仅第2层VLAN中的DHCP故障排除 — 有线

目录

简介

本文档介绍如何在SD-Access(SDA)交换矩阵中排除仅第2层网络中有线终端的DHCP故障。

先决条件

要求

Cisco 建议您了解以下主题：

- Internet协议(IP)转发
- 定位器/ID分离协议(LISP)

- 协议无关组播(PIM)稀疏模式

硬件和软件要求

- Catalyst 9000 系列交换机
- Catalyst Center版本2.3.7.9
- Cisco IOS® XE 17.12及更高版本

限制

- 只有一个L2边界可以同时切换唯一的VLAN/VNI，除非正确配置强大的环路预防机制（如用于禁用链路的FlexLink+或EEM脚本）。

仅第2层概述

概述

在典型的SD访问部署中，L2/L3边界位于交换矩阵边缘(FE)，其中FE以SVI的形式托管客户端网关，通常称为“任播网关”。第3层VNI（路由）用于子网间流量，而第2层VNI（交换）用于管理子网内流量。跨所有FE的一致配置可实现无缝客户端漫游。转发已优化：子网内(L2)流量直接桥接在FE之间，而子网间(L3)流量则在FE之间或FE与边界节点之间路由。

对于需要位于交换矩阵外部的严格网络入口点的SDA交换矩阵中的终端，SDA交换矩阵必须提供从边缘到外部网关的L2通道。

此概念类似于传统的以太网园区部署，其中第2层接入网络连接到第3层路由器。VLAN内流量保留在L2网络中，而VLAN间流量由L3设备路由，通常返回到L2网络上的其他VLAN。

在LISP情景中，站点控制平面主要跟踪MAC地址及其相应的MAC到IP绑定，非常类似于传统ARP条目。仅L2 VNI/L2池旨在专门根据这两种EID类型促进注册、解析和转发。因此，在仅支持L2的环境中任何基于LISP的转发仅依赖MAC和MAC到IP信息，它完全忽略IPv4或IPv6 EID。为了补充LISP EID，仅第2层池在很大程度上依赖于泛洪和学习机制，类似于传统交换机的行为。因此，L2泛洪成为处理此解决方案内的广播、未知单播和组播(BUM)流量的关键组件，需要使用底层组播。相反，正常单播流量使用标准LISP转发进程进行转发，主要通过映射缓存进行转发。

交换矩阵边缘和“L2边界”(L2B)都维护映射到本地VLAN的L2 VNI（此映射在SDA内对设备具有本地意义，允许不同的VLAN跨节点映射到相同的L2 VNI）。 在此特定使用案例中，在这些节点的这些VLAN上未配置SVI，这意味着没有对应的第3层VNI。

仅第2层VLAN中的DHCP行为更改

在任播网关池中，DHCP带来了挑战，因为每个交换矩阵边缘都充当其直连终端的网关，所有FE上的网关IP相同。要正确识别DHCP中继数据包的原始源，FE必须插入DHCP选项82及其子选项，包括LISP RLOC信息。这通过交换矩阵边缘的客户端VLAN上的DHCP监听来实现。DHCP监听在此环境中具有双重作用：它有助于插入选项82，关键是防止DHCP广播数据包通过网桥域(VLAN/VNI)泛洪。 即使为任播网关启用了第2层泛洪，DHCP监听也会有效地抑制广播数据包，使其作为广播从交换矩阵边缘转发出去。

相比之下，仅第2层VLAN缺少网关，从而简化了DHCP源识别。由于数据包不由任何交换矩阵边缘中继，因此无需使用复杂的源识别机制。如果L2 Only VLAN上没有DHCP监听，DHCP数据包的泛洪控制机制将被有效绕过。这允许DHCP广播通过L2泛洪转发到其最终目的地，该目的地可以是直接连接到交换矩阵节点的DHCP服务器，或提供DHCP中继功能的第3层设备。

警告：仅L2池中的“多个IP到MAC”功能在网桥VM模式下自动激活DHCP监听，从而实施DHCP泛洪控制。因此，这会导致L2 VNI池无法支持其终端的DHCP。

底层组播

由于DHCP严重依赖广播流量，因此必须利用第2层泛洪来支持此协议。与任何其他启用第2层泛洪的池一样，必须为组播流量配置底层网络，尤其是使用PIM稀疏模式的Any-Source-Multicast。当底层组播配置通过LAN自动化工作流程自动进行时，如果省略此步骤，则需要其他配置（手动或模板）。

- 在所有节点（边界、边缘、中间节点等）上启用IP组播路由。
- 在每个Border和Edge节点的Loopback0接口上配置PIM稀疏模式。

- 在每个IGP（底层路由协议）接口上启用PIM稀疏模式。
- 在所有节点（边界、边缘、中间节点）上配置PIM交汇点(RP)，建议将RP置于边界。
- 检验PIM邻居、PIM RP和PIM隧道状态。

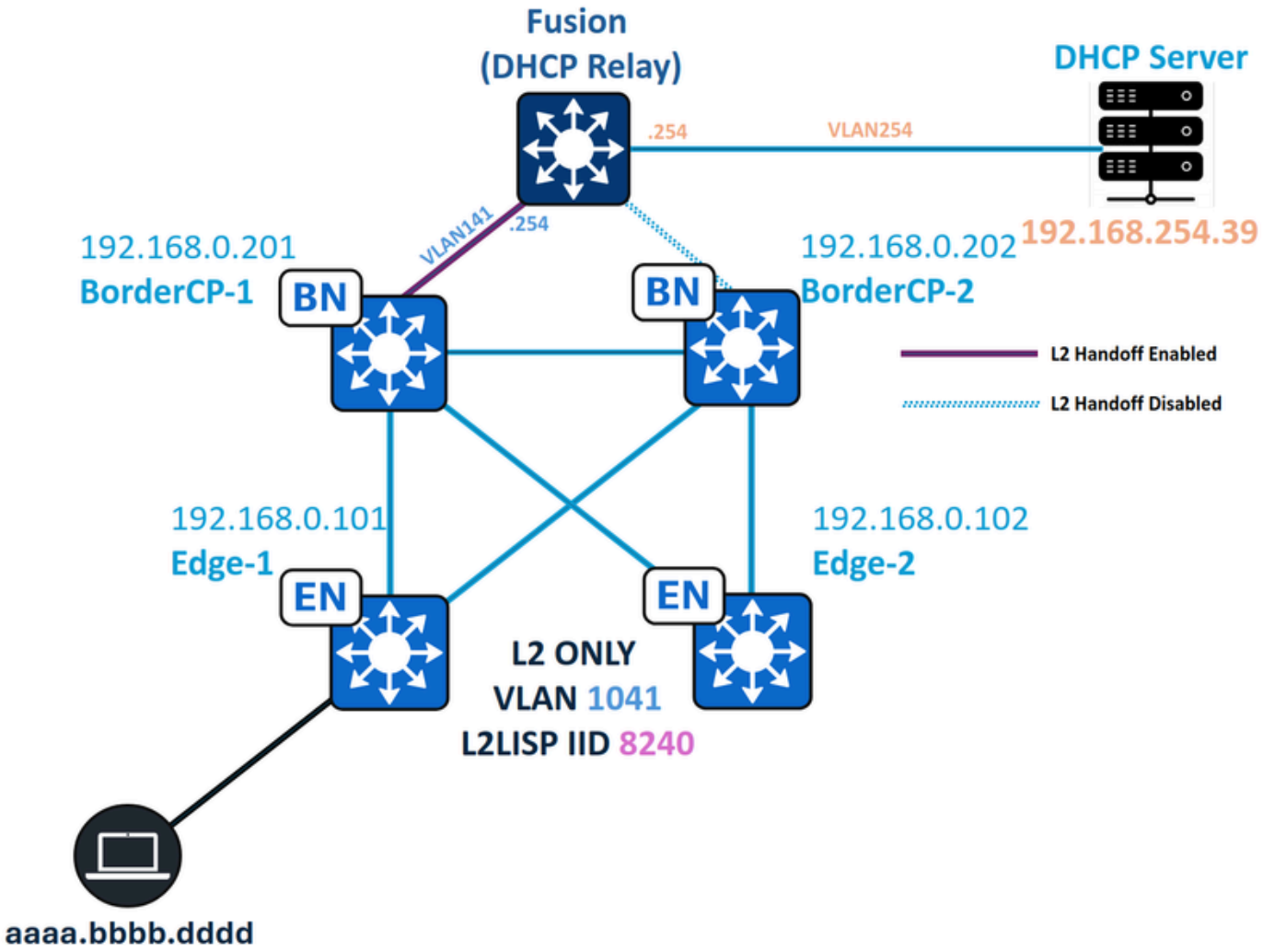
SD访问交换矩阵内部的DHCP服务器

一个常见的设计问题是是否可以在SD访问交换矩阵中部署DHCP服务器。从本质上讲，答案既是肯定的，也是否定的。

官方Cisco Validated Design建议将DHCP服务器放置在交换矩阵外部，通常放置在Shared Services块内。但是，如果情况需要DHCP服务器物理连接到交换矩阵节点（例如，边缘或边界），则唯一支持的方法是通过L2专用网络。这是因为任播网关池的固有行为，其中默认启用DHCP监听。这不仅会阻止来自服务器的DHCP提供和确认，还会阻止DHCP发现和请求数据包（即使封装在VXLAN中）被转发。虽然DHCP服务器端口上的“DHCP监听信任”允许提供和确认，但不会使用相同的方法转发发现和请求数据包。此外，不支持删除任播网关池中的DHCP监听，因为Catalyst Center会在合规性验证期间标记这样的配置偏差。

相反，当DHCP服务器置于仅第2层网络时，不会实施DHCP监听，从而允许所有DHCP数据包通过，而无需基于策略的检查或阻止。SD-Access交换矩阵上游的网络设备（例如，Fusion路由器）被配置为仅第2层网络的网关，使来自多个VRF的流量能够访问仅第2层网段中的同一DHCP服务器。

拓扑



网络拓扑

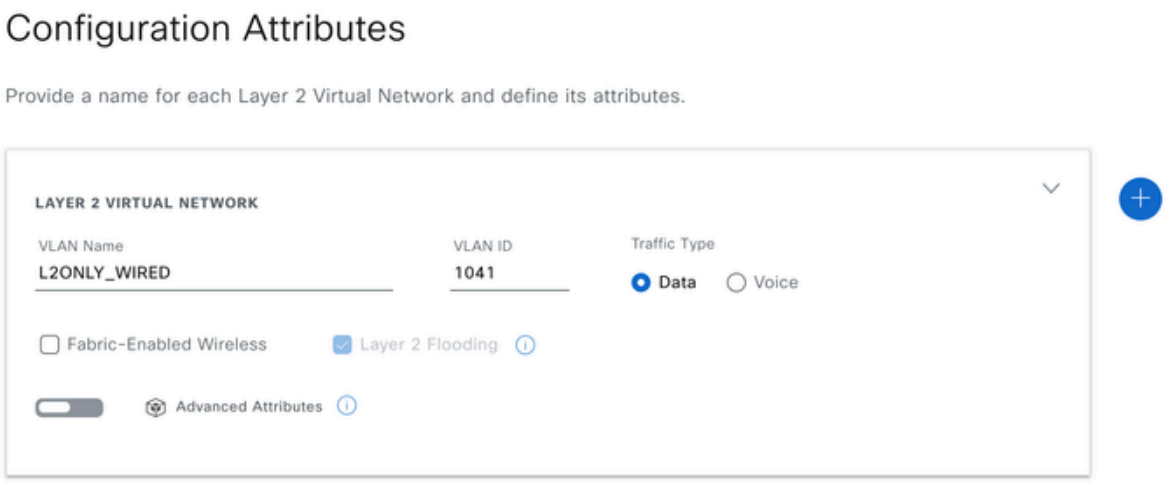
在此拓扑中：

- 192.168.0.201和192.168.0.202是交换矩阵站点的并置边界，BorderCP-1是唯一启用了第2层传递功能的边界。
- 192.168.0.101和192.168.0.102是交换矩阵边缘节点
- 192.168.254.39是DHCP服务器
- aaaa.bbbb.ddd是启用DHCP的终端
- Fusion设备用作交换矩阵子网的DHCP中继。

仅L2 VLAN配置

从Catalyst Center仅部署L2 VLAN

路径：Catalyst中心/调配/交换矩阵站点/第2层虚拟网络/编辑第2层虚拟网络



L2VNI配置

仅L2 VLAN配置 — 交换矩阵边缘

交换矩阵边缘节点将VLAN配置为启用CTS、禁用IGMP和IPv6 MLD以及所需的L2 LISP配置。此仅L2池不是无线池；因此，仅第2层无线池中通常存在的功能（如RA-Guard、DHCPGuard和泛洪接入隧道）未配置。相反，ARP数据包的泛洪使用“flood arp-nd”显式启用

交换矩阵边缘(192.168.0.101)配置

<#root>

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

1041

```
vlan
```

1041

name L2ONLY_WIRED

no ip igmp snooping vlan 1041 querier

no ip igmp snooping vlan 1041

no ipv6 mld snooping vlan 1041

```
router lisp
```

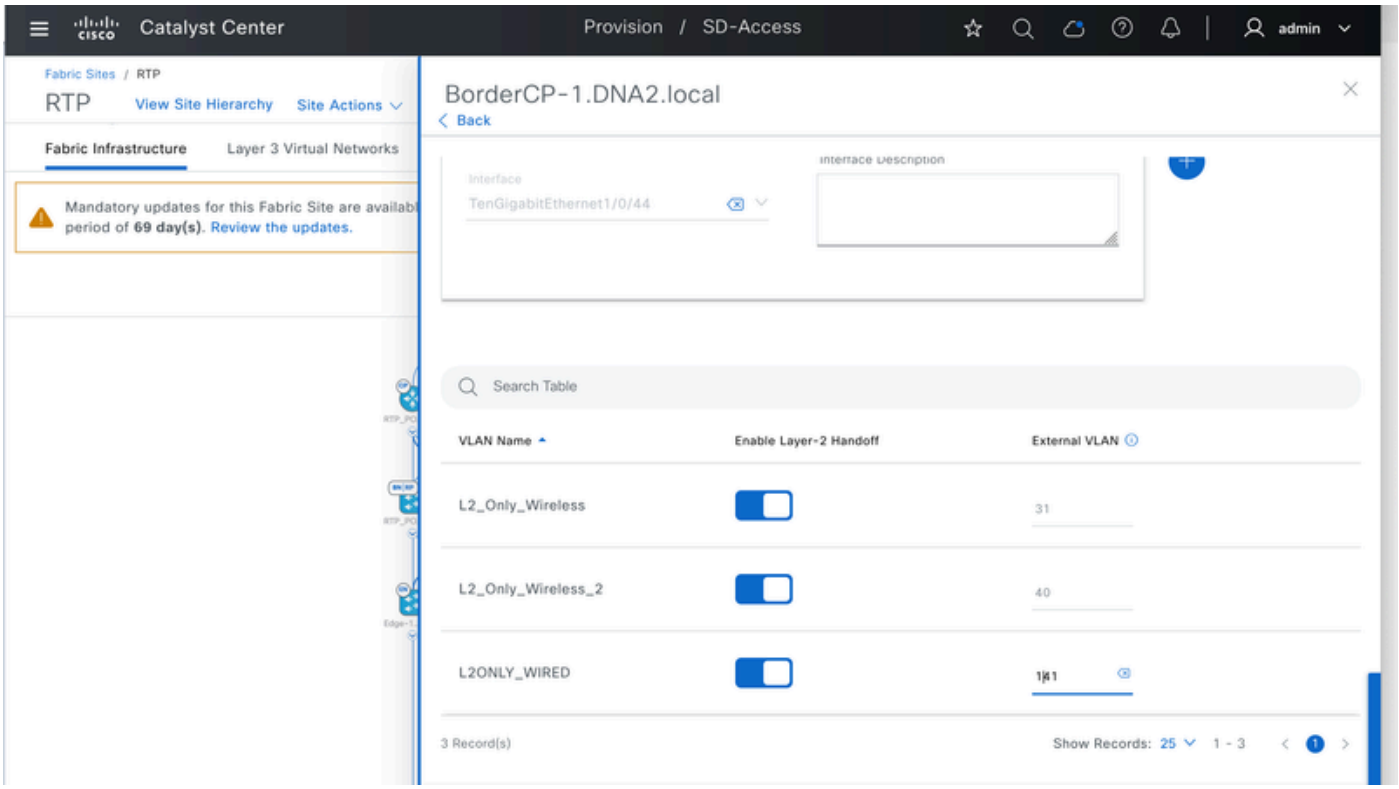
```
 instance-id
8240

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

eid-table vlan


1041

   broadcast-underlay
239.0.17.1



flood arp-nd



 flood unknown-unicast


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

L2移交配置 — 交换矩阵边界

从操作角度来看，允许DHCP服务器（或路由器/中继）连接到任何交换矩阵节点，包括边界和边缘。

建议使用Border节点连接DHCP服务器，但需要仔细考虑设计。这是因为边界必须逐个接口配置为L2转接。这样，交换矩阵池可以切换到与交换矩阵内相同的VLAN或不同的VLAN。交换矩阵边缘和边界之间的VLAN ID具有这种灵活性是可能的，因为两者都映射到相同的L2 LISP实例ID。不能使用同一VLAN同时启用L2移交物理端口，以防止SD-Access网络出现第2层环路。对于冗余，需要StackWise虚拟、FlexLink+或EEM脚本等方法。

相反，将DHCP服务器或网关路由器连接到交换矩阵边缘不需要额外配置。



L2移交配置

交换矩阵边界(192.168.0.201)配置

<#root>

cts role-based enforcement vlan-list

141

vlan

141

name L2ONLY_WIRED

no ip igmp snooping vlan 141 querier

no ip igmp snooping vlan 141

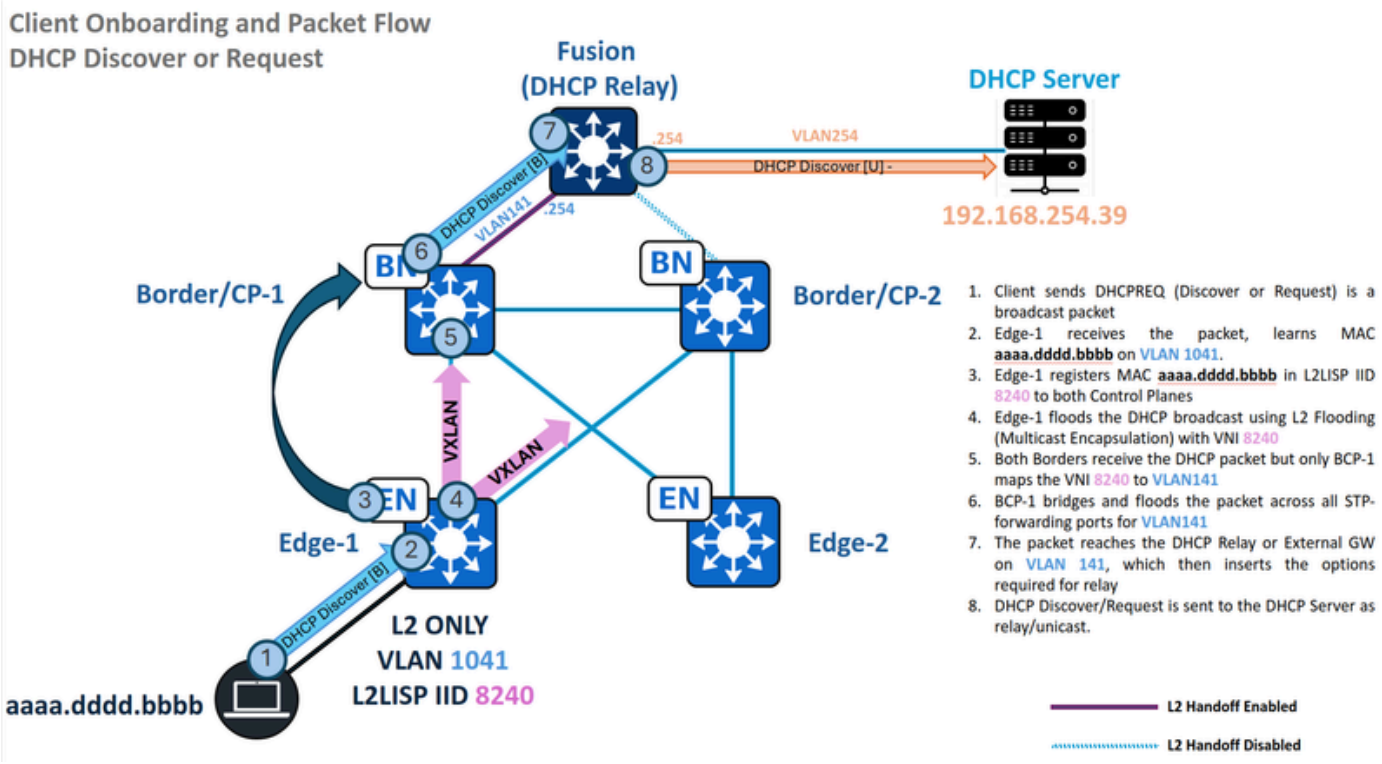
no ipv6 mld snooping vlan 141

router lisp
 instance-id

```
8240

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

eid-table


vlan 141



 broadcast-underlay 239.0.17.1


   flood arp-nd


   flood unknown-unicast


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

interface TenGigabitEthernet1/0/44


  switchport mode trunk
```

DHCP流量

DHCP发现和请求 — 边缘



流量 — 仅L2中的DHCP发现和请求

MAC学习和终端注册

当终端aaaa.dddd.bbb发送DHCP发现或请求（广播数据包）时，边缘节点必须获取终端的MAC地址，将其添加到其MAC地址表，然后到L2/MAC SISF表，最后到VLAN 1041的L2LISP数据库，映射到L2LISP实例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
```

如果终端的MAC地址已正确获知，并且交换矩阵控制平面的ACK标志已标记为“Yes”，则此阶段视为已完成。

L2泛洪中桥接的DHCP广播

当DHCP监听被禁用时，DHCP广播不会被阻止；相反，它们封装在组播中，以实现第2层泛洪。相反，启用DHCP监听可防止这些广播数据包泛洪。

<#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>
```

由于DHCP监听已禁用，因此DHCP发现/请求使用L2LISP0接口，通过L2泛洪桥接流量。根据Catalyst Center版本和应用的Fabric Banner，L2LISP0接口可能双向配置了访问列表；因此，请确

保任何访问控制条目(ACE)均未明确拒绝DHCP流量（UDP端口67和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

利用为L2LISP实例配置的广播底层组和交换矩阵边缘的Loopback0 IP地址来验证将该数据包桥接到其他交换矩阵节点的L2泛洪(S，G)条目。请查阅mroute和mfib表以验证参数，例如传入接口、传出接口列表和转发计数器。

<#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:

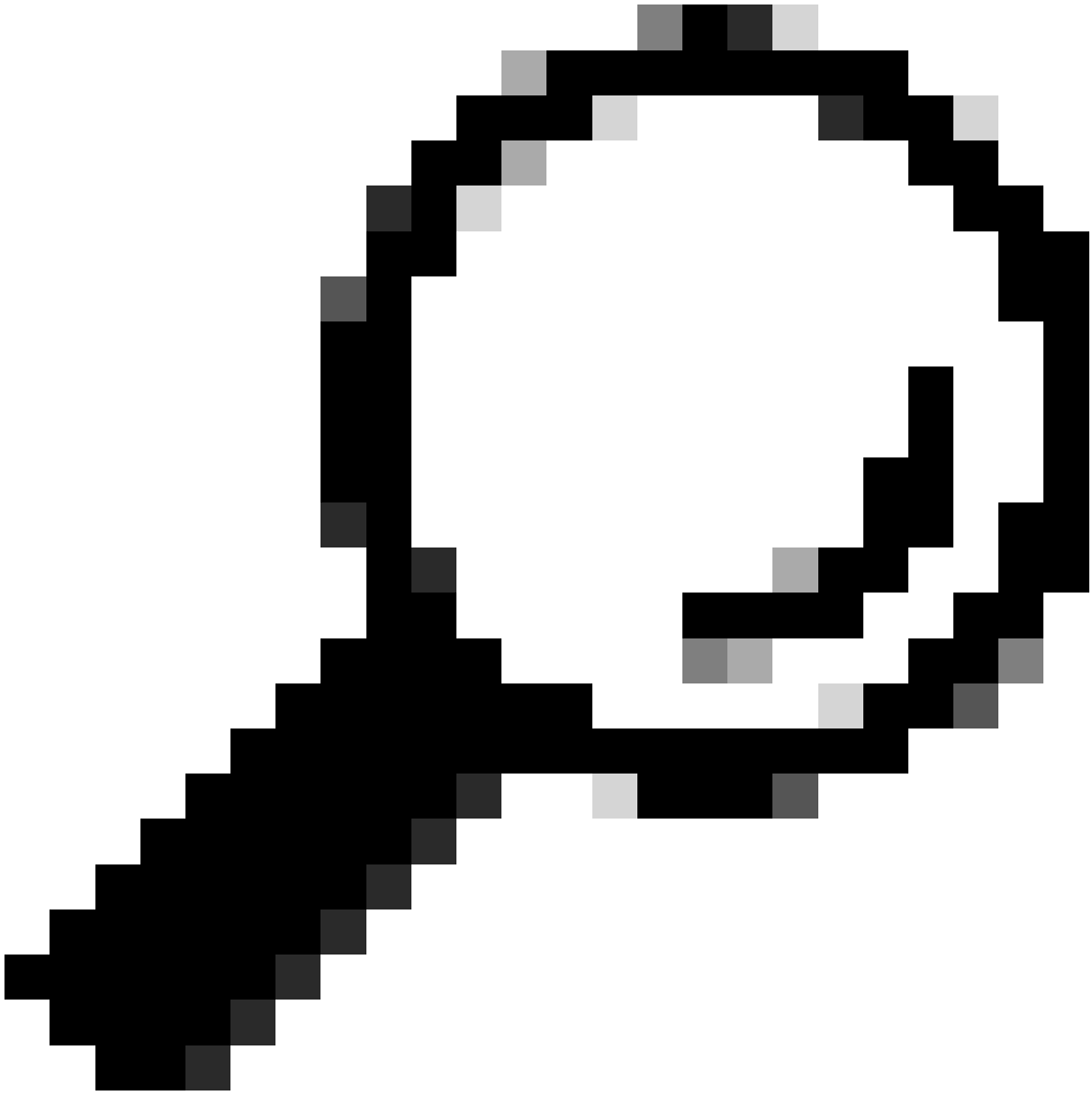
 7

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

<--

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

  Totals - Source count: 1, Packet count: 8



提示：如果未找到(S，G)条目或传出接口列表(OIL)不包含传出接口(OIF)，则表明底层组播配置或操作有问题。

数据包捕获

在交换机上配置同时嵌入式数据包捕获，以记录来自终端的传入DHCP数据包和相应的出口数据包以进行L2泛洪。捕获数据包时，应观察两个不同的数据包：原始DHCP发现/请求及其VXLAN封装的对等设备，目标为底层组(239.0.17.1)。

交换矩阵边缘(192.168.0.101)数据包捕获

<#root>

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

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

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

Edge-1#

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

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

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

356 DHCP Discover

 - Transaction ID 0xf8e

<--

356 is the Length of the original packet

   23   2.487037   0.0.0.0 -> 255.255.255.255 DHCP

406 DHCP Discover

 - Transaction ID 0xf8e

<--

406 is the Length of the VXLAN encapsulated packet

Edge-1#

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

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

406 DHCP Discover

 - Transaction ID 0xf8e

Edge-1#

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

Internet Protocol Version 4, Src:

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

Internet Protocol Version 4, Src:

0.0.0.0, Dst: 255.255.255.255

DHCP发现和请求 — L2边界

在边缘通过第2层泛洪发送DHCP发现数据包和请求数据包后（封装有广播底层组239.0.17.1），这些数据包由L2转发边界（在本场景中具体是Border/CP-1）接收。

为此，Border/CP-1必须拥有带边缘(S，G)的组播路由，其传出接口列表必须包括L2切换VLAN的L2LISP实例。请注意，L2传递边界共享相同的L2LISP实例ID，即使它们使用不同的VLAN进行传递也是如此。

<#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

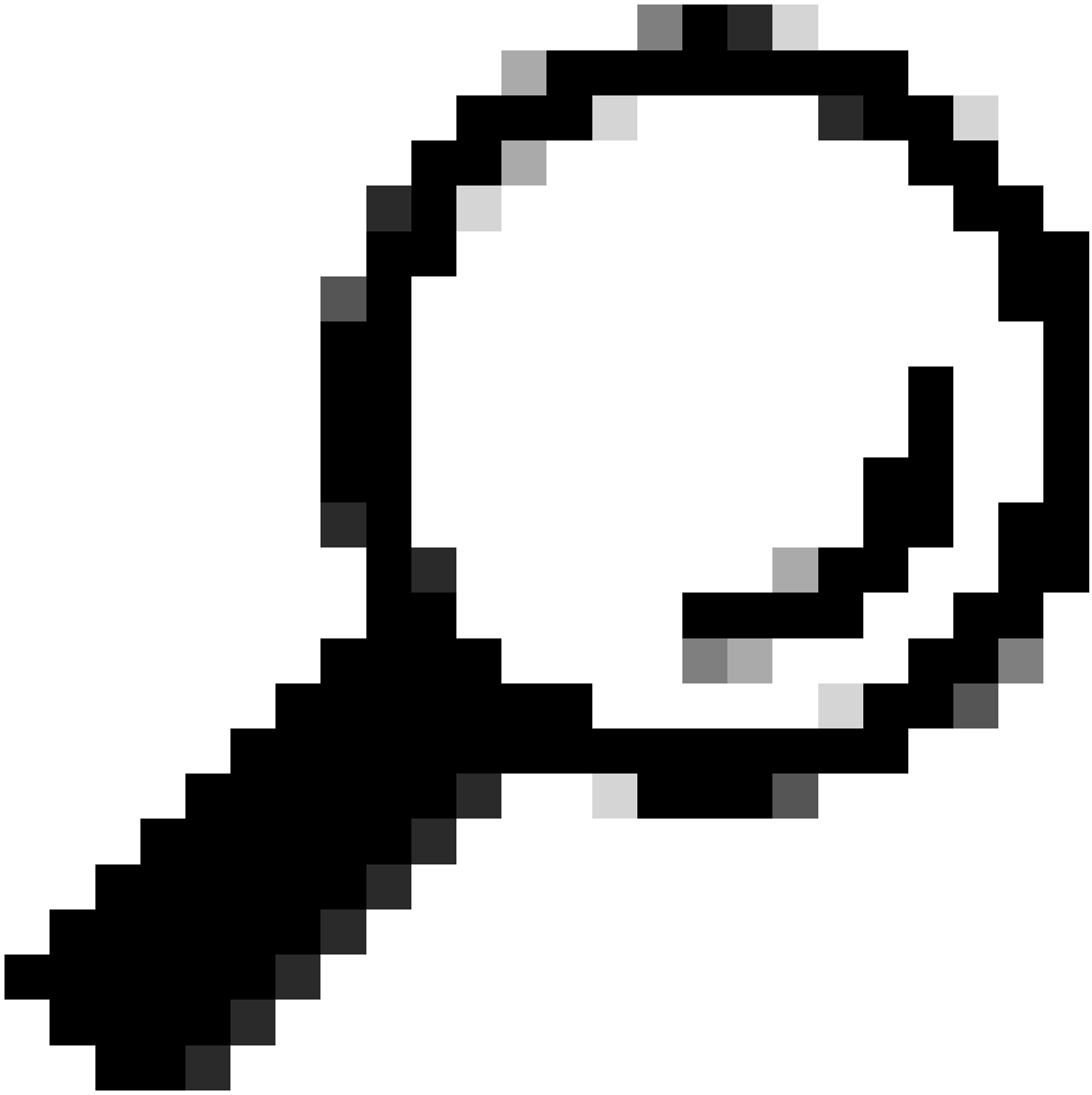
,
   SW Forwarding: 1/0/392/0, Other: 0/0/0
   HW Forwarding:

3

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

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

  Totals - Source count: 1, Packet count: 4



提示：如果未找到(S，G)条目，则表明底层组播配置或操作存在问题。如果所需实例的L2LISP未显示为OIF，则表明L2LISP子接口的操作打开/关闭状态或L2LISP接口的IGMP启用状态存在问题。

与交换矩阵边缘节点类似，请确保访问控制条目不会拒绝L2LISP0接口上的入口DHCP数据包。

<#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
```

在将数据包解封并放置在与VNI 8240匹配的VLAN上之后，其广播性质表明它从转接VLAN 141的所有生成树协议转发端口泛洪出去。

```
<#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
```

设备跟踪表确认连接到网关/DHCP中继的接口Te1/0/44必须是STP转发端口。

```
<#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
```

数据包捕获

在交换机上配置同时嵌入式数据包捕获，记录来自L2泛洪（S，G传入接口）的传入DHCP数据包和到DHCP中继的相应出口数据包。在数据包捕获时，应观察两个不同的数据包：来自Edge-1的VXLAN封装数据包，以及到达DHCP中继的解封装数据包。

交换矩阵边界/CP(192.168.0.201)数据包捕获

<#root>

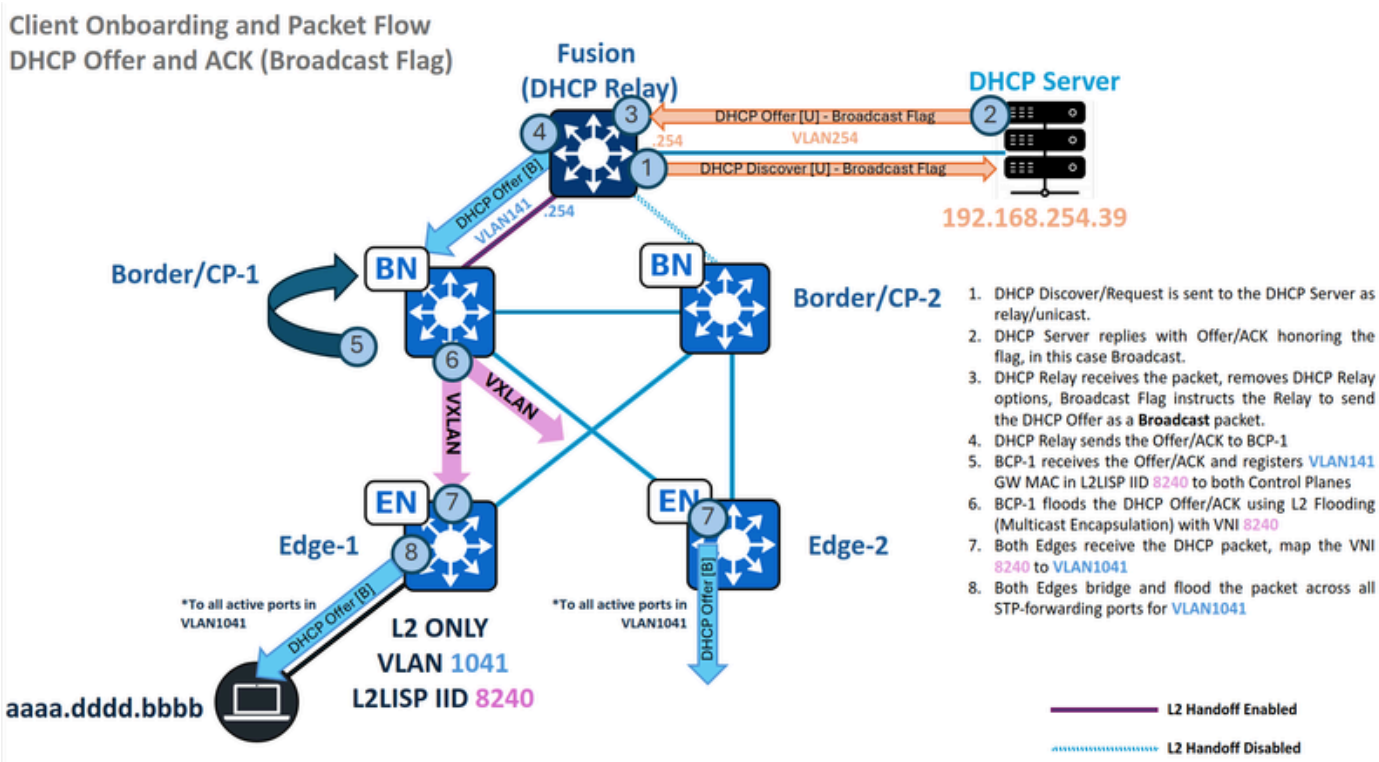
```
monitor capture cap interface TenGigabitEthernet1/0/42 IN    <-- Incoming interface for Edge's S,G Mrout

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

monitor capture cap match any

monitor capture cap buffer size 100

monitor capture cap start

monitor capture cap stop
```

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

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

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

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

```
Packet 427: VXLAN Encapsulated
```

```
BorderCP-1#
show monitor capture cap buffer display-filter "bootp and dhcp.hw.mac_addr==aaaa.dddd.bbbb and vxlan" de
Internet Protocol Version 4, Src:
192.168.0.101, Dst: 239.0.17.1

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


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

BorderCP-1#
show monitor capture cap buffer display-filter "bootp and dhcp.hw.mac_addr==aaaa.dddd.bbbb and not vxlan
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
```

DHCP提供和ACK — 广播 — L2边界



流量 — 仅第2层广播DHCP提供和ACK

现在DHCP发现已退出SD-Access交换矩阵，DHCP中继将插入传统DHCP中继选项（例如，GiAddr/GatewayIPAddress）并将数据包作为单播传输转发到DHCP服务器。在此流程中，SD-Access交换矩阵不会附加任何特殊DHCP选项。

当DHCP发现/请求到达服务器时，服务器会遵循嵌入的广播或单播标志。此标志指示DHCP中继代理将DHCP提供作为广播帧还是单播帧转发给下游设备（我们的边界）。在本演示中，假设存在广播场景。

MAC学习和网关注册

当DHCP中继发送DHCP Offer或ACK时，L2BN节点必须获取网关的MAC地址，将其添加到其MAC地址表，然后到L2/MAC SISF表，最后到VLAN 141的L2LISP数据库，映射到L2LISP实例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

如果网关的MAC地址已正确获知，并且交换矩阵控制平面的ACK标志已标记为“Yes”，则此阶段视为已完成。

L2泛洪中桥接的DHCP广播

如果未启用DHCP监听，DHCP广播不会受到阻止，而是封装在组播中，以实现第2层泛洪。相反，如果启用DHCP监听，则阻止DHCP广播数据包的泛洪。

<#root>

BorderCP-1#

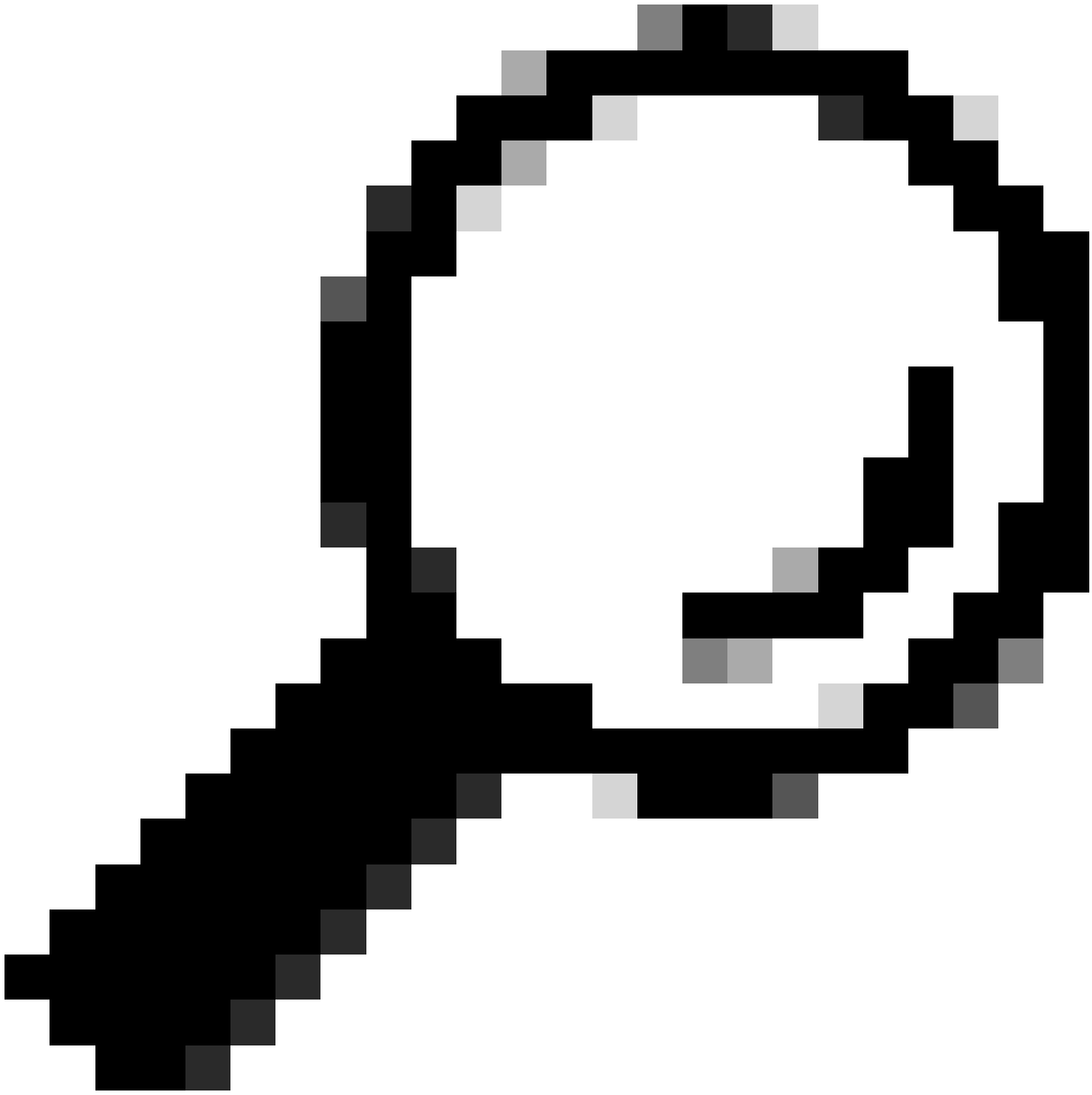
show ip dhcp snooping

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



提示：由于L2Border中未启用DHCP监听，因此不需要DHCP监听信任配置。

在此阶段，L2LISP ACL验证已在两台设备中完成。

利用为L2LISP实例配置的广播底层组和L2Border Loopback0 IP地址来验证将该数据包桥接到其他交换矩阵节点的L2泛洪(S，G)条目。请查阅mroute和mfib表以验证参数，例如传入接口、传出接口列表和转发计数器。

<#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

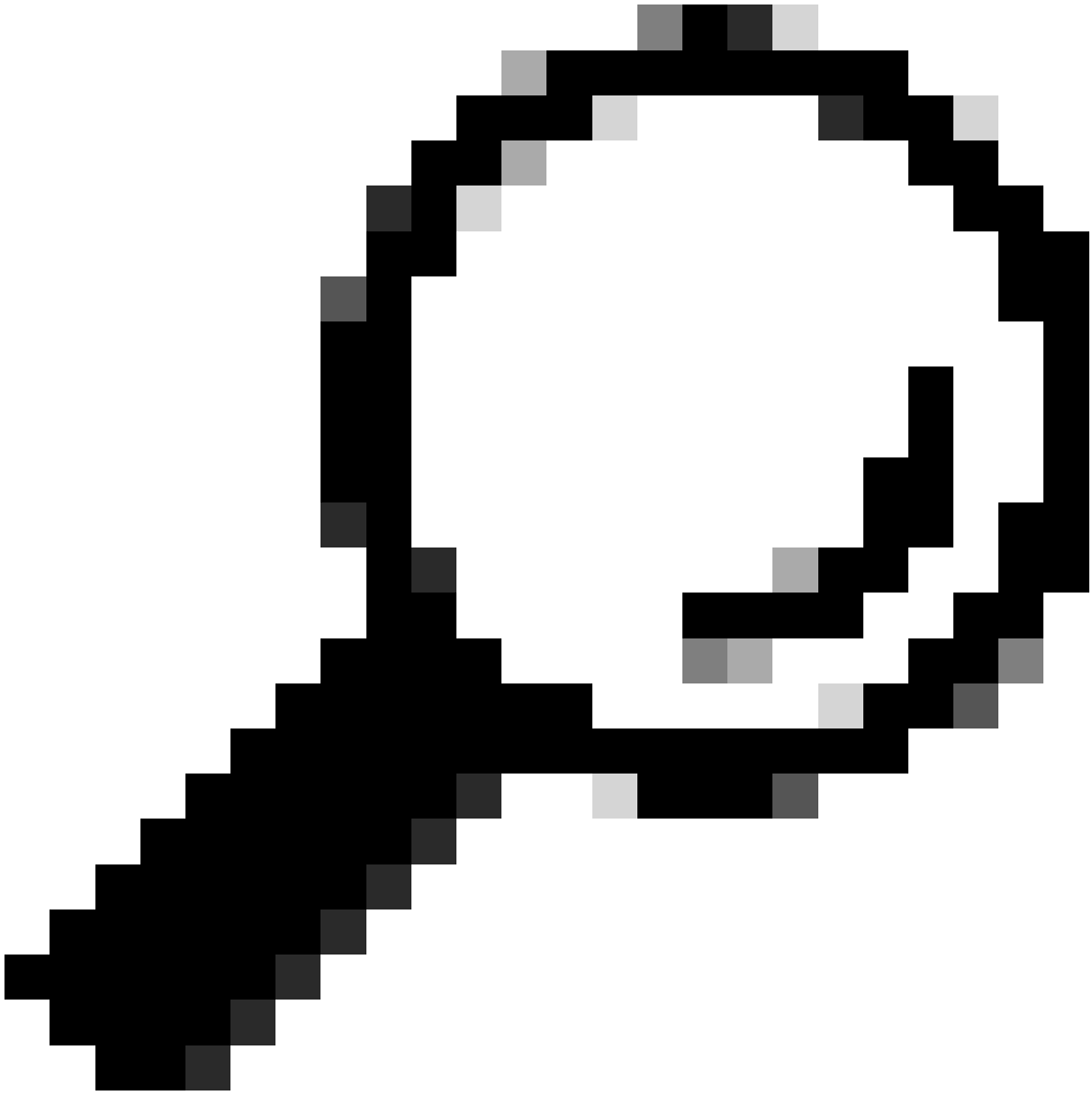
,
   SW Forwarding: 1/0/392/0, Other: 1/1/0
   HW Forwarding:

  92071

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

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

  Totals - Source count: 1, Packet count: 92071



提示：如果未找到(S，G)条目或传出接口列表(OIL)不包含传出接口(OIF)，则表明底层组播配置或操作有问题。

通过这些验证以及类似前面步骤的数据包捕获，本部分总结，因为DHCP提供使用传出接口列表内容（在本例中是接口TenGig1/0/42和TenGig1/0/43外）以广播形式转发到所有交换矩阵边缘。

DHCP提供和ACK — 广播 — 边缘

与上一个流完全一样，验证交换矩阵边缘中的L2Border S、G，其中传入接口指向L2BN，并且OIL包含映射到VLAN 1041的L2LISP实例。

<#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,

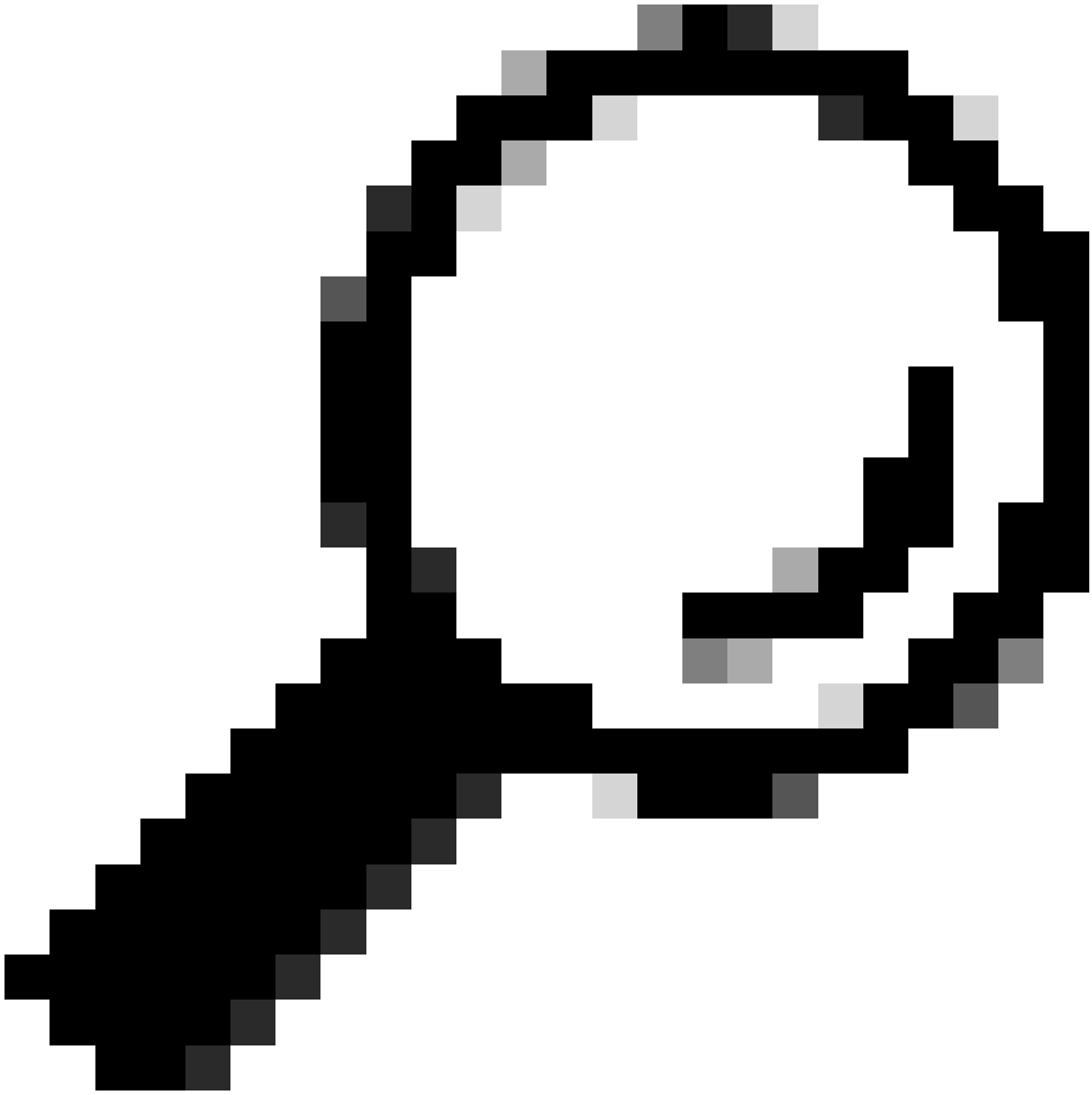
   SW Forwarding: 1/0/96/0, Other: 0/0/0
   HW Forwarding:

76236

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

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

  Totals - Source count: 1, Packet count: 4



提示：如果未找到(S，G)条目，则表明底层组播配置或操作存在问题。如果所需实例的L2LISP未显示为OIF，则表明L2LISP子接口的操作打开/关闭状态或L2LISP接口的IGMP启用状态存在问题。

两台设备都已完成L2LISP ACL验证。

在将数据包解封并放置在与VNI 8240匹配的VLAN上之后，其广播性质表明该数据包从VLAN1041的所有生成树协议转发端口泛洪出去。

<#root>

Edge-1#

show spanning-tree vlan 1041 | be Interface

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


Te1/0/2

         Desg

FWD

 20000     128.2    P2p Edge
Te1/0/17            Desg

FWD

 2000      128.17   P2p
Te1/0/18            Back

BLK

 2000      128.18   P2p
Te1/0/19            Desg

FWD

 2000      128.19   P2p
Te1/0/20            Back

BLK

 2000      128.20   P2p
```

MAC地址表将端口Te1/0/2标识为终端端口，该端口由STP处于FWD状态，数据包被泛洪到终端。

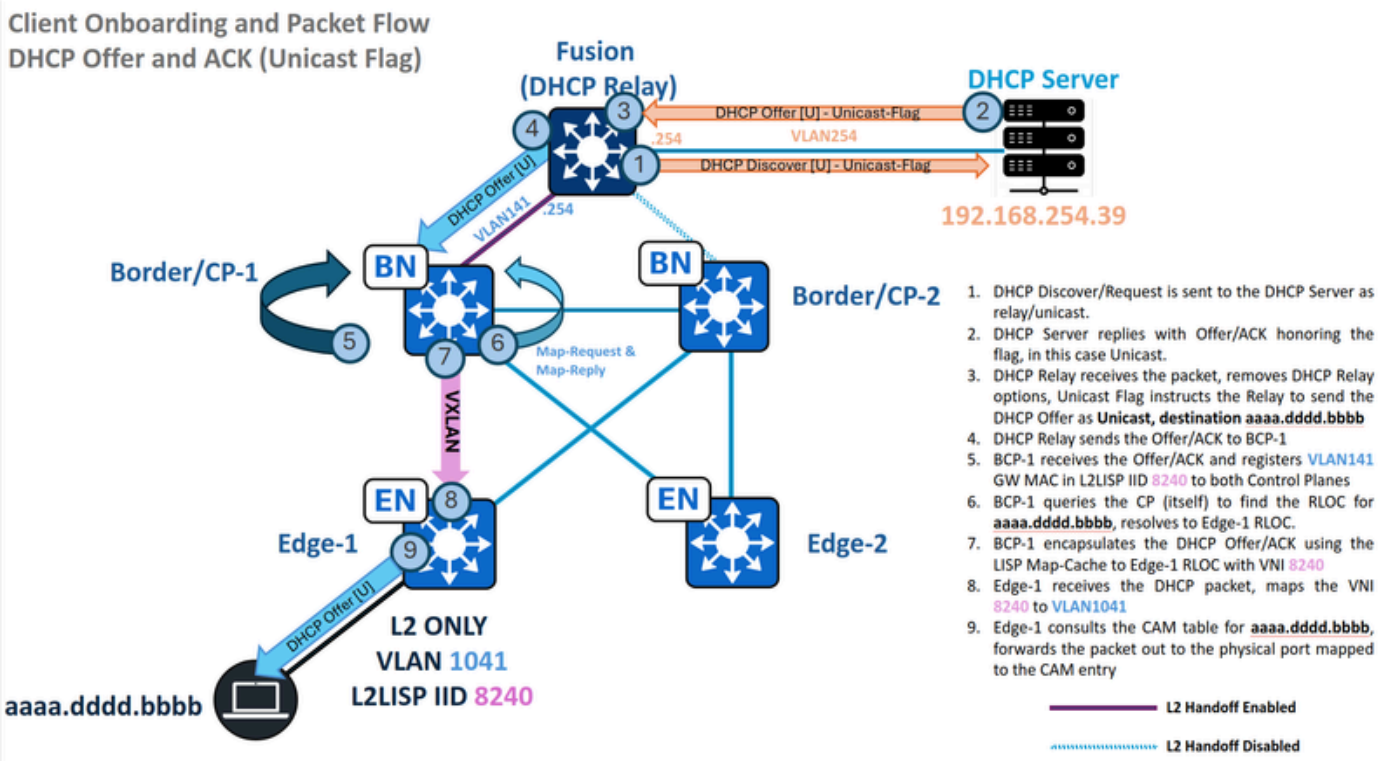
```
<#root>

Edge-1#

show mac address-table interface te1/0/2


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


1041


aaaa.dddd.bbbb

    DYNAMIC

Te1/0/2
```

DHCP提供和ACK过程保持一致。如果未启用DHCP监听，则不会在DHCP监听表中创建任何条目。因此，启用DHCP的终端的设备跟踪条目通过收集ARP数据包生成。由于DHCP监听已禁用，因此

“show platform dhcpsnooping client stats”等命令预计不会显示任何数据。

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

    Network Layer Address                   Link Layer Address     Interface  vlan       prlvl      ag

ARP


172.16.141.1


 aaaa.dddd.bbbb

       Te1/0/2

1041

       0005       45s        REACHABLE  207 s try 0

Edge-1#
show ip dhcp snooping  binding vlan 1041

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

Total number of bindings: 0
```

DHCP提供和ACK — 单播 — L2边界



流量 — 单播DHCP提供和ACK（仅限第2层）

场景稍有不同，终端将DHCP广播标志设置为unset或“0”。

DHCP中继不会将DHCP提供/ACK作为广播发送，而是作为单播数据包发送，目标MAC地址从DHCP负载内的客户端硬件地址派生。这显着修改了SD-Access交换矩阵处理数据包的方式，它使用L2LISP映射缓存转发流量，而不是第2层泛洪组播封装方法。

交换矩阵边界/CP(192.168.0.201)数据包类别：入口DHCP提供

<#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)

在此场景中，L2泛洪专门用于发现/请求，而提供/ACK则通过L2LISP映射缓存转发，从而简化了整体操作。L2边界遵循单播转发原则，向控制平面查询目的MAC地址(aaaa.dddd.bbb)。 假设在交换矩阵边缘上成功“MAC学习和终端注册”，则控制平面已注册此终端ID(EID)。

<#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
```

在边界对控制平面（本地或远程）进行查询后，LISP解析将为终端的MAC地址建立映射缓存条目。

<#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        -
```

解决RLOC后，DHCP提供被单播封装，并使用VNI 8240直接发送到Edge-1(192.168.0.101)。

<#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
```

使用与前面部分相同的方法，捕获从DHCP中继和RLOC出口接口的入口流量，以单播方式观察到边缘RLOC的VXLAN封装。

DHCP提供和ACK — 单播 — 边缘

边缘从边界接收单播DHCP提供/ACK，解封流量并查询其MAC地址表以确定正确的出口端口。与广播Offer/ACK不同，边缘节点仅将数据包转发到终端连接的特定端口，而不是将其泛洪到所有端口。

MAC地址表将端口Te1/0/2标识为客户端端口，该端口由STP处于FWD状态，数据包将被转发到终端。

```
<#root>

Edge-1#

show mac address-table interface te1/0/2


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

1041


aaaa.dddd.bbbb

    DYNAMIC

Te1/0/2
```

DHCP提供和ACK过程保持一致。如果未启用DHCP监听，则不会在DHCP监听表中创建任何条目。因此，启用DHCP的终端的设备跟踪条目由收集ARP数据包生成。由于DHCP监听已禁用，因此“show platform dhcpsnooping client stats”等命令预计不会显示任何数据。

```
<#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
```

请务必注意，SD访问交换矩阵不影响单播或广播标志的使用，因为这只是终端行为。虽然此功能可能被DHCP中继或DHCP服务器本身覆盖，但两种机制对于纯L2环境中的无缝DHCP操作都必不可少：广播提供/ACK的L2底层组播泛洪，以及单播提供/ACK的控制平面中正确的终端注册。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。