Resolución de problemas de DHCP solo en la capa 2 de VLAN - Inalámbrico

Contenido

Introducción

Este documento describe cómo resolver problemas de DHCP para terminales inalámbricos en una red de Capa 2 solamente en el entramado de Acceso SD (SDA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Reenvío de protocolo de Internet (IP)
- Protocolo de separación Localizador/ID (LISP)
- Modo disperso de multidifusión independiente de protocolo (PIM)
- Tecnología inalámbrica habilitada

Requisitos de hardware y software

- Catalyst 9000 Series Switch
- Catalyst Center Versión 2.3.7.9
- Controladores de LAN inalámbrica Catalyst serie 9800
- Puntos de acceso Catalyst serie 9100
- Cisco IOS® XE 17.12 y versiones posteriores

Limitaciones

- Solo un borde L2 puede entregar una VLAN/VNI única simultáneamente, a menos que se configuren correctamente mecanismos robustos de prevención de loops, como los scripts FlexLink+ o EEM para inhabilitar los links.

Descripción general sólo de L2

Overview

En las implementaciones habituales de SD-Access, el límite de L2/L3 reside en el Fabric Edge (FE), donde el FE aloja el gateway del cliente en forma de SVI, lo que a menudo se denomina "Anycast Gateway". Las VNI de nivel 3 (enrutadas) se establecen para el tráfico entre subredes, mientras que las VNI de nivel 2 (conmutadas) administran el tráfico entre subredes. Una configuración uniforme en todos los FE permite una itinerancia de cliente perfecta. El reenvío está optimizado: el tráfico entre subredes (L2) se conecta directamente mediante puente entre FE y el tráfico entre subredes (L3) se enruta entre FE o entre un FE y un nodo de borde.

Para los terminales de los fabrics SDA que requieren un punto de entrada de red estricto fuera del fabric, el fabric SDA debe proporcionar un canal L2 desde el perímetro a una gateway externa.

Este concepto es análogo a las implementaciones de campus Ethernet tradicionales, en las que una red de acceso de capa 2 se conecta a un router de capa 3. El tráfico intra-VLAN permanece dentro de la red L2, mientras que el tráfico inter-VLAN es ruteado por el dispositivo L3, a menudo regresa a una VLAN diferente en la red L2.

Dentro de un contexto LISP, el plano de control del sitio realiza principalmente un seguimiento de las direcciones MAC y sus correspondientes enlaces MAC a IP, de forma muy similar a las

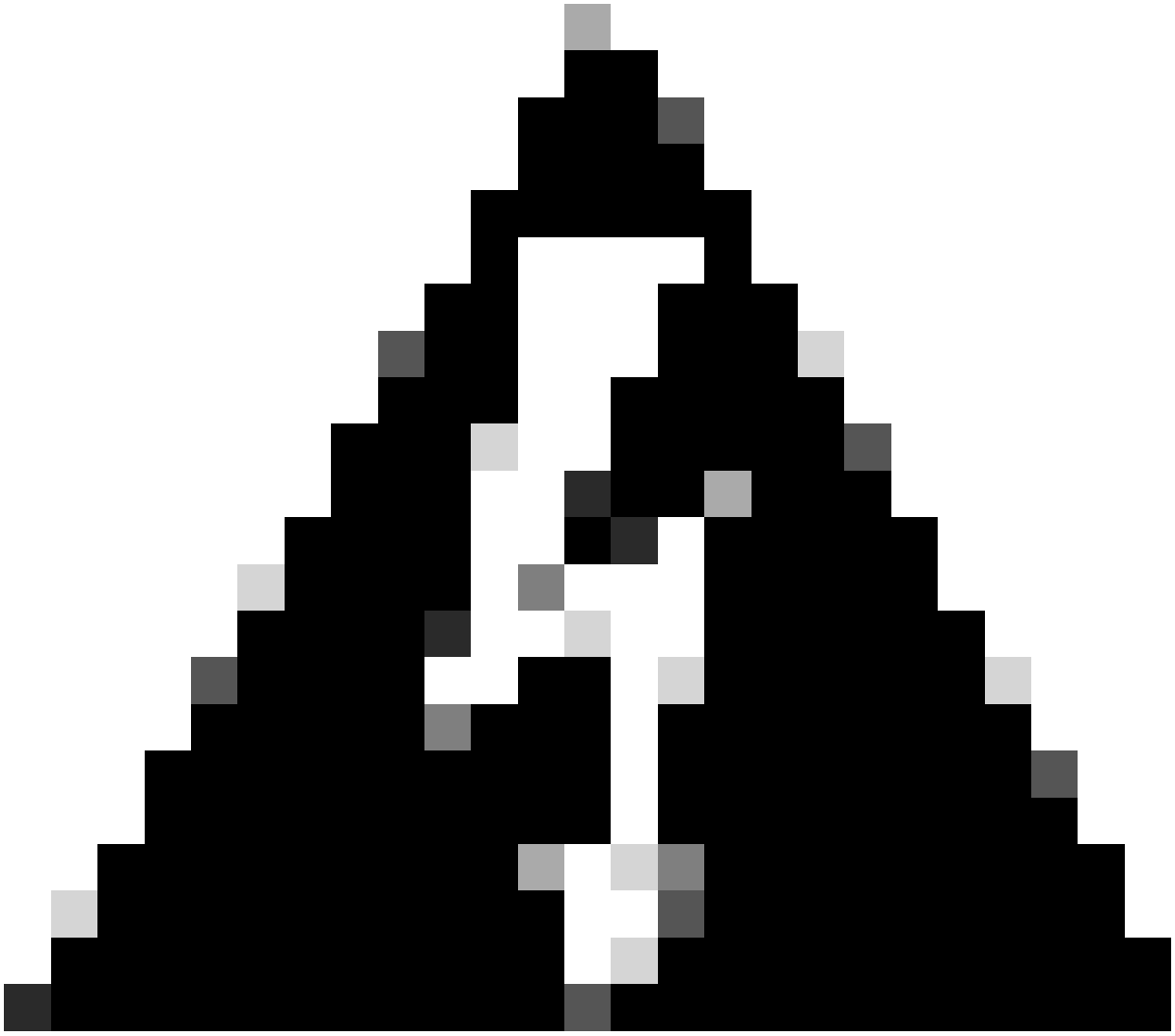
entradas ARP tradicionales. Las agrupaciones L2 VNI/L2-only están diseñadas para facilitar el registro, la resolución y el reenvío basados exclusivamente en estos dos tipos de EID. Por lo tanto, cualquier reenvío basado en LISP en un entorno solo de L2 se basa únicamente en la información de MAC y MAC a IP, ignora por completo los EID de IPv4 o IPv6. Para complementar los EID de LISP, los agrupamientos sólo de L2 dependen en gran medida de mecanismos de saturación y aprendizaje, similares al comportamiento de los switches tradicionales. En consecuencia, la inundación de capa 2 se convierte en un componente crítico para gestionar el tráfico de difusión, unidifusión desconocida y multidifusión (BUM) dentro de esta solución, que requiere el uso de multidifusión subyacente. Por el contrario, el tráfico de unidifusión normal se reenvía mediante los procesos de reenvío de LISP estándar, principalmente a través de las memorias caché de mapas.

Tanto los extremos del fabric como el "borde L2" (L2B) mantienen VNI de L2, que se asignan a VLAN locales (esta asignación es significativa para el dispositivo localmente dentro de SDA, lo que permite que diferentes VLAN se asignen a la misma VNI de L2 a través de los nodos). En este caso de uso específico, no se configura ninguna SVI en estas VLAN en estos nodos, lo que significa que no hay una VNI de L3 correspondiente.

Cambio de comportamiento de DHCP en VLAN L2 solamente

En los grupos de puertas de enlace de difusión ilimitada, DHCP presenta un reto, ya que cada extremo del fabric actúa como puerta de enlace para sus terminales conectados directamente, con la misma IP de puerta de enlace en todos los FE. Para identificar correctamente el origen original de un paquete retransmitido DHCP, los FE deben insertar la opción 82 de DHCP y sus subopciones, incluida la información LISP RLOC. Esto se logra con la indagación DHCP en la VLAN del cliente en el Fabric Edge. El snooping de DHCP tiene un doble propósito en este contexto: facilita la inserción de la opción 82 y, lo que es más importante, evita la saturación de paquetes de difusión DHCP a través del dominio de puente (VLAN/VNI). Incluso cuando la inundación de capa 2 está habilitada para un gateway de difusión ilimitada, la detección DHCP suprime eficazmente el paquete de difusión que se reenviará fuera del borde del fabric como una difusión.

Por el contrario, una VLAN solo de capa 2 carece de un gateway, lo que simplifica la identificación del origen DHCP. Dado que los paquetes no son retransmitidos por ninguna arista del entramado, no son necesarios mecanismos complejos para la identificación del origen. Sin la indagación DHCP en la VLAN L2 Only, el mecanismo de control de saturación para los paquetes DHCP se omite de manera efectiva. Esto permite que las difusiones DHCP se reenvíen mediante la inundación de capa 2 a su destino final, que podría ser un servidor DHCP conectado directamente a un nodo de fabric o un dispositivo de capa 3 que proporciona la funcionalidad de retransmisión DHCP.



Advertencia: La funcionalidad "Múltiples IP a MAC" dentro de un conjunto L2 Only activa automáticamente la detección DHCP en el modo Bridge VM, que aplica el control de saturación DHCP. En consecuencia, esto hace que el conjunto VNI L2 no pueda soportar DHCP para sus extremos.

Multidifusión subyacente

Dada la alta dependencia de DHCP del tráfico de broadcast, la inundación de Capa 2 debe ser aprovechada para soportar este protocolo. Al igual que con cualquier otro grupo habilitado para la inundación de L2, la red subyacente debe configurarse para el tráfico de multidifusión, específicamente para la multidifusión de cualquier fuente mediante el modo disperso de PIM. Mientras que la configuración de multidifusión subyacente se automatiza mediante el flujo de trabajo de automatización de LAN, si se omitió este paso, se requiere una configuración adicional (manual o de plantilla).

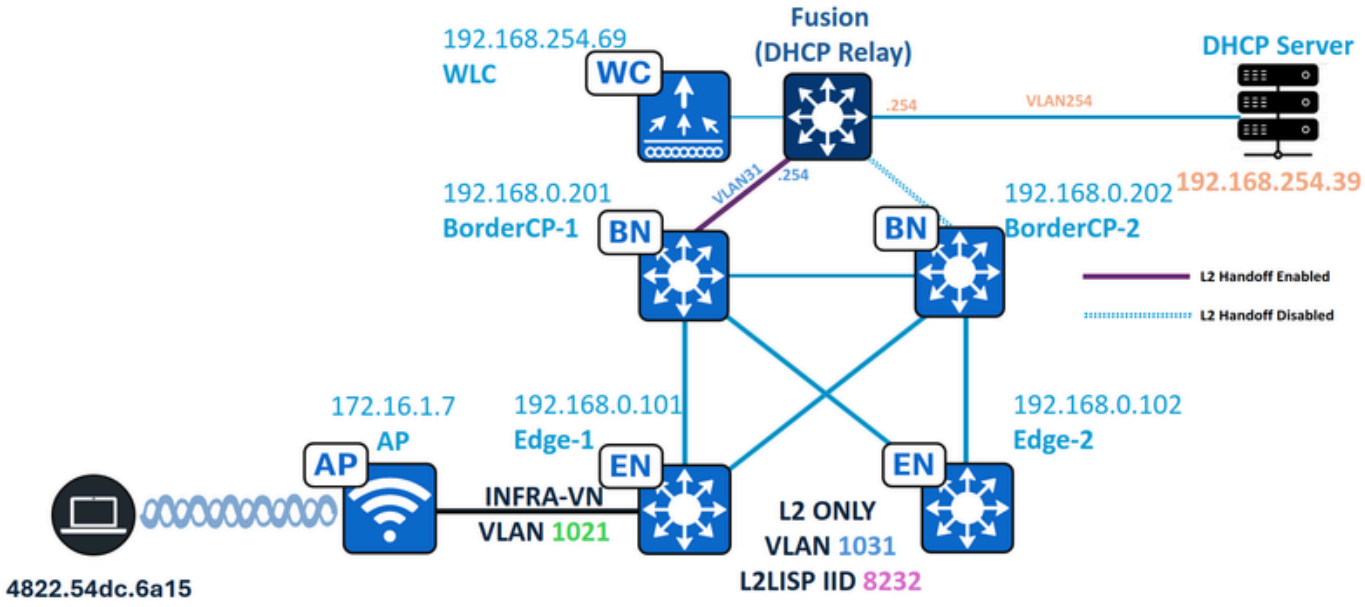
- Active el routing multidifusión IP en todos los nodos (bordes, bordes, nodos intermedios, etc.).

- Configure el modo disperso de PIM en la interfaz Loopback0 de cada nodo de borde y borde.
- Habilite el modo disperso de PIM en cada interfaz IGP (protocolo de ruteo subyacente).
- Configure el PIM Rendezvous Point (RP) en todos los nodos (Bordes, Bordes, Nodos Intermedios), se recomienda la colocación del RP en los Bordes.
- Verifique los Vecinos PIM, el RP PIM y el estado del túnel PIM.

Transmisión a través de interfaces de túnel de acceso

Fabric Enabled Wireless emplea switching local y funcionalidad VTEP en el AP y el FE. Sin embargo, una limitación IOS-XE 16.10+ impide el reenvío de broadcast de salida sobre VXLAN a AP. En las redes L2 Only, esto impide que las ofertas/ACK de DHCP lleguen a los clientes inalámbricos. La función de "túnel de acceso de inundación" soluciona este problema habilitando el reenvío de difusión en las interfaces de túnel de acceso de Fabric Edge.

Topología



Topología de red

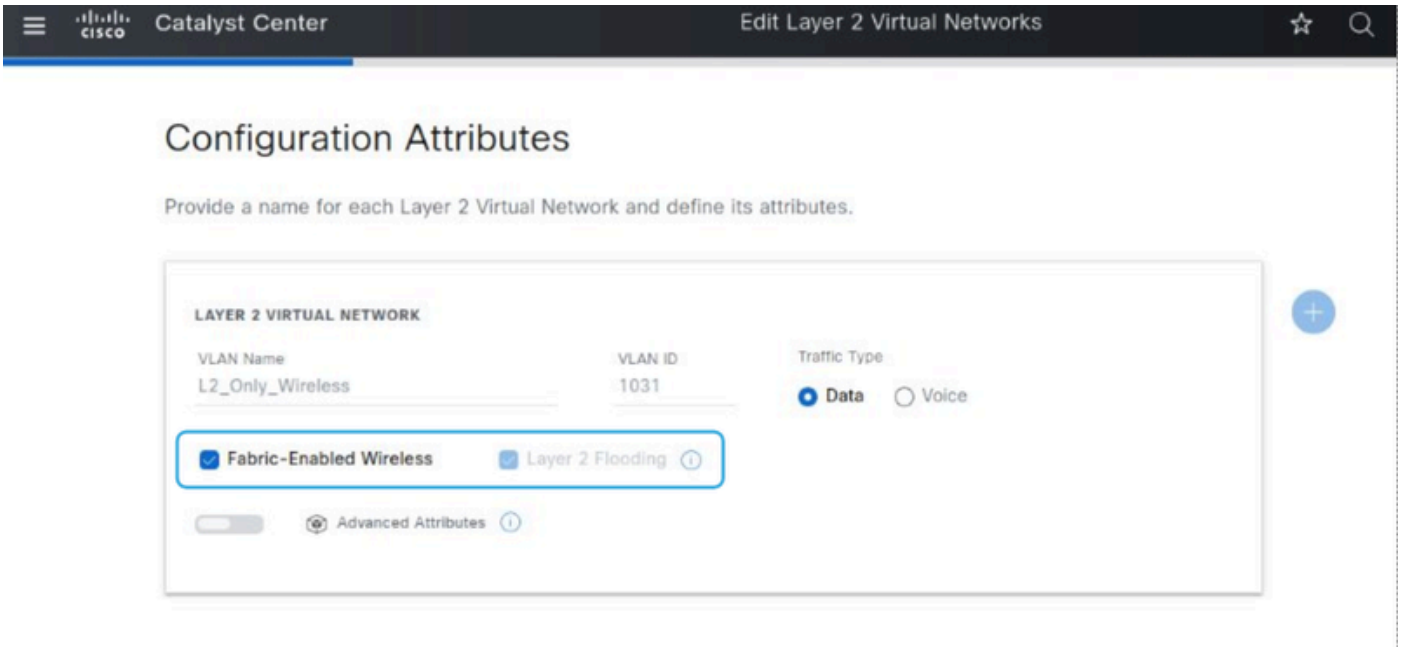
En esta topología:

- 192.168.0.201 y 192.168.0.202 son bordes colocados para el sitio de fabric. BorderCP-1 es el único borde con la función de transferencia de capa 2 habilitada.
- 192.168.0.101 y 192.168.0.102 son nodos de extremo de fabric
- 172.16.1.7 es el punto de acceso en INFRA-VN con VLAN 1021
- 192.168.254.39 es el servidor DHCP
- 192.168.254.69 es el controlador de LAN inalámbrica
- 482.54dc.6a15 es el terminal habilitado para DHCP
- El dispositivo Fusion actúa como relé DHCP para las subredes de fabric.

Configuración de VLAN solo L2

Implementación de VLAN solo de L2 desde Catalyst Center

Ruta: Centro Catalyst / Aprovisionamiento / Sitio de fabric / Redes virtuales de capa 2 / Editar redes virtuales de capa 2



Configuración de L2VNI con tecnología inalámbrica habilitada para fabric

Configuración de VLAN solo de L2 - Bordes del fabric

Los nodos de Fabric Edge tienen la VLAN configurada con CTS habilitado, IGMP e IPv6 MLD deshabilitado, y la configuración LISP L2 requerida. Este grupo L2 Only es un grupo Wireless; por lo tanto, se configuran las funciones que se encuentran típicamente en los agrupamientos inalámbricos de L2 solamente, tales como RA-Guard, DHCPGuard y el túnel de acceso de inundación. La inundación ARP no está habilitada en un grupo inalámbrico.

Configuración de 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
```

El comando flood-access tunnel se configura en su variación de replicación multicast, donde todo el tráfico BUM se encapsula a los AP usando el grupo multicast específico de origen (232.255.255.1) usando la VLAN del punto de acceso INFRA-VN como la VLAN que es consultada por la indagación IGMP para reenviar el tráfico BUM.

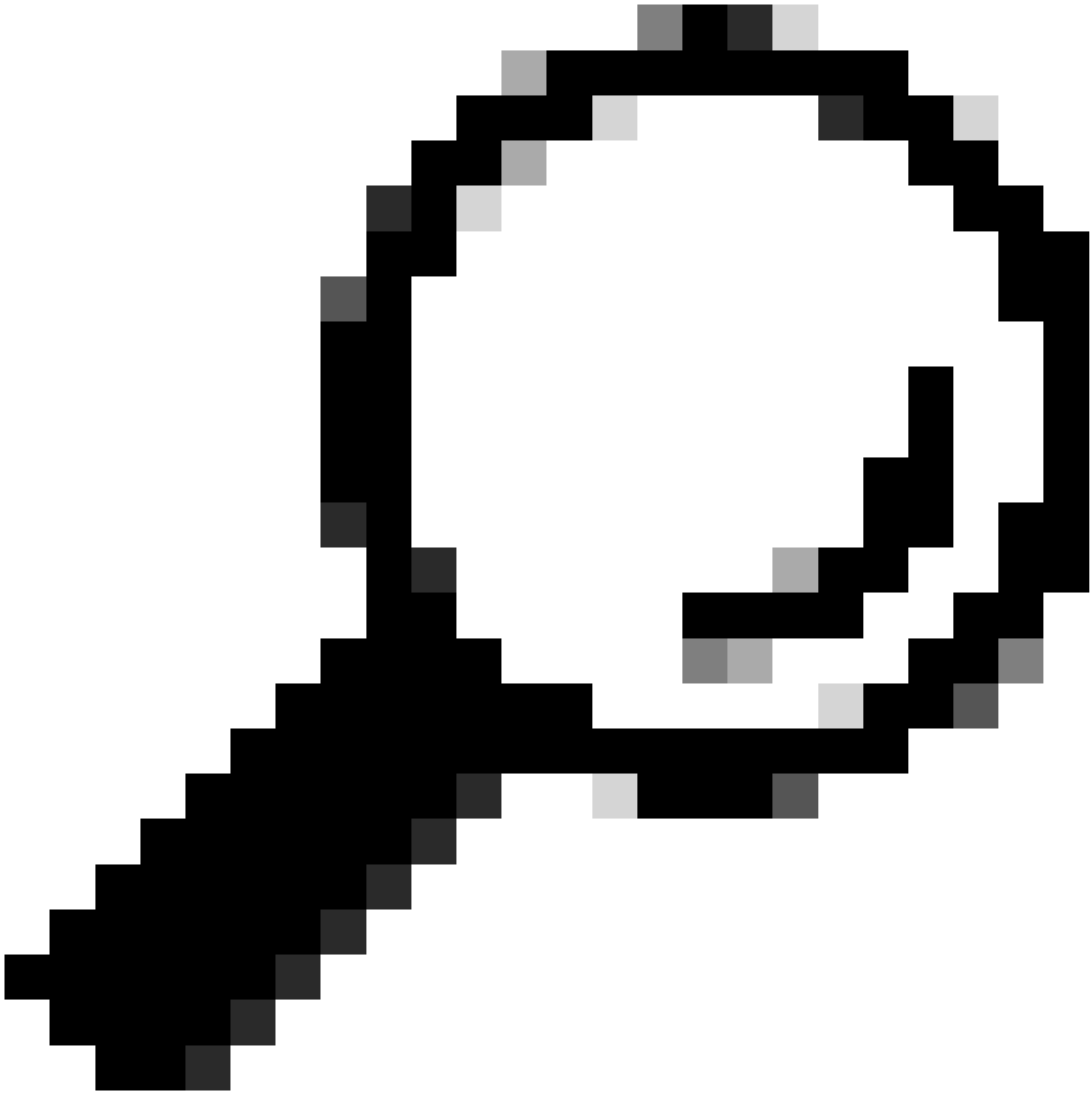
Configuración de VLAN sólo de L2: controlador de LAN inalámbrica

En el lado del WLC (controlador de LAN inalámbrica), las etiquetas de sitio asociadas con los puntos de acceso del fabric deben configurarse con "no fabric ap-arp-caching" para inhabilitar la funcionalidad ARP proxy. Además, "fabric ap-dhcp-broadcast" debe estar habilitado, esta configuración permite que los paquetes de broadcast DHCP se reenvíen desde el AP a los terminales inalámbricos.

Configuración de WLC (192.168.254.69) de fabric

<#root>

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

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



Consejo: El grupo de multidifusión inalámbrica 232.255.255.1 es el grupo predeterminado que utilizan todas las etiquetas del sitio.

<#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

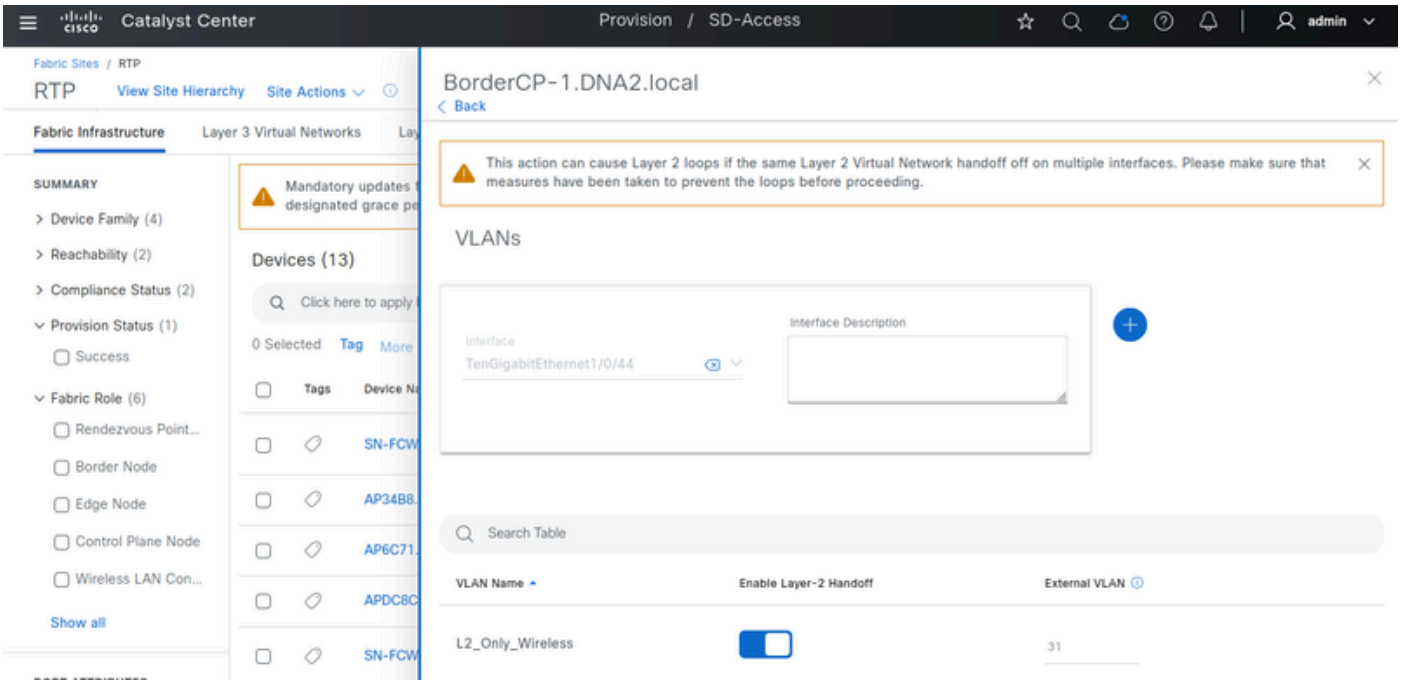
```
RTP-Site-Tag-3 Load : 0
```

Configuración de entrega de L2 (frontera del fabric)

Desde una perspectiva operativa, el servidor DHCP (o router/relé) puede conectarse a cualquier nodo de fabric, incluidos los bordes y bordes.

El uso de nodos de borde para conectar el servidor DHCP es el enfoque recomendado, sin embargo, requiere una cuidadosa consideración de diseño. Esto se debe a que el borde debe configurarse para la entrega de L2 por interfaz. Esto permite que el conjunto de fabric se transfiera a la misma VLAN que dentro del fabric o a una VLAN diferente. Esta flexibilidad en los ID de VLAN entre los bordes del entramado y los bordes es posible porque ambos están asignados al mismo ID de instancia de LISP de L2. Los puertos físicos de transferencia L2 no deben activarse simultáneamente con la misma VLAN para evitar bucles de capa 2 dentro de la red de acceso SD. Para la redundancia, se requieren métodos como StackWise Virtual, FlexLink+ o scripts EEM.

Por el contrario, la conexión del servidor DHCP o del router de la puerta de enlace a un extremo del fabric no requiere ninguna configuración adicional.



Configuración de entrega L2

Configuración de frontera de fabric/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
```

Habilitación de multidifusión inalámbrica

Los bordes del fabric se configuran para reenviar paquetes de difusión a los puntos de acceso mediante el mecanismo de túnel de acceso de inundación. estos paquetes se encapsulan en el grupo de multidifusión 232.255.255.1 en la VLAN INFRA-VN. Los puntos de acceso se unen automáticamente a este grupo de multidifusión, ya que su etiqueta de sitio está preconfigurada para utilizarlo.

```
<#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

Desde el punto de acceso, tras la asociación de un terminal inalámbrico de fabric, se forma un túnel VXLAN (dinámico en el lado del PA, siempre activo en el lado del fabric periférico). Dentro de este túnel, el grupo de multidifusión de la estructura CAPWAP se verifica con comandos del terminal AP.

<#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
```

Desde el lado del Fabric Edge, confirme que la indagación IGMP está habilitada para la VLAN de AP INFRA-VN, los puntos de acceso han formado una interfaz de túnel de acceso y se han unido al grupo multicast 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
------------------------------------------------------------------------
```

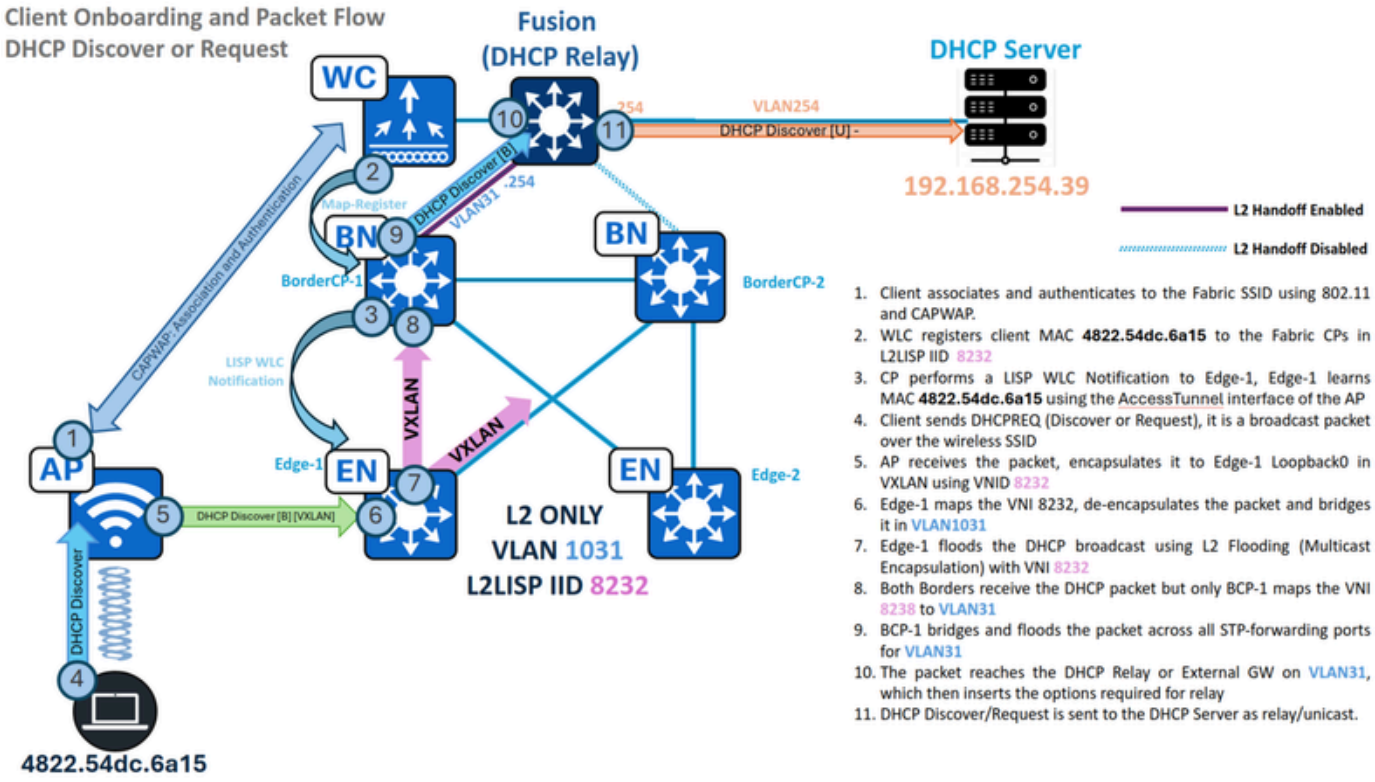
1021 232.255.255.1

```
          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>
```

Estas verificaciones confirman la correcta habilitación de la multidifusión inalámbrica en el punto de acceso, el extremo del fabric y el controlador de LAN inalámbrica.

Flujo de tráfico DHCP

Detección y solicitud de DHCP: lado inalámbrico



Flujo de tráfico: detección y solicitud de DHCP solo en L2

identifique el estado del terminal inalámbrico, su punto de acceso conectado y las propiedades de fabric asociadas.

<#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
```

Es importante confirmar que tanto las funciones de switching central como las de dhcp central están desactivadas en el perfil de políticas. Los comandos "no central dhcp" y "no central switching" deben configurarse en el perfil de política para el 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
```

Estas verificaciones confirman que el terminal está conectado a "AP1", que está asociado con el Fabric Edge RLOC 192.168.0.101. En consecuencia, su tráfico se encapsula a través de VXLAN con VNID 8232 para la transmisión desde el punto de acceso al Fabric Edge.

Detección y solicitud de DHCP - Fabric Edge

Aprendizaje de MAC con Notificación de WLC

Durante la incorporación de terminales, el WLC registra la dirección MAC del terminal inalámbrico con el plano de control del fabric. Simultáneamente, el plano de control notifica al nodo del extremo del fabric (al que está conectado el punto de acceso) que cree una entrada de aprendizaje MAC "CP_LEARN" especial, que apunte a la interfaz de túnel de acceso del punto de acceso.

<#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

Si la dirección MAC del terminal se aprende correctamente a través de la interfaz de túnel de acceso correspondiente a su punto de acceso conectado, esta etapa se considera completa.

Difusión DHCP conectada con puente en inundación de capa 2

Cuando la función DHCP Snooping está deshabilitada, las transmisiones DHCP no se bloquean; en su lugar, se encapsulan en multidifusión para la inundación de la capa 2. Por el contrario, la activación de la indagación DHCP evita la inundación de estos paquetes de difusión.

<#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>
```

Dado que la indagación DHCP está inhabilitada, la detección/solicitud DHCP utiliza la interfaz L2LISP0, puenteando el tráfico a través de la inundación L2. Dependiendo de la versión de Catalyst Center y de los Fabric Banners aplicados, la interfaz L2LISP0 puede tener listas de acceso configuradas en ambas direcciones; por lo tanto, asegúrese de que ninguna entrada de control de acceso (ACE) deniegue explícitamente el tráfico DHCP (puertos UDP 67 y 68).

<#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

Utilice el grupo de broadcast-underlay configurado para la instancia de L2LISP y la dirección IP Loopback0 del borde del entramado para verificar la entrada L2 Flooding (S,G) que une este paquete a otros nodos del entramado. Consulte las tablas mroute y mfib para validar parámetros como la interfaz entrante, la lista de interfaz saliente y los contadores de reenvío.

<#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:

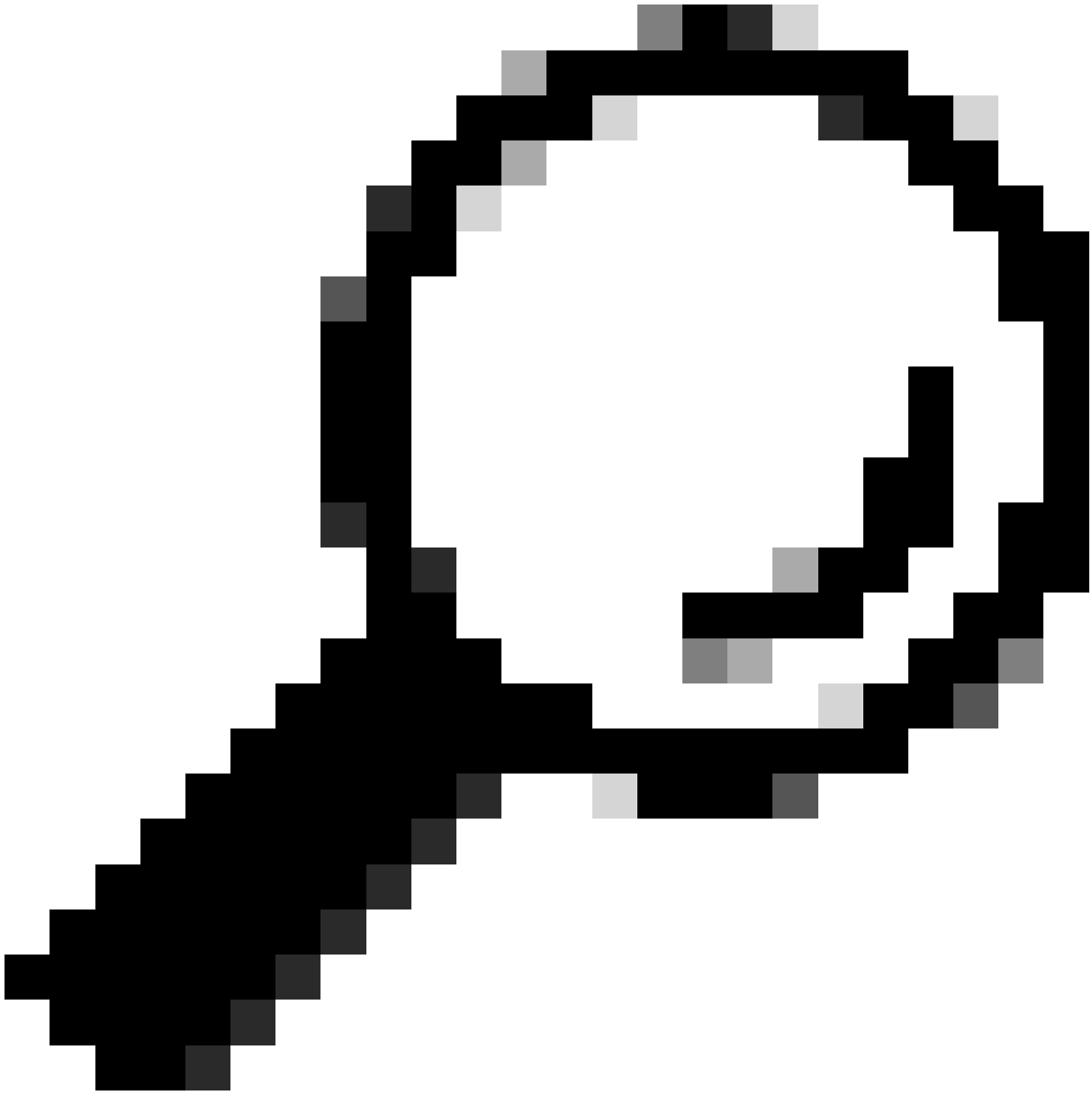
7

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

<--

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

  Totals - Source count: 1, Packet count: 8



Consejo: Consejo: Si no se encuentra una entrada (S,G) o la Lista de interfaces salientes (OIL) no contiene interfaces salientes (OIF), indica un problema con la configuración u operación de multidifusión subyacente.

Capturas de paquetes

Configure una captura de paquetes integrada simultánea en el switch para registrar tanto el paquete DHCP de ingreso del AP como el paquete de egreso correspondiente para la Inundación de L2.

Capturas de paquetes de Fabric Edge (192.168.0.101)

<#root>

```
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
```

Tras la captura de paquetes, se deben observar tres paquetes distintos:

- Detección de DHCP - VXLAN - AP al perímetro
- Detección de DHCP - CAPWAP - AP a WLC
- Detección de DHCP - VXLAN - Grupo de extremo a multidifusión

```
<#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

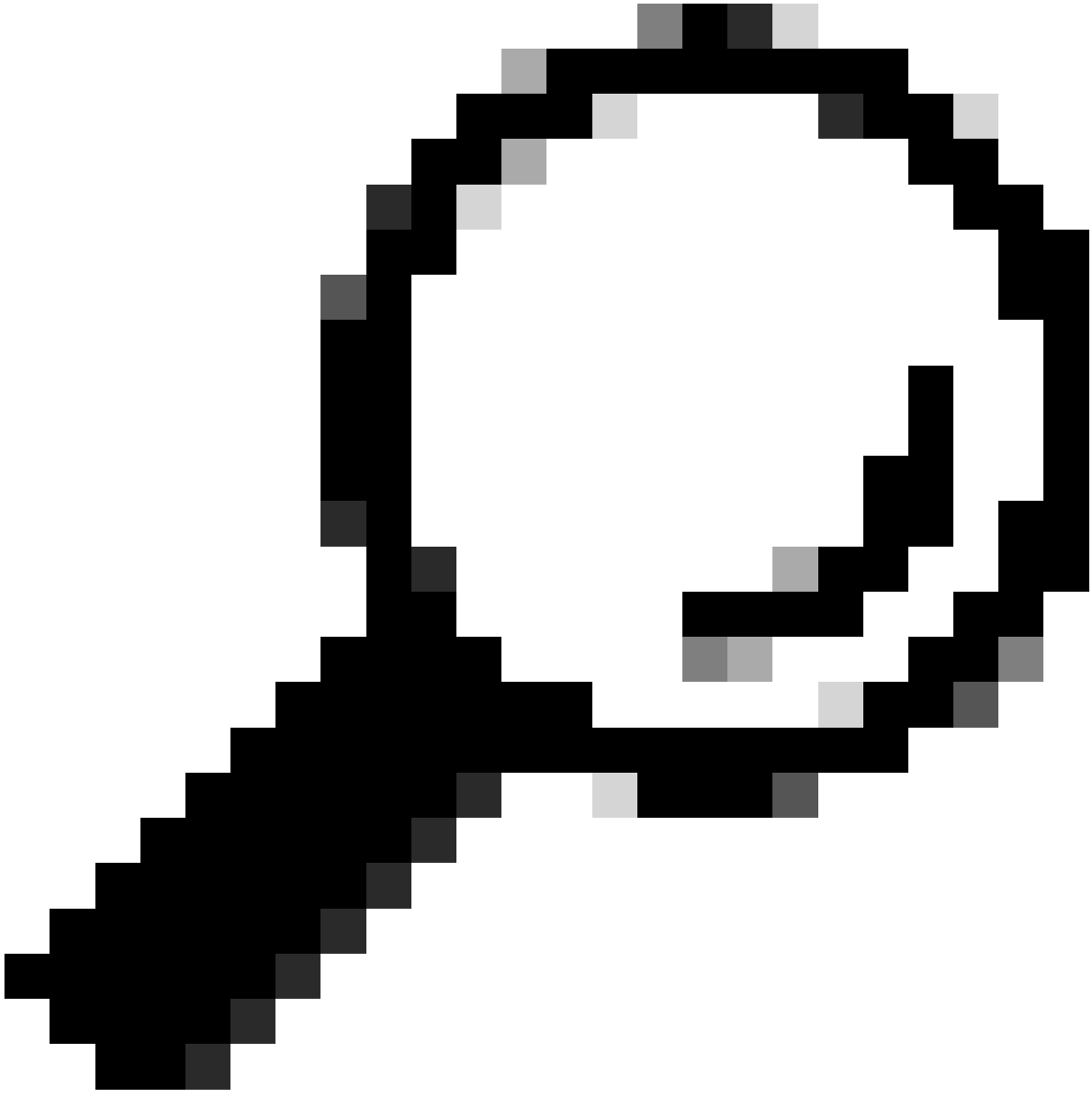
```
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
Internet Protocol Version 4, Src:
```

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



Consejo: En Fabric Enabled Wireless, los paquetes encapsulados VXLAN envían tráfico DHCP a clientes o servidores. Los paquetes encapsulados CAPWAP DATA (UDP 5247), sin embargo, transmiten al WLC únicamente con fines de seguimiento, como el estado de aprendizaje de IP o el seguimiento de dispositivos inalámbricos.

Detección y solicitud de DHCP - Borde L2

Después de que el borde envía los paquetes de detección y solicitud DHCP a través de la inundación de la capa 2, encapsulada con el grupo Broadcast-Underlay 239.0.17.1, estos paquetes son recibidos por el borde de entrega L2, específicamente el borde/CP-1 en este escenario.

Para que esto ocurra, el borde/CP-1 debe poseer una ruta multicast con el (S,G) del borde, y su lista de interfaz saliente debe incluir la instancia L2LISP de la VLAN de entrega L2. Es importante tener en cuenta que los bordes de entrega de L2 comparten el mismo ID de instancia de L2LISP, incluso si utilizan diferentes VLAN para la entrega.

<#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,

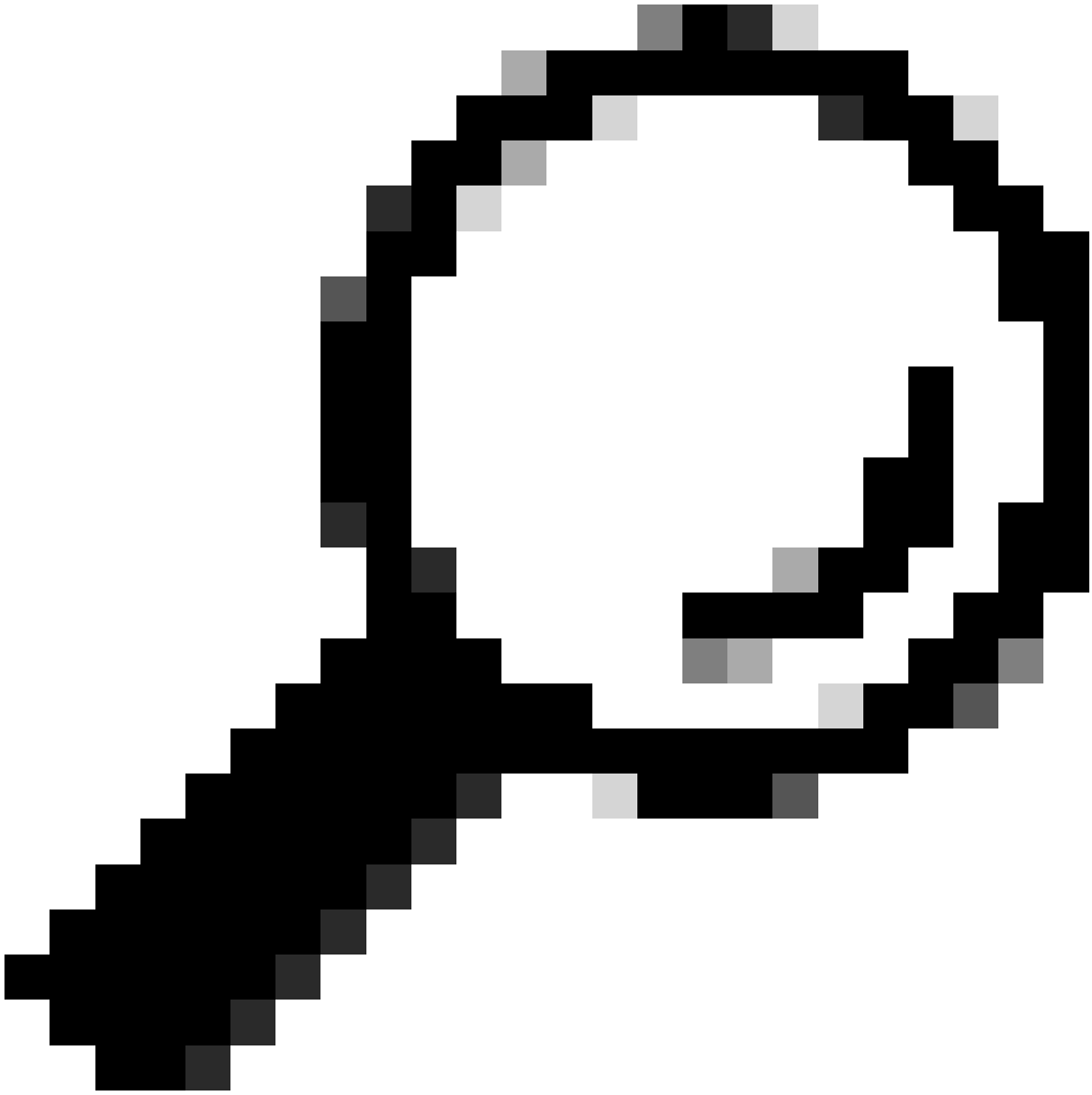
```
   SW Forwarding: 1/0/392/0, Other: 0/0/0
   HW Forwarding:
```

3

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

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

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



Consejo: Si no se encuentra una entrada (S,G), indica un problema con la configuración u operación de multidifusión subyacente. Si el L2LISP para la instancia requerida no está presente como OIF, indica un problema con el estado de operación UP/DOWN de la subinterfaz L2LISP o el estado de habilitación IGMP de la interfaz L2LISP.

De manera similar al nodo de borde del entramado, asegúrese de que ninguna entrada de control de acceso deniegue el paquete DHCP de ingreso en la interfaz L2LISP0.

<#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
```

Después de que el paquete se desencapsula y se coloca en la VLAN que coincide con VNI 8240, su naturaleza de transmisión dicta que se inundan todos los puertos de reenvío del protocolo de árbol de extensión para la VLAN de transferencia 141.

```
<#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
```

La tabla de seguimiento de dispositivos confirma que la interfaz Te1/0/44, que se conecta a la puerta de enlace/relé DHCP, debe ser un puerto de reenvío STP.

```
<#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
```

Capturas de paquetes

Configure una captura de paquetes integrada simultánea en el switch para registrar tanto el paquete DHCP entrante de L2 Flooding (interfaz entrante S,G) como el paquete de salida correspondiente a la retransmisión DHCP. En la captura de paquetes, se deben observar dos paquetes distintos: el paquete encapsulado VXLAN del Edge-1, y el paquete desencapsulado que va a la retransmisión DHCP.

Capturas de paquetes de frontera de fabric/CP (192.168.0.201)

<#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

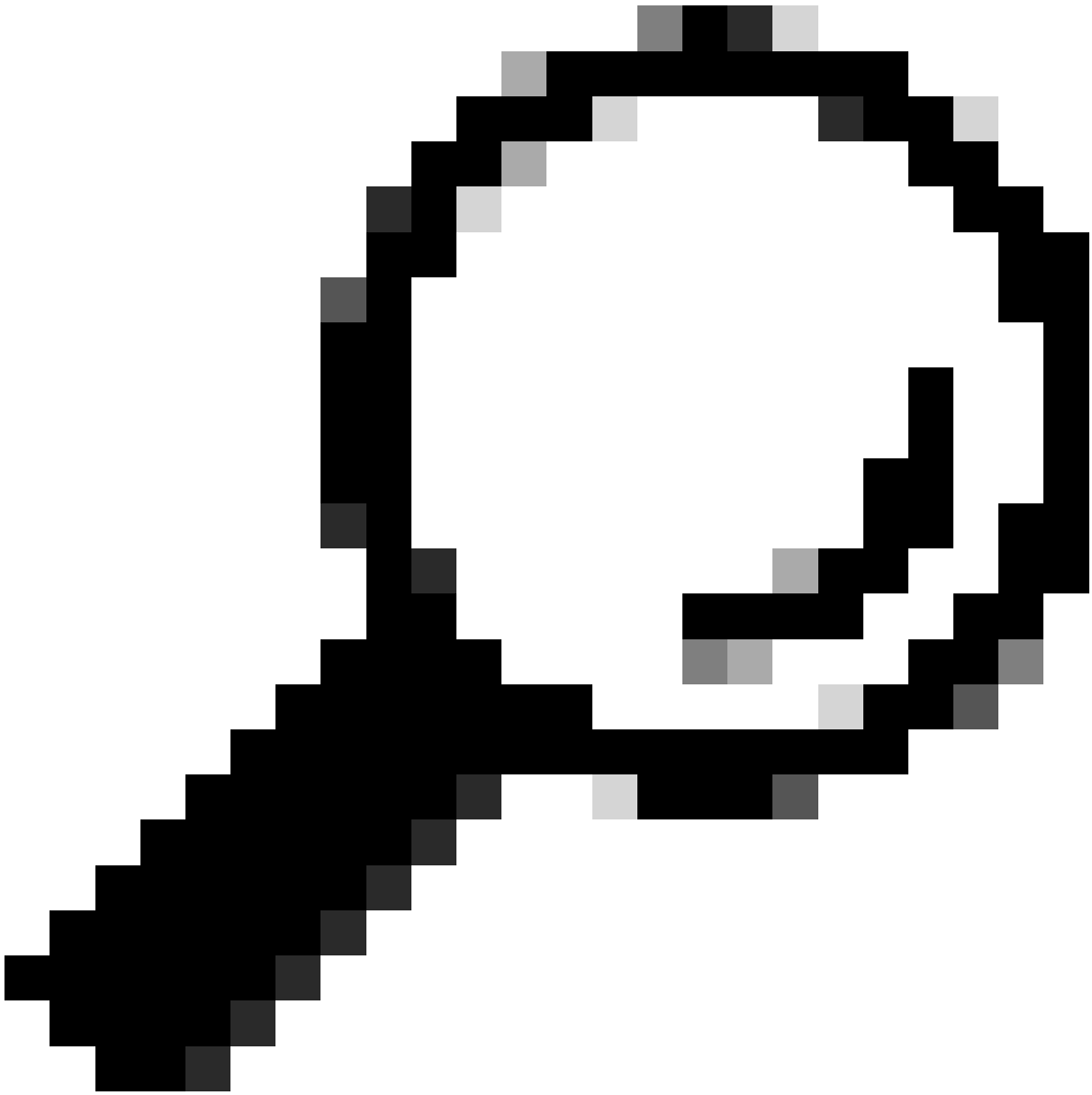
  326 16.695053 0.0.0.0 -> 255.255.255.255 DHCP

```
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
```

Llegados a este punto, el paquete Discover/Request ha salido del fabric de SD-Access, concluyendo esta sección. Sin embargo, antes de continuar, un parámetro crucial (el indicador de difusión DHCP, determinado por el propio terminal) determinará el escenario de reenvío para los paquetes Offer o ACK posteriores. Podemos examinar uno de nuestros paquetes Discover para inspeccionar este indicador.

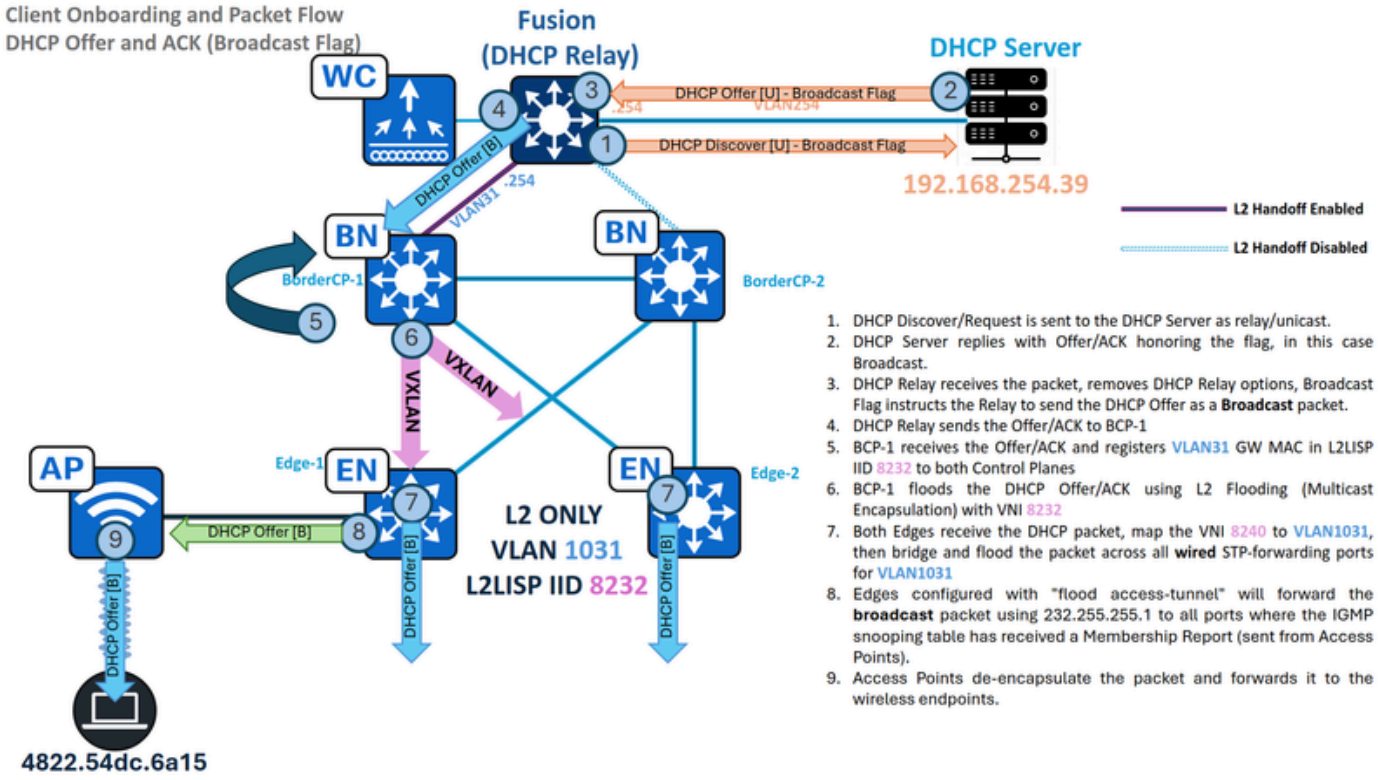
```
<#root>
BorderCP-1#
show monitor capture cap buffer display-filter "bootp.type==1 and dhcp.hw.mac_addr==4822.54dc.6a15
" detailed | sect Dynamic


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
```



Consejo: El bootp.type==1 se puede utilizar para filtrar sólo paquetes de detección y solicitud.

Oferta DHCP y ACK - Difusión - Borde L2



Flujo de tráfico: oferta de difusión de DHCP y ACK solo en L2

Ahora que DHCP Discover ha salido del entramado de acceso SD, el relé DHCP insertará las opciones de relé DHCP tradicionales (por ejemplo, GiAddr/GatewayIPAddress) y reenviará el paquete como una transmisión unicast al servidor DHCP. En este flujo, el fabric de SD-Access no anexa ninguna opción DHCP especial.

Cuando llega un DHCP Discover/Request al servidor, el servidor honra el indicador integrado Broadcast o Unicast. Este indicador determina si el Agente de retransmisión DHCP reenvía la oferta DHCP al dispositivo de flujo descendente (nuestros bordes) como una trama de difusión o unidifusión. Para esta demostración, se supone un escenario de difusión.

Registro de gateway y aprendizaje de MAC

Cuando el relé DHCP envía una oferta o ACK de DHCP, el nodo L2BN debe aprender la dirección MAC del gateway, agregarla a su tabla de direcciones MAC, luego a la tabla L2/MAC SISF y, finalmente, a la base de datos L2LISP para VLAN 141, asignada a la instancia L2LISP 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
```

Si la dirección MAC del gateway se aprende correctamente y el indicador ACK se ha marcado como "Sí" para los planos de control de fabric, esta etapa se considera completada.

Difusión DHCP conectada con puente en inundación de capa 2

Sin DHCP Snooping habilitado, las difusiones DHCP no se bloquean y se encapsulan en

multidifusión para la inundación de capa 2. Por el contrario, si se activa la función DHCP Snooping, se evita la saturación de paquetes de difusión DHCP.

<#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
```

Debido a que la detección DHCP no está habilitada en el L2Border, no se necesita la configuración DHCP Snooping Trust.

En esta etapa, la validación de L2LISP ACL ya se realiza en ambos dispositivos.

Utilice el grupo de broadcast-underlay configurado para la instancia L2LISP y la dirección IP de L2Border Loopback0 para verificar la entrada L2 Flooding (S,G) que unirá este paquete a otros nodos de fabric. Consulte las tablas mroute y mfib para validar parámetros como la interfaz entrante, la lista de interfaz saliente y los contadores de reenvío.

<#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

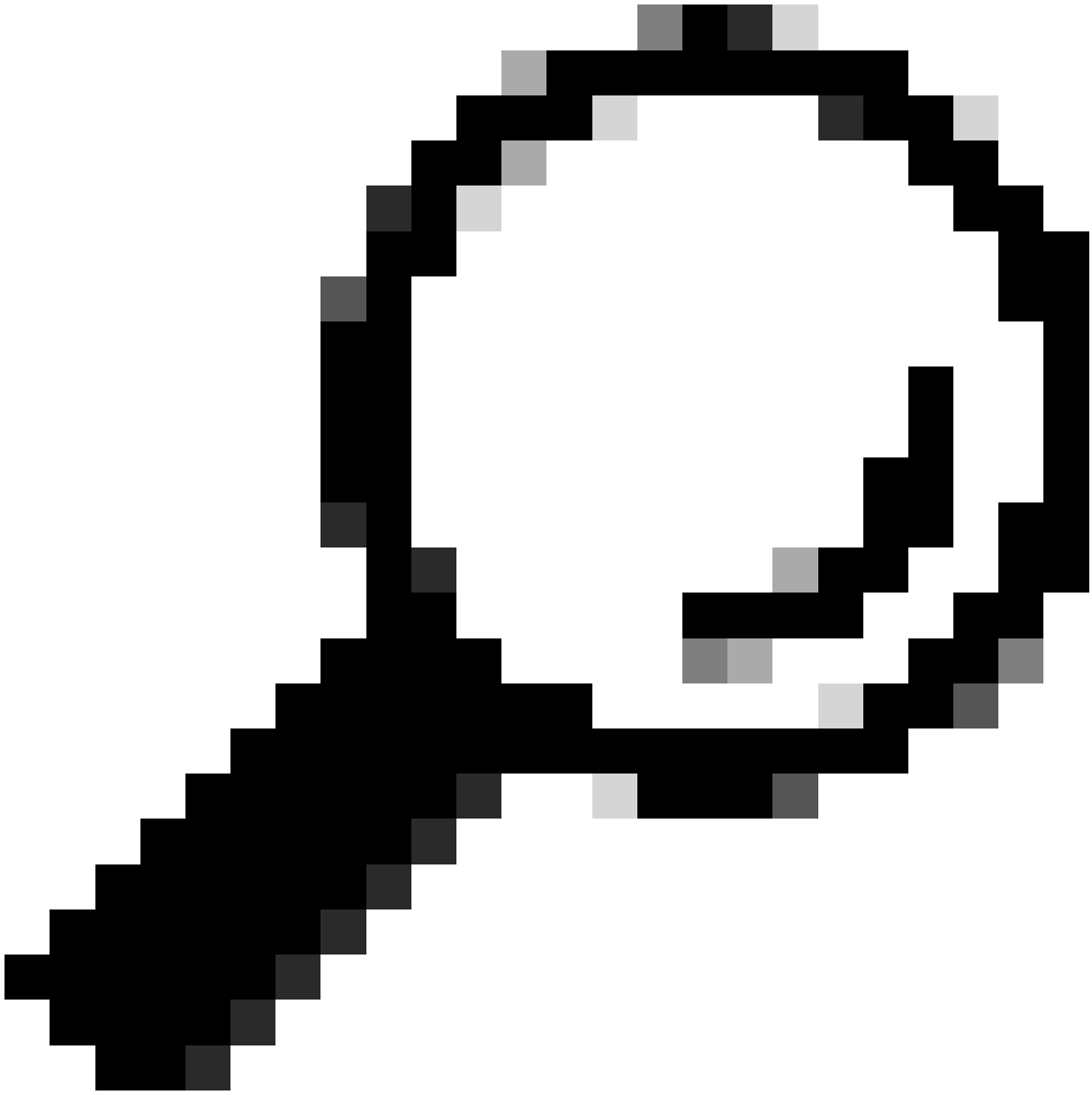
,
   SW Forwarding: 1/0/392/0, Other: 1/1/0
   HW Forwarding:

92071

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

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

  Totals - Source count: 1, Packet count: 92071



Consejo: Si no se encuentra una entrada (S,G) o la Lista de interfaces salientes (OIL) no contiene interfaces salientes (OIF), indica un problema con la configuración u operación de multidifusión subyacente.

Con estas validaciones, junto con las capturas de paquetes similares a los pasos anteriores, concluimos esta sección, ya que la oferta de DHCP se reenviará como una transmisión a todos los extremos del entramado usando el contenido de la lista de interfaz saliente, en este caso, fuera de la interfaz TenGig1/0/42 y TenGig1/0/43.

Oferta DHCP y ACK - Difusión - Extremo

Exactamente como el flujo anterior, ahora verificamos el L2Border S,G en el Fabric Edge, donde la interfaz entrante apunta hacia el L2BN y el OIL contiene la instancia L2LISP mapeada a 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,

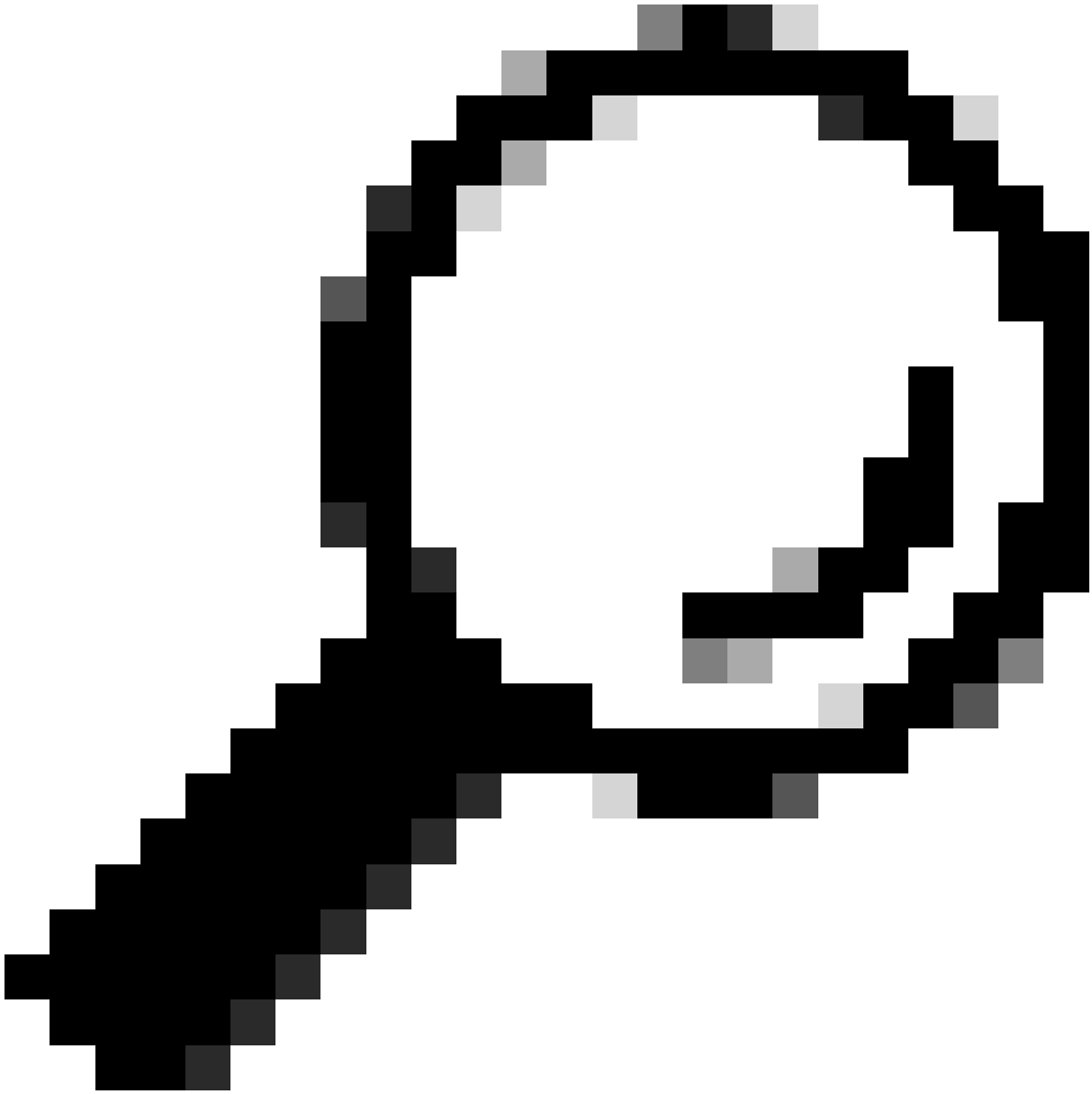
```
   SW Forwarding: 1/0/96/0, Other: 0/0/0
   HW Forwarding:
```

76236

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

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

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



Consejo: Si no se encuentra una entrada (S,G), indica un problema con la configuración u

---

operación de multidifusión subyacente. Si el L2LISP para la instancia requerida no está presente como OIF, indica un problema con el estado de operación UP/DOWN de la subinterfaz L2LISP o el estado de habilitación IGMP de la interfaz L2LISP.

La validación de L2LISP ACL ya se realiza en ambos dispositivos.

Después de que el paquete se desencapsula y se coloca en la VLAN que coincide con VNI 8232, su naturaleza de transmisión dicta que se inunden todos los puertos de reenvío del protocolo de árbol de extensión cableado para VLAN1031.

<#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
```

Sin embargo, la interfaz que buscamos para difundir la oferta de DHCP es la interfaz de túnel de acceso asociada con el punto de acceso. Esto sólo es posible porque "flood access-tunnel" está habilitado en el L2LISP ID 8232; de lo contrario, este paquete se bloquea para reenviarse a la interfaz AccessTunnel.

<#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
```

Con la entrada de indagación IGMP para el grupo de inundación multicast, las ofertas DHCP y los ACK se reenvían al puerto físico del AP.

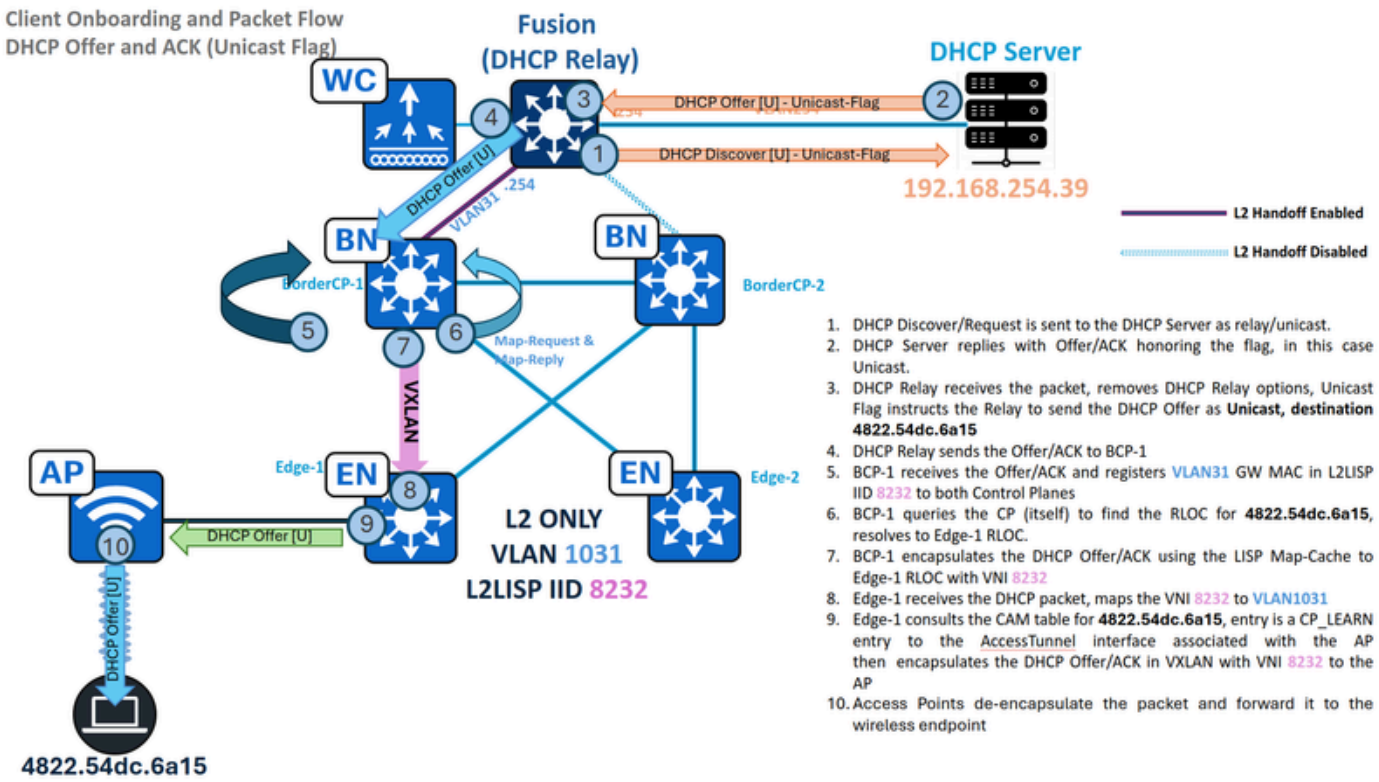
La oferta DHCP y el proceso ACK siguen siendo coherentes. Sin DHCP Snooping habilitado, no se crea ninguna entrada en la tabla DHCP Snooping. En consecuencia, la entrada de seguimiento de dispositivos para el extremo habilitado para DHCP es generada por paquetes ARP obtenidos. También se espera que los comandos como "show platform dhcpsnooping client stats" no muestren datos, ya que el snooping de DHCP está deshabilitado.

<#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
```

Oferta DHCP y ACK - Unidifusión - Borde L2



Flujo de tráfico: oferta de unidifusión de DHCP y ACK solo en L2

Aquí el escenario es un poco diferente, el punto final establece el indicador de difusión DHCP como unset o "0".

La retransmisión DHCP no envía la oferta/ACK de DHCP como difusión, sino como un paquete de unidifusión en su lugar, con una dirección MAC de destino derivada de la dirección de hardware

del cliente dentro de la carga útil DHCP. Esto modifica drásticamente la manera en que el entramado de acceso SD maneja el paquete, utiliza L2LISP Map-Cache para reenviar el tráfico, no el método de encapsulación multicast de Inundación de Capa 2 .

Captura de paquetes de frontera de fabric/CP (192.168.0.201): Oferta DHCP de entrada

<#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)

En esta situación, la inundación de capa 2 se utiliza exclusivamente para las solicitudes/detecciones, mientras que las ofertas/acks se reenvían a través de las memorias caché de mapas de L2LISP, lo que simplifica el funcionamiento general. Siguiendo los principios de reenvío de unidifusión, el borde L2 consulta al plano de control la dirección MAC de destino. Suponiendo que "MAC Learning and WLC Notification" se realice correctamente en el Fabric Edge, el plano de control tiene este ID de terminal (EID) registrado.

<#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
```

Después de la consulta del borde al plano de control (local o remoto), la resolución de LISP establece una entrada de Map-Cache para la dirección MAC del punto final.

```
<#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        -
```

Con el RLOC resuelto, la oferta DHCP se encapsula en unidifusión y se envía directamente al Edge-1 en 192.168.0.101, con 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
```

Con la misma metodología que en las secciones anteriores, capture el tráfico de entrada desde la retransmisión DHCP y a la interfaz de salida RLOC para observar la encapsulación VXLAN en unidifusión a la RLOC de borde.

Oferta DHCP y ACK - Unidifusión - Extremo

El extremo recibe la oferta/ACK de DHCP de unidifusión del borde, desencapsula el tráfico y consulta su tabla de direcciones MAC para determinar el puerto de salida correcto. A diferencia de las ofertas/ACK de difusión, el nodo perimetral reenviará el paquete solo al túnel de acceso específico en el que está conectado el terminal, en lugar de inundarlo a todos los puertos.

La tabla de direcciones MAC identifica el puerto AccessTunnel2 como nuestro puerto virtual asociado al 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

La oferta DHCP y el proceso ACK siguen siendo coherentes. Sin DHCP Snooping activado, no se crea ninguna entrada en la tabla DHCP Snooping. En consecuencia, la entrada de Seguimiento de dispositivos para el extremo habilitado para DHCP es generada por paquetes ARP obtenidos, no por DHCP. También se espera que comandos como "show platform dhcpsnooping client stats" no muestren datos, ya que la indagación DHCP está deshabilitada.

<#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
```

Es fundamental tener en cuenta que el fabric de SD-Access no influye en el uso del indicador de unidifusión o difusión, ya que se trata únicamente de un comportamiento de terminal. Aunque esta funcionalidad puede ser anulada por la retransmisión DHCP o el propio servidor DHCP, ambos mecanismos son esenciales para el funcionamiento perfecto de DHCP en un entorno L2 Only: Inundación de capa 2 con multidifusión subyacente para ofertas/ACK de difusión y registro de terminales adecuado en el plano de control para ofertas/ACK de unidifusión.

Transacción DHCP: verificación inalámbrica

Desde el WLC, la transacción DHCP se monitorea a través de 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

Al final de la transacción, el terminal se agrega a la base de datos de seguimiento de dispositivos en el controlador de LAN inalámbrica.

<#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

Toda la transacción DHCP se depura en el propio punto de acceso.

<#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:
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: 1754890669.36
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**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).