Resolución de problemas de DHCP solo en la capa 2 de VLAN con cables

Contenido

Introducción

Este documento describe cómo resolver problemas de DHCP para terminales cableados 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)

Requisitos de hardware y software

- Catalyst 9000 Series Switch
- Catalyst Center Versión 2.3.7.9
- 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

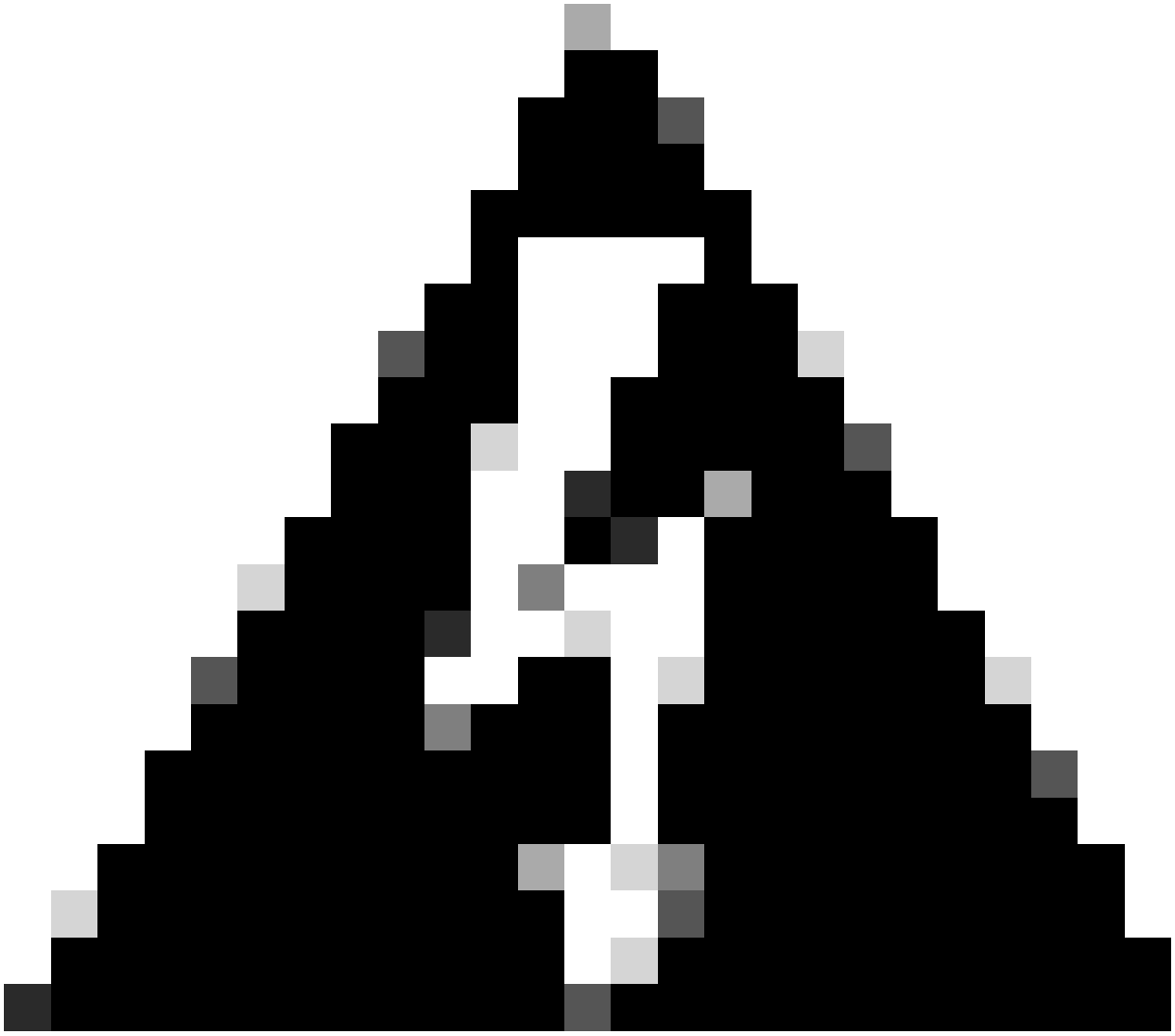
reenvía mediante los procesos de reenvío de LISP estándar, principalmente a través de las memorias caché de mapas.

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.

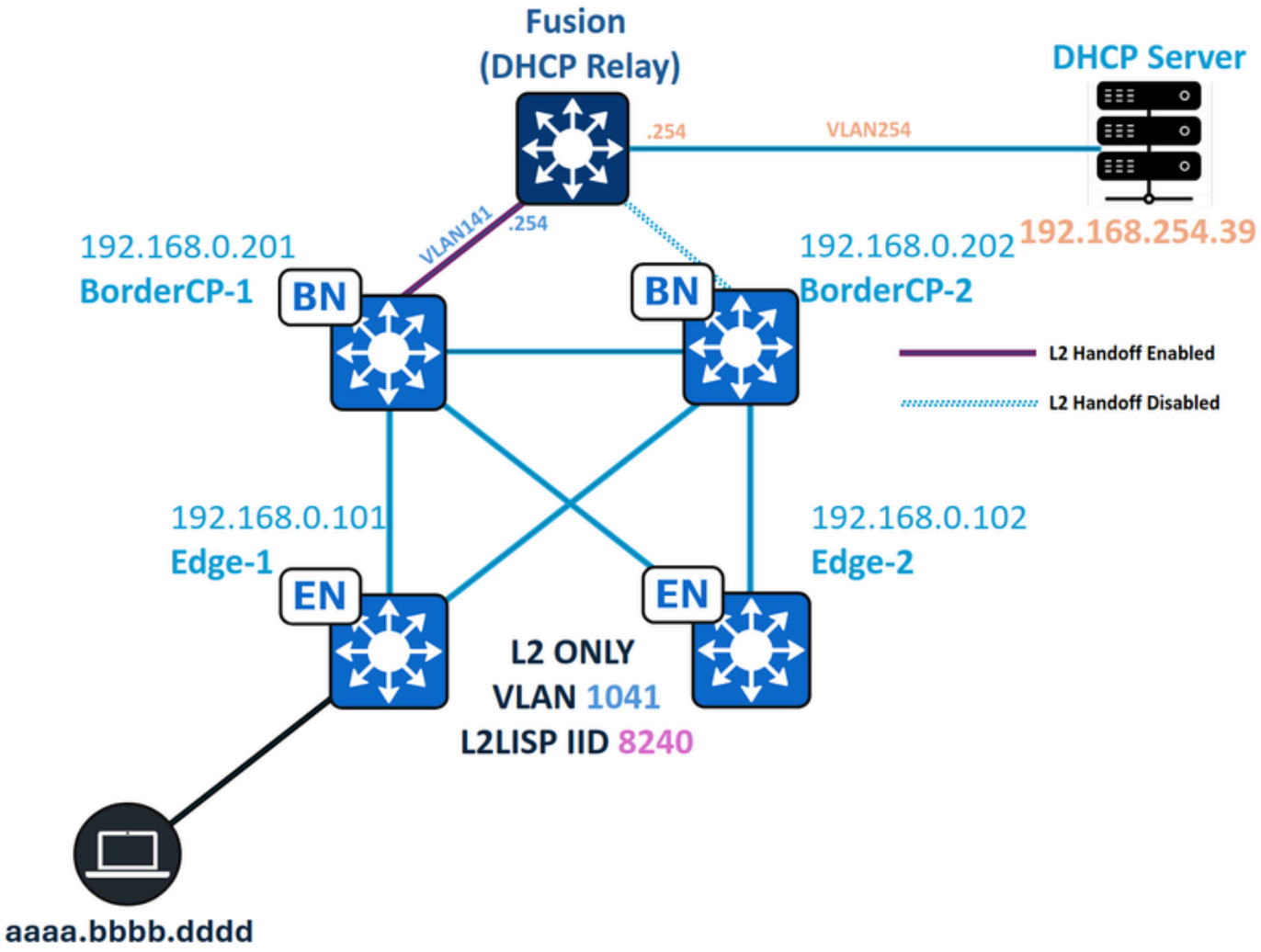
Servidor DHCP dentro del entramado de acceso SD

Una pregunta de diseño común es si un servidor DHCP se puede implementar dentro de un fabric de SD-Access. La respuesta, en esencia, es sí y no.

El Cisco Validated Design oficial recomienda que el servidor DHCP se coloque fuera del fabric, normalmente dentro del bloque de Shared Services. Sin embargo, si las circunstancias requieren la conexión física del servidor DHCP a un nodo de fabric (por ejemplo, un borde o un borde), el único método admitido es a través de una red L2 Only. Esto se debe al comportamiento inherente de los grupos de puertas de enlace de difusión ilimitada, en los que la función DHCP Snooping está activada de forma predeterminada. Esto no solo bloquea las ofertas y confirmaciones de DHCP del servidor, sino que también evita que se reenvíen los paquetes de detección y solicitud de DHCP, incluso cuando estén encapsulados en VXLAN. Mientras que "DHCP Snooping Trust" en los puertos del servidor DHCP permite que los paquetes Offers y Acknowledges, Discover y Request no se reenvíen utilizando el mismo método. Además, la eliminación de la detección DHCP en un grupo de puertas de enlace de difusión ilimitada no es una opción admitida, ya que Catalyst Center indica dicha desviación de la configuración durante la validación de conformidad.

Por el contrario, cuando el servidor DHCP se ubica dentro de una red L2 Only, no se aplica la indagación DHCP, lo que permite que todos los paquetes DHCP pasen sin inspección o bloqueo basado en políticas. El dispositivo de red de flujo ascendente del fabric de acceso SD (por ejemplo, un router Fusion) se configura como el gateway para la red de solo L2, lo que permite que el tráfico de varios VRF acceda al mismo servidor DHCP dentro de ese segmento de solo L2.

Topología



Topología de red

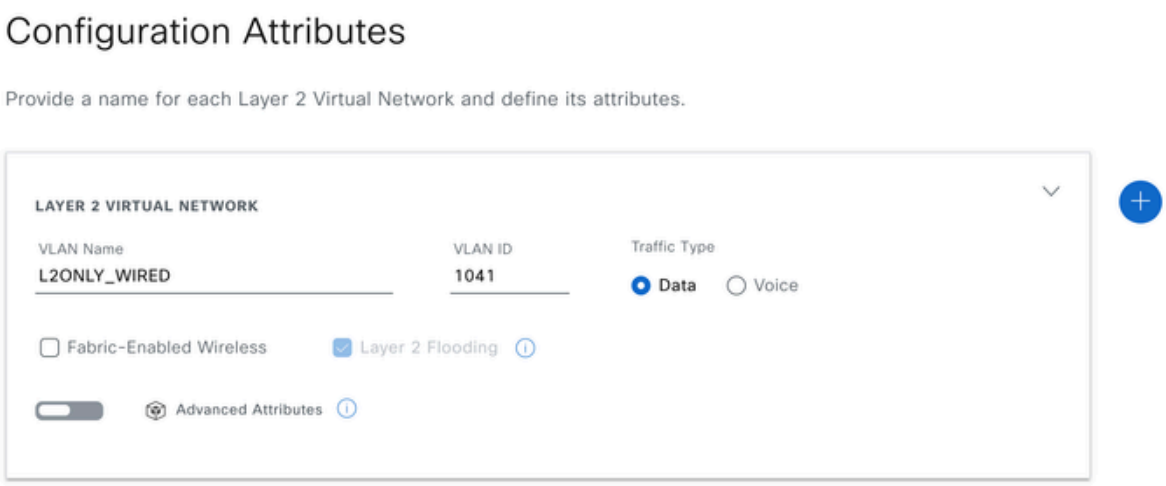
En esta topología:

- 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
- 192.168.254.39 es el servidor DHCP
- aaaa.bbbb.dddd es el punto final 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

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 solo L2 no es un grupo inalámbrico; por lo tanto, las funciones que se encuentran típicamente en los grupos inalámbricos de L2 solamente, tales como RA-Guard, DHCPGuard, y el túnel de acceso de inundación, no se configuran. En cambio, la inundación de paquetes ARP se habilita explícitamente con "flood arp-nd"

Configuración de Fabric Edge (192.168.0.101)

<#root>

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

1041

```
vlan
```

1041

name L2ONLY_WIRED

no ip igmp snooping vlan 1041 querier

no ip igmp snooping vlan 1041

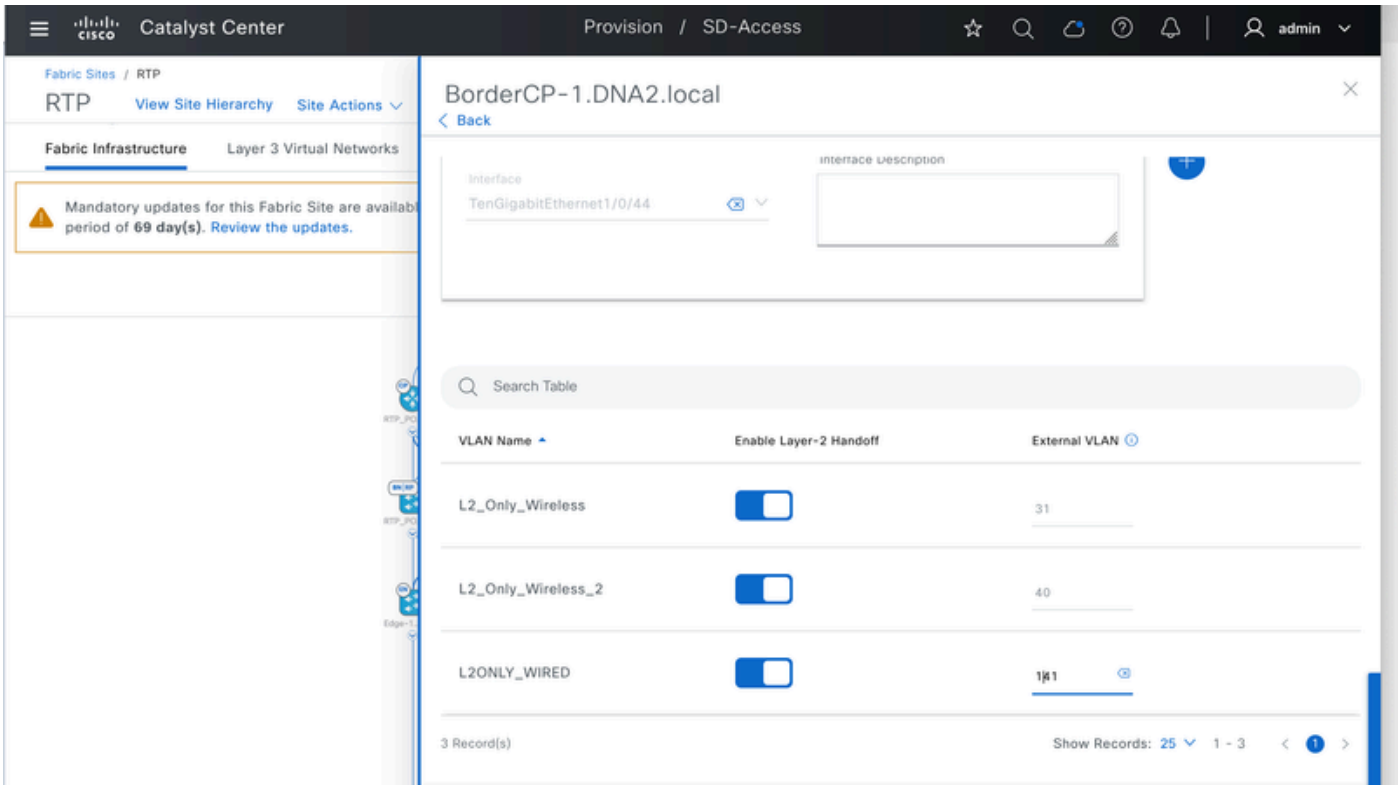
```
no ipv6 mld snooping vlan 1041


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

Configuración de entrega de L2 - Borde 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 del borde del fabric (192.168.0.201)

<#root>

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

141

```
vlan
```

141

name L2ONLY_WIRED

no ip igmp snooping vlan 141 querier

no ip igmp snooping vlan 141

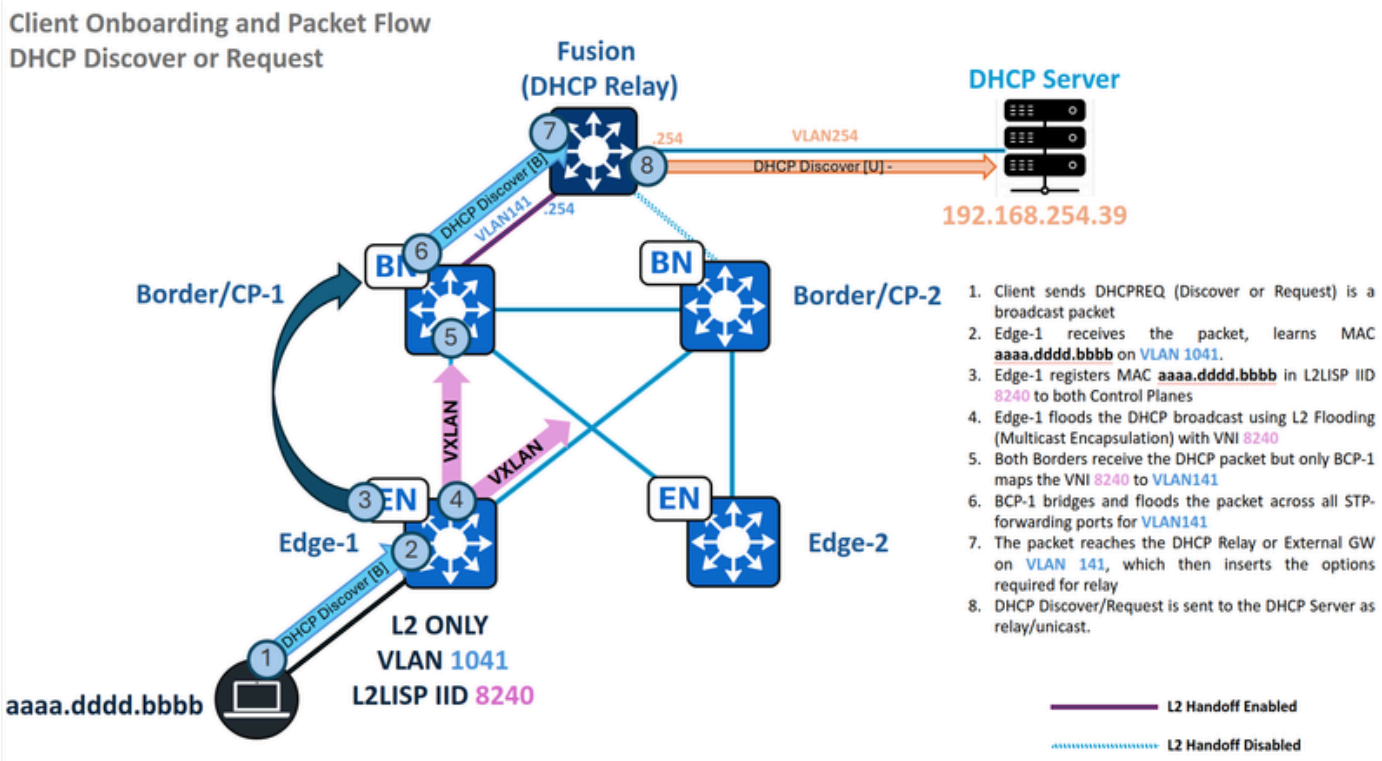
no ipv6 mld snooping vlan 141

```
router lisp
 instance-id
```

```
8240

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

eid-table


vlan 141



 broadcast-underlay 239.0.17.1


   flood arp-nd


   flood unknown-unicast


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

interface TenGigabitEthernet1/0/44


  switchport mode trunk
```

Flujo de tráfico DHCP

Detección y solicitud de DHCP - Extremo



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

Aprendizaje de MAC y registro de terminales

Cuando el punto final aaaa.dddd.bbbb envía un DHCP Discover o Request (un paquete de difusión), el nodo de borde debe aprender la dirección MAC del punto final, agregarlo a su tabla de direcciones MAC, luego a la tabla L2/MAC SISF y, finalmente, a la base de datos L2LISP para VLAN 1041, asignada a la instancia L2LISP 8240.

<#root>

Edge-1#

show mac address-table interface te1/0/2

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

1041

aaaa.dddd.bbbb

DYNAMIC

Te1/0/2

Edge-1#

show vlan id 1041

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

1041 L2ONLY_WIRED



active

    L2LI0:

8240

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

Edge-1#

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


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

Edge-1#

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


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

8240



aaaa.dddd.bbbb

   N/A           6d04h     never

0



Edge-1#

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


LISP ETR MAC Mapping Database for LISP 0 EID-table

Vlan 1041 (IID 8240)

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

aaaa.dddd.bbbb/48

,

dynamic-eid Auto-L2-group-8240

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

 192.168.0.101
```

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

  192.168.0.201

  6d04h

Yes

  0

  192.168.0.202

 6d04h

Yes

  0
```

Si la dirección MAC del terminal 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

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 is enabled


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

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


<--

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


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

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 8240

interface L2LISP0.8240

instance-id 8240

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

 broadcast-underlay 239.0.17.1

Edge-1#

show ip mroute 239.0.17.1 192.168.0.101 | be \(

(192.168.0.101, 239.0.17.1)

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

Null0

, RPF nbr 0.0.0.0

<--

Local S,G IIF must be Null0

  Outgoing interface list:

 TenGigabitEthernet1/1/2

,

Forward

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

<--

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

 TenGigabitEthernet1/1/1

,

Forward

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

<--

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

Edge-1#

show ip mfib 239.0.17.1 192.168.0.101 count

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

239.0.17.1

  Source:

192.168.0.101

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

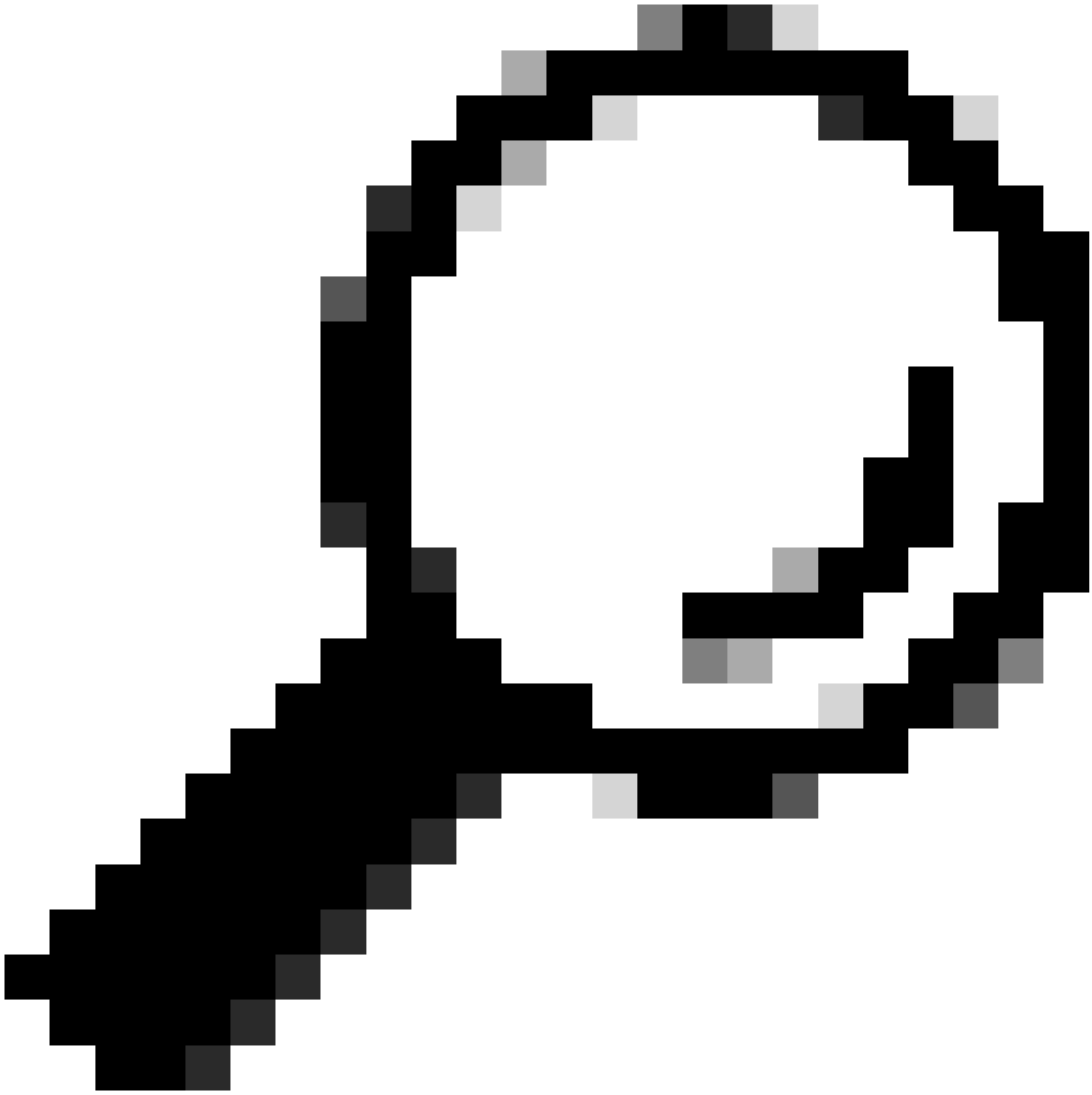
 7

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

<--

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

  Totals - Source count: 1, Packet count: 8



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 entrante del terminal como el paquete de salida correspondiente para la inundación de L2. Tras la captura de paquetes, se deben observar dos paquetes distintos: la detección/solicitud DHCP original y su equivalente encapsulado VXLAN, destinados al grupo subyacente (239.0.17.1).

Capturas de paquetes de Fabric Edge (192.168.0.101)

<#root>

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

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

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

Edge-1#

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

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

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

356 DHCP Discover

 - Transaction ID 0xf8e

<--

356 is the Length of the original packet

   23   2.487037   0.0.0.0 -> 255.255.255.255 DHCP

406 DHCP Discover

 - Transaction ID 0xf8e

<--

406 is the Length of the VXLAN encapsulated packet

Edge-1#

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

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

406 DHCP Discover

 - Transaction ID 0xf8e

Edge-1#

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

Internet Protocol Version 4, Src:

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

Internet Protocol Version 4, Src:

0.0.0.0, Dst: 255.255.255.255

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 L2 comparten el mismo ID de instancia de L2LISP, incluso si utilizan diferentes VLAN para la entrega.

<#root>

BorderCP-1#

show vlan id 141

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

141 L2ONLY_WIRED

active

    L2LI0:

8240

, Te1/0/44

BorderCP-1#

show ip mroute 239.0.17.1 192.168.0.101 | be \(

(192.168.0.101, 239.0.17.1)

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

TenGigabitEthernet1/0/42

, RPF nbr 192.168.98.3

<--

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

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

8240

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

BorderCP-1#

show ip mfib 239.0.17.1 192.168.0.101 count

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

239.0.17.1

  Source:

192.168.0.101

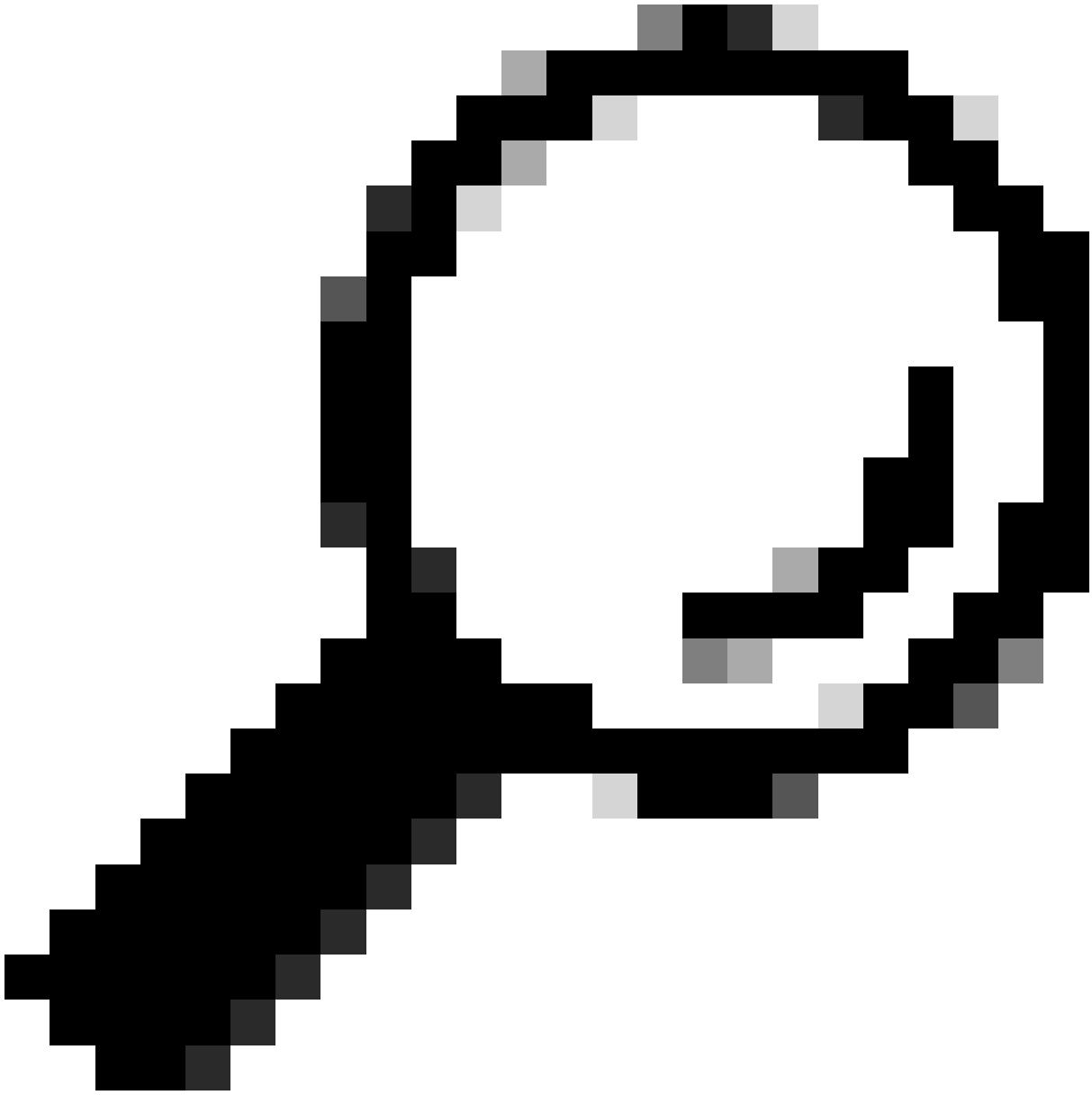
,
   SW Forwarding: 1/0/392/0, Other: 0/0/0
   HW Forwarding:

3

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

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

  Totals - Source count: 1, Packet count: 4



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 entrada en la interfaz L2LISP0.

<#root>

```
BorderCP-1#
```

show access-list SDA-FABRIC-LISP

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

40 permit ip any any
```

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 141 | 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
ARP

172.16.141.254

f87b.2003.7fc0

Te1/0/44

 141
```

```
       0005       133s       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    <-- Incoming interface for Edge's S,G Mrout

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

monitor capture cap match any

monitor capture cap buffer size 100

monitor capture cap start

monitor capture cap stop
```

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

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

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

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

Packet 427: VXLAN Encapsulated

BorderCP-1#

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

Internet Protocol Version 4, Src:

192.168.0.101, Dst: 239.0.17.1

Internet Protocol Version 4, Src:

0.0.0.0, Dst: 255.255.255.255

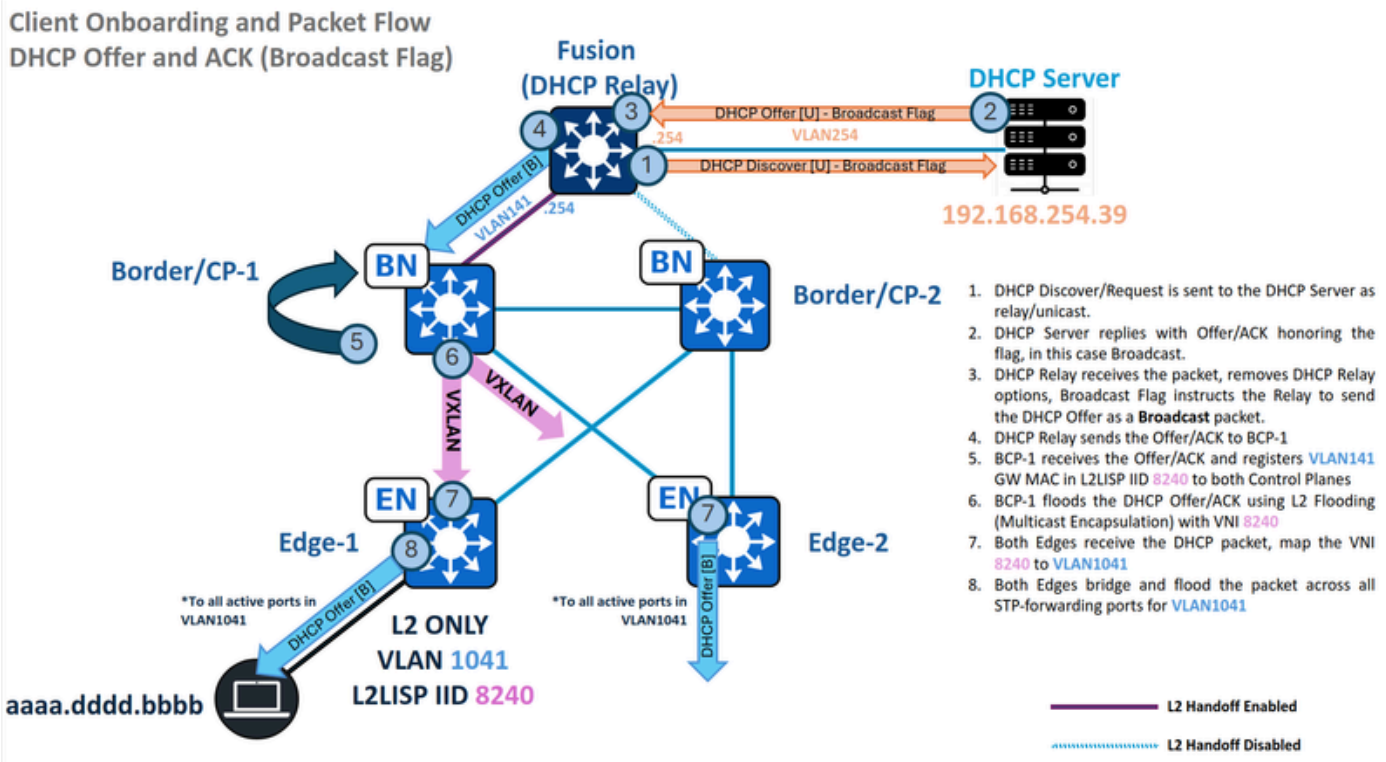
Packet 428: Plain (dot1Q cannot be captured at egress direction)

BorderCP-1#

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

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

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 inserta las opciones de relé DHCP tradicionales (por ejemplo, GiAddr/GatewayIPAddress) y reenvía 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 8240.

<#root>

BorderCP-1#

show mac address-table interface te1/0/44

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

141

f87b.2003.7fc0

    DYNAMIC

Te1/0/44
```

BorderCP-1#

show vlan id 141

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

141

L2ONLY_WIRED

               active    L2LI0:
```

8240

,

Te1/0/44

BorderCP-1#

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

MAC Interface vlan prlvl state Time left Policy

f87b.2003.7fc0

Te1/0/44 141

NO TRUST

MAC-REACHABLE

61 s LISP-DT-GLEAN-VLAN 64

BorderCP-1#

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

Dyn-EID Name Dynamic-EID Interface Uptime Last Pending

Auto-L2-group-8240

f87b.2003.7fc0

N/A 6d06h never

0

BorderCP-1#

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

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

141

(IID

8240

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

f87b.2003.7fc0/48

, dynamic-eid Auto-L2-group-8240, inherited from default locator-set rloc_0f43c5d8-f48d-48a5-a5a8-094b8
Uptime: 6d06h, Last-change: 6d06h
Domain-ID: local

```
  Service-Insertion: N/A
  Locator        Pri/Wgt  Source     State


 192.168.0.201

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


192.168.0.201

 6d06h

Yes

  0


192.168.0.202

  6d06h

Yes

  0
```

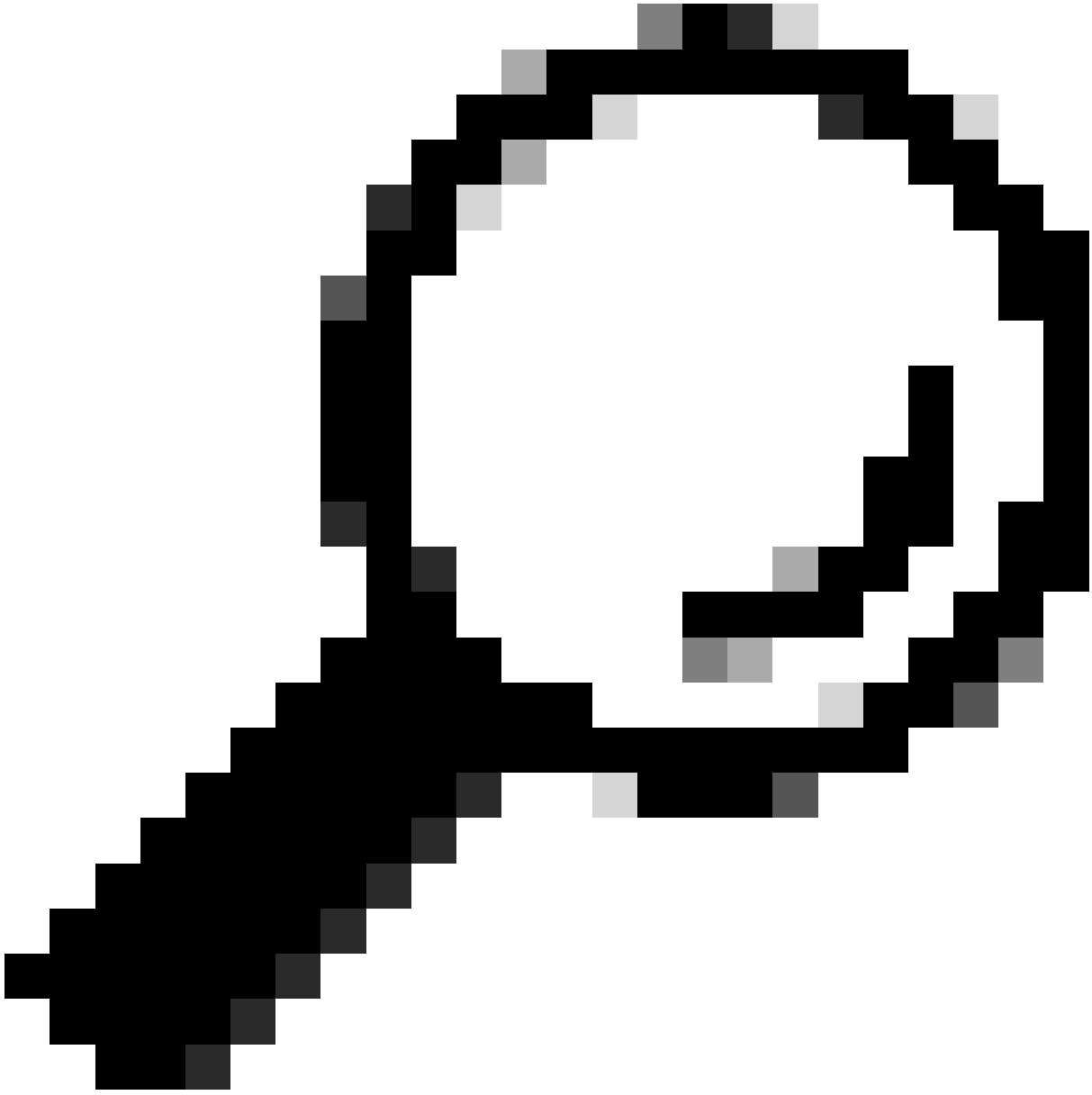
Si la dirección MAC del gateway se aprende correctamente y el indicador ACK se ha marcado como "Sí" para los planos de control de fabric, esta etapa se considera completada.

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


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



Consejo: Debido a que la indagación DHCP no está habilitada en el L2Border, la configuración de la confianza de indagación DHCP no es necesaria.

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

Utilice el grupo broadcast-underlay configurado para la instancia L2LISP y la dirección IP de L2Border Loopback0 para verificar la entrada L2 Flooding (S,G) que une 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 8240

interface L2LISP0.8240

instance-id 8240

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

broadcast-underlay 239.0.17.1

BorderCP-1#

show ip mroute 239.0.17.1 192.168.0.201 | be \(

(

192.168.0.201, 239.0.17.1

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

Null0

, RPF nbr 0.0.0.0

<-- Local S,G IIF must be Null0

  Outgoing interface list:

TenGigabitEthernet1/0/42

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

<-- Edge1 Downlink

TenGigabitEthernet1/0/43

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

<-- Edge2 Downlink

BorderCP-1#

show ip mfib 239.0.17.1 192.168.0.201 count

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

239.0.17.1

  Source:

192.168.0.201

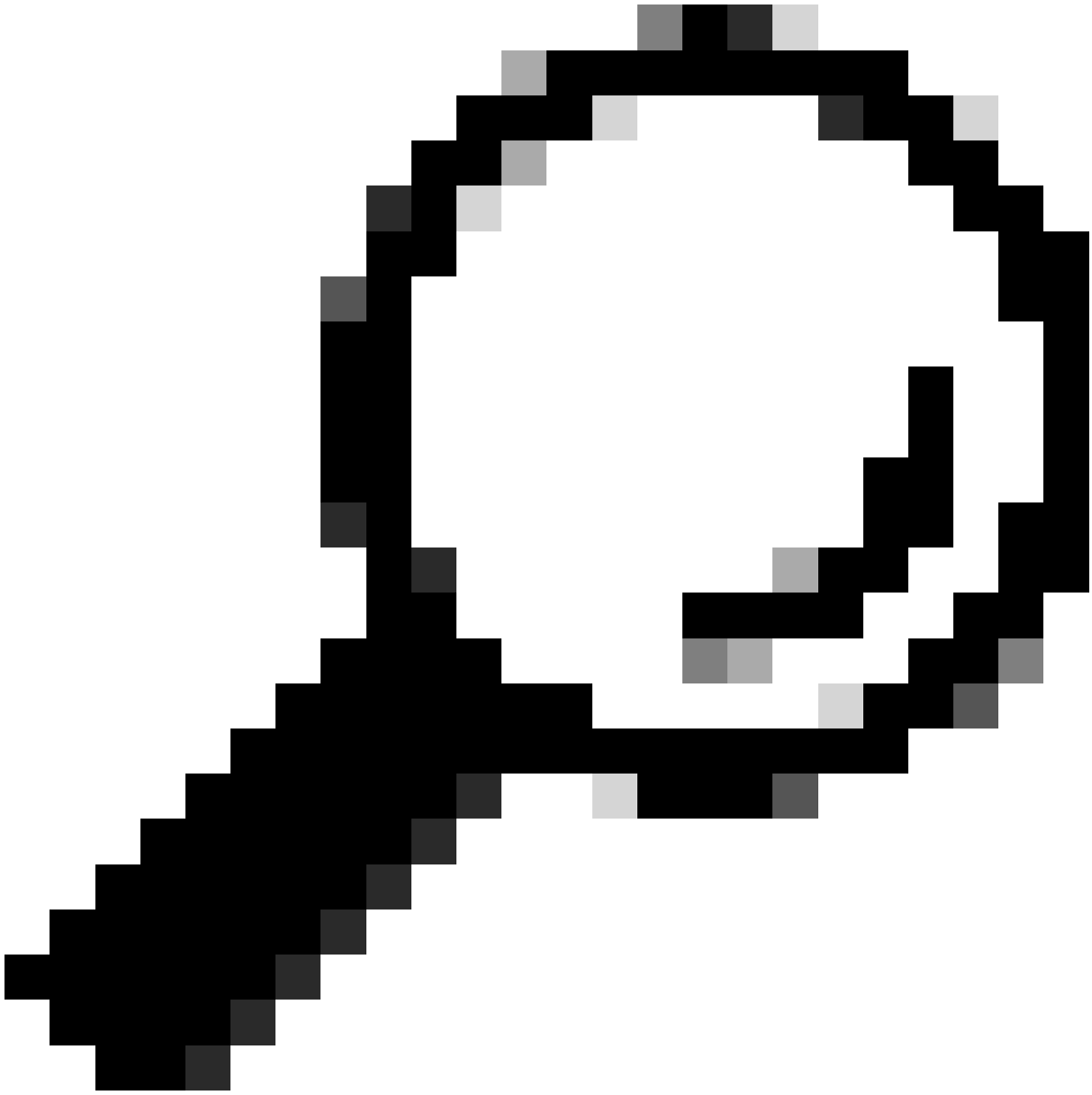
,
   SW Forwarding: 1/0/392/0, Other: 1/1/0
   HW Forwarding:

  92071

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

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

  Totals - Source count: 1, Packet count: 92071



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, se concluye esta sección, ya que la oferta DHCP se reenvía 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, verifique el L2Border S,G en el Fabric Edge, donde la interfaz entrante apunta hacia el L2BN y el OIL contiene la instancia L2LISP asignada a la VLAN 1041.

<#root>

Edge-1#

show vlan id 1041

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

1041

L2ONLY_WIRED

active

    L2LIO:

8240

,

Te1/0/2

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

Edge-1#

show ip mroute 239.0.17.1 192.168.0.201 | be \(

(

192.168.0.201

,

239.0.17.1

), 1w3d/00:01:52, flags: JT
  Incoming interface:

TenGigabitEthernet1/1/2

, RPF nbr 192.168.98.2

<-- IIF Te1/1/2 is the RPF interface for 192.168.0.201 (L2BN RLOC)

  Outgoing interface list:

L2LISP0.8240,

Forward/Sparse-Dense

,

 1w3d/00:02:23, flags:

Edge-1#

show ip mfib 239.0.17.1 192.168.0.201 count

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

239.0.17.1

  Source:

192.168.0.201,

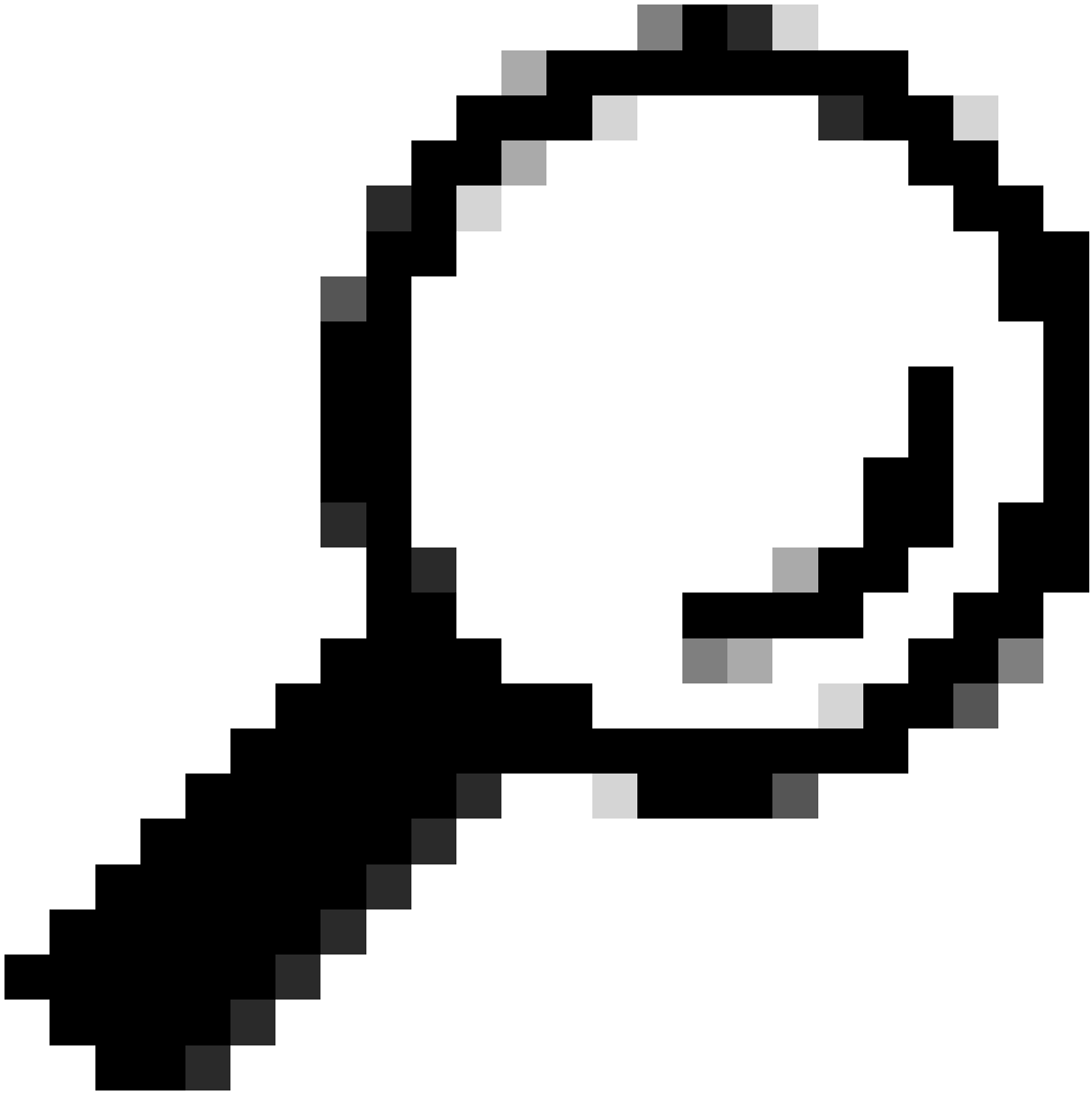
   SW Forwarding: 1/0/96/0, Other: 0/0/0
   HW Forwarding:

76236

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

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

  Totals - Source count: 1, Packet count: 4



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 8240, su naturaleza de transmisión dicta que se inundan todos los puertos de reenvío del protocolo de árbol de extensión para VLAN1041.

<#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
```

La tabla de direcciones MAC identifica el puerto Te1/0/2 como el puerto de terminal, que está en estado FWD por STP, el paquete se inunda hacia el terminal.

<#root>

Edge-1#

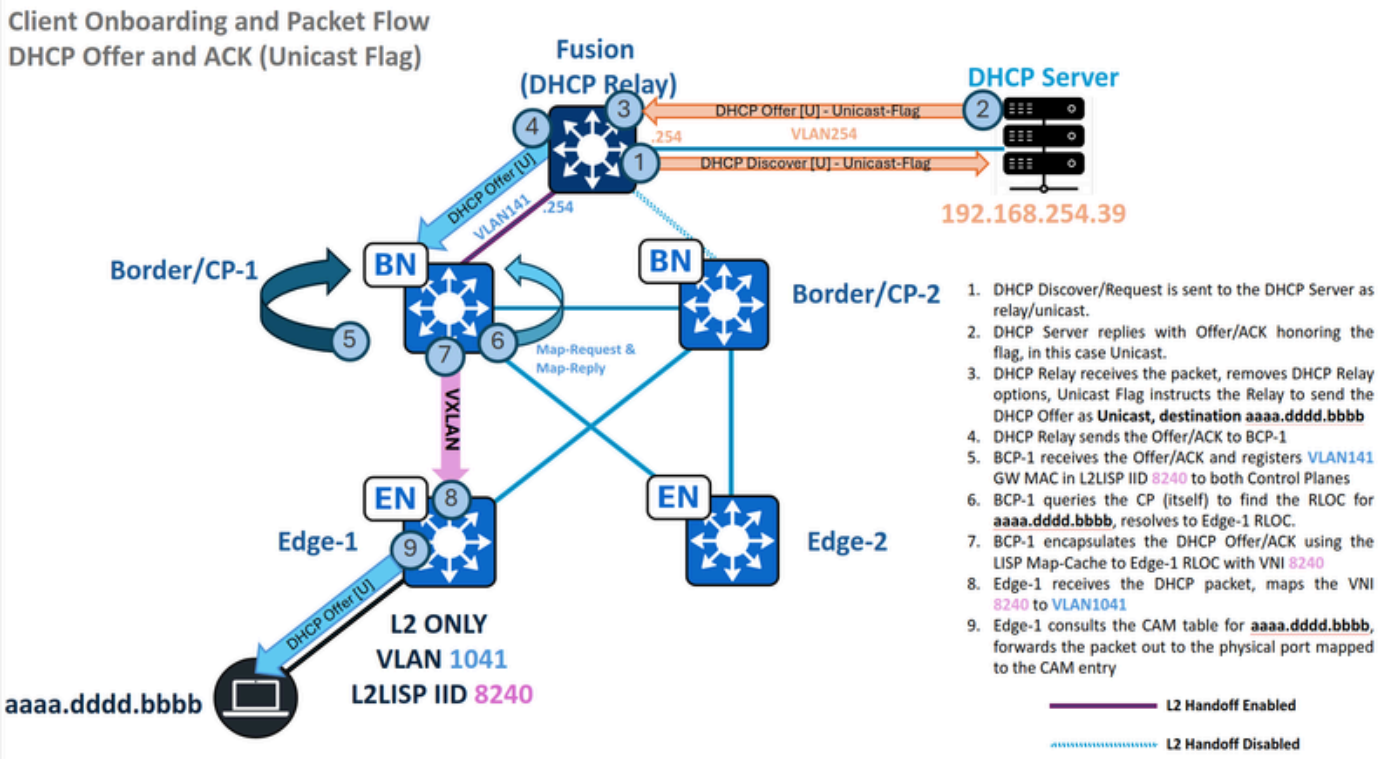
show mac address-table interface te1/0/2

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


1041


aaaa.dddd.bbbb

    DYNAMIC

Te1/0/2
```

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 Device-Tracking para el punto final habilitado para DHCP es generada por la recopilación de paquetes ARP. 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 te1/0/2 | be Network

    Network Layer Address                    Link Layer Address     Interface  vlan       prlvl      ag

ARP

172.16.141.1

 aaaa.dddd.bbbb

       Te1/0/2

1041

       0005       45s        REACHABLE  207 s try 0

Edge-1#

show ip dhcp snooping  binding vlan 1041

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

Total number of bindings: 0
```

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==aaaa.dddd.bbbb" deta


Dynamic Host Configuration Protocol (

Discover

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

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

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


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


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

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 (aaaa.dddd.bbb). Suponiendo que el "MAC Learning and Endpoint Registration" 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 8240 ethernet server aaaa.dddd.bbbb


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

aaaa.dddd.bbbb/48

 instance-id

8240


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

    Registration errors:
```

```
      Authentication failures:   0


      Allowed locators mismatch: 0



 ETR 192.168.0.101:51328

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

 192.168.0.101  yes    up          10/10   IPv4 none
```

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 8240 ethernet map-cache aaaa.dddd.bbbb


LISP MAC Mapping Cache for LISP 0 EID-table Vlan

141

 (IID

8240

), 1 entries


aaaa.dddd.bbbb/48

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

via map-reply

,

complete

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

```
  192.168.0.101
 4d07h     up      10/10        -
```

Con el RLOC resuelto, la oferta DHCP se encapsula en unidifusión y se envía directamente al Edge-1 en 192.168.0.101, utilizando VNI 8240.

```
<#root>
BorderCP-1#
show mac address-table address aaaa.dddd.bbbb

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

141

 aaaa.dddd.bbbb

CP_LEARN

L2LI0

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

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

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

Routing entry for 192.168.0.101/32
```

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


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

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 reenvía el paquete solo al puerto específico donde está conectado el terminal, en lugar de inundarlo a todos los puertos.

La tabla de direcciones MAC identifica el puerto Te1/0/2 como nuestro puerto cliente, que está en estado FWD por STP, el paquete se reenvía al terminal.

```
<#root>
Edge-1#
show mac address-table interface te1/0/2


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


1041


aaaa.dddd.bbbb

    DYNAMIC

Te1/0/2
```

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 Device-Tracking para el punto final habilitado para DHCP es generada por los 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 te1/0/2 | be Network

    Network Layer Address                    Link Layer Address     Interface  vlan       prlvl      ag

ARP


172.16.141.1


 aaaa.dddd.bbbb

       Te1/0/2

1041

       0005       45s        REACHABLE  207 s try 0

Edge-1#
show ip dhcp snooping  binding vlan 1041

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

Total number of bindings: 0
```

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.

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).