Problemen met DHCP oplossen in VLAN met alleen Layer 2 - bekabeld

Inhoud

Inleiding

In dit document wordt beschreven hoe u problemen met DHCP kunt oplossen voor bekabelde eindpunten in een Layer-2 Only-netwerk in SD-Access (SDA)-fabric.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Internet Protocol (IP) Forwarding
- Locator/ID Separation Protocol (LISP)
- Protocol Independent Multicast (PIM) Sparse-modus

Hardware- en softwarevereisten

- Catalyst 9000 Series switches
- Catalyst Center versie 2.3.7.9
- Cisco IOS® XE 10 .12 en hoger

Beperkingen

- Slechts één L2-border kan een uniek VLAN/VNI gelijktijdig overdragen, tenzij robuuste mechanismen voor luspreventie, zoals FlexLink+- of EEM-scripts om koppelingen uit te schakelen, correct zijn geconfigureerd.

Alleen L2 Overzicht

Overzicht

In typische SD-Access-implementaties bevindt de L2/L3-grens zich op de Fabric Edge (FE), waar de FE de gateway van de client host in de vorm van een SVI, die vaak "Anycast Gateway" wordt genoemd. L3 VNI's (Routed) worden ingesteld voor intersubnetverkeer, terwijl L2 VNI's (Switched) intra-subnetverkeer beheren. Consistente configuratie voor alle FE's maakt naadloze clientroaming mogelijk. Forwarding is geoptimaliseerd: intra-subnet (L2) verkeer wordt direct overbrugd tussen FE's en inter-subnet (L3) verkeer wordt gerouteerd tussen FE's of tussen een FE en een Border Node.

Voor eindpunten in SDA-verbindingen waarvoor een strikt netwerktoegangspunt buiten de verbinding vereist is, moet de SDA-structuur een L2-kanaal van de Edge naar een externe gateway bieden.

Dit concept is analoog aan traditionele Ethernet-campusimplementaties waarbij een Layer 2-toegangsnetwerk verbinding maakt met een Layer 3-router. Intra-VLAN-verkeer blijft binnen het L2-netwerk, terwijl inter-VLAN-verkeer wordt gerouteerd door het L3-apparaat, vaak terugkeert naar een ander VLAN op het L2-netwerk.

Binnen een LISP-context volgt het Site Control Plane voornamelijk MAC-adressen en hun bijbehorende MAC-naar-IP-bindingen, net als traditionele ARP-vermeldingen. L2 VNI/L2-only pools zijn ontworpen om registratie, resolutie en doorsturen uitsluitend op basis van deze twee EID-typen te vergemakkelijken. Daarom is elke LISP-gebaseerde forwarding in een L2-only-omgeving uitsluitend afhankelijk van MAC- en MAC-naar-IP-informatie, het negeert IPv4- of IPv6-EID's volledig. Ter aanvulling van LISP EIDs, L2-only zwembaden sterk afhankelijk van overstromingen en leren, vergelijkbaar met het gedrag van de traditionele switches. Bijgevolg L2 Flooding wordt een kritische component voor de behandeling van Broadcast, Unknown Unicast en Multicast (BUM) verkeer binnen deze oplossing, vereist het gebruik van Underlay Multicast. Omgekeerd wordt normaal unicastverkeer doorgestuurd met behulp van standaard LISP-

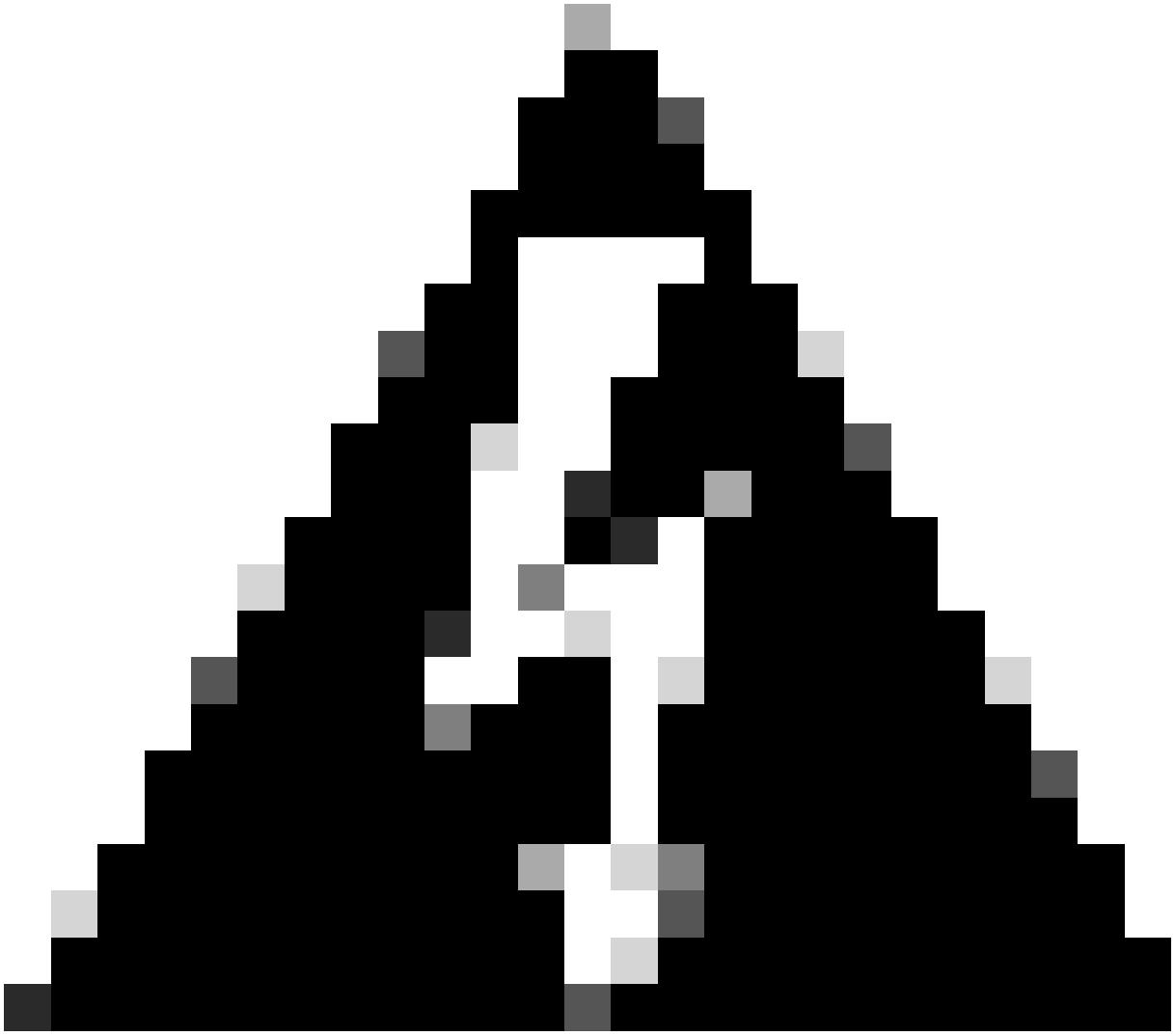
doorstuurprocessen, voornamelijk via Map-Caches.

Zowel de Fabric Edges als de "L2 Border" (L2B) onderhouden L2 VNI's, die worden toegewezen aan lokale VLAN's (deze toewijzing is lokaal apparaatsignificant binnen SDA, waardoor verschillende VLAN's kunnen worden toegewezen aan dezelfde L2 VNI over nodes). In dit specifieke gebruiksgeval is er geen SVI geconfigureerd op deze VLAN's op deze knooppunten, wat betekent dat er geen overeenkomstige L3 VNI is.

DHCP-gedragswijziging in alleen L2-VLAN's

In Anycast Gateway-pools vormt DHCP een uitdaging omdat elke Fabric Edge fungeert als de gateway voor de direct verbonden eindpunten, met dezelfde IP-gateway voor alle FE's. Om de oorspronkelijke bron van een DHCP-gerelateerd pakket correct te identificeren, moeten FE's DHCP Option 82 en de subopties ervan, inclusief de LISP RLOC-informatie, invoegen. Dit wordt bereikt met DHCP-controle op het client-VLAN aan de Fabric Edge. DHCP Snooping dient in dit verband een tweeledig doel: het vergemakkelijkt de invoeging van optie 82 en, van cruciaal belang, voorkomt de overstroming van DHCP-uitzendpakketten over het bridge-domein (VLAN / VNI). Zelfs wanneer Layer-2 Flooding is ingeschakeld voor een Anycast Gateway, onderdrukt DHCP Snooping effectief het broadcast-pakket dat als een uitzending uit de Fabric Edge wordt doorgestuurd.

Een Layer 2 Only VLAN heeft daarentegen geen gateway, wat de identificatie van de DHCP-bron vereenvoudigt. Aangezien pakketten niet worden doorgegeven door een Fabric Edges, zijn complexe mechanismen voor bronidentificatie overbodig. Zonder DHCP Snooping op het L2 Only VLAN wordt het overstromingsbeheersingsmechanisme voor DHCP-pakketten effectief omzeild. Hierdoor kunnen DHCP-uitzendingen via L2 Flooding worden doorgestuurd naar hun eindbestemming, wat een DHCP-server kan zijn die rechtstreeks is aangesloten op een Fabric Node of een Layer 3-apparaat dat DHCP-relayfunctionaliteit biedt.



Waarschuwing: de functionaliteit "Meerdere IP-naar-MAC" binnen een L2 Only-pool activeert automatisch DHCP Snooping in de Bridge VM-modus, die de DHCP-vloedcontrole afdwingt. Hierdoor is de L2 VNI-pool niet in staat om DHCP voor zijn eindpunten te ondersteunen.

onderliggend multicast

Gezien de grote afhankelijkheid van DHCP van uitzendverkeer, moet Layer 2-overstromingen worden ingezet om dit protocol te ondersteunen. Net als bij elke andere L2 Flooding-enabled pool, moet het onderliggende netwerk worden geconfigureerd voor multicast-verkeer, met name Any-Source-Multicast met behulp van PIM Sparse-Mode. Terwijl de onderliggende multicast-configuratie wordt geautomatiseerd via de werkstroom voor LAN-automatisering, is extra configuratie vereist als deze stap is weggelaten (handmatig of sjabloon).

- Schakel IP Multicast Routing in op alle nodes (randen, randen, tussenliggende nodes, enz.).
- Configureer PIM Sparse-Mode op de Loopback0 interface van elke Border and Edge node.
- Schakel PIM Sparse-Mode in op elke IGP-interface (underlay routing protocol).

- Configureer het PIM Rendez-vous Point (RP) op alle knooppunten (Randen, Randen, Tussenknooppunten), RP-plaatsing op Randen wordt aangemoedigd.
- Controleer de status PIM-buren, PIM RP en PIM Tunnel.

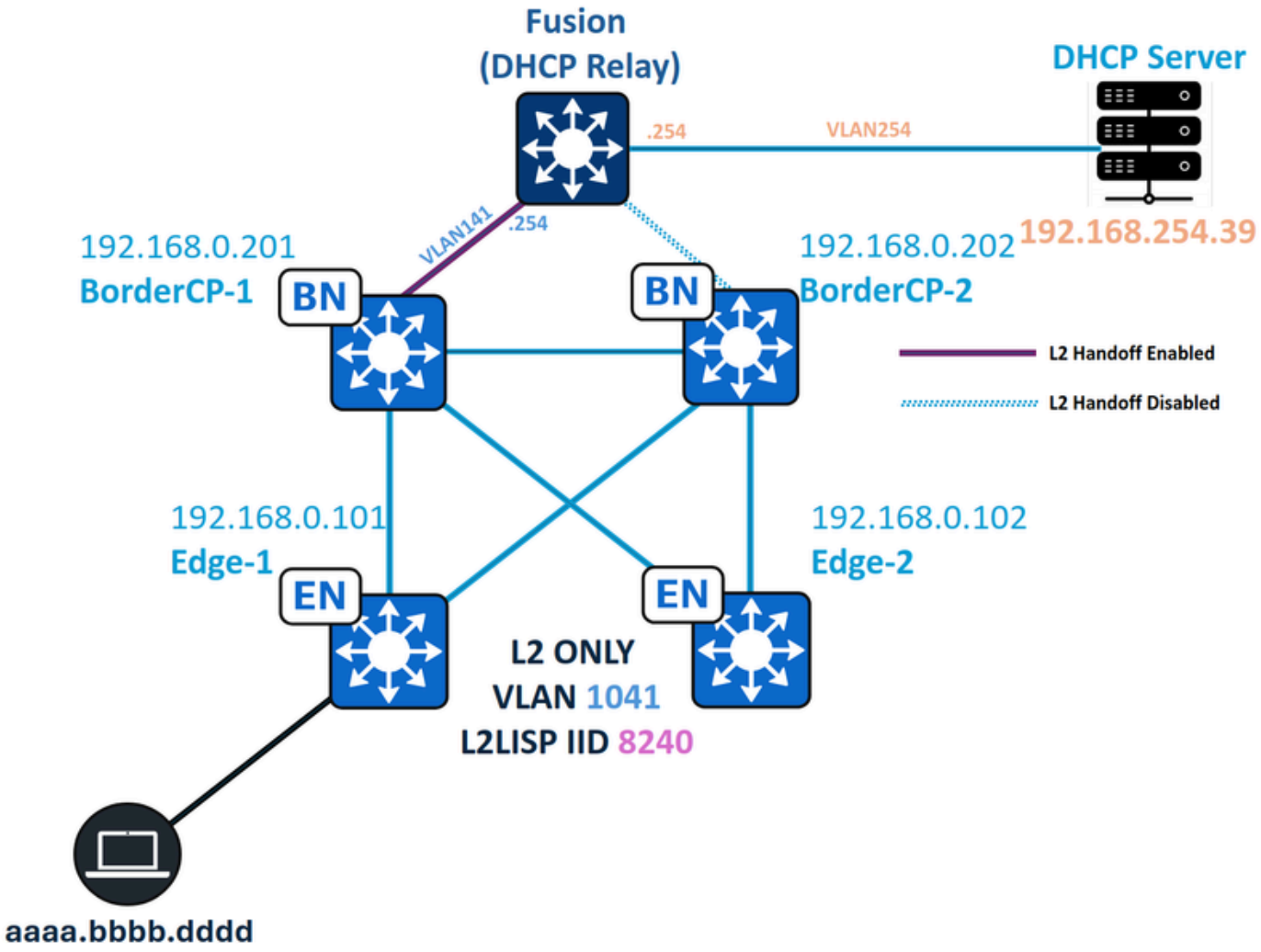
DHCP-server in de SD-Access Fabric

Een veel voorkomende ontwerpvraag is of een DHCP-server kan worden geïmplementeerd binnen een SD-Access-fabric. Het antwoord is in wezen zowel ja als nee.

Het officiële Cisco Validated Design beveelt aan dat de DHCP-server buiten de fabric moet worden geplaatst, meestal binnen het Shared Services-blok. Als de omstandigheden echter vereisen dat de DHCP-server fysiek aan een Fabric Node is gekoppeld (bijvoorbeeld een Edge of Border), is de enige ondersteunde methode via een L2 Only-netwerk. Dit is te wijten aan het inherente gedrag van Anycast Gateway-pools, waar DHCP-snooping standaard is ingeschakeld. Dit blokkeert niet alleen DHCP-aanbiedingen en -bevestigingen van de server, maar voorkomt ook dat DHCP-zoek- en -aanvraagpakketten worden doorgestuurd, zelfs wanneer deze zijn ingekapseld in VXLAN. Hoewel "DHCP Snooping Trust" op DHCP-serverpoorten Aanbiedingen en bevestigingen toestaat, worden Discover- en Request-pakketten niet met dezelfde methode doorgestuurd. Bovendien wordt het verwijderen van DHCP-snooping in een Anycast Gateway-pool niet ondersteund, omdat Catalyst Center een dergelijke configuratieafwijking signaleert tijdens de validatie van de naleving.

Omgekeerd, wanneer de DHCP-server in een L2 Only-netwerk wordt geplaatst, wordt DHCP-snooping niet afgedwongen, waardoor alle DHCP-pakketten kunnen worden doorgegeven zonder op beleid gebaseerde inspectie of blokkering. Het netwerkapparaat stroomopwaarts van de SD-Access-verbinding (bijvoorbeeld een Fusion Router) is geconfigureerd als de gateway voor het L2 Only-netwerk, waardoor verkeer van meerdere VRF's toegang heeft tot dezelfde DHCP-server binnen dat L2 Only-segment.

Topologie



Netwerktopologie

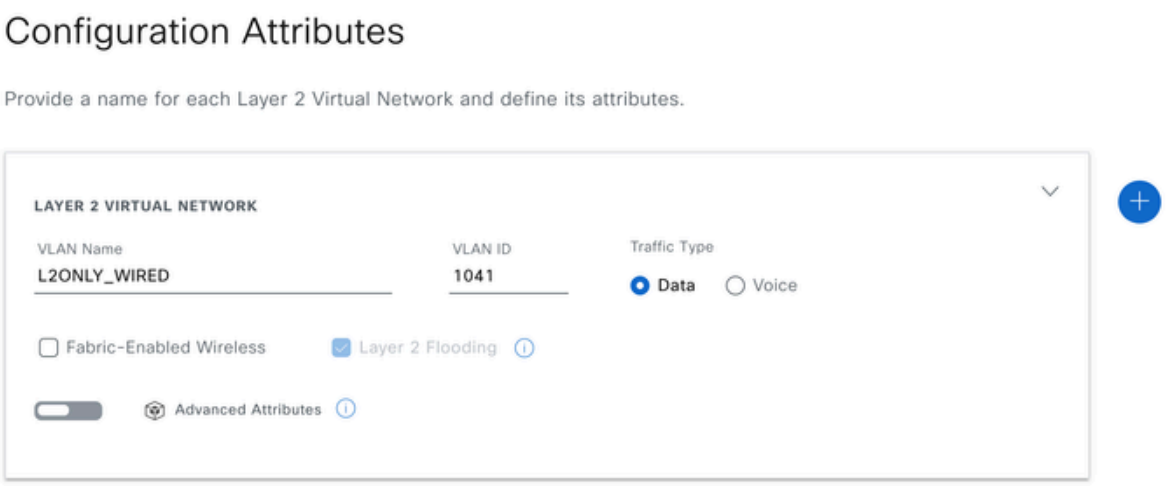
In deze topologie:

- 192.168.0.201 en 192.168.0.202 zijn samengevoegde randen voor de Fabric-site, BorderCP-1 is de enige rand met de Layer 2 Hand-off-functie ingeschakeld.
- 192.168.0.101 en 192.168.0.102 zijn Fabric Edge Nodes
- 192.168.254.39 is de DHCP Server
- aaaa.bbbb.dddd is het voor DHCP geschikte eindpunt
- Het Fusion-apparaat fungeert als DHCP-relais voor de subnetten van de stof.

L2 Alleen VLAN-configuratie

L2 Alleen VLAN-implementatie vanuit Catalyst Center

Pad: Catalyst Center / Provisioning / Fabric Site / Layer 2 Virtual Networks / Bewerken van Layer 2 Virtual Networks



L2VNI-configuratie

L2 Alleen VLAN-configuratie - Fabric-randen

Fabric Edge-nodes hebben het VLAN geconfigureerd met CTS ingeschakeld, IGMP en IPv6 MLD uitgeschakeld en de vereiste L2 LISP-configuratie. Deze L2 Only-pool is geen draadloze pool; daarom zijn functies die doorgaans worden aangetroffen in L2 Only Wireless Pools, zoals RA-Guard, DHCPGuard en Flood Access Tunnel, niet geconfigureerd. In plaats daarvan wordt het overstromen van ARP-pakketten expliciet ingeschakeld met "flood arp-nd"

Configuratie Fabric Edge (192.168.0.101)

<#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

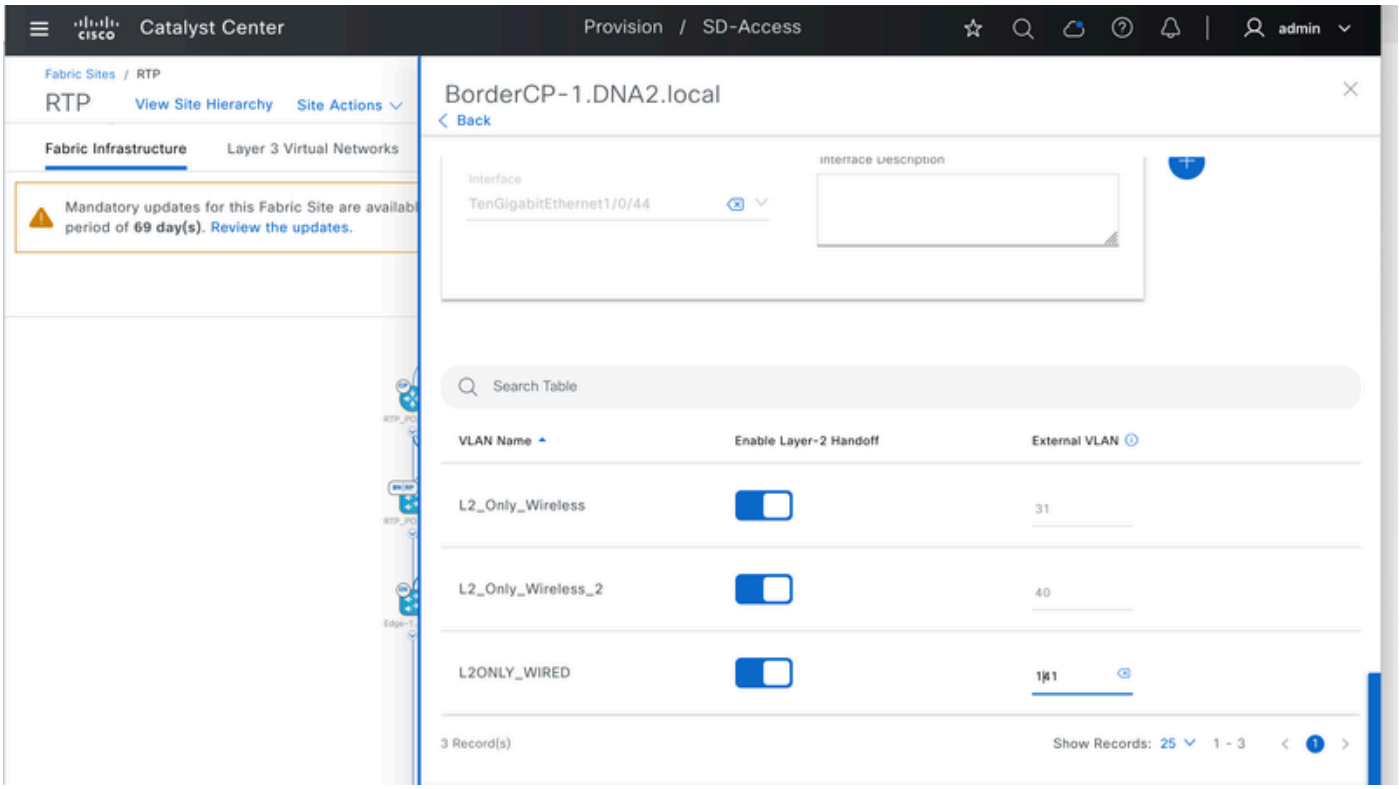
```
router lisp
 instance-id
8240
  remote-rloc-probe on-route-change
  service ethernet
eid-table vlan
1041
   broadcast-underlay
239.0.17.1
flood arp-nd
 flood unknown-unicast
   database-mapping mac locator-set rloc_91947dad-3621-42bd-ab6b-379ecebb5a2b
   exit-service-ethernet
```

L2 Hand-off Configuratie - Fabric Border

Vanuit een operationeel perspectief is het toegestaan om de DHCP-server (of Router/Relay) aan te sluiten op elke Fabric Node, inclusief zowel Borders als Edges.

Het gebruik van Border-nodes om verbinding te maken met de DHCP-server wordt aanbevolen, maar vereist zorgvuldige ontwerpoverweging. Dit komt omdat de rand moet worden geconfigureerd voor L2 Hand-Off op een per-interface basis. Hierdoor kan de Fabric Pool worden overgedragen aan hetzelfde VLAN als binnen de Fabric of aan een ander VLAN. Deze flexibiliteit in VLAN-ID's tussen Fabric Edges en Borders is mogelijk omdat beide zijn toegewezen aan dezelfde L2 LISP Instance-ID. L2 Hand-off fysieke poorten mogen niet tegelijkertijd worden ingeschakeld met hetzelfde VLAN om Layer 2-lussen binnen het SD-Access-netwerk te voorkomen. Voor redundantie zijn methoden zoals StackWise Virtual, FlexLink+ of EEM-scripts vereist.

Voor het aansluiten van de DHCP-server of gatewayrouter op een Fabric Edge is daarentegen geen extra configuratie vereist.



L2 Hand-off-configuratie

Configuratie van verbindingsrand (192.168.0.201)

<#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

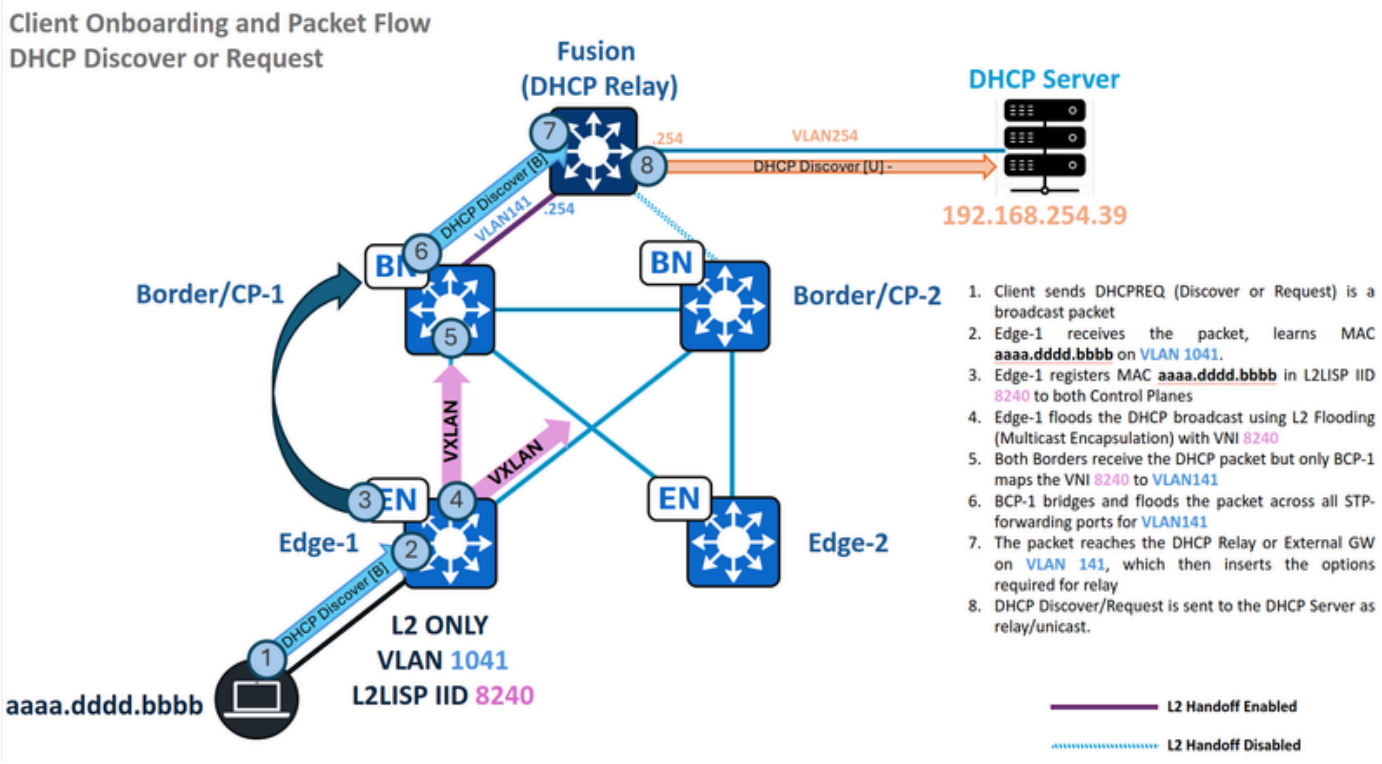
no ipv6 mld snooping vlan 141

```
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-verkeersstroom

DHCP ontdekken en aanvragen - Edge



Verkeersstroom - DHCP ontdekken en aanvragen alleen in L2

MAC Learning en Endpoint Registratie

Wanneer endpoint aaaa.dddd.bbbb een DHCP Discover of Request (een broadcast-pakket) verzendt, moet de Edge-node het MAC-adres van het eindpunt leren, het toevoegen aan de MAC-adrestabel, vervolgens aan de L2/MAC SISF-tabel en ten slotte aan de L2LISP-database voor VLAN 1041, toegewezen aan L2LISP Instance 8240.

<#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
```

Als het MAC-adres van het eindpunt correct is aangeleerd en de ACK-vlag is gemarkeerd als "Ja" voor de Fabric Control-vlakken, wordt deze fase als voltooid beschouwd.

DHCP Broadcast Bridged in L2 Flooding

Wanneer DHCP-snooping is uitgeschakeld, worden DHCP-uitzendingen niet geblokkeerd; in plaats daarvan worden ze ingekapseld in multicast voor Layer 2-overstromingen. Omgekeerd voorkomt het inschakelen van DHCP Snooping het overstromen van deze uitzendpakketten.

<#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>
```

Aangezien DHCP-controle is uitgeschakeld, maakt de DHCP Discover/Request gebruik van de

L2LISP0-interface, waarmee verkeer via L2 Flooding wordt overbrugd. Afhankelijk van de Catalyst Center-versie en de toegepaste Fabric Banners kan de L2LISP0-interface toegangslijsten in beide richtingen hebben geconfigureerd; zorg er daarom voor dat DHCP-verkeer (UDP-poorten 67 en 68) niet expliciet wordt geweigerd door toegangscontrole-items (ACE's).

<#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

Gebruik de geconfigureerde broadcast-underlay-groep voor de L2LISP-instantie en het Loopback0 IP-adres van de Fabric Edge om het item L2 Flooding (S, G) te verifiëren waarmee dit pakket naar andere Fabric-knooppunten wordt overbrugd. Raadpleeg de mroute- en mfib-tabellen om parameters zoals de inkomende interface, uitgaande interfacelijst en doorstuurtellers te valideren.

<#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:

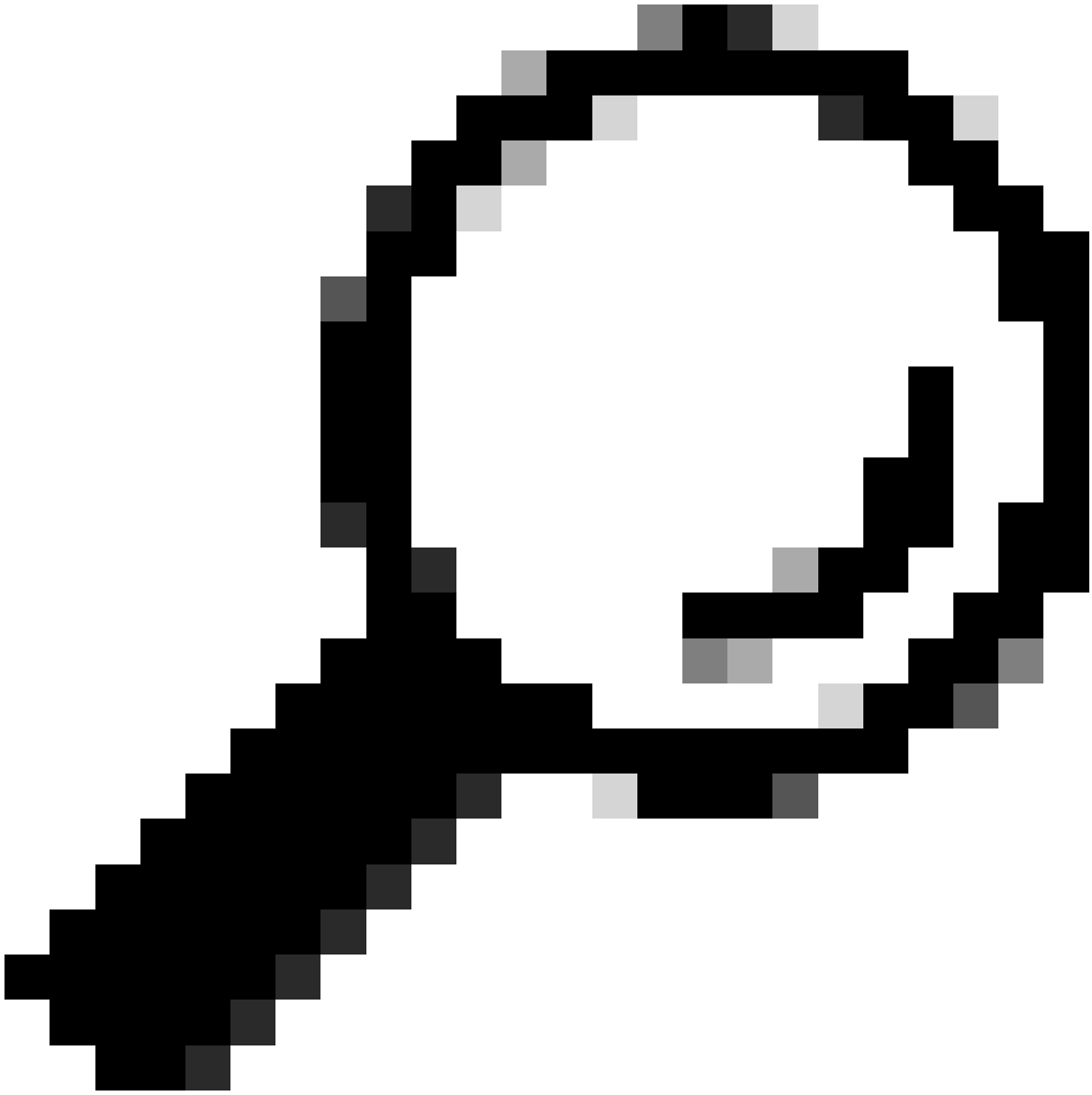
 7

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

<--

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

  Totals - Source count: 1, Packet count: 8



Tip: als een item (S, G) niet wordt gevonden of als de lijst Uitgaande interface (OIL) geen uitgaande interfaces (OIF's) bevat, duidt dit op een probleem met de onderliggende multicast-configuratie of -bewerking.

Packet Captures

Configureer een gelijktijdige ingesloten pakketopname op de switch om zowel het inkomende DHCP-pakket van het eindpunt als het bijbehorende uitgangspakket voor L2 Flooding op te nemen. Bij het vastleggen van pakketten moeten twee afzonderlijke pakketten worden waargenomen: de originele DHCP Discover/Request en de VXLAN-ingekapselde tegenhanger, bestemd voor de Underlay Group (239.0.17.1).

Fabric Edge (192.168.0.101) pakketopnames

<#root>

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 ontdekken en aanvragen - L2-grens

Nadat de Edge de DHCP Discover- en Request-pakketten via Layer 2 Flooding heeft verzonden, ingekapseld in de Broadcast-Underlay-groep 239.0.17.1, worden deze pakketten ontvangen door de L2 Hand-off Border, met name Border/CP-1 in dit scenario.

Om dit te laten gebeuren, moet Border/CP-1 een multicast-route hebben met de (S, G) van de Edge en moet de lijst met uitgaande interfaces de L2LISP-instantie van het L2 Handoff VLAN bevatten. Het is belangrijk op te merken dat L2 Hand-off Borders dezelfde L2LISP Instance-ID delen, zelfs als ze verschillende VLAN's gebruiken voor de Hand-off.

<#root>

BorderCP-1#

show vlan id 141

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

141 L2ONLY_WIRED

active

    L2LI0:

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

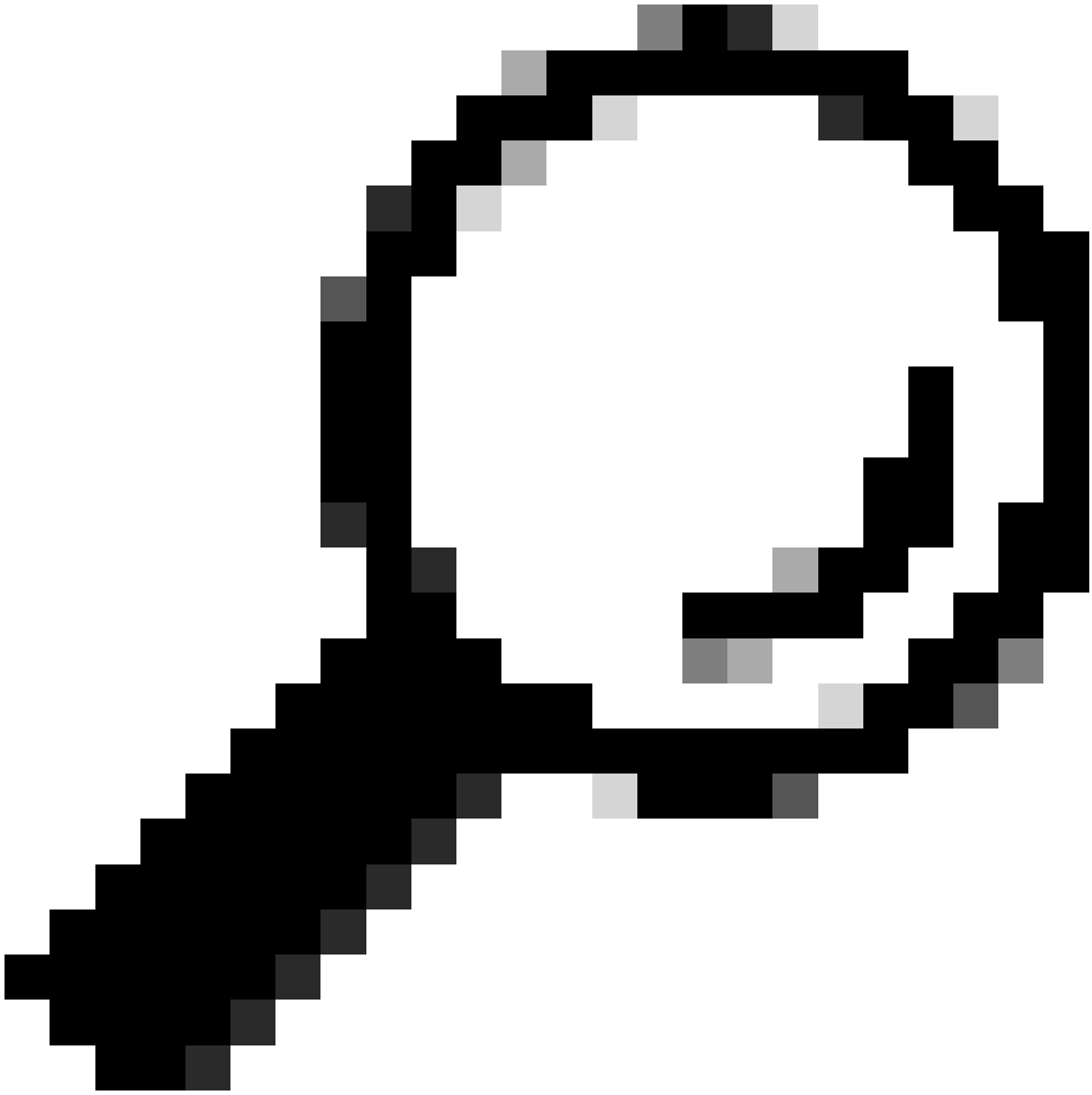
,
   SW Forwarding: 1/0/392/0, Other: 0/0/0
   HW Forwarding:

3

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

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

  Totals - Source count: 1, Packet count: 4



Tip: Als een item (S, G) niet wordt gevonden, duidt dit op een probleem met de onderliggende multicastconfiguratie of -bewerking. Als de L2LISP voor de vereiste instantie niet aanwezig is als OIF, duidt dit op een probleem met de status UP/DOWN van de L2LISP-subinterface of de IGMP-machtigingsstatus van de L2LISP-interface.

Net als bij de Fabric Edge-node moet u ervoor zorgen dat geen toegangscontrole-invoer het gehele DHCP-pakket op de L2LISP0-interface ontkent.

<#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
```

Nadat het pakket is gedecapsuleerd en op het VLAN is geplaatst dat overeenkomt met VNI 8240, dicteert de uitzendaard dat het alle Spanning Tree Protocol-doorstuurpoorten voor hand-off VLAN 141 uitstroomt.

```
<#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
```

De Device-Tracking tabel bevestigt dat interface Te1/0/44, die verbinding maakt met de Gateway/DHCP Relay, een STP-doorstuurpoort moet zijn.

```
<#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
```

Packet Captures

Configureer een gelijktijdige ingesloten pakketopname op de switch om zowel het inkomende DHCP-pakket van L2 Flooding (S, G inkomende interface) als het bijbehorende uitgangspakket naar de DHCP-relais op te nemen. Bij het vastleggen van pakketten moeten twee afzonderlijke pakketten worden waargenomen: het VXLAN-ingekapselde pakket van Edge-1 en het de-ingekapselde pakket dat naar de DHCP-relais gaat.

Fabric Border/CP (192.168.0.201) pakketopnames

<#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

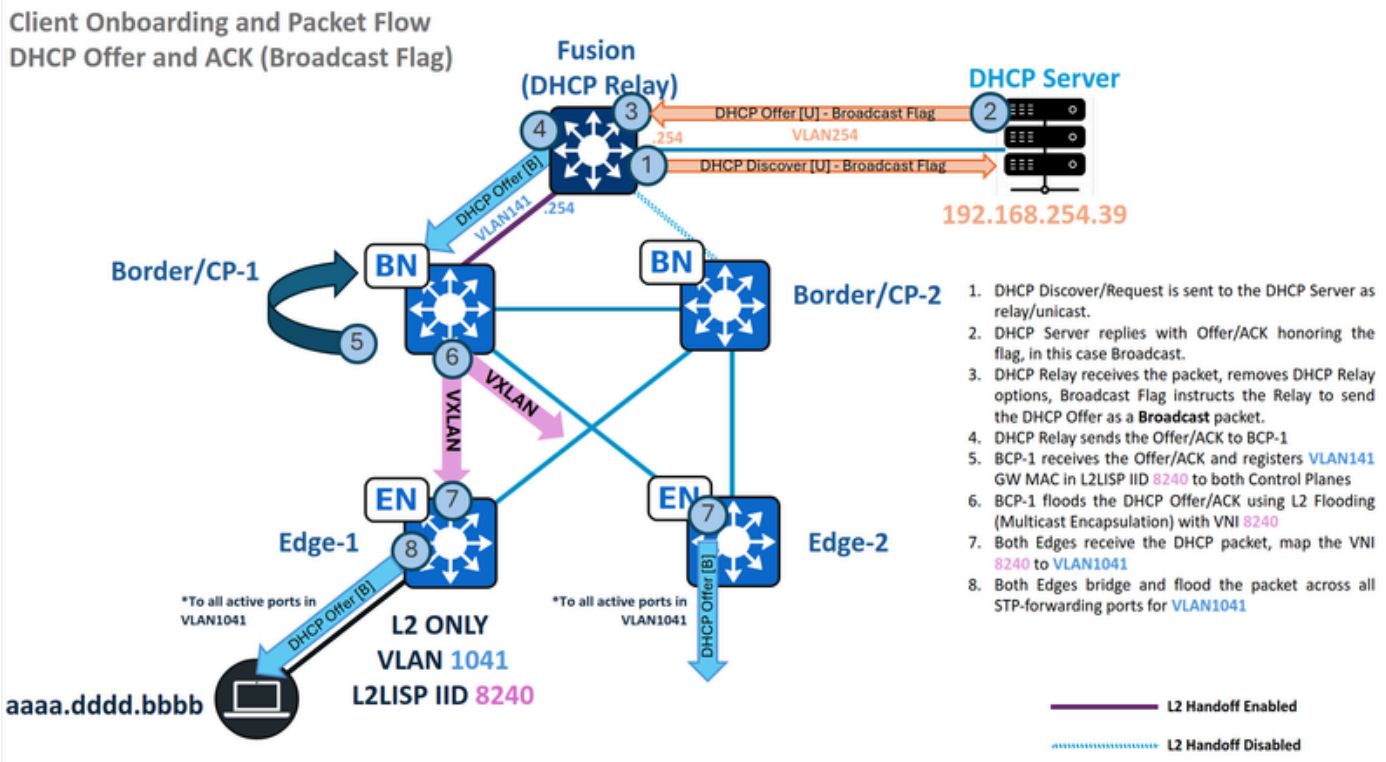
Packet 428: Plain (dot1Q cannot be captured at egress direction)

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-aanbieding en ACK - Uitzending - L2-grens



Verkeersstroom - Uitzending DHCP-aanbieding en ACK alleen in L2

Nu de DHCP Discover de SD-Access-verbinding heeft verlaten, voegt het DHCP-relais traditionele DHCP-relaisopties in (bijv. GiAdr / GatewayIPAaddress) en stuurt het pakket door als een unicasttransmissie naar de DHCP-server. In deze stroom voegt de SD-Access-verbinding geen speciale DHCP-opties toe.

Wanneer een DHCP Discover/Request naar de server wordt verzonden, wordt de vlag van de geïntegreerde Broadcast of Unicast door de server in acht genomen. Deze vlag bepaalt of de DHCP Relay Agent het DHCP-aanbod doorstuurt naar het downstream-apparaat (onze grenzen) als een broadcast- of unicastframe. Voor deze demonstratie wordt uitgegaan van een uitzendscenario.

MAC Learning en Gateway Registratie

Wanneer het DHCP-relais een DHCP-aanbieding of ACK verzendt, moet de L2BN-node het MAC-adres van de gateway leren, deze toevoegen aan de MAC-adrestabel, vervolgens aan de L2/MAC SISF-tabel en ten slotte aan de L2LISP-database voor VLAN 141, toegewezen aan L2LISP-instantie 8240.

<#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
```

Als het MAC-adres van de gateway correct is aangeleerd en de ACK-vlag is gemarkeerd als "Ja" voor de Fabric Control-vlakken, wordt deze fase als voltooid beschouwd.

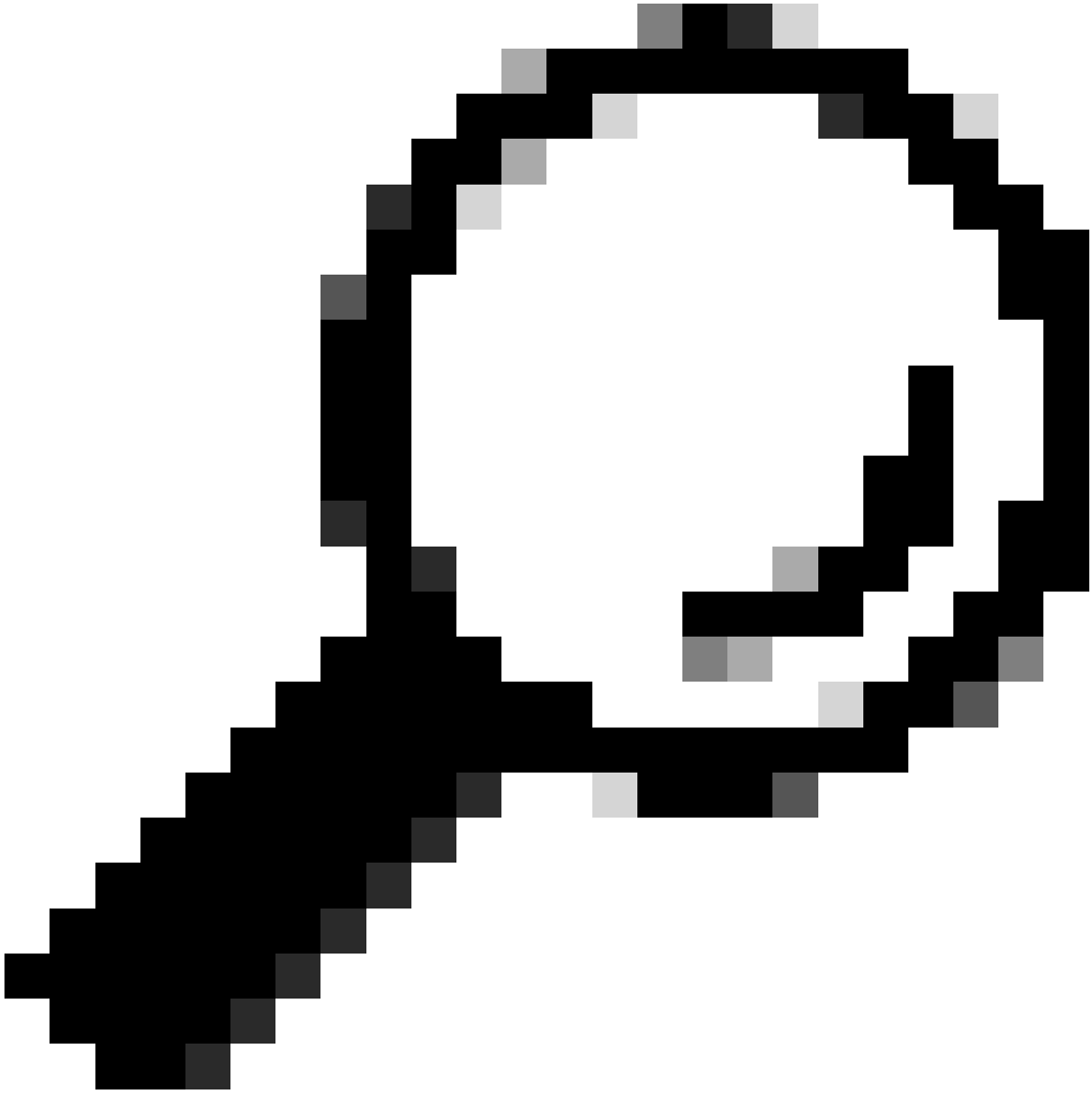
DHCP Broadcast Bridged in L2 Flooding

Zonder DHCP Snooping ingeschakeld, worden DHCP-uitzendingen niet geblokkeerd en zijn ingekapseld in multicast voor Layer 2-overstromingen. Omgekeerd, als DHCP Snooping is ingeschakeld, wordt de stroom van DHCP Broadcast-pakketten voorkomen.

<#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



Tip: omdat DHCP-snooping niet is ingeschakeld in de L2Border, is de configuratie van DHCP-snooping Trust niet nodig.

In dit stadium wordt L2LISP ACL-validatie al uitgevoerd in beide apparaten.

Gebruik de geconfigureerde broadcast-underlay-groep voor de L2LISP-instantie en het IP-adres L2Border Loopback0 om het item L2 Flooding (S, G) te verifiëren dat dit pakket overbrugt naar andere Fabric-knooppunten. Raadpleeg de mroute- en mfib-tabellen om parameters zoals de

inkomende interface, uitgaande interfacelijst en doorstuurtellers te valideren.

<#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

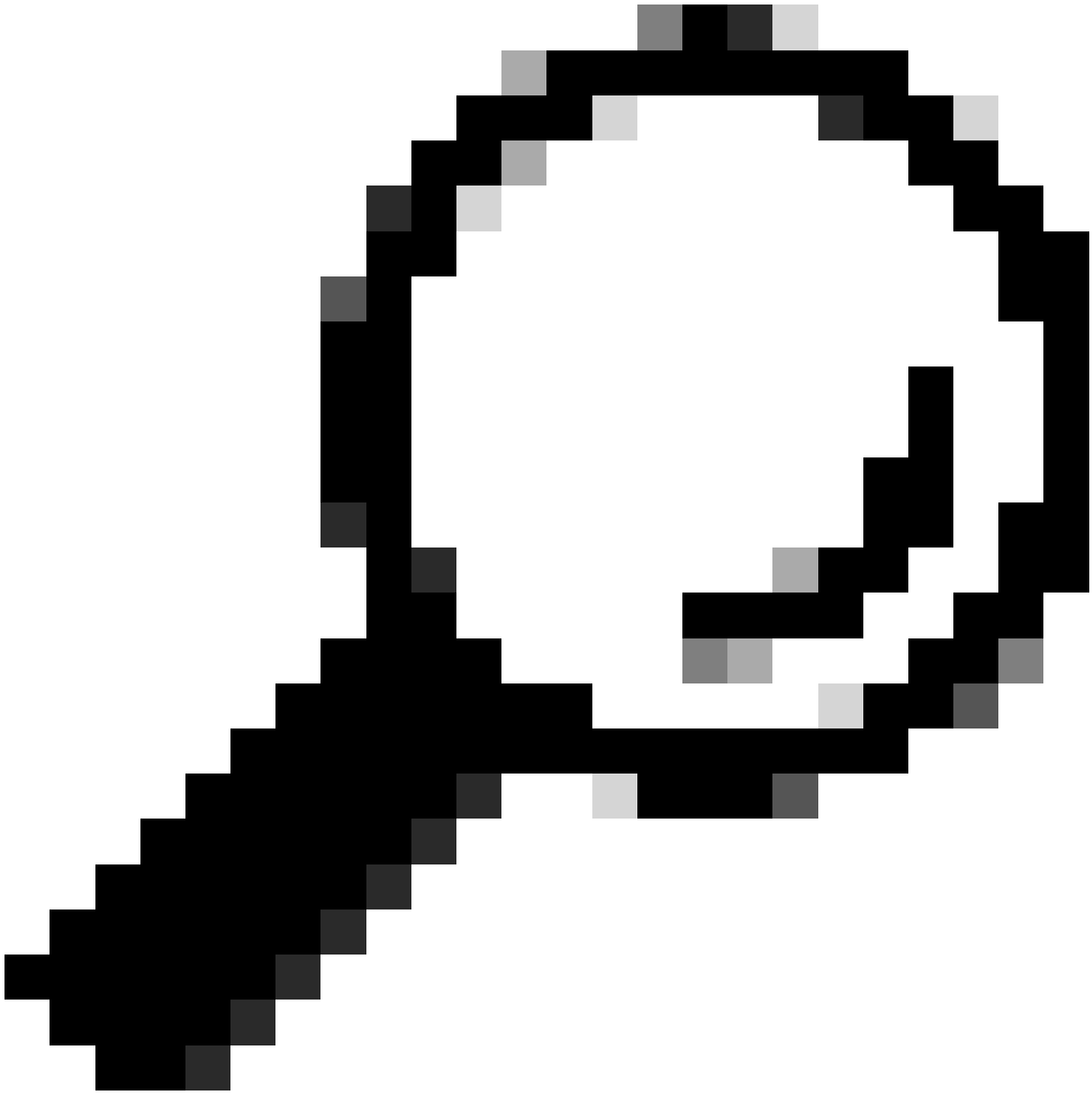
,
SW Forwarding: 1/0/392/0, Other: 1/1/0
HW Forwarding:

92071

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

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

Totals - Source count: 1, Packet count: 92071



Tip: als een item (S, G) niet wordt gevonden of als de lijst Uitgaande interface (OIL) geen uitgaande interfaces (OIF's) bevat, duidt dit op een probleem met de onderliggende multicast-configuratie of -bewerking.

Met deze validaties, samen met pakketopnames vergelijkbaar met de vorige stappen, wordt deze sectie afgesloten, omdat de DHCP-aanbieding wordt doorgestuurd als een uitzending naar alle Fabric Edges met behulp van de inhoud van de uitgaande interfacelijst, in dit geval uit de interface TenGig1/0/42 en TenGig1/0/43.

DHCP-aanbieding en ACK - Uitzending - Edge

Controleer net als de vorige stroom de L2Border S, G in de Fabric Edge, waar de inkomende interface naar de L2BN wijst en de OIL de L2LISP-instantie bevat die is toegewezen aan VLAN 1041.

<#root>

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,

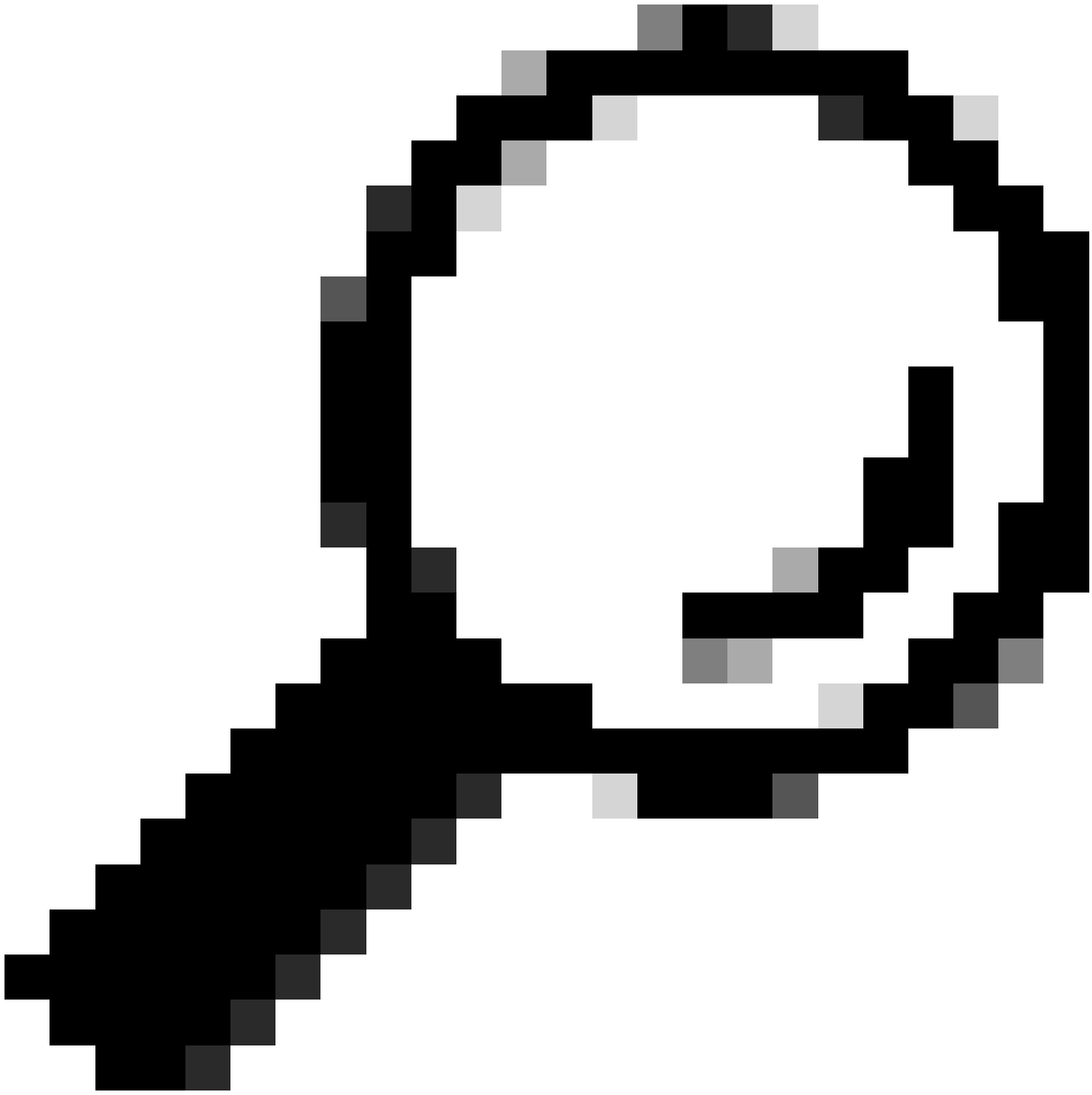
   SW Forwarding: 1/0/96/0, Other: 0/0/0
   HW Forwarding:

76236

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

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

  Totals - Source count: 1, Packet count: 4



Tip: Als een item (S, G) niet wordt gevonden, duidt dit op een probleem met de onderliggende multicastconfiguratie of -bewerking. Als de L2LISP voor de vereiste instantie niet aanwezig is als OIF, duidt dit op een probleem met de status UP/DOWN van de L2LISP-subinterface of de IGMP-machtigingsstatus van de L2LISP-interface.

L2LISP ACL-validatie is al uitgevoerd in beide apparaten.

Nadat het pakket is gedecapsuleerd en op het VLAN is geplaatst dat overeenkomt met VNI 8240, dicteert de uitzendaard dat het alle Spanning Tree Protocol-doorstuurpoorten voor VLAN1041 uitstroomt.

<#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

De MAC-adrestabel identificeert poort Te1/0/2 als de eindpuntpoort, die in FWD-status is door STP, het pakket wordt overstroomd naar het eindpunt.

<#root>

Edge-1#

show mac address-table interface te1/0/2

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

1041

aaaa.dddd.bbbb

DYNAMIC

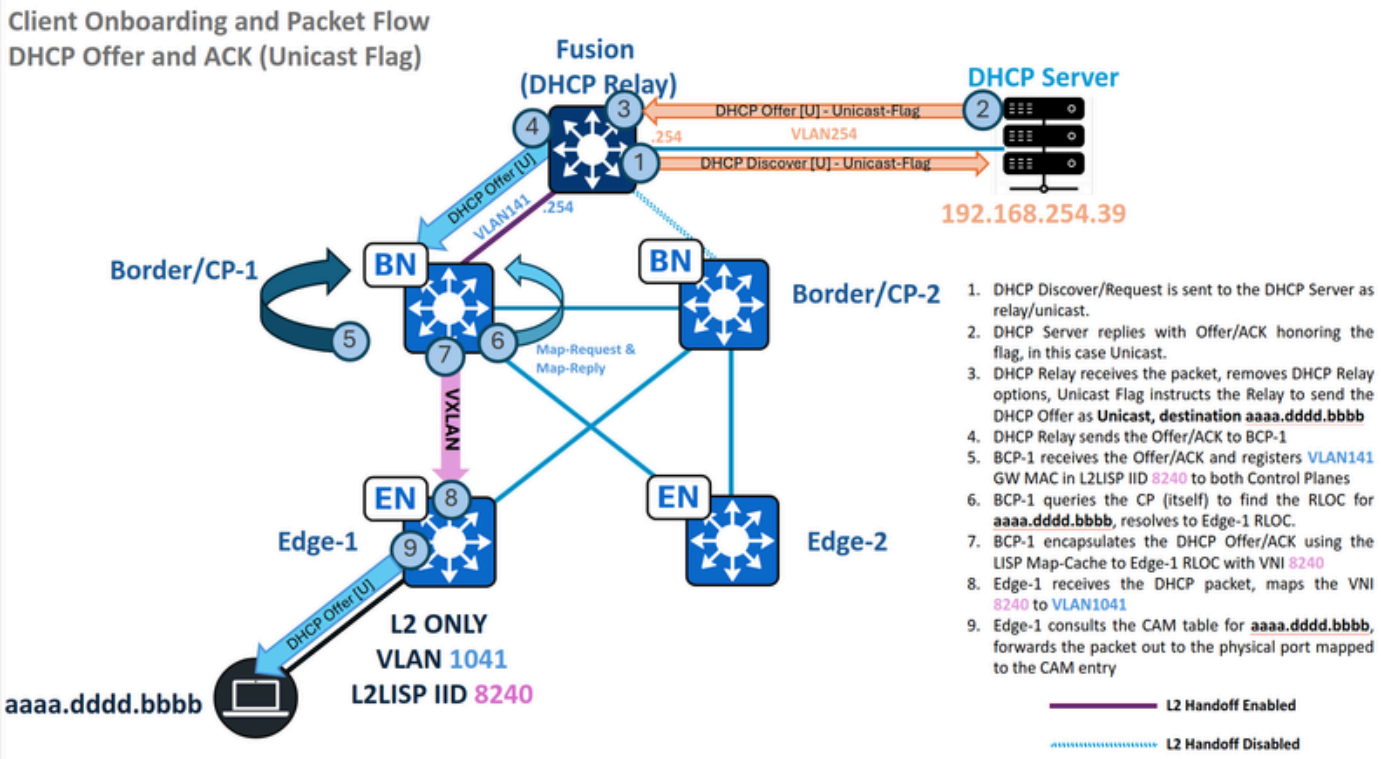
Te1/0/2

Het DHCP-aanbod en het ACK-proces blijven consistent. Zonder dat DHCP-snooping is ingeschakeld, worden er geen items gemaakt in de DHCP-snooptabel. Bijgevolg wordt de vermelding Device-Tracking voor het DHCP-enabled eindpunt gegenereerd door de verzameling van ARP-pakketten. Het is ook te verwachten dat opdrachten zoals "show platform dhcpsnooping client stats" geen gegevens weergeven, omdat DHCP-snooping is uitgeschakeld.

<#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-aanbieding en ACK - Unicast - L2-rand



Verkeersstroom - Unicast DHCP-aanbieding en ACK alleen in L2

Hier is het scenario een beetje anders, het eindpunt stelt de DHCP Broadcast Flag in als unset of "0".

De DHCP-relais verzendt de DHCP-aanbieding/ACK niet als uitzending, maar als een unicastpakket, met een MAC-adres voor de bestemming dat is afgeleid van het hardwareadres van de client in de DHCP-payload. Dit verandert drastisch de manier waarop het pakket wordt behandeld door de SD-Access-fabric, het gebruikt de L2LISP Map-Cache om het verkeer door te sturen, niet de Layer 2 Flooding multicast-inkapselingsmethode.

Fabric Border/CP (192.168.0.201) pakketopname: Ingress DHCP-aanbieding

<#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)
```

In dit scenario wordt L2 Flooding uitsluitend gebruikt voor Discover/Requests, terwijl Aanbiedingen/ACK's worden doorgestuurd via L2LISP Map-Caches, waardoor de algemene werking wordt vereenvoudigd. De L2-grens houdt zich aan de unicast-doorstuurprincipes en zoekt in het controlevlak naar het MAC-adres van de bestemming (aaaa.dddd.bbbb). Ervan uitgaande dat "MAC Learning and Endpoint Registration" op de Fabric Edge succesvol is, heeft het Control Plane deze Endpoint ID (EID) geregistreerd.

<#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
```

Na de vraag van de Rand naar het Control Plane (lokaal of extern), stelt de LISP-resolutie een Map-Cache-vermelding in voor het MAC-adres van het eindpunt.

```
<#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        -
```

Als het RLOC is opgelost, wordt de DHCP-aanbieding ingekapseld in unicast en rechtstreeks naar Edge-1 verzonden op 192.168.0.101, met behulp van VNI 8240.

<#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
```

Met dezelfde methodologie als in de vorige secties legt u verkeer vast dat binnenkomt vanuit het DHCP-relais en naar de RLOC-interface om de VXLAN-inkapseling in unicast naar de Edge RLOC te observeren.

DHCP-aanbieding en ACK - Unicast - Edge

De Edge ontvangt de unicast DHCP Offer/ACK van de Border, ontkapselt het verkeer en raadpleegt de MAC-adrestabel om de juiste uitgang te bepalen. In tegenstelling tot broadcast Offer/ACK's stuurt de Edge-node het pakket alleen door naar de specifieke poort waar het eindpunt is aangesloten, in plaats van het naar alle poorten te laten stromen.

De MAC-adrestabel identificeert poort Te1/0/2 als onze clientpoort, die in FWD-status is door STP, het pakket wordt doorgestuurd naar het eindpunt.

```
<#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
```

Het DHCP-aanbod en het ACK-proces blijven consistent. Zonder dat DHCP-snooping is

ingeschakeld, worden er geen items gemaakt in de DHCP-snooptabel. Bijgevolg wordt de vermelding Device-Tracking voor het DHCP-enabled eindpunt gegenereerd door de ARP-pakketten. Het is ook te verwachten dat opdrachten zoals "show platform dhcpsnooping client stats" geen gegevens weergeven, omdat DHCP-snooping is uitgeschakeld.

<#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

Het is van cruciaal belang op te merken dat de SD-Access-fabric geen invloed heeft op het gebruik van de Unicast- of Broadcast-vlag, omdat dit alleen een eindpuntgedrag is. Hoewel deze functionaliteit kan worden overschreven door de DHCP-relais of de DHCP-server zelf, zijn beide mechanismen essentieel voor een naadloze werking van DHCP in een L2 Only-omgeving: L2 Flooding met Underlay Multicast voor uitzendaanbiedingen / ACK's en een juiste registratie van het eindpunt in het controlevlak voor Unicast-aanbieding / ACK's.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.