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

Inhoud

- Inleiding
- Voorwaarden
  - Vereisten
- Alleen L2 Overzicht
  - Overzicht
  - DHCP-gedragswijziging in alleen L2-VLAN's
  - onderliggend multicast
  - uitzending via toegangstunnelinterfaces
- Topologie
- L2 Alleen VLAN-configuratie
  - L2 Alleen VLAN-implementatie vanuit Catalyst Center
  - L2 Alleen VLAN-configuratie - Fabric-randen
  - L2 Alleen VLAN-configuratie - Draadloze LAN-controller
  - L2 Hand-off-configuratie (verbindingsrand)
  - Draadloze multicast inschakelen
- DHCP-verkeersstroom
  - DHCP ontdekken en aanvragen - draadloze kant
  - DHCP ontdekken en aanvragen - Fabric Edge
    - MAC-leren met behulp van WLC-melding
    - DHCP Broadcast Bridged in L2 Flooding
    - Packet Captures
  - DHCP ontdekken en aanvragen - L2-grens
    - Packet Captures
  - DHCP-aanbieding en ACK - Uitzending - L2-grens
    - MAC Learning en Gateway Registratie
    - DHCP Broadcast Bridged in L2 Flooding
  - DHCP-aanbieding en ACK - Uitzending - Edge
  - DHCP-aanbieding en ACK - Unicast - L2-rand
  - DHCP-aanbieding en ACK - Unicast - Edge
  - DHCP-transactie - Draadloze verificatie

Inleiding

In dit document wordt beschreven hoe problemen met DHCP voor draadloze eindpunten in een Layer-2 Only-netwerk in SD-Access (SDA)-fabric kunnen worden opgelost.

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
- Draadloze verbinding ingeschakeld

Hardware- en softwarevereisten

- Catalyst 9000 Series switches
- Catalyst Center versie 2.3.7.9
- Catalyst 9800-reeks draadloze LAN-controllers
- Toegangspunten voor de Catalyst 9100-reeks
- 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

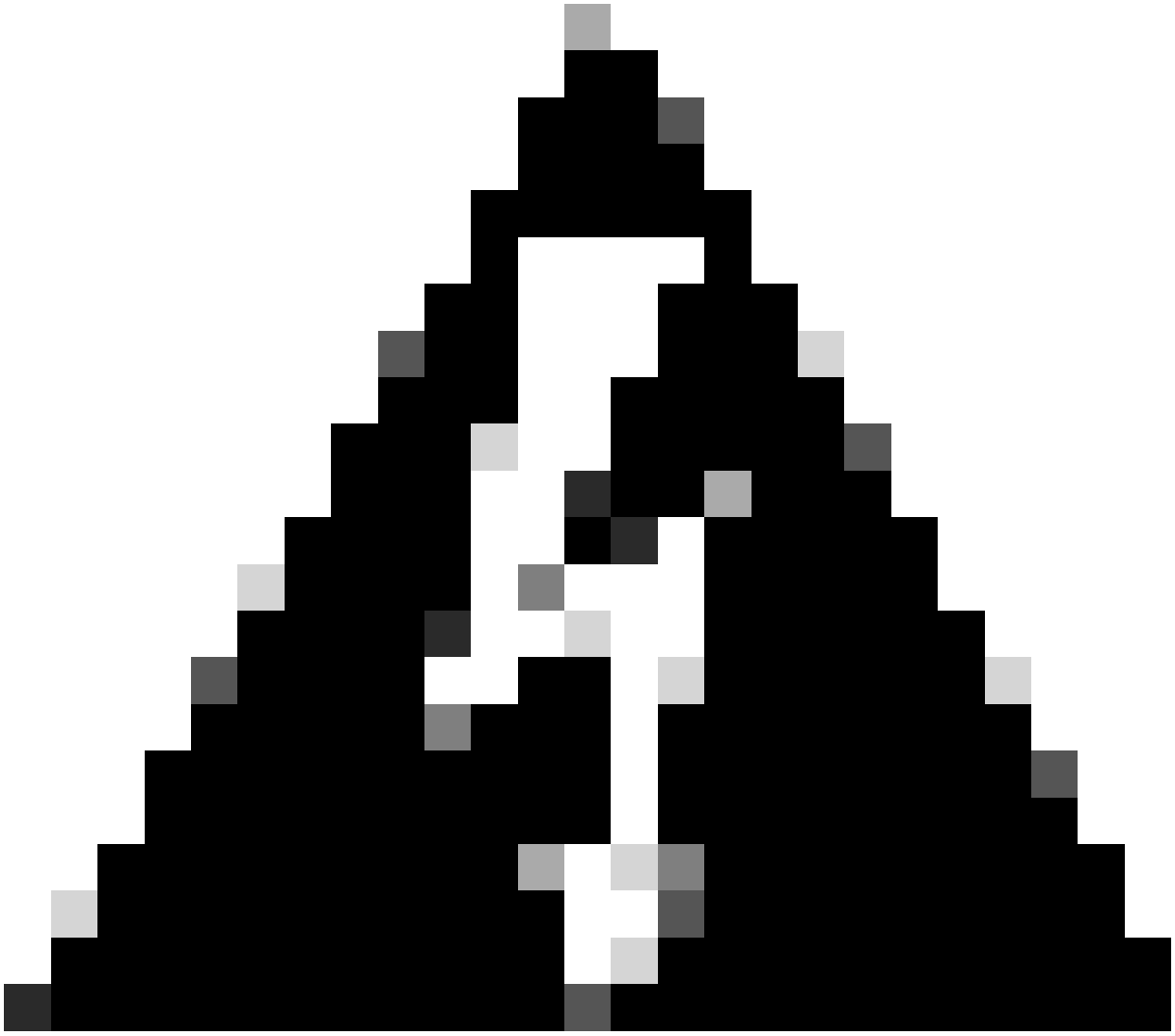
bijbehorende MAC-naar-IP-bindingen, net als traditionele ARP-vermeldingen. L2 VNI/L2-only pools zijn ontworpen om registratie, resolutie en doorsturen uitsluitend op basis van deze twee EID-typen te vergemakkelijken. Daarom is elke LISP-gebaseerde forwarding in een L2-only-omgeving uitsluitend afhankelijk 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).

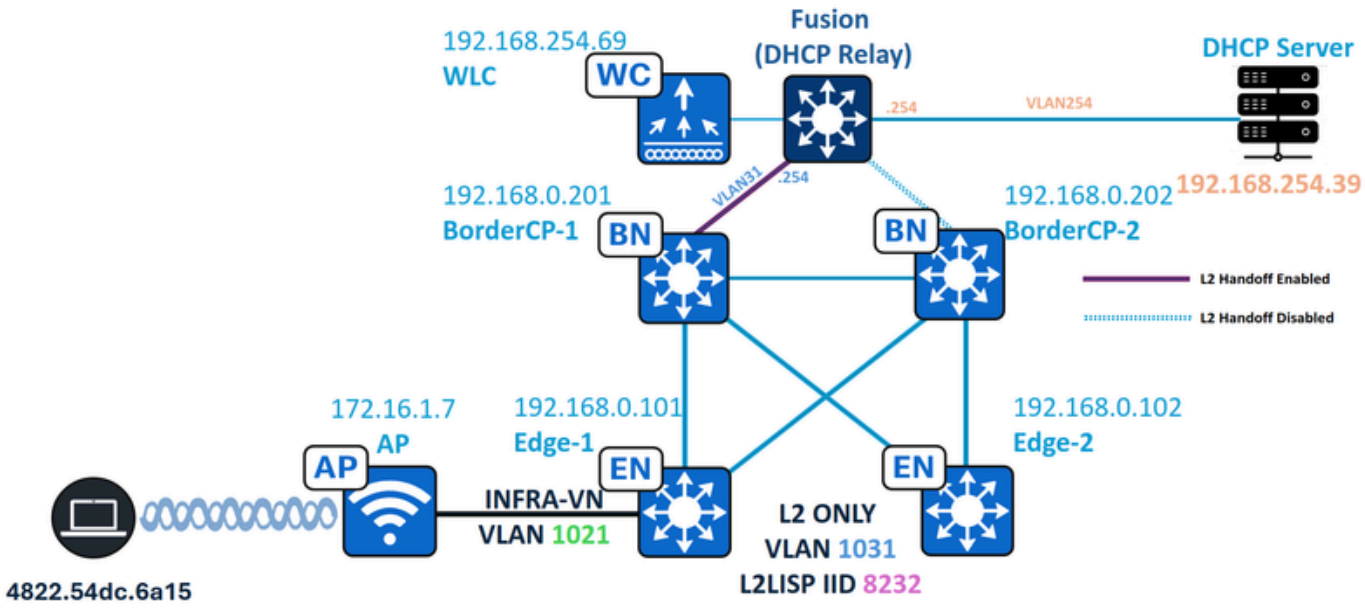
- Schakel IP Multicast Routing in op alle nodes (randen, randen, tussenliggende nodes, enz.).
- Configureer PIM Sparse-Mode op de Loopback0 interface van elke Border and Edge node.
- Schakel PIM Sparse-Mode in op elke IGP-interface (underlay routing protocol).

- 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.

uitzending via toegangstunnelinterfaces

Fabric Enabled Wireless maakt gebruik van lokale switching- en VTEP-functionaliteit op het toegangspunt en de FE. Een beperking van IOS-XE 10 .10+ voorkomt echter dat uitzendingen via VXLAN naar AP's worden doorgestuurd. In L2 Only-netwerken blokkeert dit DHCP Offers/ACK's om draadloze clients te bereiken. De functie "flood access-tunnel" pakt dit aan door broadcast-forwarding op Fabric Edge-toegangstunnelinterfaces mogelijk te maken.

Topologie



Netwerktopologie

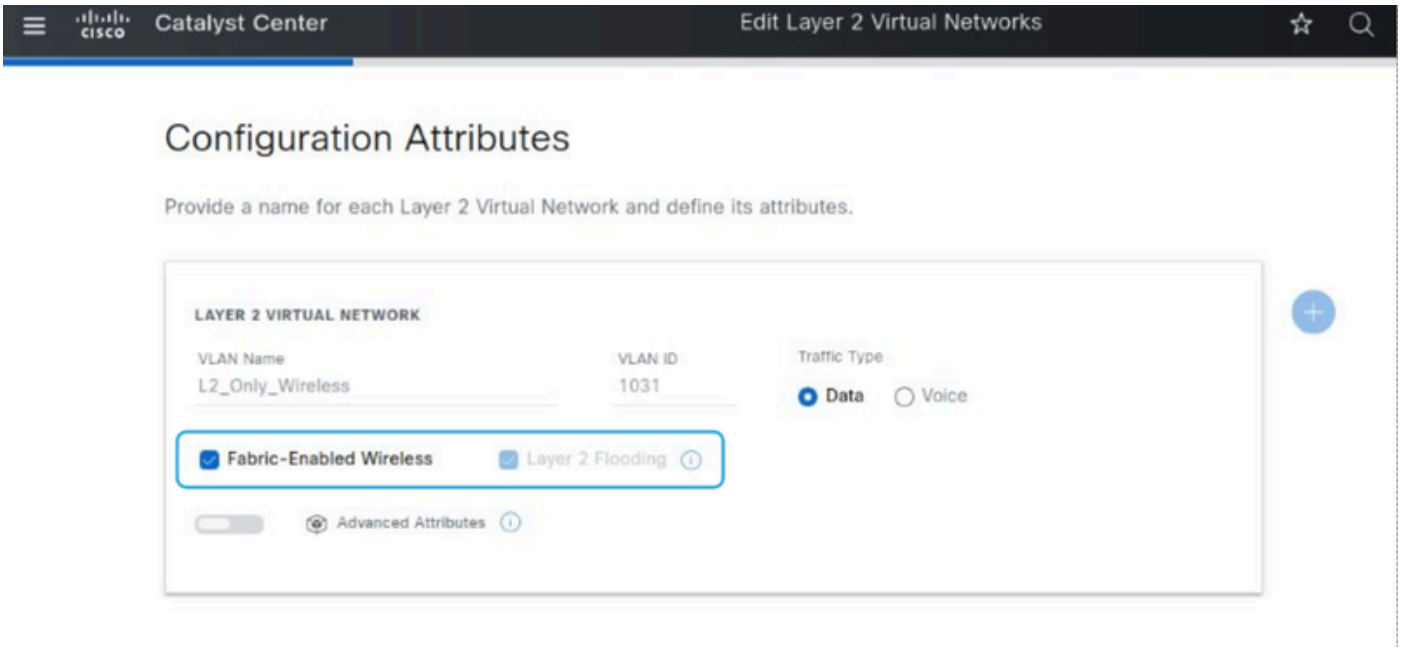
In deze topologie:

- 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
- 172.16.1.7 is het toegangspunt in INFRA-VN met VLAN 1021
- 192.168.254.39 is de DHCP Server
- 192.168.254.69 is de draadloze LAN-controller
- 4822.54dc.6a15 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 met draadloze verbinding

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 een draadloze pool; daarom zijn functies die doorgaans worden aangetroffen in L2 Only Wireless Pools, zoals RA-Guard, DHCPGuard en Flood Access Tunnel, geconfigureerd. ARP Flooding is niet ingeschakeld in een draadloze pool.

Configuratie Fabric Edge (192.168.0.101)

<#root>

```
ipv6 nd raguard policy
```

dnac-sda-permit-nd-raguardv6

```
 device-role router
ipv6 dhcp guard policy
```

dnac-sda-permit-dhcpv6

```
 device-role server

vlan configuration
```

1031

```
 ipv6 nd raguard attach-policy
```

dnac-sda-permit-nd-raguardv6

```
 ipv6 dhcp guard attach-policy
dnac-sda-permit-dhcpv6


cts role-based enforcement vlan-list
1031

vlan
1031


name L2_Only_Wireless



ip igmp snooping querier
no ip igmp snooping vlan 1031 querier


no ip igmp snooping vlan 1031


no ipv6 mld snooping vlan 1031



router lisp


 instance-id
8240


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


 eid-table vlan 1031



 broadcast-underlay 239.0.17.1


   flood unknown-unicast
   flood access-tunnel 232.255.255.1 vlan 1021


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

De tunnelopdracht voor vloedtoegang is geconfigureerd in de multicast-replicatievariatie, waarbij al het BUM-verkeer wordt ingekapseld in toegangspunten met behulp van de bronspecifieke multicastgroep (232.255.255.1) met behulp van het INFRA-VN Access Point VLAN als het VLAN dat wordt geraadpleegd door IGMP-snuffelaars om het BUM-verkeer door te sturen.

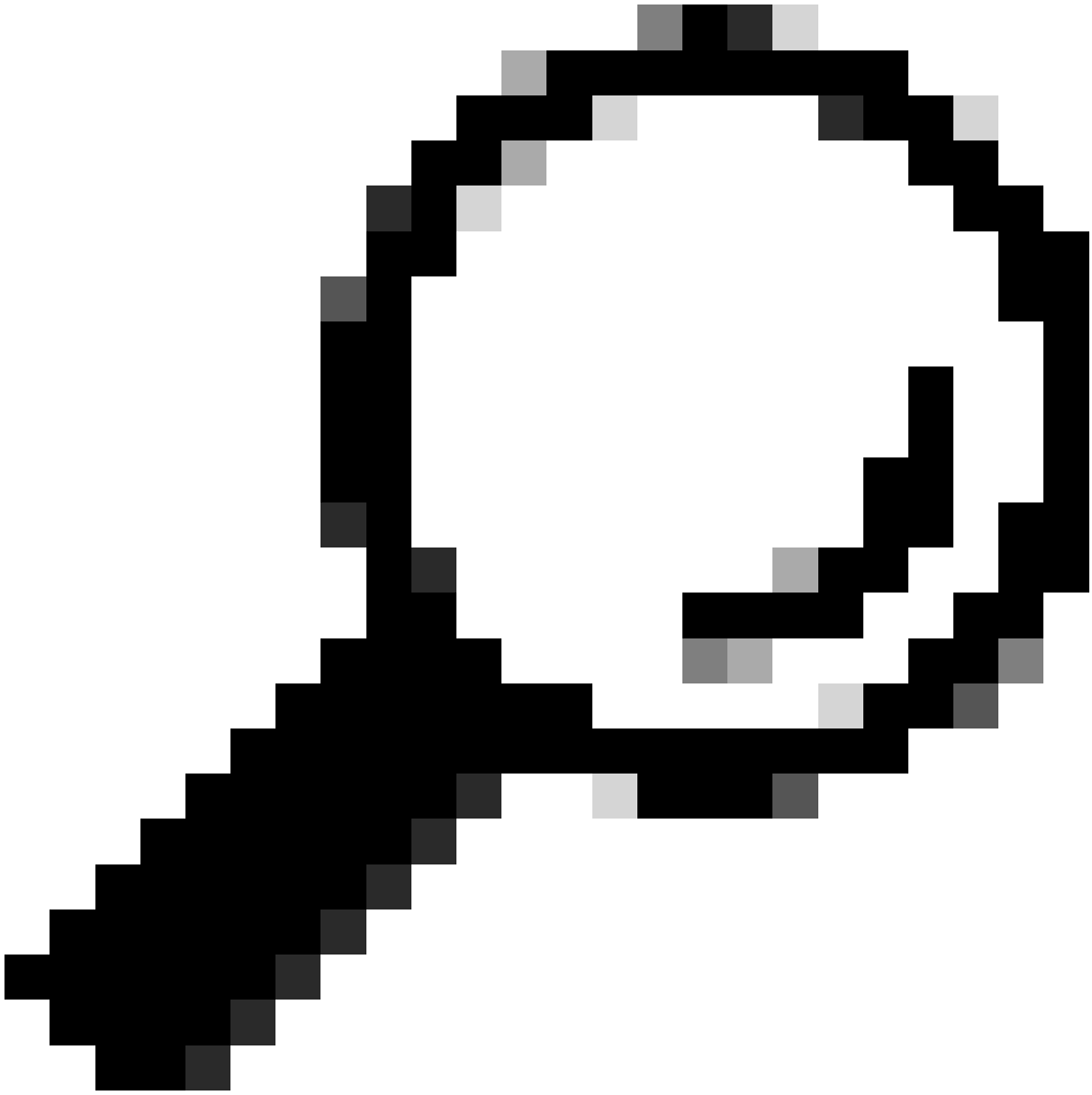
L2 Alleen VLAN-configuratie - Draadloze LAN-controller

Aan de kant van de WLC (Wireless LAN Controller) moeten sitetags die zijn gekoppeld aan fabric-toegangspunten worden geconfigureerd met "geen fabric ap-arp-caching" om de proxy-ARP-functionaliteit uit te schakelen. Bovendien moet "fabric ap-dhcp-broadcast" zijn ingeschakeld. Met deze configuratie kunnen DHCP-broadcast-pakketten worden doorgestuurd van het toegangspunt naar draadloze eindpunten.

Fabric WLC-configuratie (192.168.254.69)

<#root>

```
wireless tag site RTP-Site-Tag-3
 description "Site Tag RTP-Site-Tag-3"

 no fabric ap-arp-caching
 fabric ap-dhcp-broadcast
```



Tip: De draadloze multicastgroep 232.255.255.1 is de standaardgroep die wordt gebruikt door alle site-tags.

<#root>

```
WLC#
show wireless tag site detailed RTP-Site-Tag-3

Site Tag Name        :
 RTP-Site-Tag-3

Description          : Site Tag RTP-Site-Tag-3
---------------------------------------
AP Profile           : default-ap-profile
```

```
Local-site           : Yes
Image Download Profile: default
Fabric AP DHCP Broadcast :
```

Enabled

```
Fabric Multicast Group IPv4 Address :
```

232.255.255.1

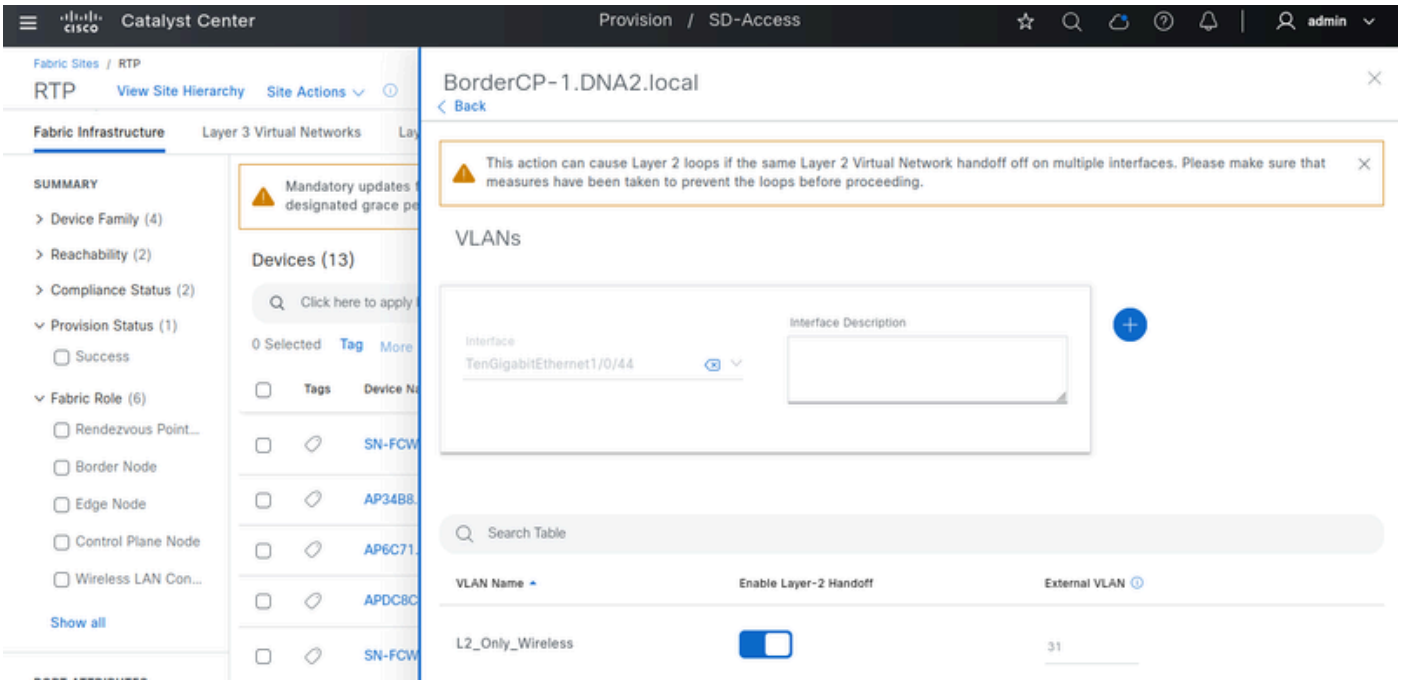
```
RTP-Site-Tag-3 Load : 0
```

L2 Hand-off-configuratie (verbindingsrand)

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 verbindingsrand/CP (192.168.0.201)

<#root>

```
ipv6 nd raguard policy
dnac-sda-permit-nd-raguardv6

 device-role router
ipv6 dhcp guard policy
dnac-sda-permit-dhcpv6

 device-role server
vlan configuration
3
1

 ipv6 nd raguard attach-policy
dnac-sda-permit-nd-raguardv6

 ipv6 dhcp guard attach-policy
dnac-sda-permit-dhcpv6


cts role-based enforcement vlan-list
31

vlan
3


1


name L2_Only_Wireless



ip igmp snooping querier
no ip igmp snooping vlan 1031 querier


no ip igmp snooping vlan 1031


no ipv6 mld snooping vlan 1031
```

```
router lisp

 instance-id
8240

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

 eid-table vlan 31



 broadcast-underlay 239.0.17.1


   flood unknown-unicast
   flood access-tunnel 232.255.255.1 vlan 1021

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

interface TenGigabitEthernet1/0/44



switchport mode trunk
<--

DHCP Relay/Server interface
```

Draadloze multicast inschakelen

Fabric Edges zijn geconfigureerd om broadcast-pakketten door te sturen naar toegangspunten via het mechanisme van de toegangstunnel voor overstromingen. Deze pakketten zijn ingekapseld in de 232.255.255.1 multicast-groep op het INFRA-VN VLAN. Toegangspunten worden automatisch lid van deze multicast-groep, omdat hun site-tag vooraf is geconfigureerd om deze te gebruiken.

```
<#root>
WLC#
show ap name AP1 config general | i Site

Site Tag Name                                 :
RTP-Site-Tag-3
```

```
WLC#
show wireless tag site detailed RTP-Site-Tag-3


Site Tag Name        :
RTP-Site-Tag-3


Description          : Site Tag RTP-Site-Tag-3
---------------------------------------
AP Profile           : default-ap-profile
Local-site           :
 Yes


Image Download Profile: default
Fabric AP DHCP Broadcast :
Enabled


Fabric Multicast Group IPv4 Address :
 232.255.255.1


RTP-Site-Tag-3 Load : 0
```

Vanaf het toegangspunt wordt na de koppeling van een draadloos verbindingseindpunt een VXLAN-tunnel gevormd (dynamisch aan de AP-zijde, altijd aan de Fabric Edge-zijde). Binnen deze tunnel wordt de CAPWAP-fabric multicastgroep geverifieerd met opdrachten van de AP-terminal.

<#root>

```
AP1#
show ip tunnel fabric


Fabric GWs Information:
Tunnel-Id         GW-IP            GW-MAC        Adj-Status Encap-Type  Packet-I
n   Bytes-In Packet-Out Bytes-out
        1
192.168.0.101
 00:00:0C:9F:F2:BC
Forward


 VXLAN
111706302
```

```
6 1019814432 1116587492 980205146
AP APP Fabric Information:
GW_ADDR ENCAP_TYPE VNID SGT FEATURE_FLAG GW_SRC_MAC GW_DST_MAC

AP1#
```

show capwap mcast

```
IPv4 Multicast:
Vlan      Group IP Version      Query Timer   Sent QRV left Port
   0
```

232.255.255.1

```
       2 972789.691334200 140626        2    0
```

Bevestig aan de kant van Fabric Edge dat IGMP-snooping is ingeschakeld voor het INFRA-VN AP VLAN, de toegangspunten hebben een toegangstunnelinterface gevormd en ze zijn toegetreden tot de multicastgroep 232.255.255.1

<#root>

```
Edge-1#
```

show ip igmp snooping vlan 1021 | i IGMP

```
Global IGMP Snooping configuration:
IGMP snooping                :
```

Enabled

```
IGMPv3 snooping              :
```

Enabled

```
IGMP snooping                      :
```

Enabled

```
IGMPv2 immediate leave             : Disabled
CGMP interoperability mode         : IGMP_ONLY

Edge-1#
```

show ip igmp snooping groups vlan

1021 232.255.255.1

```
Vlan      Group                    Type        Version     Port List
------------------------------------------------------------------------
```

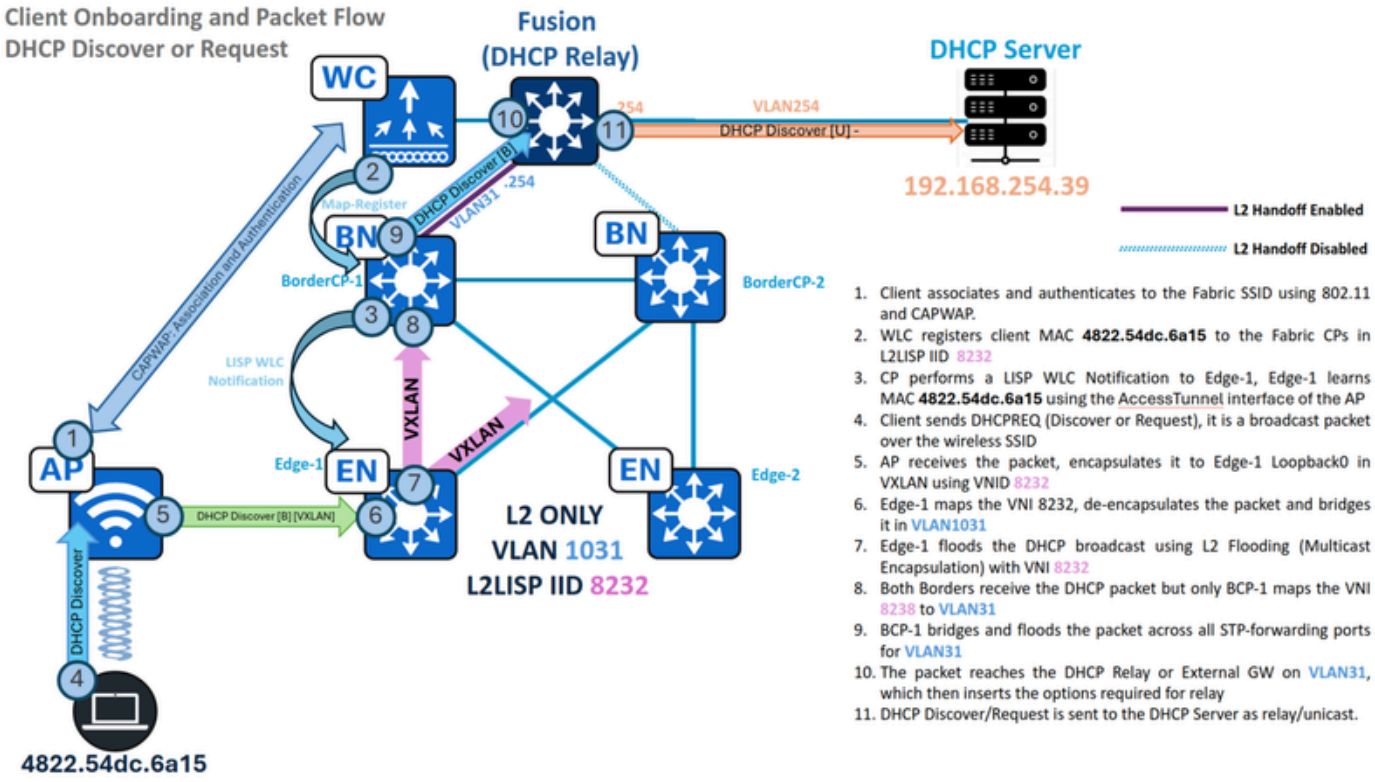
1021 232.255.255.1

```
          igmp        v2

 Te1/0/12   ----- Access Point Port


Edge-1#

show device-tracking database interface te1/0/12 | be Network


   Network Layer Address                    Link Layer Address
Interface  vlan       prlvl      age        state      Time left


DH4 172.16.1.7

                            dc8c.3756.99bc

Te1/0/12   1021

      0024       1s         REACHABLE  251 s(76444 s)
Edge-1#

show access-tunnel summary


Access Tunnels General Statistics:
  Number of AccessTunnel Data Tunnels       = 1
Name    RLOC IP(Source)  AP IP(Destination)  VRF ID  Source Port  Destination Port
------  ---------------  ------------------  ------  -----------  ----------------


Ac2



192.168.0.101



172.16.1.7

       0       N/A          4789
<snip>
```

Deze verificaties bevestigen de succesvolle activering van draadloze multicast voor de Access Point, Fabric Edge en Wireless LAN Controller.

DHCP-verkeersstroom

DHCP ontdekken en aanvragen - draadloze kant



Verkeersstroom - DHCP ontdekken en aanvragen alleen in L2

Identificeer de status van het draadloze eindpunt, het aangesloten toegangspunt en de bijbehorende fabric-eigenschappen.

<#root>

```
WLC#
show wireless client summary | i MAC|-|4822.54dc.6a15

MAC Address    AP Name                                          Type ID   State            Protocol Meth
-------------------------------------------------------------------------------------------------------

4822.54dc.6a15

AP1

                              WLAN

17

Run

               11n(2.4) MAB        Local

WLC#
show wireless client mac 4822.54dc.6a15 detail | se AP Name|Policy Profile|Fabric

AP Name:
```

```
AP1

Policy Profile :
RTP_POD1_SSID_profile

Fabric status :
Enabled

  RLOC    :
192.168.0.101

  VNID    :
8232

  SGT     : 0
  Control plane name  :
default-control-plane
```

Het is belangrijk om te bevestigen dat zowel centrale-switching als centrale-dhcp-functies zijn uitgeschakeld in het beleidsprofiel. De opdrachten "geen centrale dhcp" en "geen centrale switching" moeten worden geconfigureerd in het beleidsprofiel voor de SSID.

```
<#root>
WLC#
show wireless profile policy detailed RTP_POD1_SSID_profile | i Central

  Flex Central Switching            : DISABLED

  Flex Central Authentication       : ENABLED

 Flex Central DHCP                 : DISABLED

  VLAN based Central Switching      : DISABLED
```

Deze verificaties bevestigen dat het eindpunt is verbonden met "AP1", dat is gekoppeld aan de Fabric Edge RLOC 192.168.0.101. Bijgevolg wordt het verkeer ingekapseld via VXLAN met VNID 8232 voor overdracht van het toegangspunt naar de Fabric Edge.

DHCP ontdekken en aanvragen - Fabric Edge

MAC-leren met behulp van WLC-melding

Tijdens de onboarding van het eindpunt registreert de WLC het MAC-adres van het draadloze eindpunt met het Fabric Control Plane. Tegelijkertijd waarschuwt het Control Plane de Fabric Edge-node (waarmee het toegangspunt is verbonden) om een speciaal "CP_LEARN" MAC-leeritem te maken, wijzend naar de toegangstunnelinterface van het toegangspunt.

<#root>

Edge-1#

show lisp session

Sessions for VRF default, total: 2, established: 2
Peer State Up/Down In/Out Users

192.168.0.201:4342 Up

2w2d 806/553 44

192.168.0.202:4342 Up

2w2d 654/442 44

Edge-1#

show lisp instance-id 8232 ethernet database wlc 4822.54dc.6a15

WLC clients/access-points information for LISP 0 EID-table Vlan

1031

(IID

8232

)
Hardware Address:

4822.54dc.6a15

Type: client
Sources: 2
Tunnel Update: Signalled
Source MS:

192.168.0.201

RLOC:

192.168.0.101

Up time: 1w6d
Metadata length: 34
Metadata (hex): 00 01 00 22 00 01 00 0C AC 10 01 07 00 00 10 01
00 02 00 06 00 00 00 03 00 0C 00 00 00 00 68 99

```
                  6A D2

Edge-1#

show mac address-table address 4822.54dc.6a15


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


1031


4822.54dc.6a15


CP_LEARN


 Ac2
```

Als het MAC-adres van het eindpunt correct wordt aangeleerd via de toegangstunnelinterface die overeenkomt met het aangesloten toegangspunt, 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 isenabled


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

DHCP snooping isoperationalon following VLANs:


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

<--

VLAN1031 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 8232

interface L2LISP0.8232
instance-id 8232

  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 1031

 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:

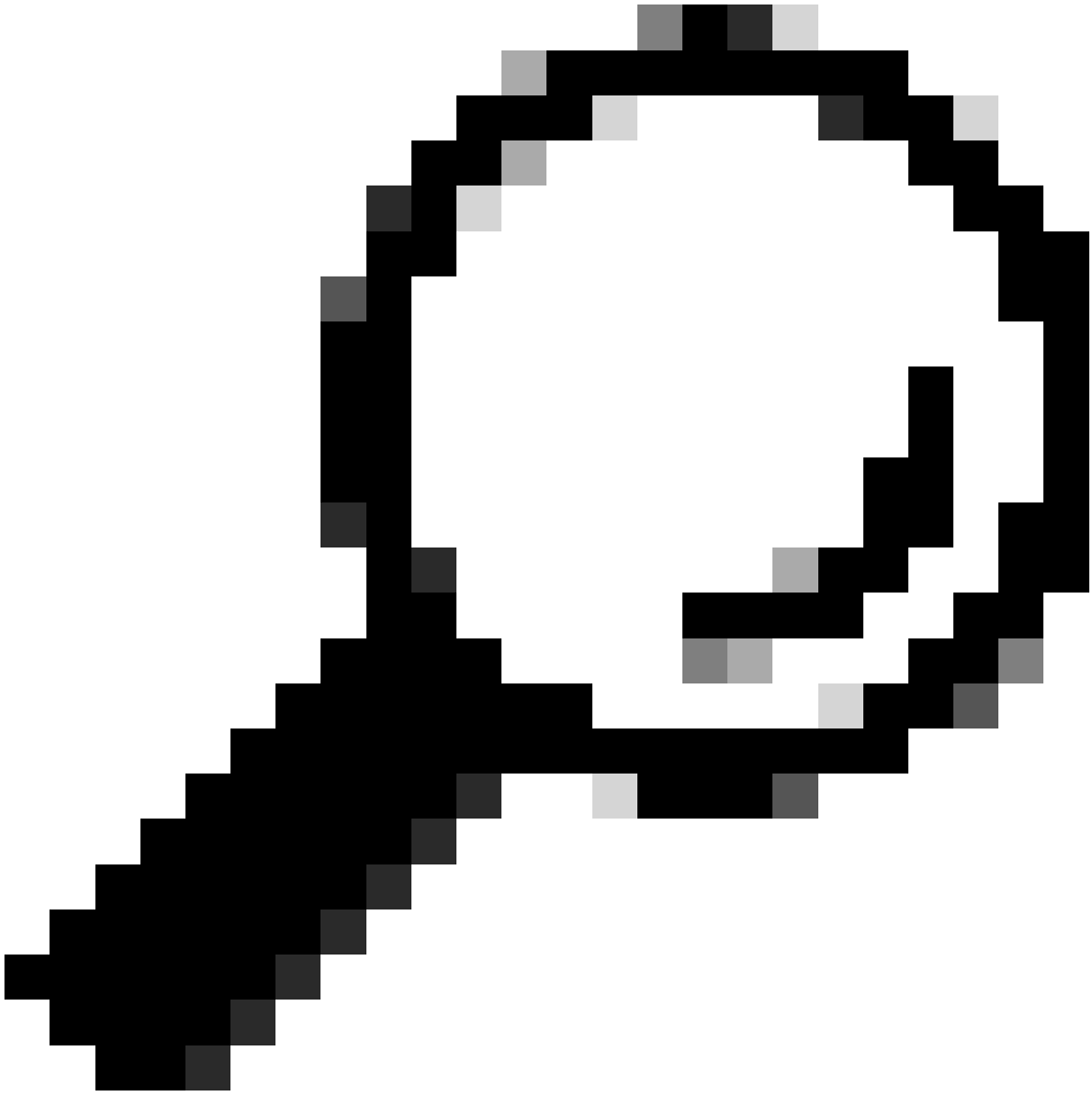
7

/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 de lijst met uitgaande interfaces (OIL) geen uitgaande interfaces (OIF's) bevat, duidt dit op een probleem met de onderliggende multicastconfiguratie of -bewerking.

Packet Captures

Configureer een gelijktijdige ingesloten pakketopname op de switch om zowel het ingangen DHCP-pakketje van het toegangspunt als het bijbehorende uitgangspakket voor L2 Flooding op te nemen.

Fabric Edge (192.168.0.101) pakketopnames

```
monitor capture cap interface TenGigabitEthernet1/0/12 IN    <-- Access Point Port

monitor capture cap interface TenGigabitEthernet1/1/1 OUT    <-- Multicast Route (L2 Flooding) OIF

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
```

Bij het vastleggen van pakketten moeten drie verschillende pakketten worden waargenomen:

- DHCP Discover - VXLAN - AP to Edge
- DHCP Discover - CAPWAP - AP naar WLC
- DHCP Discover - VXLAN - Edge-to-Multicast-groep

<#root>

```
Edge-1#

show monitor capture cap buffer display-filter "bootp and dhcp.hw.mac_addr==4822.54dc.6a15"

<-- 4822.54dc.6a15 is the endpoint MAC


Starting the packet display ........ Press Ctrl + Shift + 6 to exit
  129   4.865410      0.0.0.0 -> 255.255.255.255 DHCP

394

 DHCP Discover - Transaction ID 0x824bdf45

<--

 From AP to Edge


  130   4.865439      0.0.0.0 -> 255.255.255.255 DHCP

420

 DHCP Discover - Transaction ID 0x824bdf45

<--

 From AP to WLC
```

```
  131   4.865459      0.0.0.0 -> 255.255.255.255 DHCP
```

394

```
 DHCP Discover - Transaction ID 0x824bdf45
```

<--

From Edge to L2 Flooding Group

```
Edge-1#
```

show monitor capture cap buffer display-filter "bootp and dhcp.hw.mac_addr==4822.54dc.6a15

and vxlan"

```
Starting the packet display ........ Press Ctrl + Shift + 6 to exit
  129   4.865410      0.0.0.0 -> 255.255.255.255 DHCP
```

394

```
 DHCP Discover - Transaction ID 0x824bdf45
  131   4.865459      0.0.0.0 -> 255.255.255.255 DHCP
```

394

```
 DHCP Discover - Transaction ID 0x824bdf45
Edge-1#
```

show monitor capture cap buffer display-filter "bootp and dhcp.hw.mac_addr==4822.54dc.6a15

and udp.port==5247"

```
Starting the packet display ........ Press Ctrl + Shift + 6 to exit
  130   4.865439      0.0.0.0 -> 255.255.255.255 DHCP
```

420

```
 DHCP Discover - Transaction ID 0x824bdf45
Edge-1#
```

show monitor capture cap buffer display-filter "bootp and dhcp.hw.mac_addr==4822.54dc.6a15 and vxlan"

detail

| i Internet

```
Internet Protocol Version 4, Src:
```

172.16.1.7

```
, Dst:
```

192.168.0.101   <-- From AP to Edge

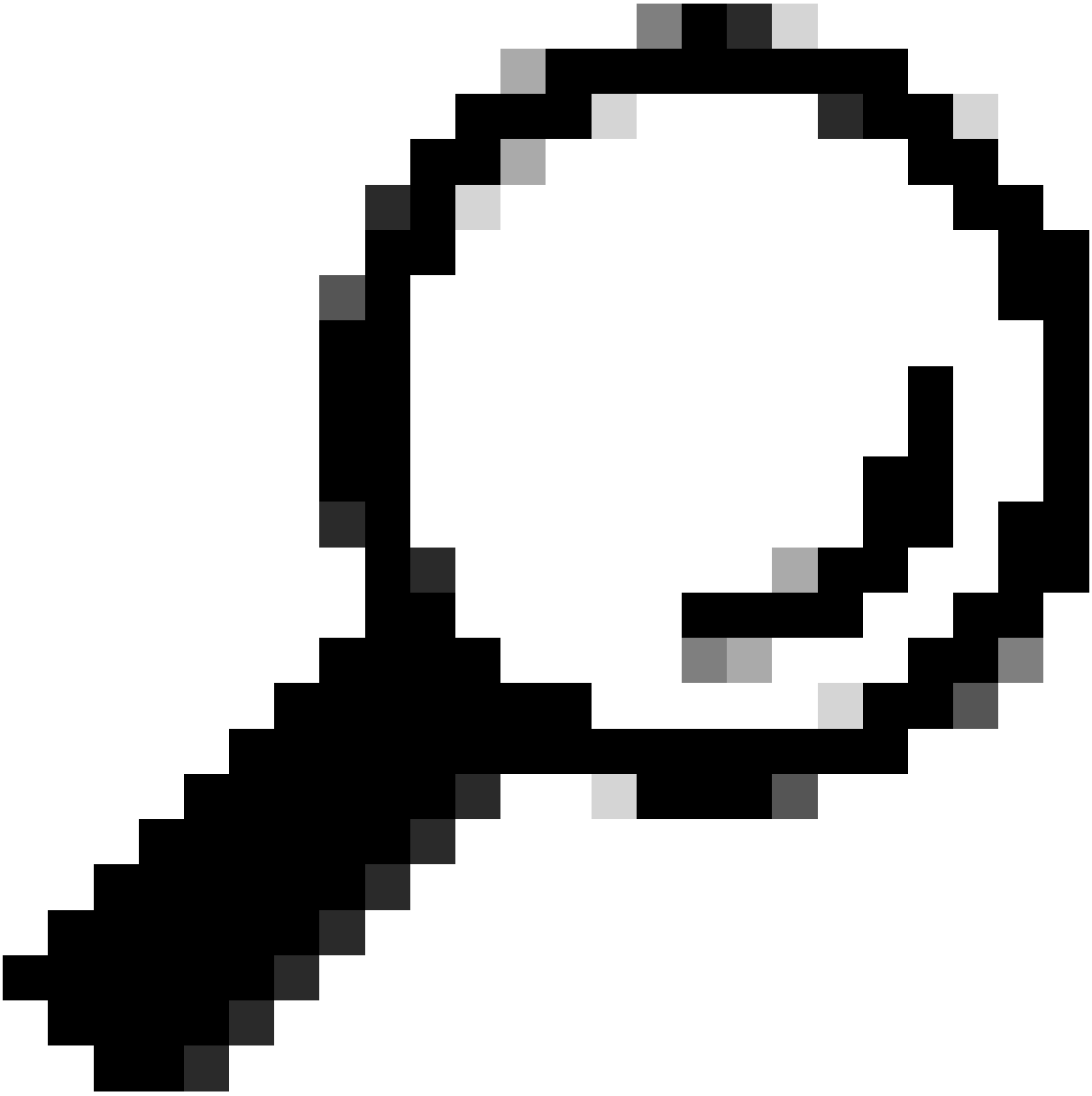
```
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
Internet Protocol Version 4, Src:
```

192.168.0.101

, Dst:

239.0.17.1 <-- From Edge to Upstream (Layer 2 Flooding)

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



Tip: voor draadloze verbindingen met VXLAN leveren ingekapselde pakketten DHCP-verkeer naar clients of servers. CAPWAP DATA (UDP 5247) ingekapselde pakketten verzenden echter alleen naar de WLC voor trackingdoeleinden, zoals de IP Learn-status of Wireless Device-Tracking.

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 31

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

31

L2_Only_Wireless

active

L2LI0:

8232

,

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

<-- IIF 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:

L2LISP0.8232

, 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,

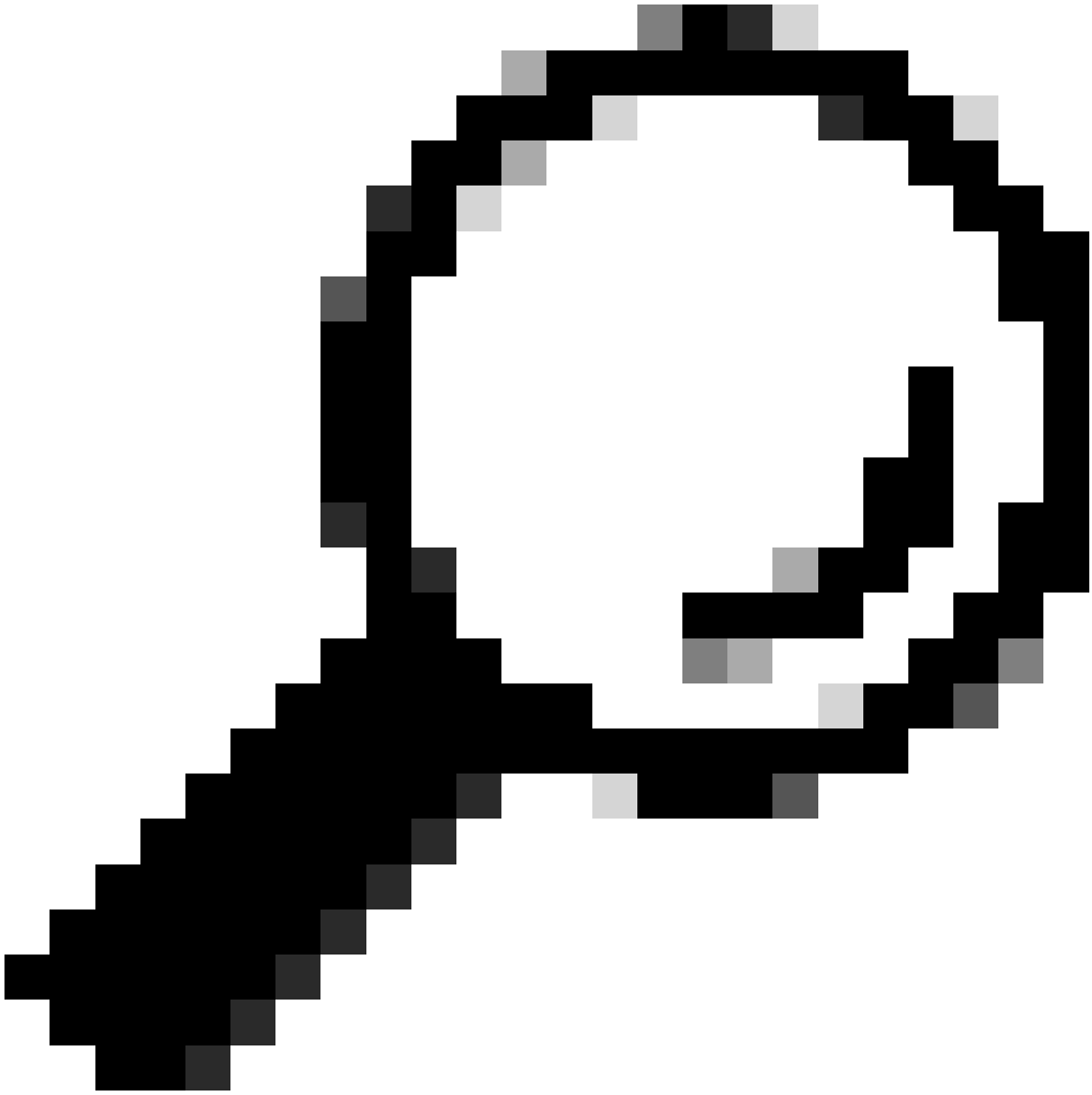
SW Forwarding: 1/0/392/0, Other: 0/0/0
HW Forwarding:

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 DHCP-pakket op de L2LISP0-interface ontkent.

<#root>

BorderCP-1#

show ip access-lists 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 31 | 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        state      Time left
ARP
```

172.16.131.254

f87b.2003.7fd5

Te1/0/44

31

0005 34s 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

<--

Ingress interface for Edge's S,G Mroute (192.168.0.101, 239.0.17.1)

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

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==4822.54dc.6a15"

Starting the packet display ..... Press Ctrl + Shift + 6 to exit
  324 16.695022   0.0.0.0 -> 255.255.255.255 DHCP

394

DHCP Discover - Transaction ID 0x824bdf45

<-- 394 is the Lenght of the VXLAN encapsulated packet

  325 10.834141   0.0.0.0 -> 255.255.255.255 DHCP

420

DHCP Discover - Transaction ID 0x168bd882

<-- 420 is the Lenght of the CAPWAP encapsulated packet

  326 16.695053   0.0.0.0 -> 255.255.255.255 DHCP

```
352
 DHCP Discover - Transaction ID 0x824bdf45
<-- 352 is the Lenght of the VXLAN encapsulated packet



Packet 324: VXLAN Encapsulated

BorderCP-1#
show monitor capture cap buffer display-filter "frame.number==324" detail | i Internet
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 326: Plain (dot1Q cannot be captured at egress due to EPC limitations)

BorderCP-1#
show monitor capture cap buffer display-filter "frame.number==326" detailed | i Internet
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
```

Op dit punt heeft het Discover/Request-pakket de SD-Access-fabric verlaten en dit gedeelte afgesloten. Voordat u doorgaat, zal echter een cruciale parameter - de DHCP Broadcast Flag, bepaald door het eindpunt zelf - het doorstuurscenario voor volgende Offer- of ACK-pakketten dicteren. We kunnen een van onze Discover-pakketten onderzoeken om deze vlag te inspecteren.

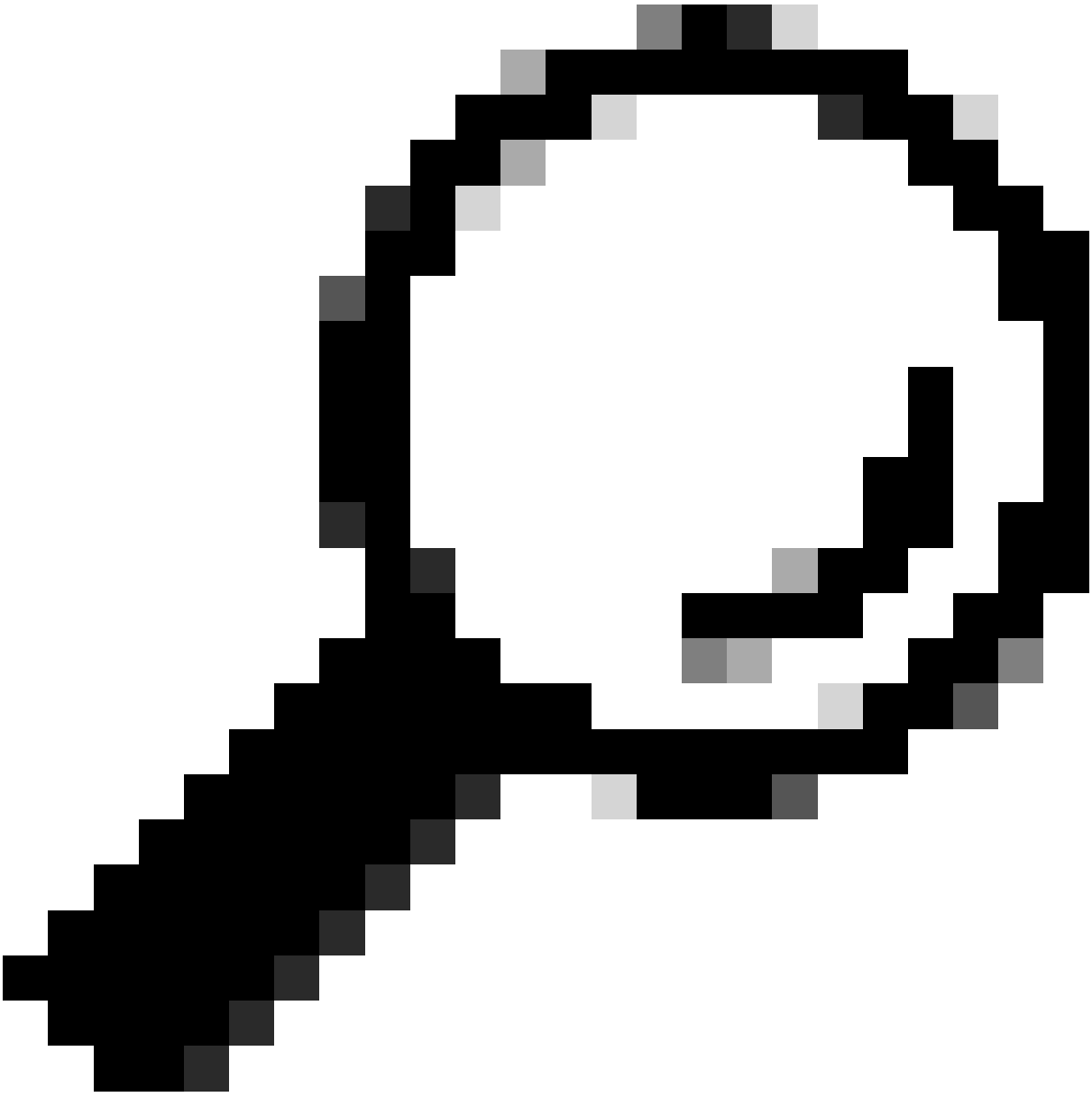
```
<#root>
BorderCP-1#
show monitor capture cap buffer display-filter "bootp.type==1 and dhcp.hw.mac_addr==4822.54dc.6a15
" detailed | sect Dynamic


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: 3
```

Bootp flags: 0x8000, Broadcast flag (Broadcast)

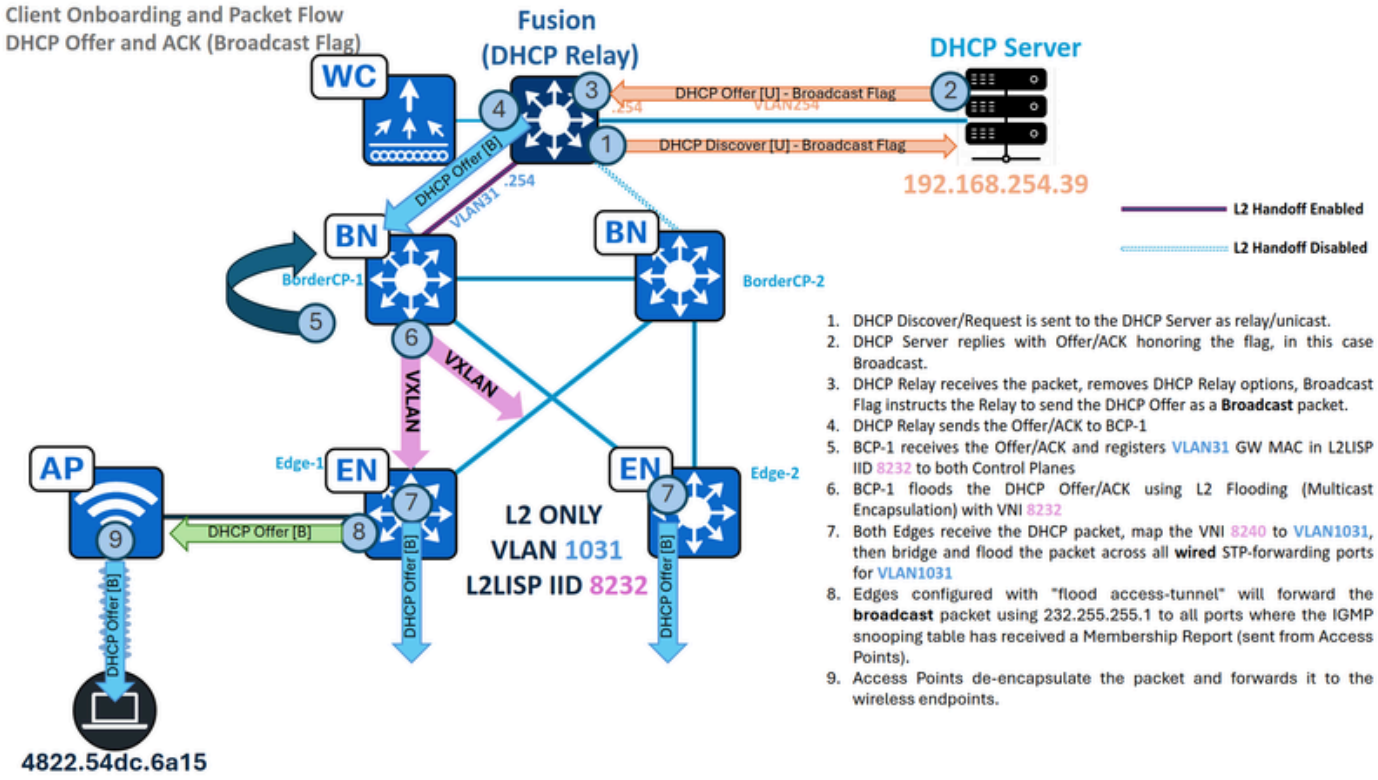
1... .... = Broadcast flag: Broadcast   <-- Broadcast Flag set by the Endpoint

```
        .000 0000 0000 0000 = Reserved flags: 0x0000
```



Tip: De bootp.type==1 kan worden gebruikt om alleen Discover- en Request-pakketten te filteren.

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, zal het DHCP-relais traditionele DHCP-relaisopties invoegen (bijv. GiAdr/GatewayIPAaddress) en het pakket doorsturen 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 8232.

<#root>

```
BorderCP-1#
```

show mac address-table interface te1/0/44

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

31


f87b.2003.7fd5

    DYNAMIC

Te1/0/44

BorderCP-1#

show vlan id 31

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


31

  L2_Only_Wireless               active    L2LI0:

8232

,

Te1/0/44

BorderCP-1#

show device-tracking database mac | i 7fd5|vlan

 MAC                    Interface  vlan       prlvl      state            Time left        Policy

 f87b.2003.7fd5


 Te1/0/44    31

        NO TRUST

 MAC-REACHABLE

    61 s             LISP-DT-GLEAN-VLAN 64

BorderCP-1#

show lisp ins 8232 dynamic-eid summary | i Name|f87b.2003.7fd5

Dyn-EID Name         Dynamic-EID      Interface     Uptime    Last      Pending

Auto-L2-group-8232
```

```
f87b.2003.7fd5

 N/A           6d06h     never

  0



BorderCP-1#

show lisp instance-id 8232 ethernet database

f87b.2003.7fd5


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

31

 (IID

8232

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


f87b.2003.7fd5/48

,
 dynamic-eid Auto-L2-group-8240, inherited from default locator-set
rloc_0f43c5d8-f48d-48a5-a5a8-094b87f3a5f7, auto-discover-rlocs
  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 <-- VLAN31 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

Omdat DHCP Snooping niet is ingeschakeld in de L2Border, is geen configuratie van DHCP Snooping Trust 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 de vermelding L2 Flooding (S, G) te verifiëren die dit pakket naar andere Fabric Nodes zal overbruggen. 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 8232

interface L2LISP0.8232

instance-id 8232

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

1031

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

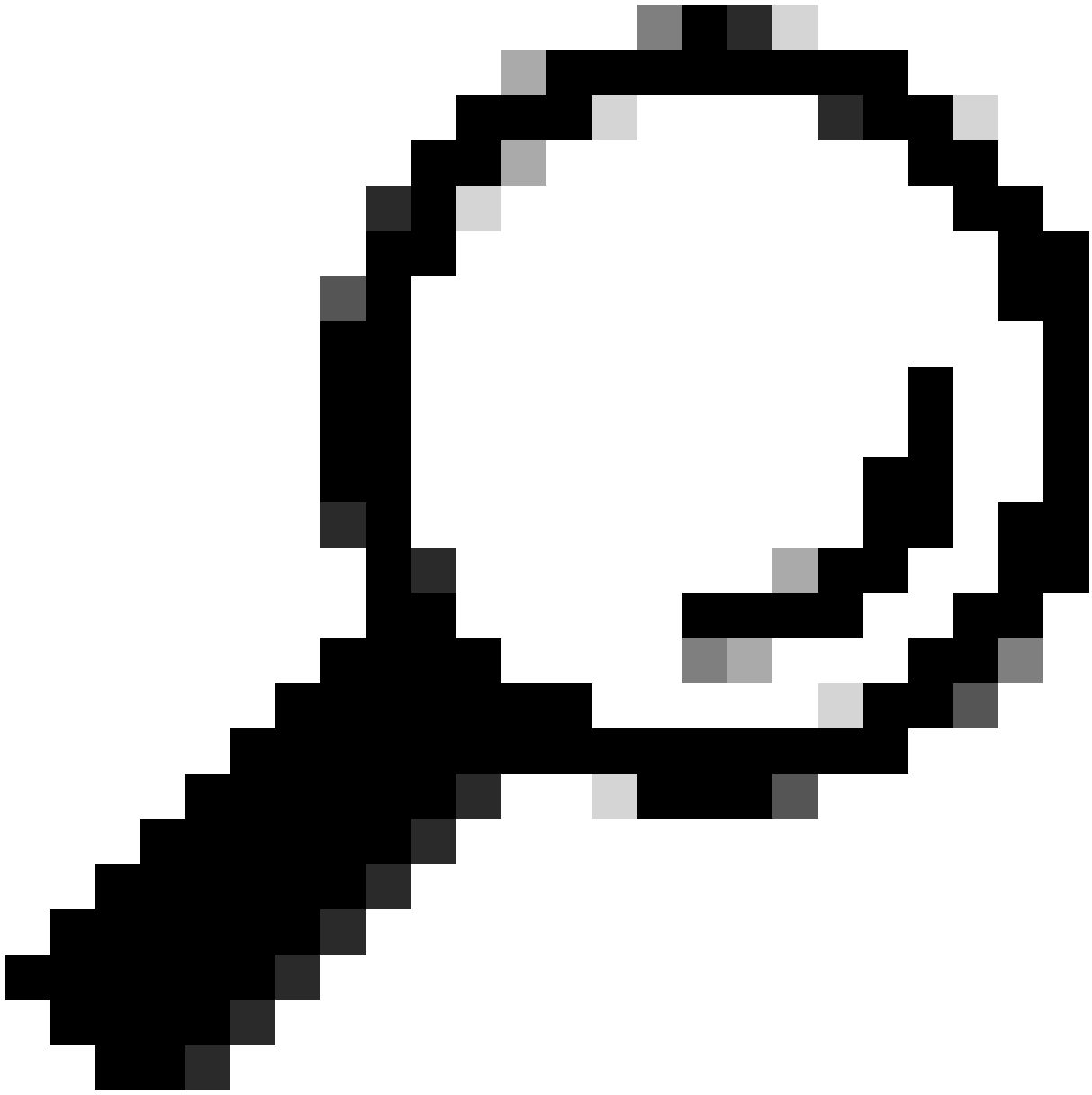
,
   SW Forwarding: 1/0/392/0, Other: 1/1/0
   HW Forwarding:

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, sluiten we dit gedeelte af, omdat het DHCP-aanbod wordt doorgestuurd als een uitzending naar alle Fabric Edges met behulp van de inhoud van de uitgaande interfacelijst, in dit geval buiten de interface TenGig1/0/42 en TenGig1/0/43.

DHCP-aanbieding en ACK - Uitzending - Edge

Precies zoals de vorige stroom controleren we nu 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 1031.

<#root>

Edge-1#show vlan id 1031

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

1031

L2_Only_Wireless

active   L2LI0:

8232

, 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)a

  Outgoing interface list:

L2LISP0.8232

, 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,

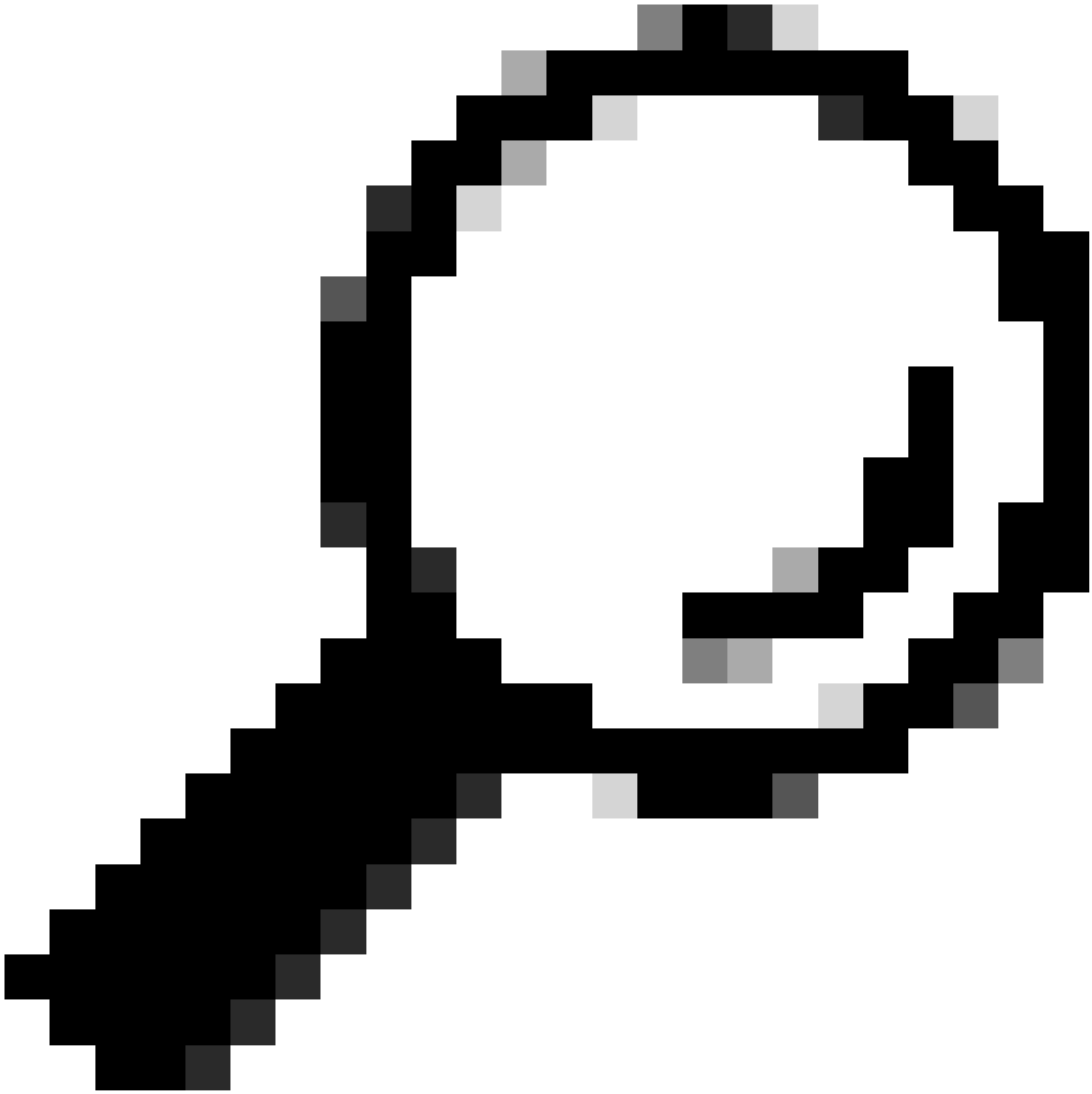
```
   SW Forwarding: 1/0/96/0, Other: 0/0/0
   HW Forwarding:
```

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 8232, dicteert de uitzendaard dat het alle bekabelde Spanning Tree Protocol-doorstuurpoorten voor VLAN1031 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 interface waarnaar we op zoek zijn om het DHCP-aanbod uit te zenden, is echter de Access-Tunnel-interface die is gekoppeld aan het Access-Point. Dit is alleen mogelijk omdat "flood access-tunnel" is ingeschakeld op de L2LISP IID 8232, anders wordt dit pakket geblokkeerd om te worden doorgestuurd naar de AccessTunnel-interface.

<#root>

```
Edge-1#
show lisp instance-id 8232 ethernet | se Multicast Flood

  Multicast Flood Access-Tunnel:
enabled

    Multicast Address:
232.255.255.1

    Vlan ID:
1021


Edge-1#
show ip igmp snooping  groups vlan 1021 232.255.255.1

Vlan      Group                   Type        Version     Port List
------------------------------------------------------------------------------

1021      232.255.255.1
         igmp        v2
Te1/0/12    <-- AP1 Port
```

Met het IGMP-snuffelpunt voor de multicast-overstromingsgroep worden DHCP-aanbiedingen en ACK's doorgestuurd naar de fysieke poort van de AP.

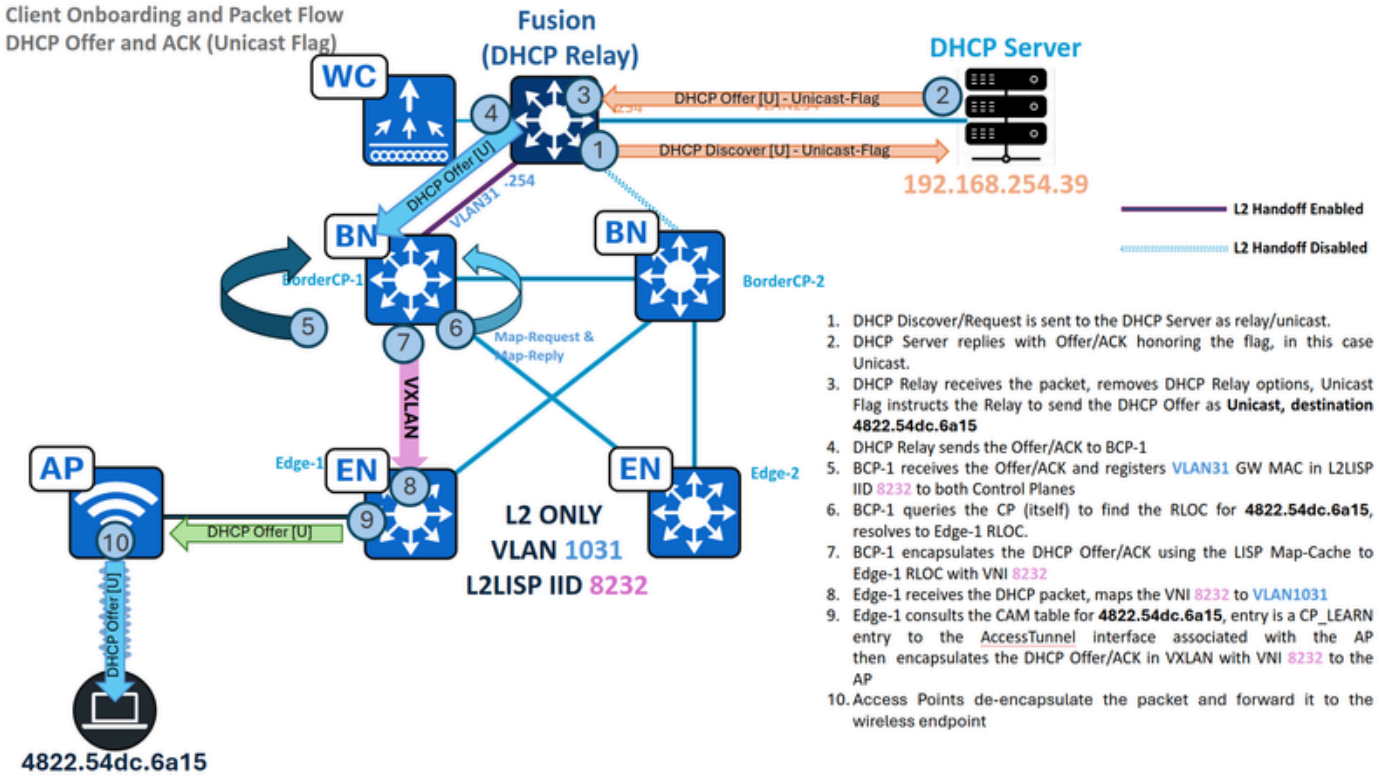
Het DHCP-aanbod en het ACK-proces blijven consistent. Zonder dat DHCP-snooping is ingeschakeld, worden er geen items gemaakt in de DHCP-snooptabel. Bijgevolg wordt de vermelding Device-Tracking voor het DHCP-enabled eindpunt gegenereerd door verzamelde ARP-pakketten. Het is ook te verwachten dat opdrachten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

<#root>

```
Edge-1#
show device-tracking database interface Ac2 | be Network

   Network Layer Address                  Link Layer Address
Interface  vlan       prlvl      age        state      Time left

ARP


172.16.131.4
```

```
 4822.54dc.6a15


Ac2


1031
       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==4822.54dc.6a15" detailed | sect Dynamic


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: 48:22:54:dc:6a:15 (48:22:54:dc:6a:15)
```

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. Als u zich houdt aan de principes voor het doorsturen van unicast, zoekt de L2-rand in het controlevlak naar het MAC-adres van de bestemming. Ervan uitgaande dat "MAC Learning en WLC Notification" op de Fabric Edge succesvol is, heeft het Control Plane deze Endpoint ID (EID) geregistreerd.

<#root>

```
BorderCP-1#

show lisp instance-id 8232 ethernet server 4822.54dc.6a15
```

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

4822.54dc.6a15/48

```
 instance-id 8232
    First registered:     00:53:30
    Last registered:      00:53:30
    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 00:53:30, proxy-reply, map-notify
                             TTL 1d00h, no merge, hash-function sha1
                             state complete, no security-capability
                             nonce 0xBB7A4AC0-0x46676094
                             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
```

ETR 192.168.254.69:58507

```
, last registered 00:53:30, no proxy-reply, no map-notify
```

<-- Registered by the Wireless LAN Controller

```
                              TTL 1d00h, no merge, hash-function sha2
```

state complete

```
, no security-capability
                              nonce 0x00000000-0x00000000
```

```
                              xTR-ID N/A
                              site-ID N/A
                              sourced by reliable transport
                              Affinity-id: 0 , 0

WLC AP bit: Clear

      Locator        Local  State      Pri/Wgt  Scope

192.168.0.101

 yes

up

         0/0    IPv4 none

<-- RLOC of Fabric Edge with the Access Point where the endpoint is connected
```

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 8232 ethernet map-cache 4822.54dc.6a15

LISP MAC Mapping Cache for LISP 0 EID-table Vlan

31

 (IID

8232

), 1 entries

4822.54dc.6a15/48

, 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 VNI 8240.

```
<#root>

BorderCP-1#

show mac address-table address aaaa.dddd.bbbb


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

31


 4822.54dc.6a15


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         diHandle   *a_time  *e_time  ports
                   Con
-------------------------------------------------------------------------------------------------------


31    4822.54dc.6a15

  0x1000001    0      0    64  0x718eb52c48e8  0x718eb52c8b68  0x718eb44c6c18      0x0            0

 RLOC 192.168.0.101

adj_id 1044  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, zal de Edge-node het pakket vervolgens alleen doorsturen naar de specifieke Access-Tunnel waar het eindpunt is aangesloten, in plaats van het naar alle poorten te laten overstromen.

De MAC-adrestabel identificeert poort AccessTunnel2 als onze virtuele poort die is gekoppeld aan AP1.

<#root>

Edge-1#show mac address-table address 4822.54dc.6a15

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

1031

4822.54dc.6a15

CP_LEARN

Ac2

```
Edge-1#show interfaces accessTunnel 2 description

Interface                      Status         Protocol Description

Ac2

up             up

      Radio MAC: dc8c.37ce.58a0,

IP: 172.16.1.7



Edge-1#show device-tracking database address 172.16.1.7 | be Network

   Network Layer Address                    Link Layer Address
Interface  vlan       prlvl      age        state      Time left
DH4

 172.16.1.7

                            dc8c.3756.99bc

Te1/0/12

   1021       0024       6s         REACHABLE  241 s try 0(86353 s)

Edge-1#show cdp neighbors tenGigabitEthernet 1/0/12 | be Device

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

AP1              Ten 1/0/12

      119              R T   AIR-AP480 Gig 0
```

Het DHCP-aanbod en het ACK-proces blijven consistent. Zonder DHCP Snooping ingeschakeld, worden er geen vermeldingen gemaakt in de DHCP Snooping-tabel. Bijgevolg wordt de vermelding Device-Tracking voor het DHCP-enabled eindpunt gegenereerd door verzamelde ARP-pakketten, niet door DHCP. Het is ook te verwachten dat opdrachten zoals "show platform dhcpsnooping client stats" geen gegevens zullen 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      age        state      Time left
```

```
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.

DHCP-transactie - Draadloze verificatie

Vanuit de WLC wordt de DHCP-transactie gemonitord via RA-Traces.

<#root>

```
WLC#debug wireless mac 48:22:54:DC:6A:15 to-file bootflash:client6a15


    RA tracing start event,
       conditioned on MAC address: 48:22:54:dc:6a:15
       Trace condition will be automatically stopped in 1800 seconds.
       Execute 'no debug wireless mac 48:22:54:dc:6a:15' to manually stop RA tracing on this condition.



WLC#no debug wireless mac 48:22:54:dc:6a:15

    RA tracing stop event,
       conditioned on MAC address: 48:22:54:dc:6a:15


WLC#more flash:client6a15 | i DHCP


2025/08/11 06:13:48.600929726 {wncd_x_R0-0}{1}: [sisf-packet] [15981]: (info): RX: DHCPv4 from interfac

SISF_DHCPDISCOVER
```

```
, giaddr: 0.0.0.0, yiaddr: 0.0.0.0, CMAC: 4822.54dc.6a15
2025/08/11 06:13:50.606037404 {wncd_x_R0-0}{1}: [sisf-packet] [15981]: (info): RX: DHCPv4 from interfac

SISF_DHCPOFFER

, giaddr: 172.16.131.254, yiaddr: 172.16.131.4, CMAC: 4822.54dc.6a15
2025/08/11 06:13:50.609855406 {wncd_x_R0-0}{1}: [sisf-packet] [15981]: (info): RX: DHCPv4 from interfac

SISF_DHCPREQUEST

, giaddr: 0.0.0.0, yiaddr: 0.0.0.0, CMAC: 4822.54dc.6a15
2025/08/11 06:13:50.613054692 {wncd_x_R0-0}{1}: [sisf-packet] [15981]: (info): RX: DHCPv4 from interfac

SISF_DHCPACK

, giaddr: 172.16.131.254, yiaddr: 172.16.131.4, CMAC: 4822.54dc.6a15
```

Aan het einde van de transactie wordt het eindpunt toegevoegd aan de database Apparaat bijhouden op de draadloze LAN-controller.

<#root>

```
WLC#show wireless device-tracking database mac 4822.54dc.6a15

  MAC             VLAN  IF-HDL      IP                                                  ZONE-ID/VRF-NAME
  ----------------------------------------------------------------------------------------------------

  4822.54dc.6a15

 1     0x90000006

 172.16.131.4

                          0x00000000
                                    fe80::b070:b7e1:cc52:69ed                    0x80000001
```

De volledige DHCP-transactie wordt gedetecteerd op het toegangspunt zelf.

<#root>

```
AP1#debug client 48:22:54:DC:6A:15

AP1#term mon

AP1#
Aug 11 05:37:47 AP1 kernel: [*08/11/2025 05:37:47.3530] [1754890667:353058] [AP1] [48:22:54:dc:6a:15] <

[U:W]

DHCP_DISCOVER
```

 : TransId 0x76281006
Aug 11 05:37:47 AP1 kernel: [*08/11/2025 05:37:47.3531] chatter: dhcp_req_local_sw_nonat: 1754890667.35
Aug 11 05:37:47 AP1 kernel: [*08/11/2025 05:37:47.3533] chatter: dhcp_from_inet: 1754890667.353287600: (
Aug 11 05:37:47 AP1 kernel: [*08/11/2025 05:37:47.3533] chatter: dhcp_reply_nonat: 1754890667.353287600
Aug 11 05:37:49 AP1 kernel: [*08/11/2025 05:37:49.3587] chatter: dhcp_from_inet: 1754890669.358709760: 1
Aug 11 05:37:49 AP1 kernel: [*08/11/2025 05:37:49.3588] chatter: dhcp_reply_nonat: 1754890669.358709760
Aug 11 05:37:49 AP1 kernel: [*08/11/2025 05:37:49.3589] [1754890669:358910] [AP1] [48:22:54:dc:6a:15]

[D:W]

DHCP_OFFER

 : TransId 0x76281006 tag:534

Aug 11 05:37:49 AP1 kernel: [*08/11/2025 05:37:49.3671] [1754890669:367110] [AP1] [48:22:54:dc:6a:15] <

[U:W] DHCP_REQUEST

 : TransId 0x76281006
Aug 11 05:37:49 AP1 kernel: [*08/11/2025 05:37:49.3671] chatter: dhcp_req_local_sw_nonat: 1754890669.367
Aug 11 05:37:49 AP1 kernel: [*08/11/2025 05:37:49.3709] [1754890669:370945] [AP1] [48:22:54:dc:6a:15]

[D:W]

DHCP_ACK

 : TransId 0x76281006 tag:536

Aug 11 05:37:49 AP1 kernel: [*08/11/2025 05:37:49.3733] [1754890669:373312] [AP1] [48:22:54:dc:6a:15] <

[D:A] DHCP_OFFER

 : TransId 0x76281006 [

Tx Success

] tag:534
Aug 11 05:37:49 AP1 kernel: [*08/11/2025 05:37:49.3983] [1754890669:398318] [AP1] [48:22:54:dc:6a:15] <

[D:A]

DHCP_ACK

: TransId 0x76281006 [

Tx Success

] tag:53

*** U:W = Uplink Packet from Client to Wireless Driver**

*** D:W = Downlink Packet from Client to Click Module**

*** D:A = Downlink Packet from Client sent over the air**

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.