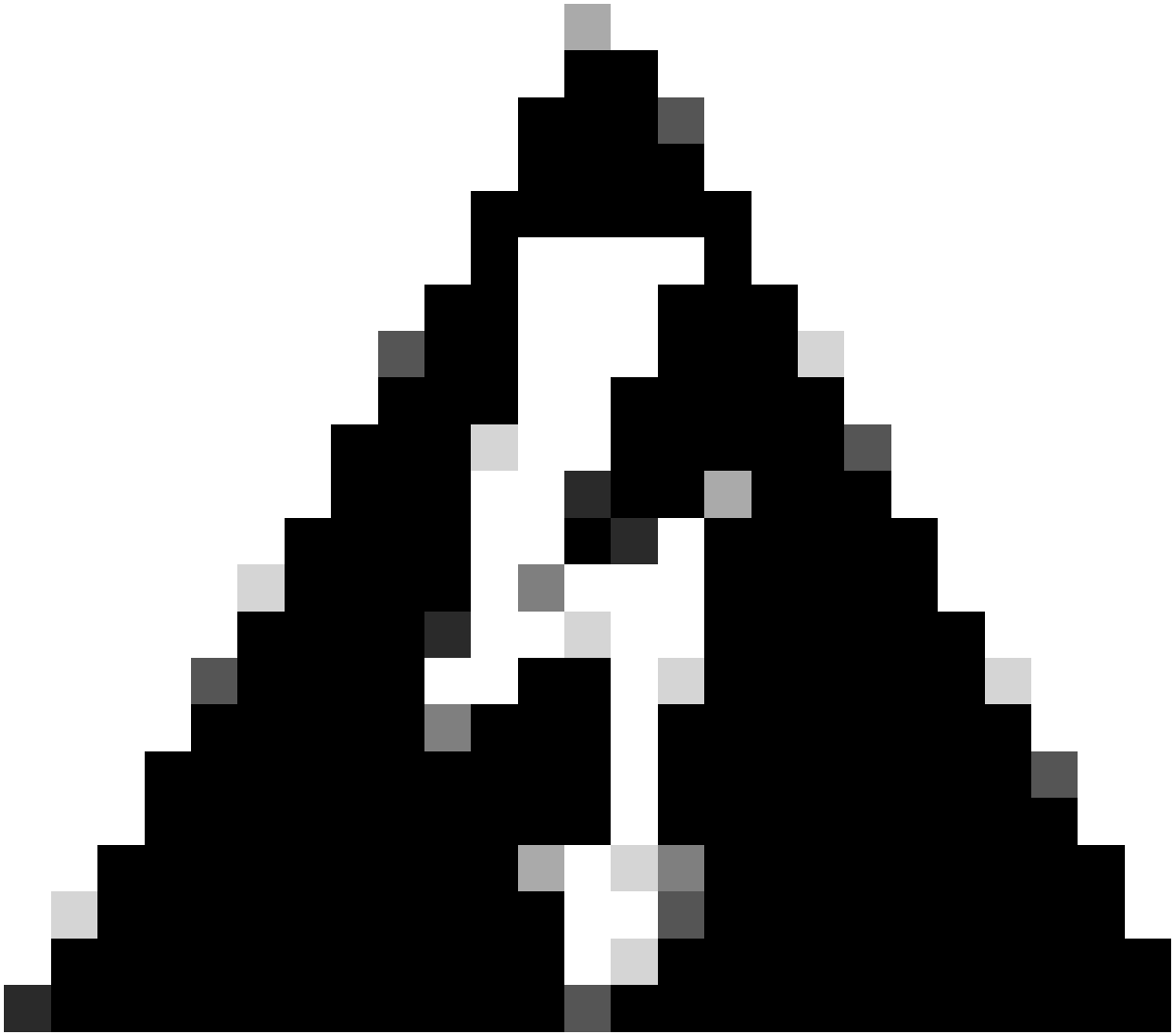
LISP 컨텍스트 내에서 Site Control Plane은 주로 기존 ARP 엔트리와 마찬가지로 MAC 주소와 해당 MAC-IP 바인딩을 추적합니다. L2 VNI/L2 전용 풀은 이 두 가지 EID 유형을 기반으로 하여 등록, 해결 및 포워딩을 간편하게 하도록 설계되었습니다. 따라서 L2 전용 환경의 모든 LISP 기반 전달은 MAC 및 MAC-to-IP 정보에만 의존하며 IPv4 또는 IPv6 EID는 완전히 무시합니다. LISP EID를 보완하기 위해 L2 전용 풀은 기존 스위치와 마찬가지로 플러드 앤 런(flood-and-learn) 메커니즘에 크게 의존합니다. 따라서 L2 플러딩은 이 솔루션 내에서 브로드캐스트, 알 수 없는 유니캐스트 및 멀티캐스트(BUM) 트래픽을 처리하기 위한 중요한 구성 요소가 되며 언더레이 멀티캐스트를 사용해야 합니다. 반대로 일반 유니캐스트 트래픽은 주로 맵 캐시를 통해 표준 LISP 포워딩 프로세스를 사용하여 포워딩됩니다.

패브릭 에지와 "L2 보더"(L2B)는 모두 로컬 VLAN에 매핑되는 L2 VNI를 유지 관리합니다. 이 매핑은 SDA 내에서 로컬로 디바이스 중요하므로 여러 VLAN이 노드 간에 동일한 L2 VNI에 매핑할 수 있습니다. 이 특정 활용 사례에서는 이러한 노드의 VLAN에 SVI가 구성되지 않으므로 해당하는 L3 VNI가 없습니다.

L2 전용 VLAN의 DHCP 동작 변경

Anycast Gateway 풀에서는 모든 패브릭 에지가 모든 FE에서 동일한 게이트웨이 IP를 사용하여 직접 연결된 엔드포인트의 게이트웨이 역할을 하기 때문에 DHCP가 어려움을 겪습니다. DHCP 릴레이된 패킷의 원래 소스를 제대로 식별하려면 FE는 LISP RLOC 정보를 포함하여 DHCP 옵션 82 및 하위 옵션을 삽입해야 합니다. 이는 패브릭 에지의 클라이언트 VLAN에서 DHCP 스누핑을 통해 구현됩니다. DHCP Snooping은 이러한 상황에서 이중 목적을 제공합니다. 이는 옵션 82의 삽입을 용이하게 하며, 특히 브리지 도메인(VLAN/VNI)을 통한 DHCP 브로드캐스트 패킷의 범람을 방지합니다. Anycast Gateway에 레이어 2 플러딩이 활성화된 경우에도 DHCP 스누핑은 브로드캐스트 패킷이 Fabric Edge에서 브로드캐스트로 전달되는 것을 효과적으로 억제합니다.

이와 달리 레이어 2 전용 VLAN에는 게이트웨이가 없으므로 DHCP 소스 식별이 간소화됩니다. 패킷은 어떤 Fabric Edge에서도 릴레이되지 않으므로 소스 식별을 위한 복잡한 메커니즘이 필요하지 않습니다. L2 Only VLAN에서 DHCP 스누핑을 수행하지 않으면 DHCP 패킷에 대한 플러드 제어 메커니즘이 효과적으로 우회됩니다. 이를 통해 DHCP 브로드캐스트가 L2 플러딩을 통해 최종 대상으로 전달될 수 있습니다. 최종 대상은 패브릭 노드 또는 DHCP 릴레이 기능을 제공하는 레이어 3 디바이스에 직접 연결된 DHCP 서버일 수 있습니다.



경고: L2 Only 풀 내의 "MAC에 다중 IP" 기능은 DHCP 플러드 제어를 적용하는 Bridge VM 모드에서 DHCP Snooping을 자동으로 활성화합니다. 따라서 L2 VNI 풀이 해당 엔드포인트에 대해 DHCP를 지원할 수 없게 됩니다.

언더레이 멀티캐스트

DHCP가 브로드캐스트 트래픽에 크게 의존하는 점을 감안할 때, 레이어 2 플러딩을 활용하여 이 프로토콜을 지원해야 합니다. 다른 L2 플러딩 지원 풀과 마찬가지로, 언더레이 네트워크는 멀티캐스트 트래픽, 특히 PIM Sparse-Mode를 사용하는 Any-Source-Multicast에 대해 구성해야 합니다. 언더레이 멀티캐스트 컨피그레이션은 LAN 자동화 워크플로를 통해 자동화되지만, 이 단계를 생략한 경우 추가 컨피그레이션(수동 또는 템플릿)이 필요합니다.

- 모든 노드(경계, 에지, 중간 노드 등)에서 IP 멀티캐스트 라우팅을 활성화합니다.
- 각 보더 및 에지 노드의 Loopback0 인터페이스에 PIM Sparse-Mode를 구성합니다.
- 각 IGP(언더레이 라우팅 프로토콜) 인터페이스에서 PIM Sparse-Mode를 활성화합니다.
- 모든 노드(경계, 가장자리, 중간 노드)에서 PIM RP(Rendezvous Point)를 구성하면 경계에 RP를 배치하는 것이 좋습니다.
- PIM 네이버, PIM RP 및 PIM 터널 상태를 확인합니다.

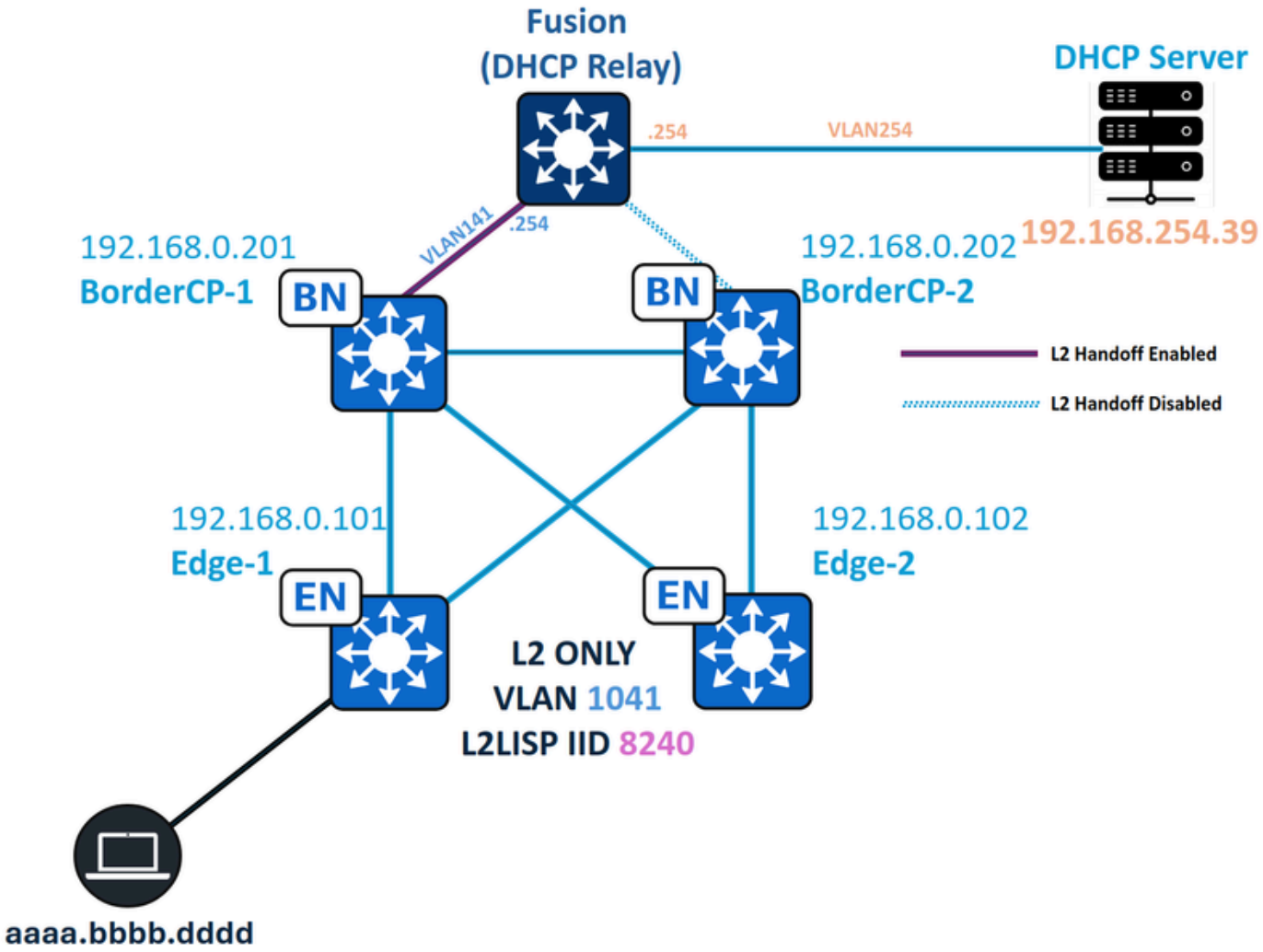
SD-Access 패브릭 내부의 DHCP 서버

일반적인 설계 질문은 DHCP 서버를 SD-Access 패브릭 내에 구축할 수 있는지입니다. 그 답은 본질적으로 '그렇다'와 '아니다'다.

공식 Cisco Validated Design에서는 DHCP 서버를 패브릭 외부, 일반적으로 Shared Services 블록 내에 배치할 것을 권장합니다. 그러나 패브릭 노드(예: 에지 또는 경계)에 DHCP 서버의 물리적 연결이 필요한 경우에는 L2 전용 네트워크를 통해서만 지원됩니다. 이는 기본적으로 DHCP 스누핑이 활성화되어 있는 Anycast 게이트웨이 풀의 고유한 동작 때문입니다. 이렇게 하면 서버의 DHCP 제공 및 확인이 차단될 뿐만 아니라 VXLAN에서 캡슐화된 경우에도 DHCP 검색 및 요청 패킷이 전달되지 않습니다. DHCP 서버 포트의 "DHCP Snooping Trust"는 제공 및 확인을 허용하지만 검색 및 요청 패킷은 동일한 방법을 사용하여 전달되지 않습니다. 또한 Catalyst Center에서 규정 준수 검증 중에 컨피그레이션 편차에 대해 플래그를 지정하므로 Anycast Gateway 풀에서 DHCP 스누핑을 제거하는 것은 지원되지 않는 옵션입니다.

반대로, DHCP 서버가 L2 전용 네트워크 내에 있는 경우 DHCP 스누핑이 적용되지 않으므로 정책 기반 검사 또는 차단 없이 모든 DHCP 패킷이 통과될 수 있습니다. SD-Access 패브릭(예: Fusion Router)의 네트워크 디바이스 업스트림은 L2 Only 네트워크의 게이트웨이로 구성되어 여러 VRF의 트래픽이 해당 L2 Only 세그먼트 내에서 동일한 DHCP 서버에 액세스할 수 있게 합니다.

토폴로지



네트워크 토폴로지

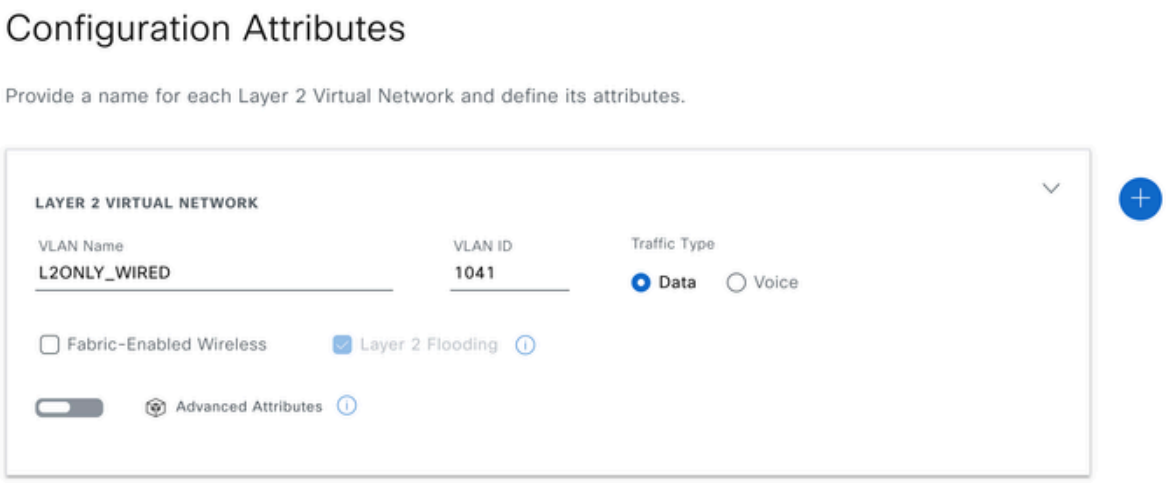
이 토폴로지에서는

- 192.168.0.201 및 192.168.0.202는 패브릭 사이트의 배치된 경계이며, BorderCP-1은 레이어 2 핸드오프 기능이 활성화된 유일한 경계입니다.
- 192.168.0.101 및 192.168.0.102는 패브릭 에지 노드입니다.
- 192.168.254.39는 DHCP 서버입니다.
- aaaa.bbb.ddd는 DHCP 지원 엔드포인트입니다.
- Fusion 디바이스는 패브릭 서브넷에 대한 DHCP 릴레이 역할을 합니다.

L2 전용 VLAN 컨피그레이션

Catalyst Center에서 L2 전용 VLAN 구축

경로: Catalyst Center/프로비저닝/패브릭 사이트/레이어 2 가상 네트워크/레이어 2 가상 네트워크 수정



L2VNI 컨피그레이션

L2 전용 VLAN 컨피그레이션 - 패브릭 에지

패브릭 에지 노드에는 CTS가 활성화되고 IGMP 및 IPv6 MLD가 비활성화되며 필수 L2 LISP 컨피그레이션으로 구성된 VLAN이 있습니다. 이 L2 전용 풀은 무선 풀이 아닙니다. 따라서 RA-Guard, DHCPGuard 및 Flood Access Tunnel과 같은 L2 전용 무선 풀에서 일반적으로 발견되는 기능은 구성되지 않습니다. 대신 ARP 패킷의 플러딩은 "flood arp-nd"를 사용하여 명시적으로 활성화됩니다

패브릭 에지(192.168.0.101) 구성

<#root>

```
cts role-based enforcement vlan-list
```

1041

```
vlan
```

1041

name L2ONLY_WIRED

no ip igmp snooping vlan 1041 querier

no ip igmp snooping vlan 1041

no ipv6 mld snooping vlan 1041

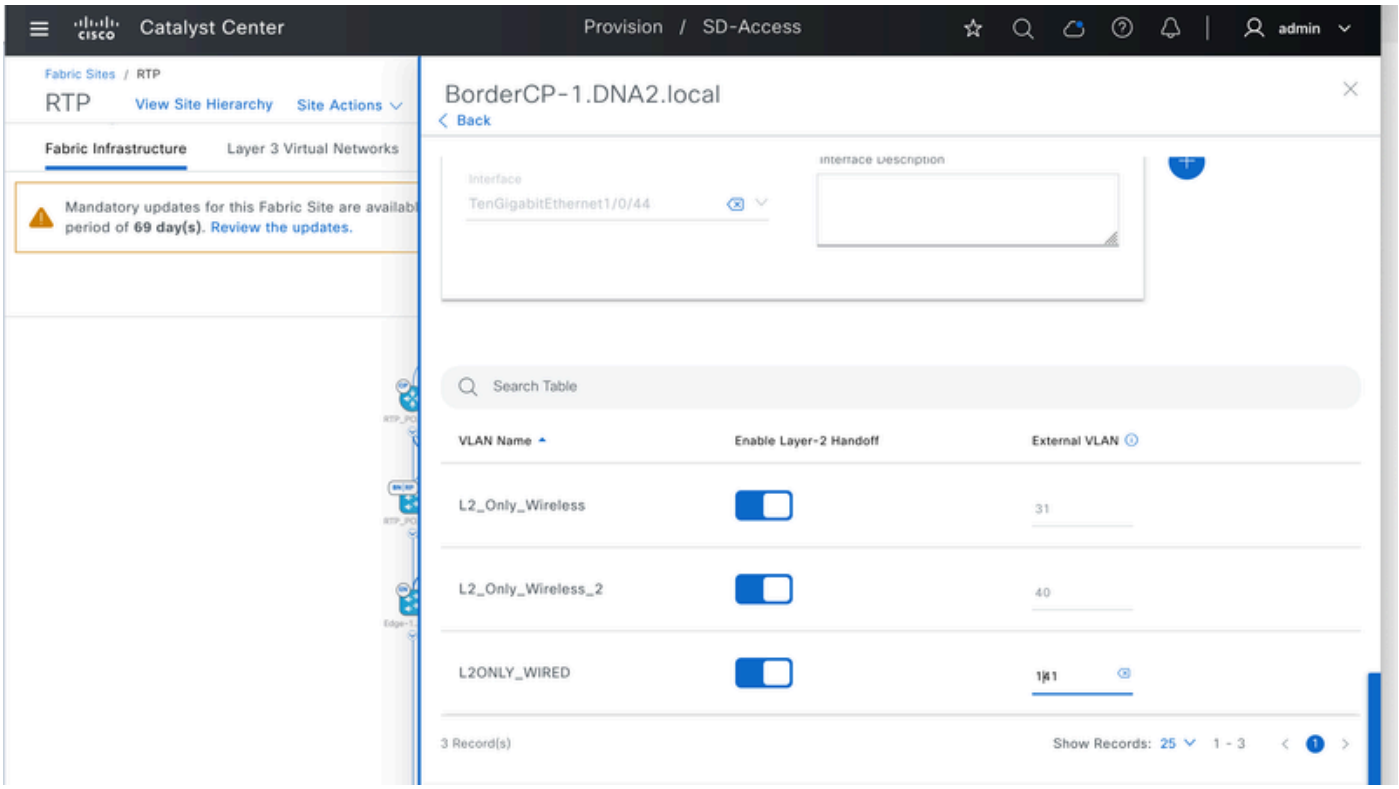
```
router lisp
 instance-id
8240
  remote-rloc-probe on-route-change
  service ethernet
eid-table vlan
1041
   broadcast-underlay
239.0.17.1
flood arp-nd
 flood unknown-unicast
   database-mapping mac locator-set rloc_91947dad-3621-42bd-ab6b-379ecebb5a2b
   exit-service-ethernet
```

L2 핸드오프 컨피그레이션 - 패브릭 보더

운영의 관점에서 볼 때 DHCP 서버(또는 라우터/릴레이)는 테두리와 가장자리를 모두 포함한 모든 패브릭 노드에 연결할 수 있습니다.

DHCP 서버를 연결하기 위해 보더 노드를 사용하는 것이 권장되는 방법이지만, 신중하게 설계해야 합니다. 인터페이스별로 L2 핸드오프에 대한 Border를 구성해야 하기 때문입니다. 이를 통해 패브릭 풀이 패브릭 내부와 동일한 VLAN에 또는 다른 VLAN에 전달될 수 있습니다. 패브릭 에지와 경계 사이의 VLAN ID를 유연하게 사용할 수 있습니다. 둘 다 동일한 L2 LISP Instance-ID에 매핑되기 때문입니다. SD-Access 네트워크 내에서 레이어 2 루프를 방지하려면 L2 핸드오프 물리적 포트를 동일한 VLAN과 동시에 활성화해서는 안 됩니다. 이중화를 위해서는 StackWise Virtual, FlexLink+ 또는 EEM 스크립트와 같은 메서드가 필요합니다.

이와 달리 DHCP 서버 또는 게이트웨이 라우터를 패브릭 에지에 연결하면 추가 컨피그레이션이 필요하지 않습니다.



L2 핸드오프 컨피그레이션

패브릭 보더(192.168.0.201) 구성

<#root>

```
cts role-based enforcement vlan-list
```

141

```
vlan
```

141

name L2ONLY_WIRED

no ip igmp snooping vlan 141 querier

no ip igmp snooping vlan 141

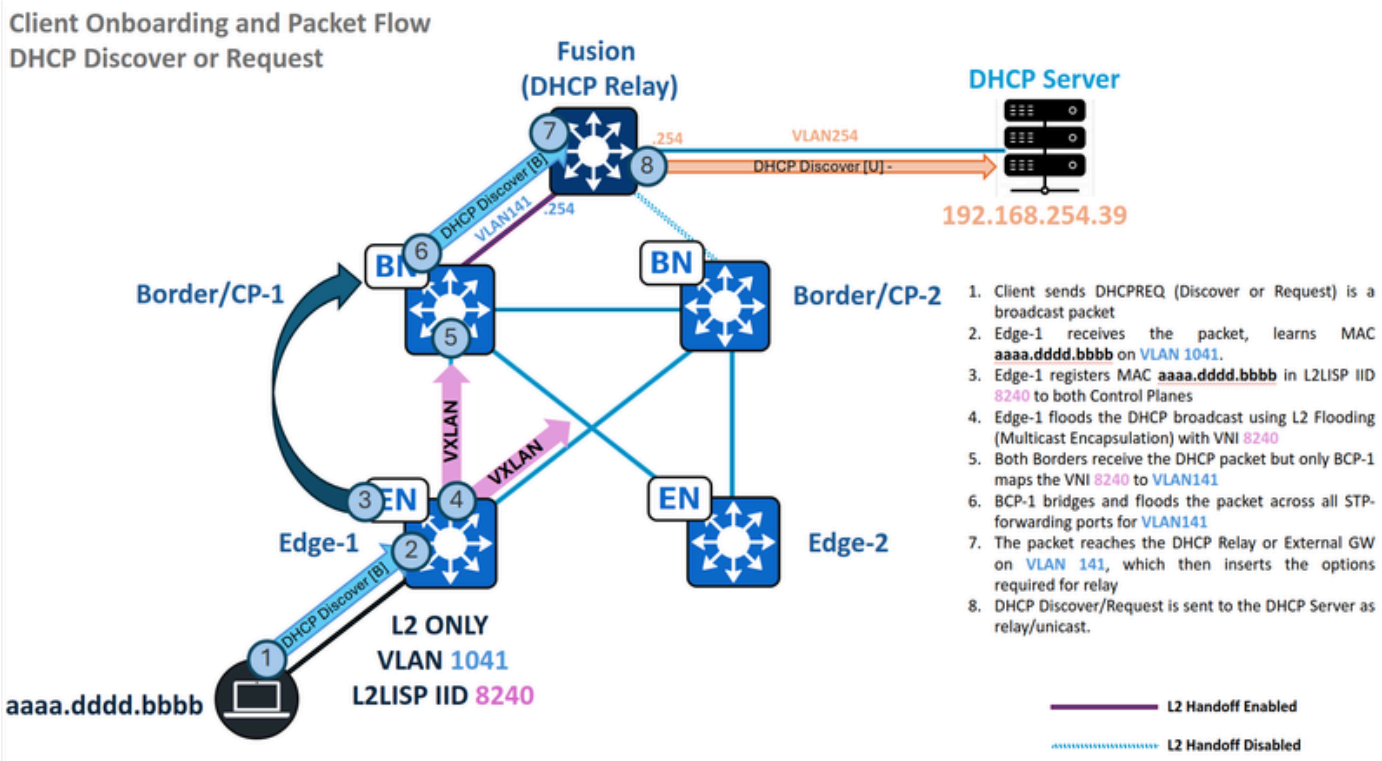
no ipv6 mld snooping vlan 141

```
router lisp
 instance-id
```

```
8240

  remote-rloc-probe on-route-change
  service ethernet

eid-table


vlan 141



 broadcast-underlay 239.0.17.1


   flood arp-nd


   flood unknown-unicast


   database-mapping mac locator-set rloc_91947dad-3621-42bd-ab6b-379ecebb5a2b
   exit-service-ethernet

interface TenGigabitEthernet1/0/44


  switchport mode trunk
```

DHCP 트래픽 흐름

DHCP 검색 및 요청 - 에지



트래픽 흐름 - L2에서만 DHCP 검색 및 요청

MAC 학습 및 엔드포인트 등록

엔드포인트 aaaa.ddd.bbb가 DHCP 검색 또는 요청(브로드캐스트 패킷)을 전송할 때 에지 노드는 엔드포인트의 MAC 주소를 학습하고 이를 MAC 주소 테이블에 추가한 다음 L2/MAC SISF 테이블에 추가하고 마지막으로 L2LISP 인스턴스 8240에 매핑된 VLAN 1041용 L2LISP 데이터베이스에 추가해야 합니다.

<#root>

Edge-1#

show mac address-table interface te1/0/2

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

1041

aaaa.dddd.bbbb

DYNAMIC

Te1/0/2

Edge-1#

show vlan id 1041

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- --------------------------------

1041 L2ONLY_WIRED



active

    L2LI0:

8240

, Te1/0/2, Te1/0/17, Te1/0/18, Te1/0/19, Te1/0/20, Ac2, Po1

Edge-1#

show device-tracking database mac | i aaaa.dddd.bbbb|vlan


 MAC                   Interface  vlan       prlvl      state            Time left        Policy
 aaaa.dddd.bbbb        Te1/0/2    1041       NO TRUST   MAC-REACHABLE    123 s            IPDT_POLICY

Edge-1#

show lisp instance-id 8240 dynamic-eid summary | i Name|aaaa.dddd.bbbb


Dyn-EID Name         Dynamic-EID      Interface     Uptime    Last      Pending
Auto-L2-group-

8240



aaaa.dddd.bbbb

   N/A           6d04h     never

0



Edge-1#

show lisp instance-id 8240 ethernet database aaaa.dddd.bbbb


LISP ETR MAC Mapping Database for LISP 0 EID-table

Vlan 1041 (IID 8240)

, LSBs: 0x1
Entries total 1, no-route 0, inactive 0, do-not-register 0

aaaa.dddd.bbbb/48

,

dynamic-eid Auto-L2-group-8240

, inherited from default locator-set rloc_91947dad-3621-42bd-ab6b-379ecebb5a2b
  Uptime: 6d04h, Last-change: 6d04h
  Domain-ID: local
  Service-Insertion: N/A
  Locator        Pri/Wgt  Source     State

 192.168.0.101
```

```
   10/10   cfg-intf   site-self, reachable
  Map-server     Uptime         ACK  Domain-ID

  192.168.0.201

  6d04h

Yes

  0

  192.168.0.202

 6d04h

Yes

  0
```

엔드포인트의 MAC 주소가 올바르게 학습되고 ACK 플래그가 패브릭 제어 평면에 대해 "Yes"로 표시된 경우 이 단계는 완료된 것으로 간주됩니다.

L2 플러딩 브리지된 DHCP 브로드캐스트

DHCP Snooping이 비활성화되면 DHCP 브로드캐스트가 차단되지 않습니다. 대신 레이어 2 플러딩에 대한 멀티캐스트에서 캡슐화됩니다. 반대로 DHCP 스누핑을 활성화하면 이러한 브로드캐스트 패킷의 플러딩을 방지할 수 있습니다.

<#root>

```
Edge-1#

show ip dhcp snooping


Switch DHCP snooping is enabled


Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
12-13,50,52-53,333,1021-1026
DHCP snooping is operational on following VLANs:

12-13,50,52-53,333,1021-1026


<--

VLAN1041 should not be listed, as DHCP snooping must be disabled in L2 Only pools.


 Proxy bridge is configured on following VLANs:
1024
 Proxy bridge is operational on following VLANs:
1024
<snip>
```

DHCP Snooping이 비활성화되어 있으므로 DHCP Discover/Request는 L2LISP0 인터페이스를 활

용하여 L2 플러딩을 통해 트래픽을 브리징합니다. Catalyst Center 버전 및 적용된 Fabric Banners에 따라 L2LISP0 인터페이스에는 양방향으로 구성된 액세스 목록이 있을 수 있습니다. 따라서 DHCP 트래픽(UDP 포트 67 및 68)이 ACE(Access Control Entry)에 의해 명시적으로 거부되지 않는지 확인합니다.

<#root>

interface L2LISP0

 ip access-group

SDA-FABRIC-LISP

in

 ip access-group

SDA-FABRIC-LISP out

Edge-1#

show access-list SDA-FABRIC-LISP

Extended IP access list SDA-FABRIC-LISP
    10 deny ip any host 224.0.0.22
    20 deny ip any host 224.0.0.13
    30 deny ip any host 224.0.0.1

40 permit ip any any

L2LISP 인스턴스 및 Fabric Edge의 Loopback0 IP 주소에 대해 구성된 브로드캐스트 언더레이 그룹을 활용하여 이 패킷을 다른 Fabric Node에 브리징하는 L2 Flooding (S,G) 항목을 확인합니다. 수신 인터페이스, 발신 인터페이스 목록 및 전달 카운터와 같은 매개변수를 검증하려면 mroute 및 mfib 테이블을 참조하십시오.

<#root>

Edge-1#

show ip interface loopback 0 | i Internet

  Internet address is

192.168.0.101/32

Edge-1#

show running-config | se 8240

interface L2LISP0.8240

instance-id 8240

  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 1041

 broadcast-underlay 239.0.17.1

Edge-1#

show ip mroute 239.0.17.1 192.168.0.101 | be \(

(192.168.0.101, 239.0.17.1)

, 00:00:19/00:03:17, flags: FT
  Incoming interface:

Null0

, RPF nbr 0.0.0.0

<--

Local S,G IIF must be Null0

  Outgoing interface list:

 TenGigabitEthernet1/1/2

,

Forward

/Sparse, 00:00:19/00:03:10, flags:

<--

1st OIF = Te1/1/2 = Border2 Uplink

 TenGigabitEthernet1/1/1

,

Forward

/Sparse, 00:00:19/00:03:13, flags:

<--

2nd OIF = Te1/1/1 = Border1 Uplink

Edge-1#

show ip mfib 239.0.17.1 192.168.0.101 count

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Default
 13 routes, 6 (*,G)s, 3 (*,G/m)s
Group:

239.0.17.1

  Source:

192.168.0.101

,
   SW Forwarding: 1/0/392/0, Other: 1/1/0
   HW Forwarding:

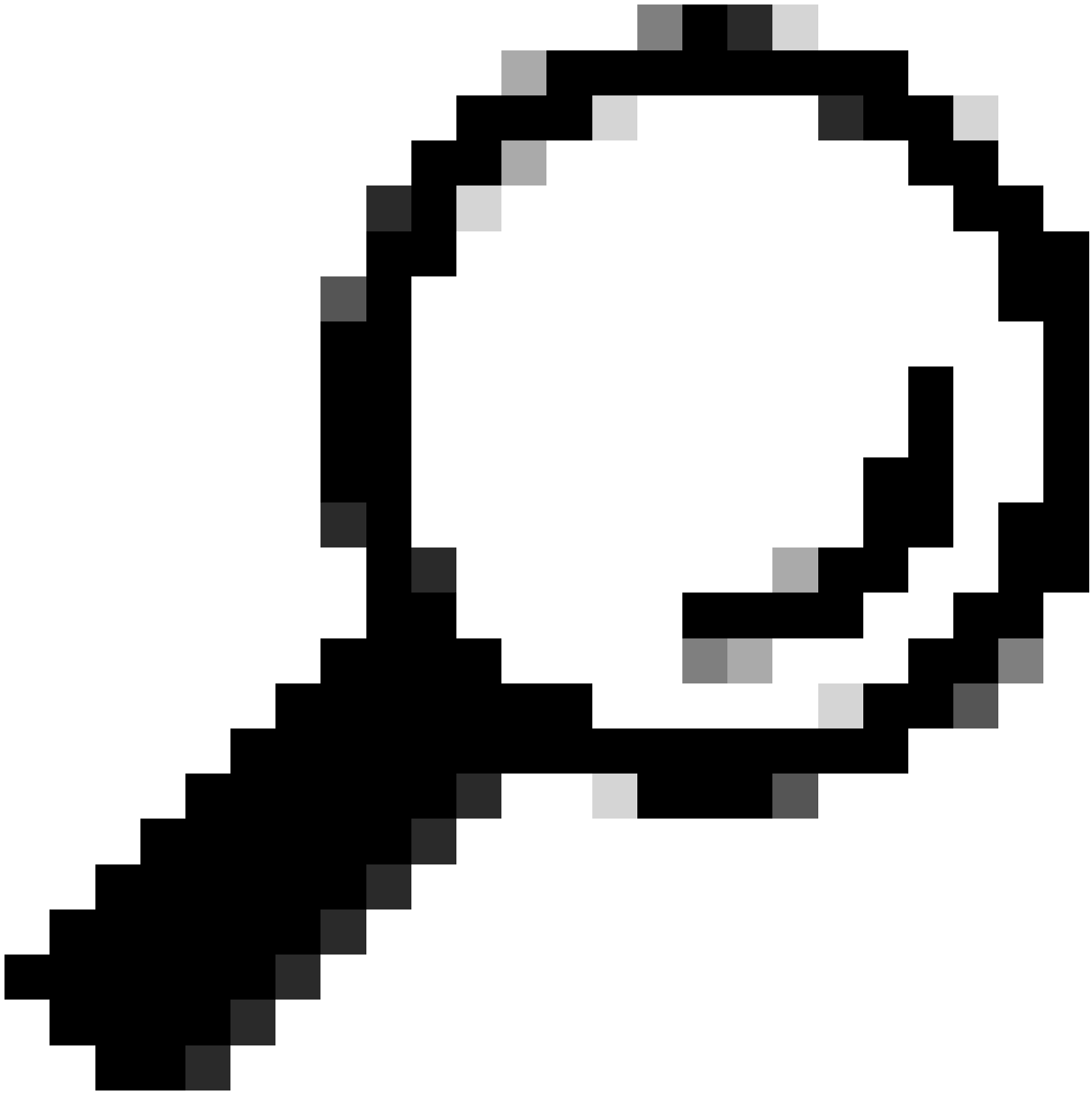
 7

/0/231/0, Other: 0/0/0

<--

HW Forwarding counters (First counter = Pkt Count) must increase

  Totals - Source count: 1, Packet count: 8



팁: (S,G) 항목을 찾을 수 없거나 OIL(Outgoing Interface List)에 OIF(Outgoing Interface)가 포함되어 있지 않으면 언더레이 멀티캐스트 컨피그레이션 또는 작업에 문제가 있음을 나타냅니다.

패킷 캡처

엔드포인트에서 들어오는 DHCP 패킷과 L2 플러딩에 해당하는 이그레스 패킷을 모두 기록하도록 스위치에서 동시에 포함된 패킷 캡처를 구성합니다. 패킷 캡처 시 두 개의 고유한 패킷을 관찰해야 합니다. 언더레이 그룹(239.0.17.1)을 대상으로 하는 원래 DHCP Discover/Request 및 VXLAN으로 캡슐화된 대응 제품입니다.

패브릭 에지(192.168.0.101) 패킷 카탈로그

monitor capture cap interface TenGigabitEthernet1/0/2 IN   <-- Endpoint Interface

monitor capture cap interface TenGigabitEthernet1/1/1 OUT   <-- One of the OIFs from the multicast rout

monitor capture cap match any
monitor capture cap buffer size 100
monitor capture cap limit pps 1000
monitor capture cap start
monitor capture cap stop

Edge-1#

show monitor capture cap buffer display-filter "bootp and dhcp.hw.mac_addr==aaaa.dddd.bbbb"

<-- aaaa.dddd.bbbb is the endpoint MAC

Starting the packet display .... Press Ctrl + Shift + 6 to exit
   22   2.486991   0.0.0.0 -> 255.255.255.255 DHCP

356 DHCP Discover

 - Transaction ID 0xf8e

<--

356 is the Length of the original packet

   23   2.487037   0.0.0.0 -> 255.255.255.255 DHCP

406 DHCP Discover

 - Transaction ID 0xf8e

<--

406 is the Length of the VXLAN encapsulated packet

Edge-1#

show monitor capture cap buffer display-filter "bootp and dhcp.hw.mac_addr==aaaa.dddd.bbbb and vxlan"

Starting the packet display .... Press Ctrl + Shift + 6 to exit
   23   2.487037   0.0.0.0 -> 255.255.255.255 DHCP

406 DHCP Discover

 - Transaction ID 0xf8e

Edge-1#

show monitor capture cap buffer display-filter "bootp and dhcp.hw.mac_addr==aaaa.dddd.bbbb and vxlan" de

Internet Protocol Version 4, Src:

192.168.0.101, Dst: 239.0.17.1 <-- DHCP Discover is encapsulated for Layer 2 Flooding

Internet Protocol Version 4, Src:

0.0.0.0, Dst: 255.255.255.255

DHCP 검색 및 요청 - L2 경계

Edge가 Broadcast-Underlay 그룹 239.0.17.1로 캡슐화된 레이어 2 플러딩을 통해 DHCP Discover 및 Request 패킷을 전송한 후 이러한 패킷은 L2 Hand-off Border, 특히 Border/CP-1에서 수신됩니다.

이를 위해서는 Border/CP-1이 에지의 (S,G)와 함께 멀티캐스트 경로를 가져야 하며, 그 발신 인터페이스 목록에 L2 핸드오프 VLAN의 L2LISP 인스턴스가 포함되어야 합니다. L2 핸드오프 경계는 핸드오프에 서로 다른 VLAN을 사용하더라도 동일한 L2LISP Instance-ID를 공유합니다.

<#root>

BorderCP-1#

show vlan id 141

VLAN Name Status Ports
---- -------------------------------- --------- --------------------------------

141 L2ONLY_WIRED

active

L2LIO:

8240

, Te1/0/44

BorderCP-1#

show ip mroute 239.0.17.1 192.168.0.101 | be \(

(192.168.0.101, 239.0.17.1)

, 00:03:20/00:00:48, flags: MTA
Incoming interface:

TenGigabitEthernet1/0/42

, RPF nbr 192.168.98.3

<--

Incoming Interface Te1/0/42 is the RPF interface for 192.168.0.101 (Edge RLOC)

```
  Outgoing interface list:
   TenGigabitEthernet1/0/26, Forward/Sparse, 00:03:20/00:03:24, flags:
    L2LISP0.
```

8240

```
, Forward/Sparse-Dense, 00:03:20/00:02:39, flags:

BorderCP-1#
```

show ip mfib 239.0.17.1 192.168.0.101 count

```
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:      Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Default
 13 routes, 6 (*,G)s, 3 (*,G/m)s
Group:
```

239.0.17.1

```
  Source:
```

192.168.0.101

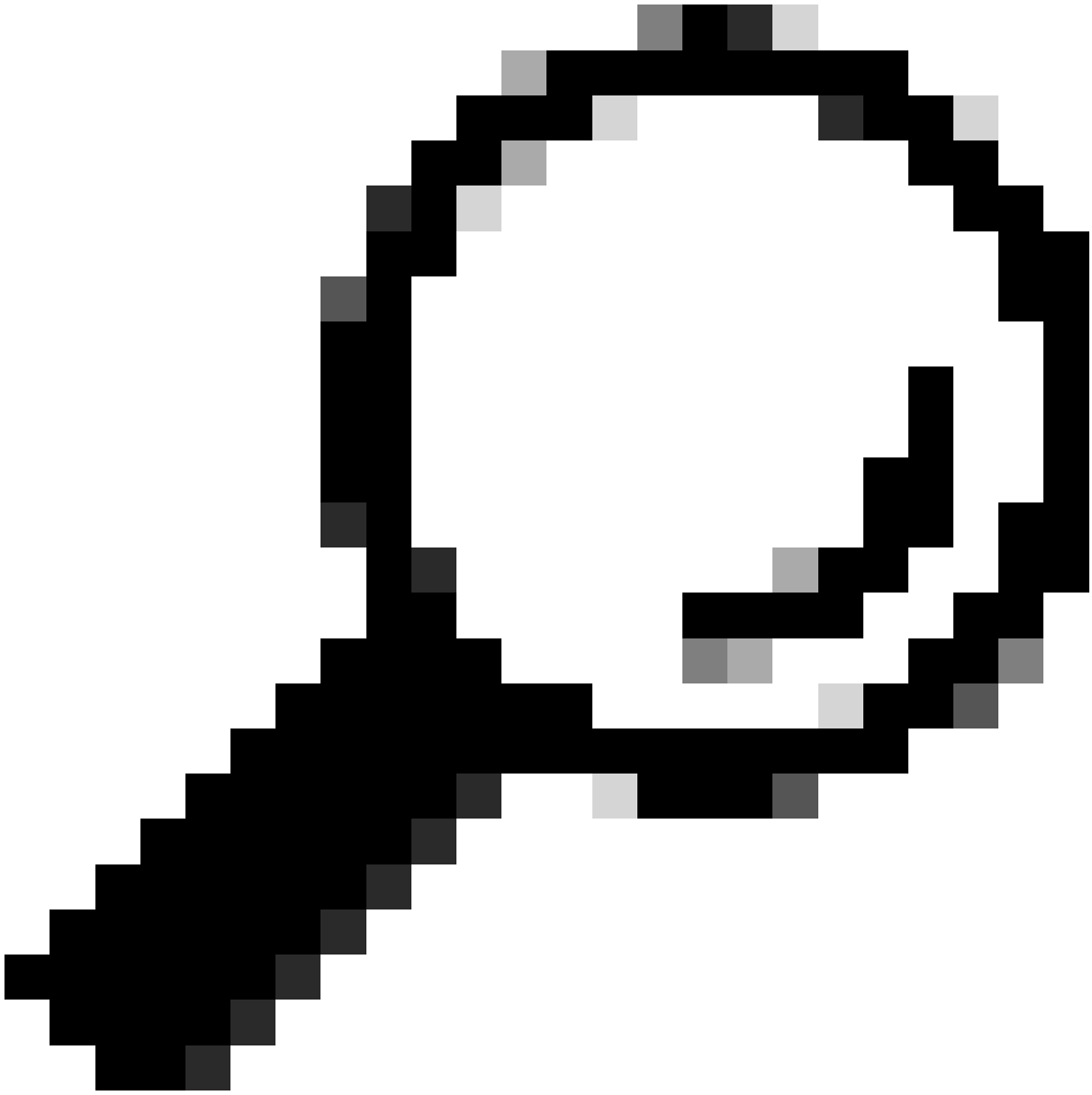
```
,
   SW Forwarding: 1/0/392/0, Other: 0/0/0
   HW Forwarding:
```

3

```
/0/317/0, Other: 0/0/0
```

<-- HW Forwarding counters (First counter = Pkt Count) must increase

```
  Totals - Source count: 1, Packet count: 4
```



팁: (S,G) 항목을 찾을 수 없는 경우 언더레이 멀티캐스트 컨피그레이션 또는 작업에 문제가 있음을 나타냅니다. 필요한 인스턴스에 대한 L2LISP가 OIF로 표시되지 않으면 L2LISP 하위 인터페이스의 작동 UP/DOWN 상태 또는 L2LISP 인터페이스의 IGMP 활성화 상태에 문제가 있음을 나타냅니다.

패브릭 에지 노드와 마찬가지로, L2LISP0 인터페이스의 수집 DHCP 패킷을 거부하는 Access Control Entry가 없는지 확인합니다.

<#root>

```
BorderCP-1#
```

show access-list SDA-FABRIC-LISP

```
Extended IP access list SDA-FABRIC-LISP
    10 deny ip any host 224.0.0.22
    20 deny ip any host 224.0.0.13
    30 deny ip any host 224.0.0.1

40 permit ip any any
```

패킷의 캡슐화가 해제되고 VLAN 일치 VNI 8240에 배치되면 해당 브로드캐스트 특성은 핸드오프 VLAN 141을 위해 모든 스패닝 트리 프로토콜 포워딩 포트에 플러딩됨을 지시합니다.

<#root>

```
BorderCP-1#

show spanning-tree vlan 141 | be Interface

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------

Te1/0/44

          Desg

FWD

 2000      128.56   P2p
```

디바이스 추적 테이블에서는 게이트웨이/DHCP 릴레이에 연결되는 인터페이스 Te1/0/44가 STP 포워딩 포트여야 함을 확인합니다.

<#root>

```
BorderCP-1#

show device-tracking database address 172.16.141.254 | be Network

   Network Layer Address                    Link Layer Address     Interface  vlan       prlvl      age
ARP

172.16.141.254

f87b.2003.7fc0

Te1/0/44

 141

       0005       133s       REACHABLE  112 s try 0
```

패킷 캡처

L2 플러딩(S,G 수신 인터페이스)에서 들어오는 DHCP 패킷과 해당 이그레스 패킷을 모두 DHCP 릴레이에 기록하도록 스위치에 내장된 동시 패킷 캡처를 구성합니다. 패킷 캡처 시 두 개의 고유 패킷을 관찰해야 합니다. Edge-1에서 VXLAN으로 캡슐화된 패킷 및 DHCP 릴레이로 이동하는 캡슐화되지 않은 패킷.

패브릭 보더/CP(192.168.0.201) 패킷 범주

<#root>

```
monitor capture cap interface TenGigabitEthernet1/0/42 IN    <-- Incoming interface for Edge's S,G Mrout

monitor capture cap interface TenGigabitEthernet1/0/44 OUT   <-- Interface that connects to the DHCP Rel

monitor capture cap match any

monitor capture cap buffer size 100

monitor capture cap start

monitor capture cap stop


BorderCP-1#
show monitor capture cap buffer display-filter "bootp and dhcp.hw.mac_addr==aaaa.dddd.bbbb"

Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  427  16.695022      0.0.0.0 -> 255.255.255.255 DHCP
406
 DHCP Discover - Transaction ID 0x2030
<-- 406 is the Lenght of the VXLAN encapsulated packet

  428  16.695053      0.0.0.0 -> 255.255.255.255 DHCP
364
 DHCP Discover - Transaction ID 0x2030
<-- 364 is the Lenght of the VXLAN encapsulated packet
```

Packet 427: VXLAN Encapsulated

BorderCP-1#

show monitor capture cap buffer display-filter "bootp and dhcp.hw.mac_addr==aaaa.dddd.bbbb and vxlan" de

Internet Protocol Version 4, Src:

192.168.0.101, Dst: 239.0.17.1

Internet Protocol Version 4, Src:

0.0.0.0, Dst: 255.255.255.255

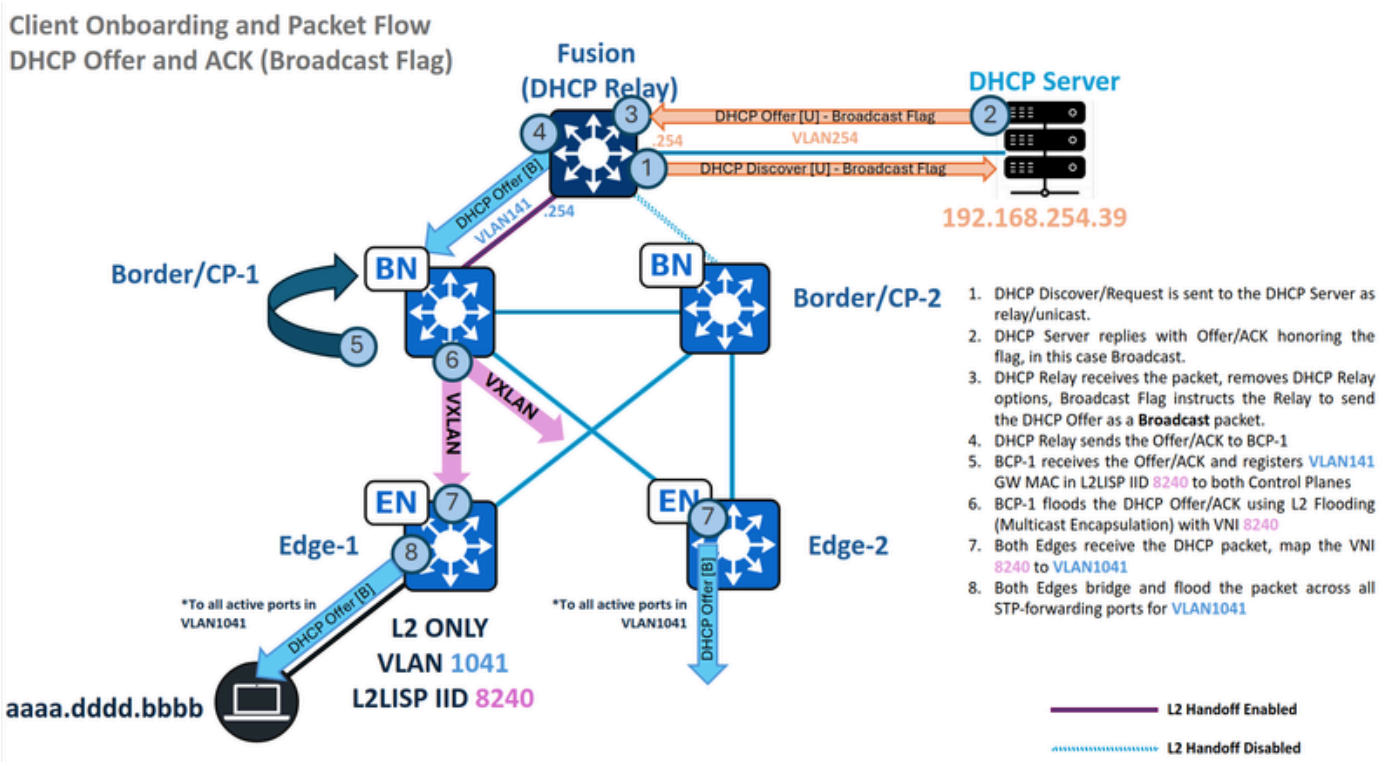
Packet 428: Plain (dot1Q cannot be captured at egress direction)

BorderCP-1#

show monitor capture cap buffer display-filter "bootp and dhcp.hw.mac_addr==aaaa.dddd.bbbb and not vxlan

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

DHCP 오퍼 및 ACK - 브로드캐스트 - L2 경계



트래픽 흐름 - L2에서만 DHCP 제공 및 ACK 브로드캐스트

이제 DHCP Discover가 SD-Access 패브릭을 종료했으므로 DHCP 릴레이는 기존 DHCP 릴레이 옵

션(예: GiAddr/GatewayIPAddress)을 삽입하고 패킷을 유니캐스트 전송으로 DHCP 서버에 전달합니다. 이 흐름에서 SD-Access 패브릭은 특별한 DHCP 옵션을 추가하지 않습니다.

서버에 DHCP Discover/Request가 도착하면 서버는 포함된 브로드캐스트 또는 유니캐스트 플래그를 그대로 사용합니다. 이 플래그는 DHCP 릴레이 에이전트가 DHCP 제공을 브로드캐스트 또는 유니캐스트 프레임으로 다운스트림 디바이스(경계)에 전달할지 여부를 나타냅니다. 이 데모에서는 브로드캐스트 시나리오를 가정합니다.

MAC 학습 및 게이트웨이 등록

DHCP 릴레이가 DHCP Offer 또는 ACK를 전송할 때 L2BN 노드는 게이트웨이의 MAC 주소를 학습하고 MAC 주소 테이블에 추가한 다음 L2/MAC SISF 테이블에 추가하고 마지막으로 L2LISP 인스턴스 8240에 매핑된 VLAN 141용 L2LISP 데이터베이스에 추가해야 합니다.

<#root>

BorderCP-1#

show mac address-table interface te1/0/44

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

141

f87b.2003.7fc0

    DYNAMIC

Te1/0/44
```

BorderCP-1#

show vlan id 141

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------

141

L2ONLY_WIRED

               active    L2LI0:

8240
```

,

Te1/0/44

BorderCP-1#

show device-tracking database mac | i 7fc0|vlan

MAC Interface vlan prlvl state Time left Policy

f87b.2003.7fc0

Te1/0/44 141

NO TRUST

MAC-REACHABLE

61 s LISP-DT-GLEAN-VLAN 64

BorderCP-1#

show lisp ins 8240 dynamic-eid summary | i Name|f87b.2003.7fc0

Dyn-EID Name Dynamic-EID Interface Uptime Last Pending

Auto-L2-group-8240

f87b.2003.7fc0

N/A 6d06h never

0

BorderCP-1#

show lisp instance-id 8240 ethernet database f87b.2003.7fc0

LISP ETR MAC Mapping Database for LISP 0 EID-table Vlan

141

(IID

8240

), LSBs: 0x1
Entries total 1, no-route 0, inactive 0, do-not-register 0

f87b.2003.7fc0/48

, dynamic-eid Auto-L2-group-8240, inherited from default locator-set rloc_0f43c5d8-f48d-48a5-a5a8-094b8
Uptime: 6d06h, Last-change: 6d06h
Domain-ID: local
Service-Insertion: N/A
Locator Pri/Wgt Source State

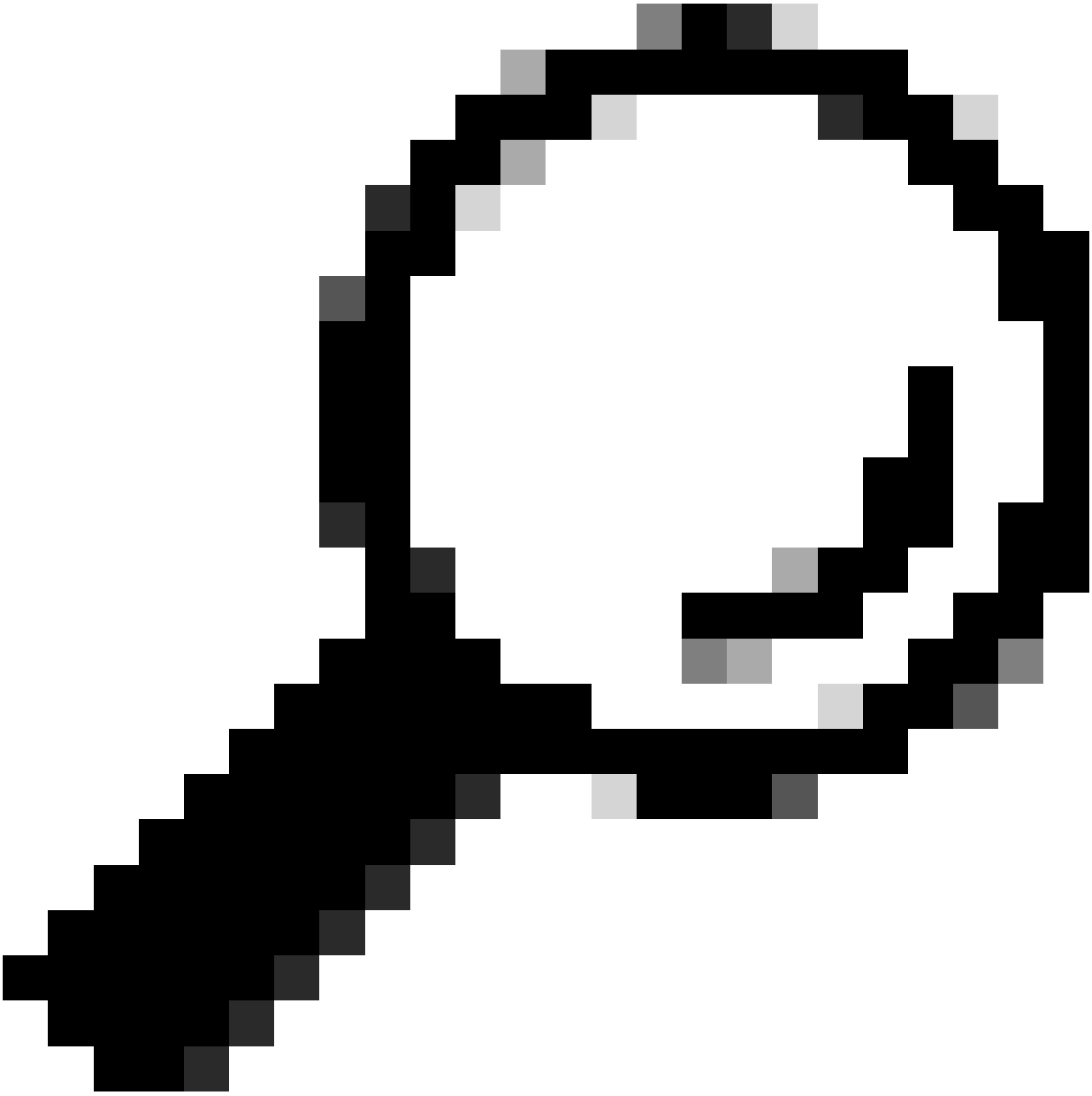
```
 192.168.0.201

  10/10   cfg-intf   site-self, reachable
  Map-server     Uptime         ACK  Domain-ID


192.168.0.201

 6d06h

Yes

  0


192.168.0.202

  6d06h

Yes

  0
```

게이트웨이의 MAC 주소가 올바르게 학습되고 ACK 플래그가 패브릭 제어 플레인에 대해 "예"로 표시된 경우 이 단계는 완료된 것으로 간주됩니다.

L2 플러딩 브리지된 DHCP 브로드캐스트

DHCP Snooping을 활성화하지 않으면 DHCP 브로드캐스트가 차단되지 않으며 레이어 2 플러딩을 위해 멀티캐스트에서 캡슐화됩니다. 반대로, DHCP Snooping이 활성화된 경우 DHCP 브로드캐스트 패킷의 플러드가 방지됩니다.

```
<#root>

BorderCP-1#

show ip dhcp snooping


Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
1001

DHCP snooping is operational on following VLANs:


1001     <-- VLAN141 should not be listed, as DHCP snooping must be disabled in L2 Only pools.


 Proxy bridge is configured on following VLANs:
none
 Proxy bridge is operational on following VLANs:
none
```



팁: L2Border에서는 DHCP Snooping이 활성화되지 않으므로 DHCP Snooping Trust 컨피그레이션이 필요하지 않습니다.

이 단계에서는 두 디바이스 모두에서 L2LISP ACL 검증이 이미 완료되었습니다.

L2LISP 인스턴스 및 L2Border Loopback0 IP 주소에 대해 구성된 브로드캐스트 언더레이 그룹을 활용하여 이 패킷을 다른 패브릭 노드에 연결하는 L2 플러딩(S,G) 항목을 확인합니다. 수신 인터페이스, 발신 인터페이스 목록 및 전달 카운터와 같은 매개변수를 검증하려면 mroute 및 mfib 테이블을 참조하십시오.

<#root>

```
BorderCP-1#
```

show ip int loopback 0 | i Internet

  Internet address is

192.168.0.201/32

BorderCP-1#

show run | se 8240

interface L2LISP0.8240

instance-id 8240

  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 1041

broadcast-underlay 239.0.17.1

BorderCP-1#

show ip mroute 239.0.17.1 192.168.0.201 | be \(

(

192.168.0.201, 239.0.17.1

), 1w5d/00:02:52, flags: FTA
  Incoming interface:

Null0

, RPF nbr 0.0.0.0

<-- Local S,G IIF must be Null0

  Outgoing interface list:

TenGigabitEthernet1/0/42

, Forward/Sparse, 1w3d/00:02:52, flags:

<-- Edge1 Downlink

TenGigabitEthernet1/0/43

, Forward/Sparse, 1w3d/00:02:52, flags:

<-- Edge2 Downlink

BorderCP-1#

show ip mfib 239.0.17.1 192.168.0.201 count

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Default
13 routes, 6 (*,G)s, 3 (*,G/m)s
Group:

239.0.17.1

Source:

192.168.0.201

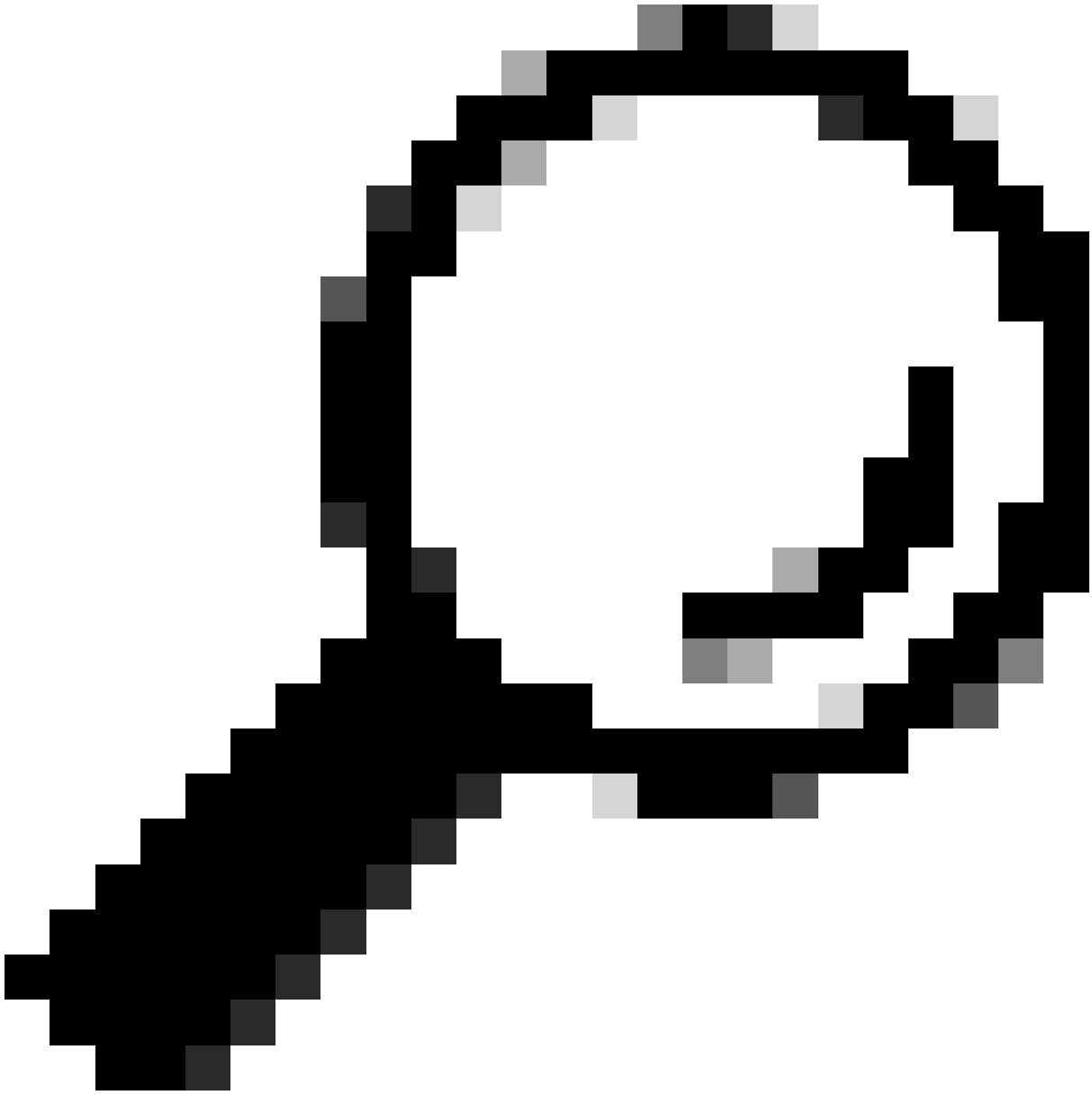
,
SW Forwarding: 1/0/392/0, Other: 1/1/0
HW Forwarding:

92071

/0/102/0, Other: 0/0/0

<-- HW Forwarding counters (First counter = Pkt Count) must increase

Totals - Source count: 1, Packet count: 92071



팁: (S,G) 항목을 찾을 수 없거나 OIL(Outgoing Interface List)에 OIF(Outgoing Interface)가 포함되어 있지 않으면 언더레이 멀티캐스트 컨피그레이션 또는 작업에 문제가 있음을 나타냅니다.

이러한 검증과 함께 이전 단계와 유사한 패킷 캡처를 함께 사용하면, DHCP 서비스가 발신 인터페이스 목록 콘텐츠를 사용하여 모든 패브릭 에지에 브로드캐스트로 전달되므로(이 경우, 인터페이스 TenGig1/0/42 및 TenGig1/0/43 외부) 이 섹션이 종료됩니다.

DHCP 오퍼 및 ACK - 브로드캐스트 - 에지

이전 흐름과 마찬가지로 패브릭 에지에서 L2Border S,G를 확인합니다. 여기서 들어오는 인터페이스는 L2BN을 가리키고 OIL에는 VLAN 1041에 매핑된 L2LISP 인스턴스가 포함되어 있습니다.

```
Edge-1#
show vlan id 1041

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------


1041


L2ONLY_WIRED


active
    L2LIO:
8240
,
Te1/0/2
, Te1/0/17, Te1/0/18, Te1/0/19, Te1/0/20, Ac2, Po1
Edge-1#
show ip mroute 239.0.17.1 192.168.0.201 | be \(

(
192.168.0.201
,
239.0.17.1
), 1w3d/00:01:52, flags: JT
  Incoming interface:
TenGigabitEthernet1/1/2
, RPF nbr 192.168.98.2
<-- IIF Te1/1/2 is the RPF interface for 192.168.0.201 (L2BN RLOC)

  Outgoing interface list:

L2LISP0.8240,
Forward/Sparse-Dense
,
 1w3d/00:02:23, flags:
Edge-1#
show ip mfib 239.0.17.1 192.168.0.201 count

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
```

Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Default
 13 routes, 6 (*,G)s, 3 (*,G/m)s
Group:

239.0.17.1

  Source:

192.168.0.201,

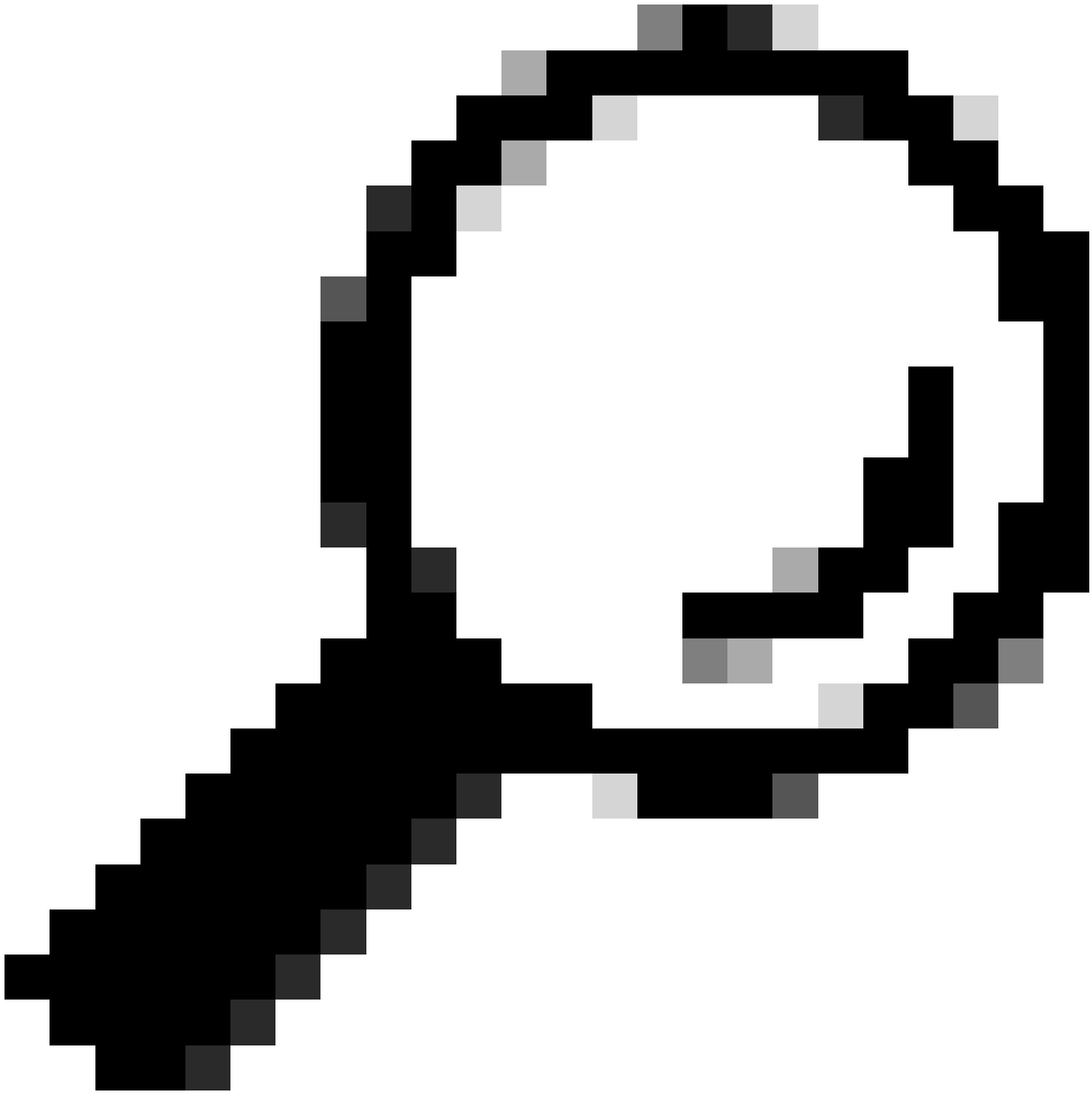
   SW Forwarding: 1/0/96/0, Other: 0/0/0
   HW Forwarding:

76236

/0/114/0, Other: 0/0/0

<-- HW Forwarding counters (First counter = Pkt Count) must increase

  Totals - Source count: 1, Packet count: 4



팁: (S,G) 항목을 찾을 수 없는 경우 언더레이 멀티캐스트 컨피그레이션 또는 작업에 문제가 있음을 나타냅니다. 필요한 인스턴스에 대한 L2LISP가 OIF로 표시되지 않으면 L2LISP 하위 인터페이스의 작동 UP/DOWN 상태 또는 L2LISP 인터페이스의 IGMP 활성화 상태에 문제가 있음을 나타냅니다.

L2LISP ACL 검증은 두 디바이스 모두에서 이미 수행되었습니다.

패킷의 캡슐화가 해제되어 VNI 8240과 일치하는 VLAN에 배치되면 해당 브로드캐스트 특성으로 인해 VLAN1041에 대한 모든 스패닝 트리 프로토콜 포워딩 포트가 플러딩됩니다.

<#root>

```
Edge-1#
```

show spanning-tree vlan 1041 | be Interface

```
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------


Te1/0/2

         Desg

FWD

 20000     128.2    P2p Edge
Te1/0/17            Desg

FWD

 2000      128.17   P2p
Te1/0/18            Back

BLK

 2000      128.18   P2p
Te1/0/19            Desg

FWD

 2000      128.19   P2p
Te1/0/20            Back

BLK

 2000      128.20   P2p
```

MAC 주소 테이블은 포트 Te1/0/2를 엔드포인트 포트로 식별합니다. 이 포트는 STP에 의해 FWD 상태이며 패킷이 엔드포인트로 플러딩됩니다.

```
<#root>

Edge-1#

show mac address-table interface te1/0/2


          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----


1041


aaaa.dddd.bbbb

    DYNAMIC

Te1/0/2
```

DHCP 오퍼 및 ACK 프로세스는 일관되게 유지됩니다. DHCP Snooping을 활성화하지 않으면

DHCP Snooping 테이블에 항목이 생성되지 않습니다. 따라서 DHCP 지원 엔드포인트의 Device-Tracking 항목은 ARP 패킷의 대폭적인 수집에 의해 생성됩니다. 또한 DHCP 스누핑이 비활성화되어 있으므로 "show platform dhcpsnooping client stats" 같은 명령에서는 데이터가 표시되지 않습니다.

<#root>

Edge-1#

show device-tracking database interface te1/0/2 | be Network

```
    Network Layer Address                    Link Layer Address     Interface  vlan       prlvl      ag
```

ARP

172.16.141.1

aaaa.dddd.bbbb

Te1/0/2

1041

0005 45s REACHABLE 207 s try 0

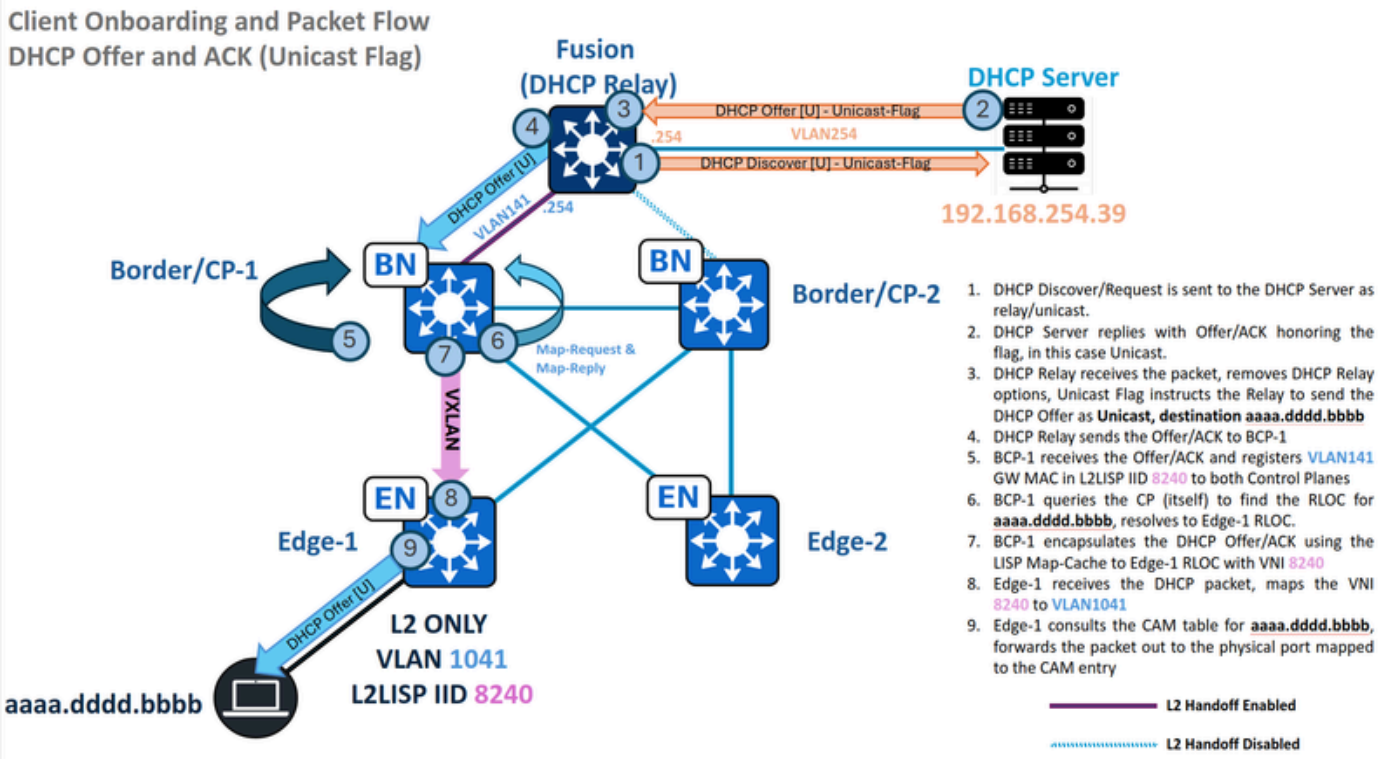
Edge-1#

show ip dhcp snooping binding vlan 1041

```
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
```

Total number of bindings: 0

DHCP 오퍼 및 ACK - 유니캐스트 - L2 경계



트래픽 흐름 - L2에서만 유니캐스트 DHCP 제공 및 ACK

시나리오가 약간 다를 경우 엔드포인트는 DHCP 브로드캐스트 플래그를 unset 또는 "0"으로 설정합니다.

DHCP 릴레이는 DHCP Offer/ACK를 브로드캐스트로 보내지 않고 대신 유니캐스트 패킷으로 DHCP 페이로드 내의 클라이언트 하드웨어 주소에서 파생된 대상 MAC 주소를 보냅니다. 이는 SD-Access 패브릭에서 패킷을 처리하는 방식을 크게 수정하며, L2LISP Map-Cache를 사용하여 트래픽을 전달하지만 Layer 2 Flooding 멀티캐스트 캡슐화 방법은 사용하지 않습니다.

패브릭 보더/CP(192.168.0.201) 패킷 카탈로그: 인그레스 DHCP 오퍼

```
<#root>

BorderCP-1#

show monitor capture cap buffer display-filter "bootp.type==1 and dhcp.hw.mac_addr==aaaa.dddd.bbbb" deta


Dynamic Host Configuration Protocol (

Discover

)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00002030
    Seconds elapsed: 0

    Bootp flags: 0x0000, Broadcast flag (Unicast)
```

```
        0... .... .... .... = Broadcast flag: Unicast


        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0


Client MAC address: aa:aa:dd:dd:bb:bb (aa:aa:dd:dd:bb:bb)
```

이 시나리오에서는 L2 플러딩이 검색/요청에만 사용되는 반면, 제안/ACK는 L2LISP 맵 캐시를 통해 전달되므로 전체 작업이 간소화됩니다. 유니캐스트 포워딩 원칙을 준수하기 위해 L2 Border는 제어 플레인에서 대상 MAC 주소(aaaa.dddd.bbb)를 쿼리합니다. 패브릭 에지에서 "MAC 학습 및 엔드포인트 등록"이 성공하면 컨트롤 플레인에는 이 엔드포인트 ID(EID)가 등록됩니다.

<#root>

```
BorderCP-1#

show

 lisp instance-id 8240 ethernet server aaaa.dddd.bbbb


LISP Site Registration Information
Site name: site_uci
Description: map-server configured from Catalyst Center
Allowed configured locators: any
Requested EID-prefix:
  EID-prefix:

aaaa.dddd.bbbb/48

 instance-id

8240


    First registered:     00:36:37
    Last registered:      00:36:37
    Routing table tag:    0
    Origin:               Dynamic, more specific of any-mac
    Merge active:         No
    Proxy reply:          Yes
    Skip Publication:     No
    Force Withdraw:       No
    TTL:                  1d00h
    State:                complete
    Extranet IID:         Unspecified

    Registration errors:


      Authentication failures:   0


      Allowed locators mismatch: 0
```

ETR 192.168.0.101:51328

, last registered 00:36:37, proxy-reply, map-notify
TTL 1d00h, no merge, hash-function sha1
state complete, no security-capability
nonce 0x1BF33879-0x707E9307
xTR-ID 0xDEF44F0B-0xA801409E-0x29F87978-0xB865BF0D
site-ID unspecified
Domain-ID 1712573701
Multihoming-ID unspecified
sourced by reliable transport

Locator	Local	State	Pri/Wgt	Scope
192.168.0.101	**yes**	**up**	**10/10**	**IPv4 none**

컨트롤 플레인(로컬 또는 원격)에 대한 보더의 쿼리 후 LISP 해상도는 엔드포인트의 MAC 주소에 대한 맵 캐시 항목을 설정합니다.

<#root>

BorderCP-1#

show lisp instance-id 8240 ethernet map-cache aaaa.dddd.bbbb

LISP MAC Mapping Cache for LISP 0 EID-table Vlan

141

(IID

8240

), 1 entries

aaaa.dddd.bbbb/48

, uptime: 4d07h, expires: 16:33:09,

via map-reply

,

complete

, local-to-site
Sources: map-reply
State: complete, last modified: 4d07h, map-source: 192.168.0.206
Idle, Packets out: 46(0 bytes), counters are not accurate (~ 00:13:12 ago)
Encapsulating dynamic-EID traffic

Locator	Uptime	State	Pri/Wgt	Encap-IID
192.168.0.101	4d07h	up	10/10	-

RLOC가 해결되면 DHCP 오퍼가 유니캐스트로 캡슐화되어 VNI 8240을 사용하여 192.168.0.101의 Edge-1로 직접 전송됩니다.

<#root>

BorderCP-1#

show mac address-table address aaaa.dddd.bbbb

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

141

 aaaa.dddd.bbbb

CP_LEARN

L2LI0

BorderCP-1#
show platform software fed switch active matm macTable vlan 141 mac aaaa.dddd.bbbb

VLAN   MAC                  Type  Seq# EC_Bi  Flags  machandle      siHandle        riHandle         di
-------------------------------------------------------------------------------------------------------

141    aaaa.dddd.bbbb
  0x1000001    0      0    64  0x718eb5271228  0x718eb52b4d68  0x718eb52be578   0x0            0     10
 RLOC 192.168.0.101
adj_id 747  No
BorderCP-1#
show ip route 192.168.0.101

Routing entry for 192.168.0.101/32
  Known via "
isis
```

```
", distance 115, metric 20, type level-2
  Redistributing via isis, bgp 65001T
  Advertised by bgp 65001 level-2 route-map FABRIC_RLOC
  Last update from 192.168.98.3 on TenGigabitEthernet1/0/42, 1w3d ago
  Routing Descriptor Blocks:
  * 192.168.98.3, from 192.168.0.101, 1w3d ago,
```

via TenGigabitEthernet1/0/42

```
      Route metric is 20, traffic share count is 1
```

이전 섹션과 동일한 방법론으로 DHCP 릴레이의 인그레스 및 RLOC 이그레스 인터페이스에서 트래픽을 캡처하여 에지 RLOC로의 유니캐스트에서 VXLAN 캡슐화를 관찰합니다.

DHCP 오퍼 및 ACK - 유니캐스트 - 에지

에지는 경계에서 유니캐스트 DHCP Offer/ACK를 수신하고, 트래픽을 캡슐화하고 MAC 주소 테이블을 참조하여 올바른 이그레스 포트를 확인합니다. 브로드캐스트 오퍼/ACK와 달리 에지 노드는 모든 포트에 패킷을 플러딩하지 않고 엔드포인트가 연결된 특정 포트에만 패킷을 전달합니다.

MAC 주소 테이블은 포트 Te1/0/2를 클라이언트 포트로 식별합니다. 이 포트는 STP에 의해 FWD 상태이며 패킷이 엔드포인트로 전달됩니다.

<#root>

Edge-1#

show mac address-table interface te1/0/2

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

1041

aaaa.dddd.bbbb

    DYNAMIC

Te1/0/2

DHCP 오퍼 및 ACK 프로세스는 일관되게 유지됩니다. DHCP Snooping을 활성화하지 않으면 DHCP Snooping 테이블에 항목이 생성되지 않습니다. 따라서 DHCP 지원 엔드포인트에 대한 Device-Tracking 항목은 일반 ARP 패킷에 의해 생성됩니다. 또한 DHCP 스누핑이 비활성화되어 있으므로 "show platform dhcpsnooping client stats" 같은 명령에서는 데이터가 표시되지 않습니다.

<#root>

```
Edge-1#
show device-tracking database interface te1/0/2 | be Network

    Network Layer Address                    Link Layer Address     Interface  vlan       prlvl      ag

ARP


172.16.141.1


 aaaa.dddd.bbbb

       Te1/0/2

1041

       0005       45s        REACHABLE  207 s try 0

Edge-1#
show ip dhcp snooping  binding vlan 1041

MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------

Total number of bindings: 0
```

SD-Access 패브릭은 유니캐스트 또는 브로드캐스트 플래그의 사용에 영향을 주지 않습니다. 이는 단지 엔드포인트 동작이기 때문입니다. 이 기능은 DHCP 릴레이 또는 DHCP 서버 자체에서 재정의할 수 있지만 L2 전용 환경에서 원활한 DHCP 작업을 위해서는 두 가지 메커니즘이 모두 필요합니다. 브로드캐스트 오퍼/ACK에 대한 언더레이 멀티캐스트 및 유니캐스트 오퍼/ACK에 대한 제어 평면에 적절한 엔드포인트 등록을 포함하는 L2 플러딩

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.