排除仅第2层VLAN中的DHCP故障 — 无线

目录

简介

本文档介绍如何在SD-Access(SDA)交换矩阵中的仅第2层网络中排除无线终端的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
- 支持交换矩阵的无线

硬件和软件要求

- Catalyst 9000 系列交换机
- Catalyst Center版本2.3.7.9
- Catalyst 9800系列无线LAN控制器
- Catalyst 9100系列接入点
- 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

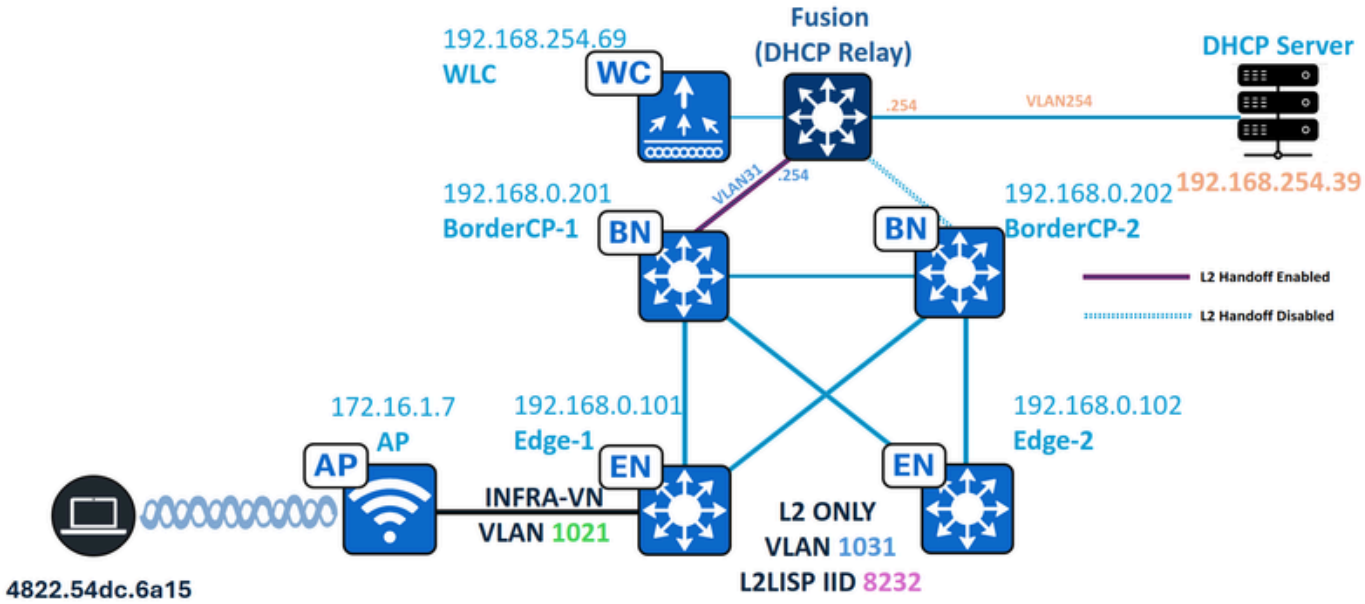
由于DHCP严重依赖广播流量，因此必须利用第2层泛洪来支持此协议。与任何其他启用第2层泛洪的池一样，必须为组播流量配置底层网络，尤其是使用PIM稀疏模式的Any-Source-Multicast。当底层组播配置通过LAN自动化工作流程自动进行时，如果省略此步骤，则需要其他配置（手动或模板）。

- 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。

通过接入隧道接口广播

支持矩阵的无线在AP和FE上采用本地交换和VTEP功能。但是，IOS-XE 16.10+限制会阻止通过VXLAN向AP转发出口广播。在仅第2层网络中，这会阻止DHCP提供/ACK访问无线客户端。“泛洪接入隧道”功能通过在交换矩阵边缘接入隧道接口上启用广播转发来解决这一问题。

拓扑



网络拓扑

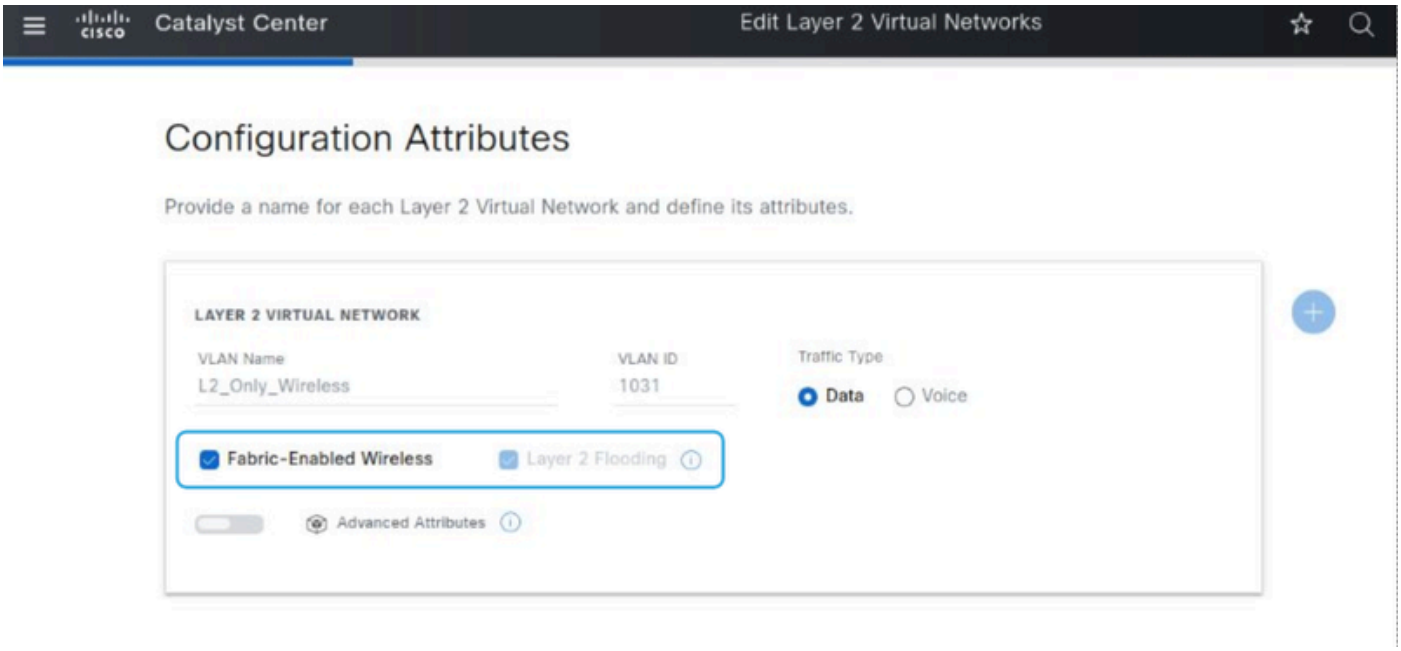
在此拓扑中：

- 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
- 172.16.1.7是具有VLAN 1021的INFRA-VN中的接入点
- 192.168.254.39是DHCP服务器
- 192.168.254.69是无线局域网控制器
- 4822.54dc.6a15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



支持矩阵的无线的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）已配置。无线池上未启用ARP泛洪。

交换矩阵边缘(192.168.0.101)配置

```
<#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
```

flood-access tunnel命令在其组播复制变体中配置，其中所有BUM流量使用源特定组播组(232.255.255.1)封装到AP，使用INFRA-VN接入点VLAN作为IGMP监听所咨询的VLAN以转发BUM流量。

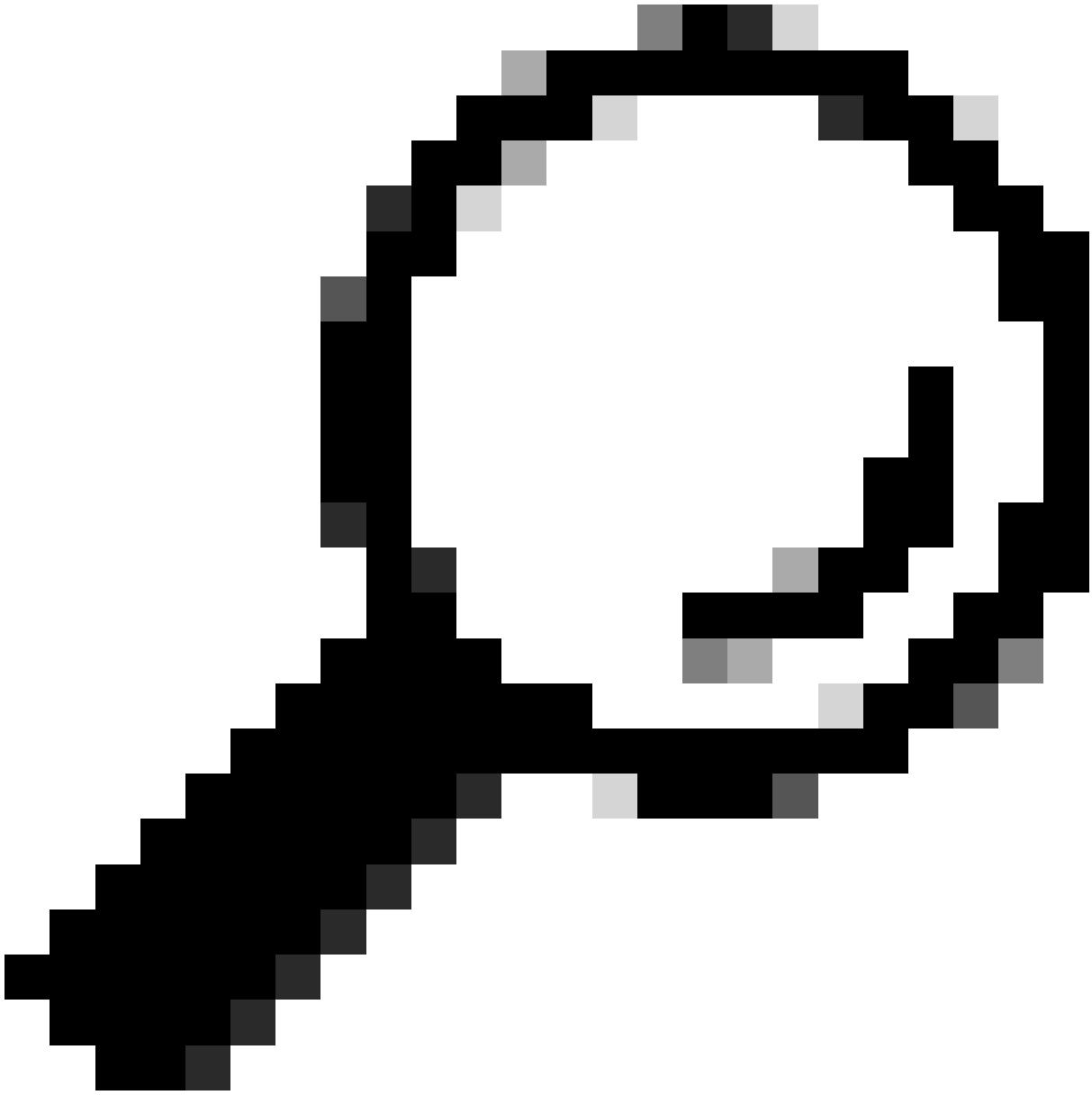
仅L2的VLAN配置 — 无线LAN控制器

在WLC（无线LAN控制器）端，与交换矩阵接入点关联的站点标记必须配置为“no fabric ap-arp-caching”以禁用代理ARP功能。此外，必须启用“fabric ap-dhcp-broadcast”，此配置允许将DHCP广播数据包从AP转发到无线终端。

交换矩阵WLC(192.168.254.69)配置

<#root>

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

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



提示：无线组播组232.255.255.1是所有站点标签使用的默认组。

<#root>

```
WLC#
```

show wireless tag site detailed RTP-Site-Tag-3

```
Site Tag Name        :
```

RTP-Site-Tag-3

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

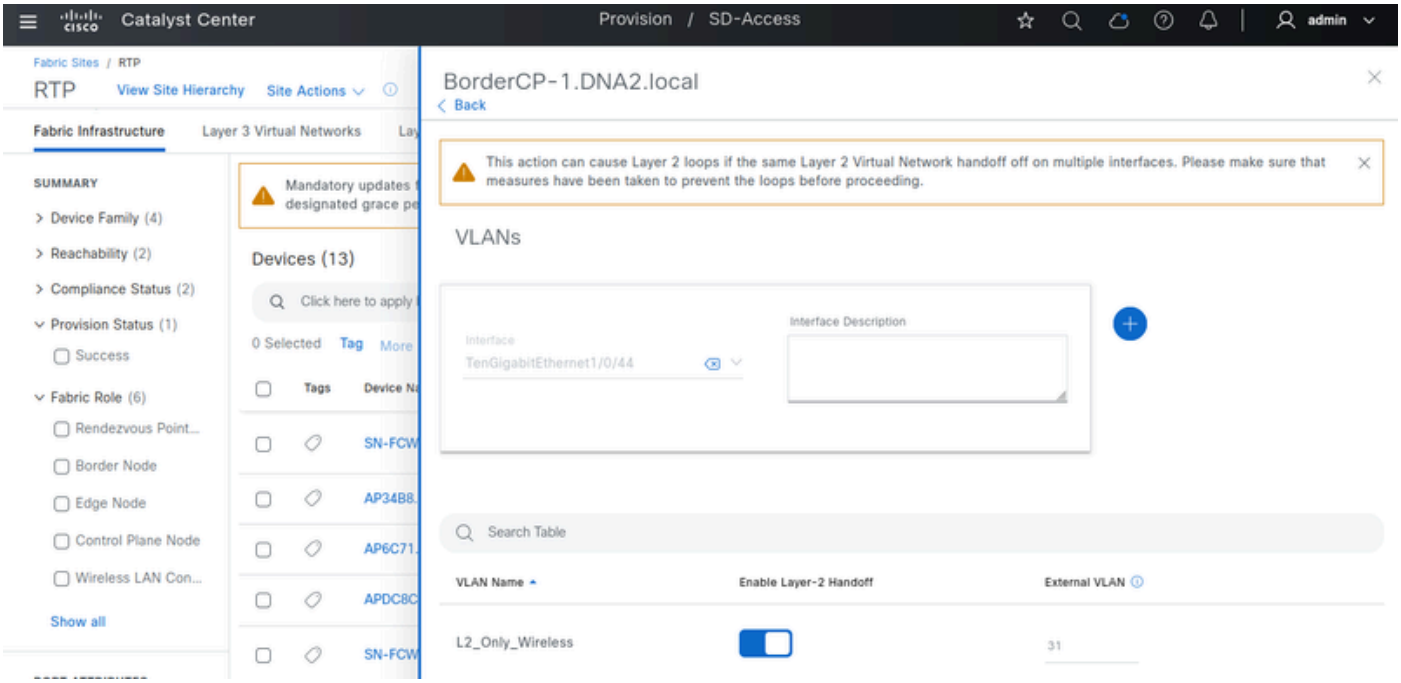
```
Fabric AP DHCP Broadcast :
Enabled

Fabric Multicast Group IPv4 Address :
232.255.255.1

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

L2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/CP(192.168.0.201)配置

```
<#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
```

无线组播支持

交换矩阵边缘配置为通过泛洪接入隧道机制将广播数据包转发到接入点。这些数据包封装到INFRA-VN　VLAN上的232.255.255.1组播组中。接入点自动加入此组播组，因为它们的站点标签已预配置为使用它。

```
<#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
```

从接入点，在交换矩阵无线终端关联时，会形成VXLAN隧道（在AP端是动态的，在交换矩阵边缘端是始终在线的）。 在此隧道中，CAPWAP交换矩阵组播组使用来自AP终端的命令进行验证。

<#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
```

从交换矩阵边缘端，确认已为INFRA-VN　AP　VLAN启用IGMP监听，接入点已形成接入隧道接口，并已加入组播组232.255.255.1

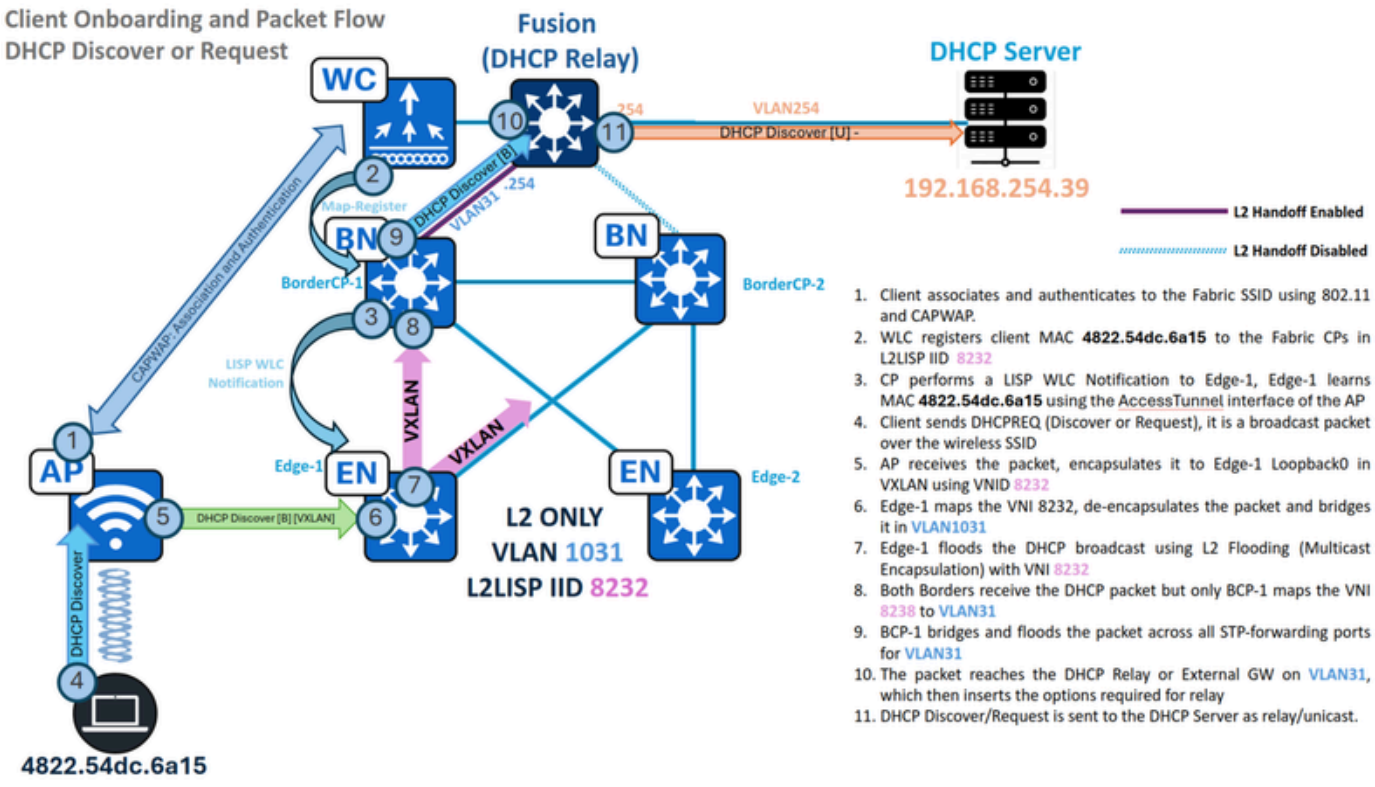
```
<#root>

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>
```

这些验证确认无线组播已成功在接入点、交换矩阵边缘和无线LAN控制器上启用。

DHCP流量

DHCP发现和请求 — 无线端



确定无线终端的状态、其连接的接入点和关联的交换矩阵属性。

<#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

必须确认在策略配置文件中禁用了中心交换和中心dhcp功能。必须在SSID的策略配置文件中配置“no central dhcp”和“no central switching”命令。

<#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

这些验证确认终端已连接到“AP1”，后者与交换矩阵边缘RLOC 192.168.0.101关联。因此，其流量通过VXLAN封装并使用VNID 8232从接入点传输到交换矩阵边缘。

DHCP发现和请求 — 交换矩阵边缘

使用WLC通知的MAC学习

在终端自注册过程中，WLC向交换矩阵控制平面注册无线终端的MAC地址。同时，控制平面会通知交换矩阵边缘节点（接入点连接到该节点），以创建一个特殊的“CP_LEARN”MAC学习条目，指向接入点的接入隧道接口。

<#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
```

如果终端的MAC地址通过与其连接的接入点对应的接入隧道接口正确获取，则此阶段被视为完成。

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 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>

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
```

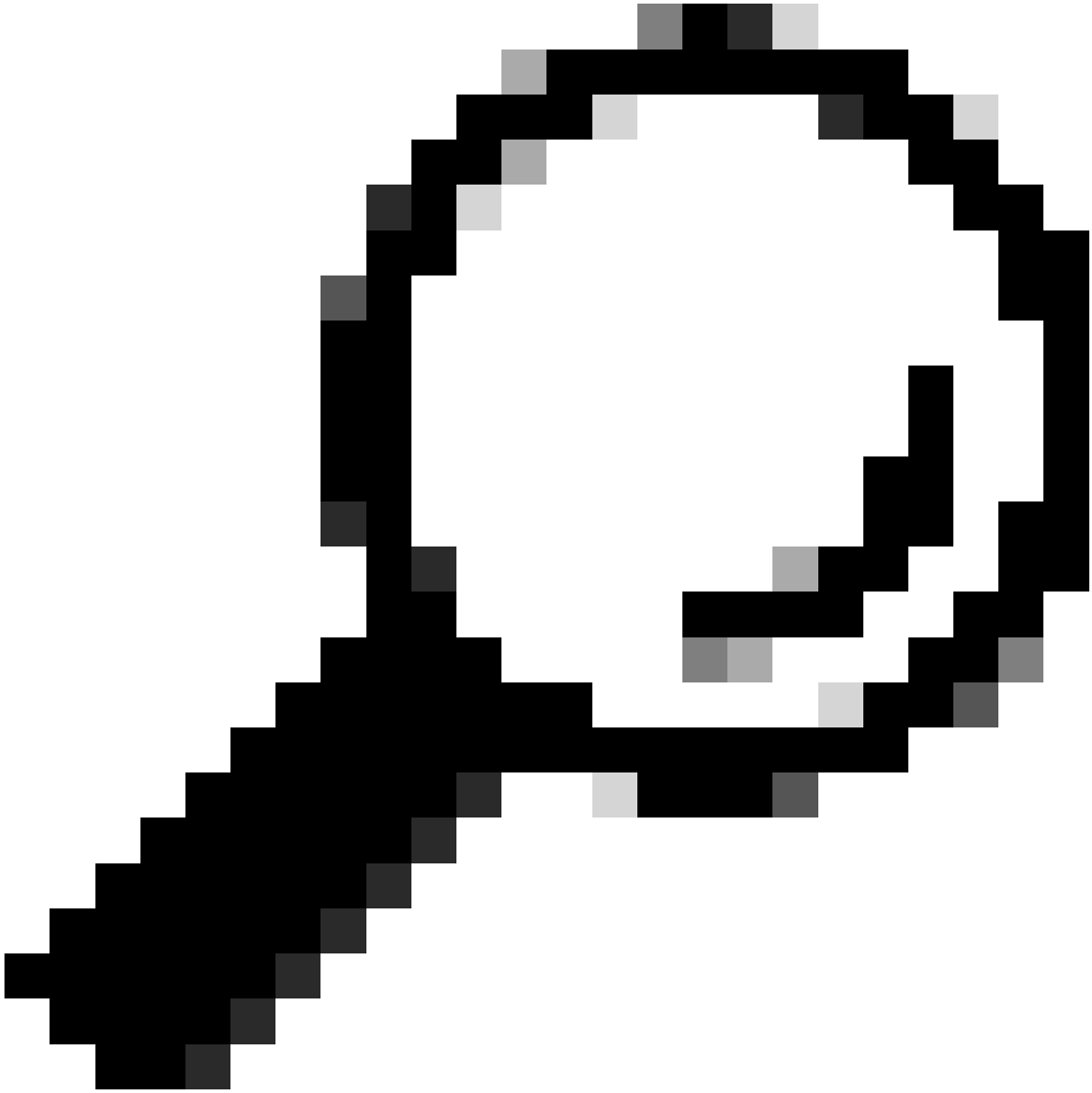
利用为L2LISP实例配置的广播底层组和交换矩阵边缘的Loopback0 IP地址来验证将该数据包桥接到其他交换矩阵节点的L2泛洪(S，G)条目。请查阅mroute和mfib表以验证参数，例如传入接口、传出接口列表和转发计数器。

<#root>

```
Edge-1#
show ip interface loopback 0 | i Internet

  Internet address is
192.168.0.101/32


Edge-1#
show running-config | se 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
```



提示：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，记录来自AP的入口DHCP数据包和相应的出口数据包，以进行L2泛洪。

交换矩阵边缘(192.168.0.101)数据包捕获

<#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

捕获数据包时，必须观察三个不同的数据包：

- DHCP发现 — VXLAN - AP到边缘
- DHCP发现 — CAPWAP - AP到WLC
- DHCP发现 — VXLAN — 边缘到组播组

<#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
```

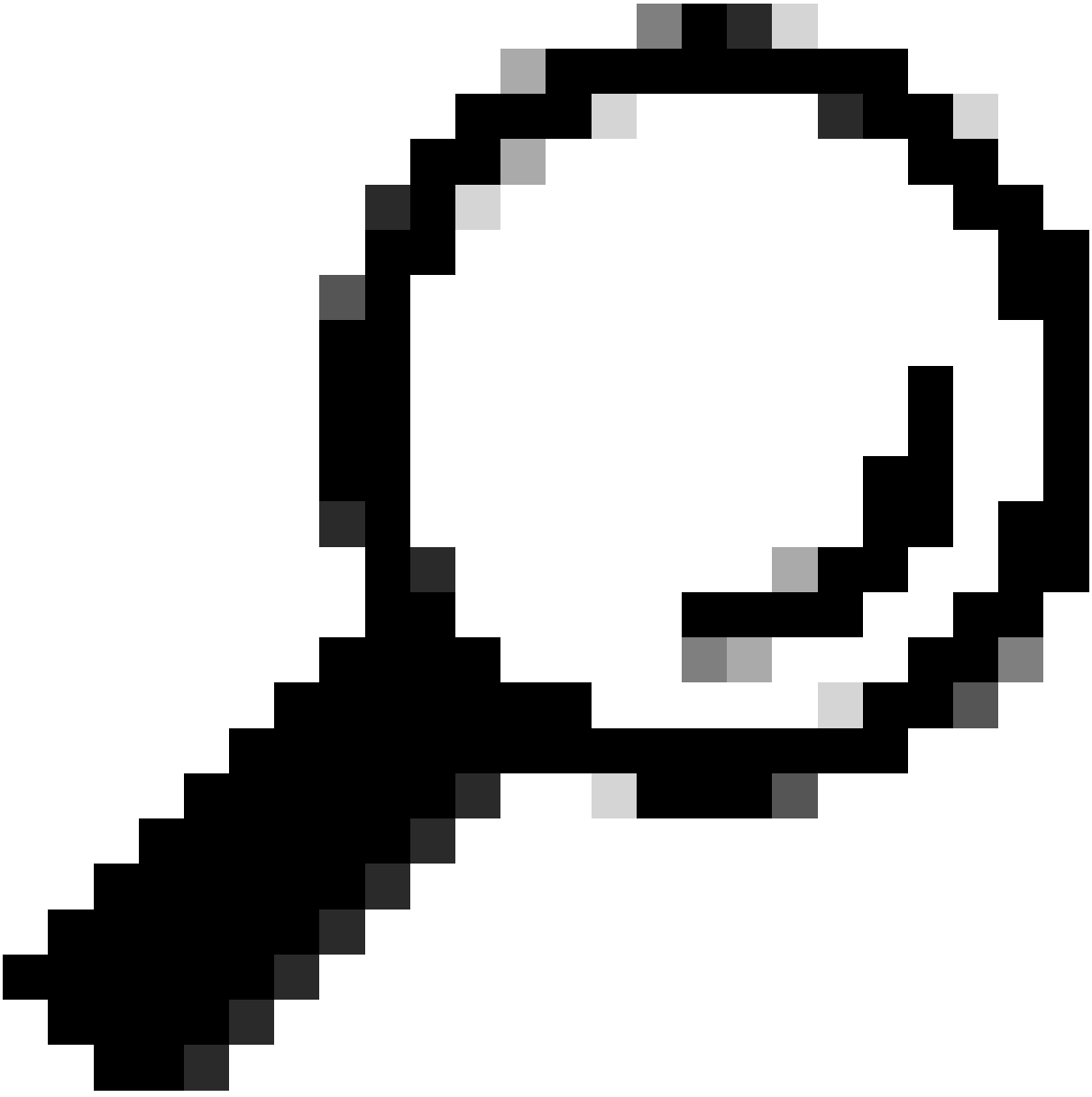
Internet Protocol Version 4, Src:

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



提示：在支持交换矩阵的无线上，VXLAN封装的数据包将DHCP流量传送到客户端或服务器。但是，CAPWAP DATA(UDP 5247)封装的数据包仅出于跟踪目的传输到WLC，例如IP Learn状态或无线设备跟踪。

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 31

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

31

L2_Only_Wireless

active

    L2LIO:

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,

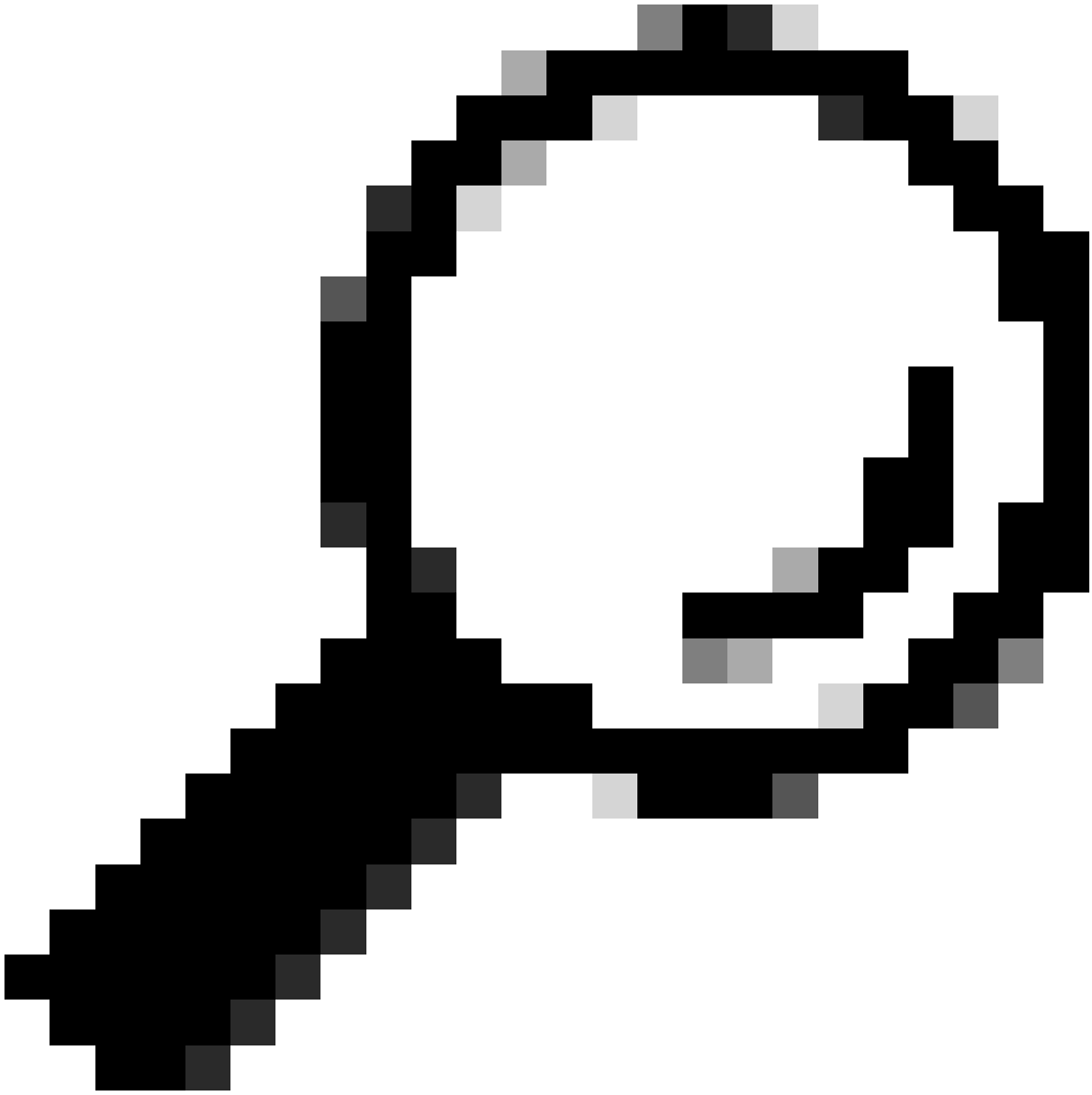
SW Forwarding: 1/0/392/0, Other: 0/0/0
HW Forwarding:

3

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

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

Totals - Source count: 1, Packet count: 4



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 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
```

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 31 | 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        state      Time left
ARP

172.16.131.254

                        f87b.2003.7fd5

Te1/0/44


 31

       0005       34s       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

<--

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

此时，发现/请求数据包已退出SD-Access交换矩阵，此部分结束。但是，在继续操作之前，一个关键参数（由终端本身确定的DHCP广播标志）将规定后续的Offer或ACK数据包的转发方案。我们可以检查其中一个Discover数据包以检查此标志。

<#root>

BorderCP-1#

show monitor capture cap buffer display-filter "bootp.type==1 and dhcp.hw.mac_addr==4822.54dc.6a15

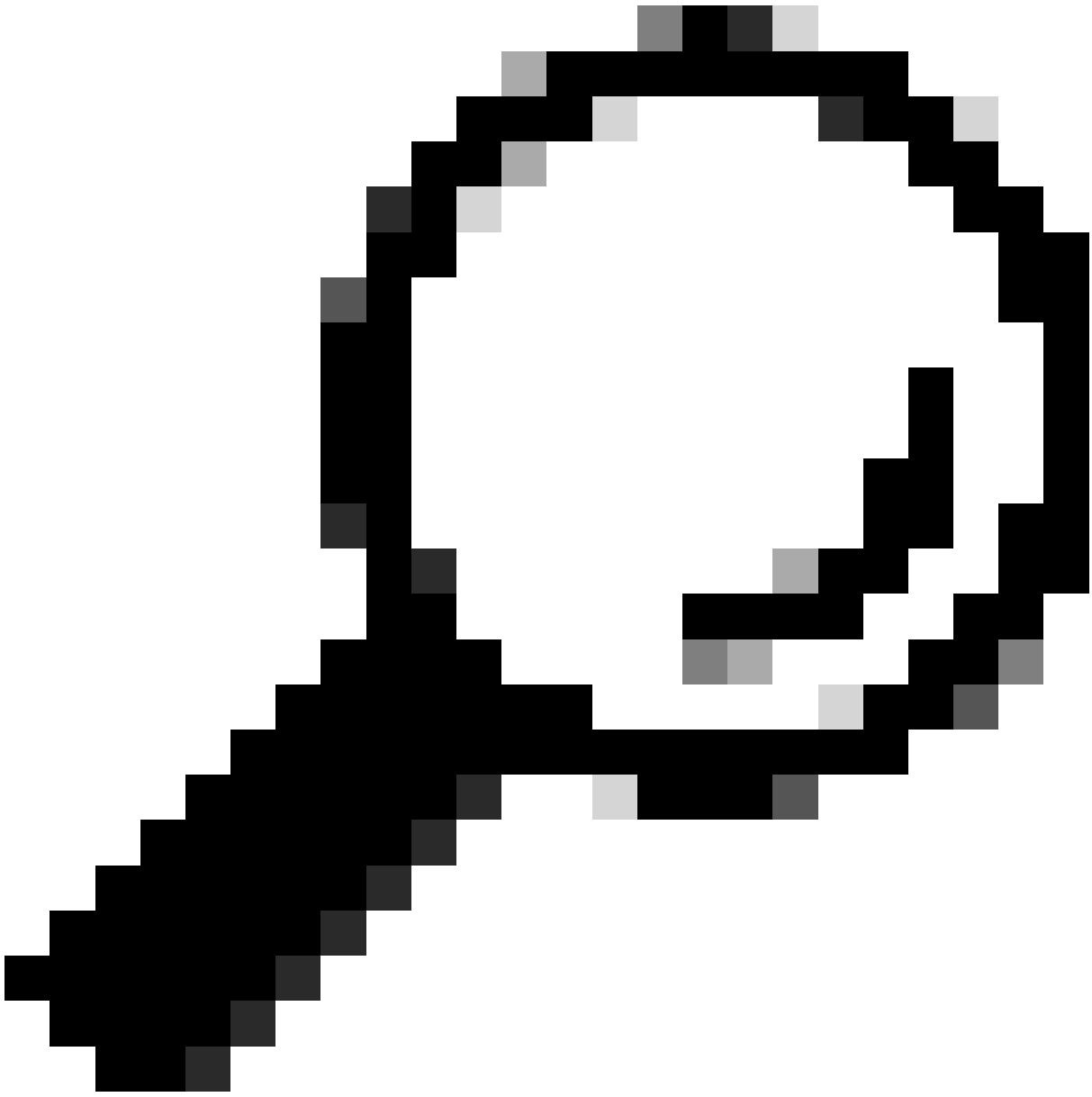
" detailed | sect Dynamic

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
```

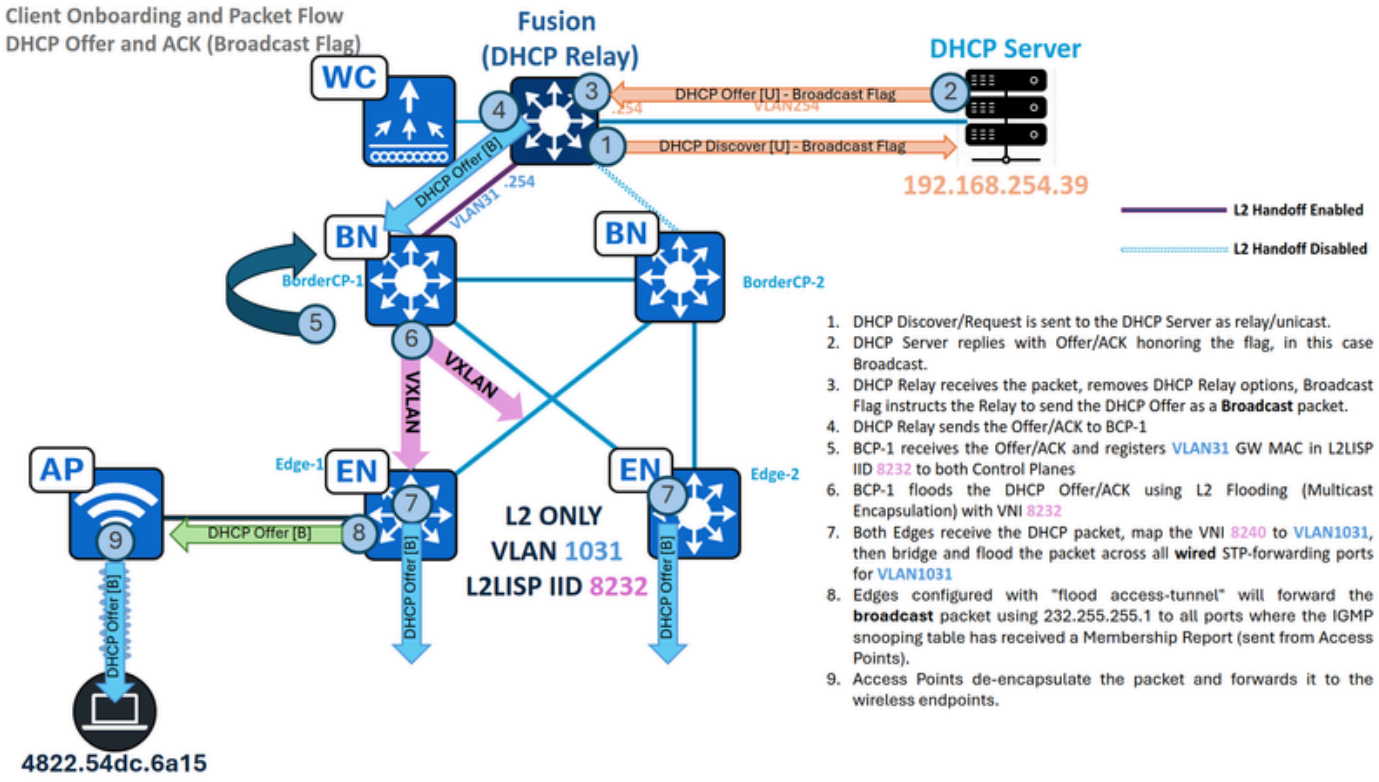
Bootp flags: 0x8000, Broadcast flag (Broadcast)

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

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



提示：bootp.type.1==以仅用于过滤Discover和Request数据包。

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8232。

<#root>

```
BorderCP-1#
```

show mac address-table interface te1/0/44

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

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
```

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          <-- 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
```

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地址来验证将桥接此数据包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 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:
```

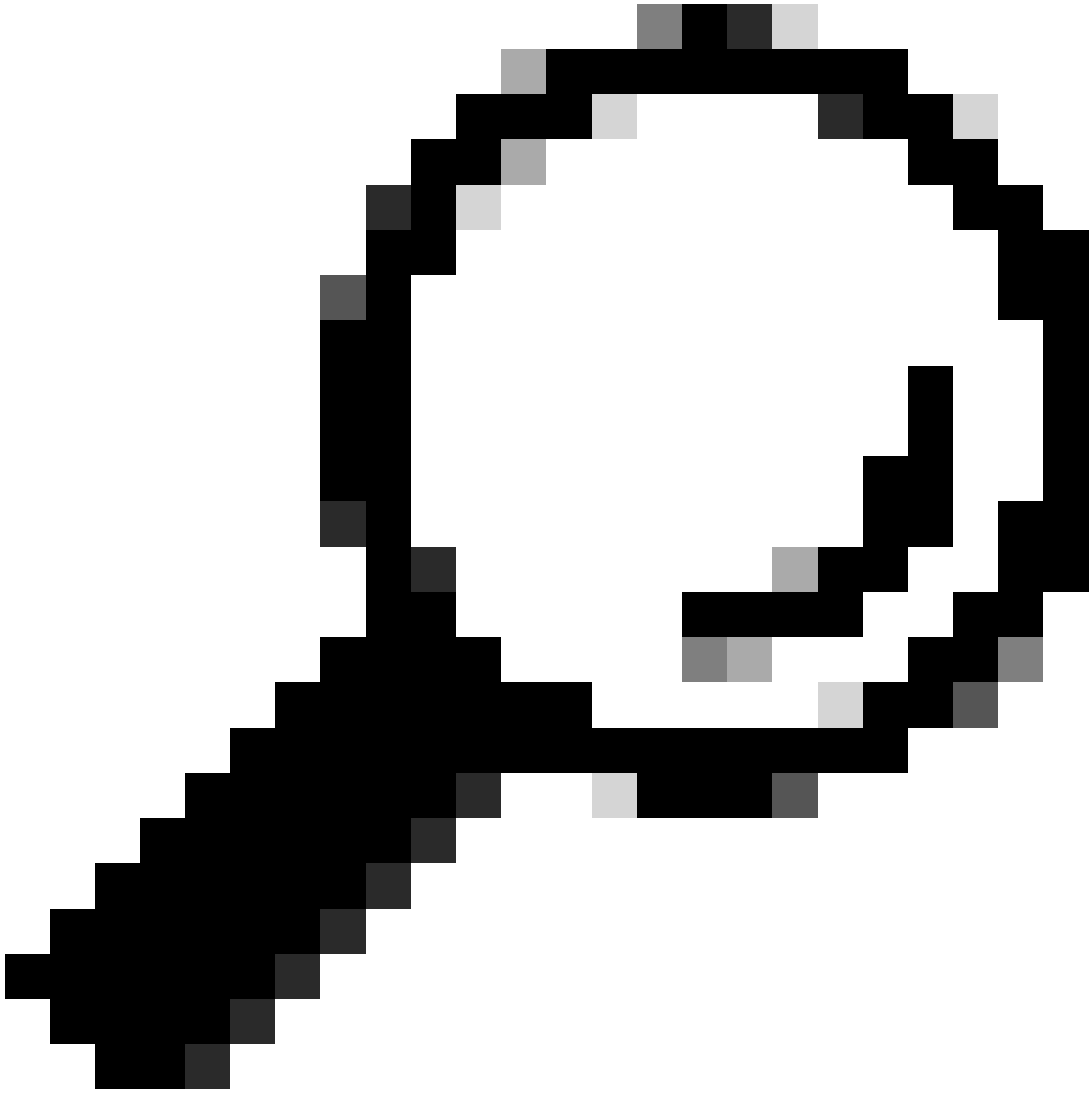
239.0.17.1

```
  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
```



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，随着数据包捕获类似前面的步骤，我们总结本节内容，因为DHCP提供将使用传出接口列表内容(在本例中，从接口TenGig1/0/42和TenGig1/0/43转发，作为广播转发到所有交换矩阵边缘。

DHCP提供和ACK — 广播 — 边缘

与上一个流完全相同，我们现在检查交换矩阵边缘中的L2Border S，G，其中传入接口指向L2BN，而OIL包含映射到VLAN 1031的L2LISP实例。

<#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,

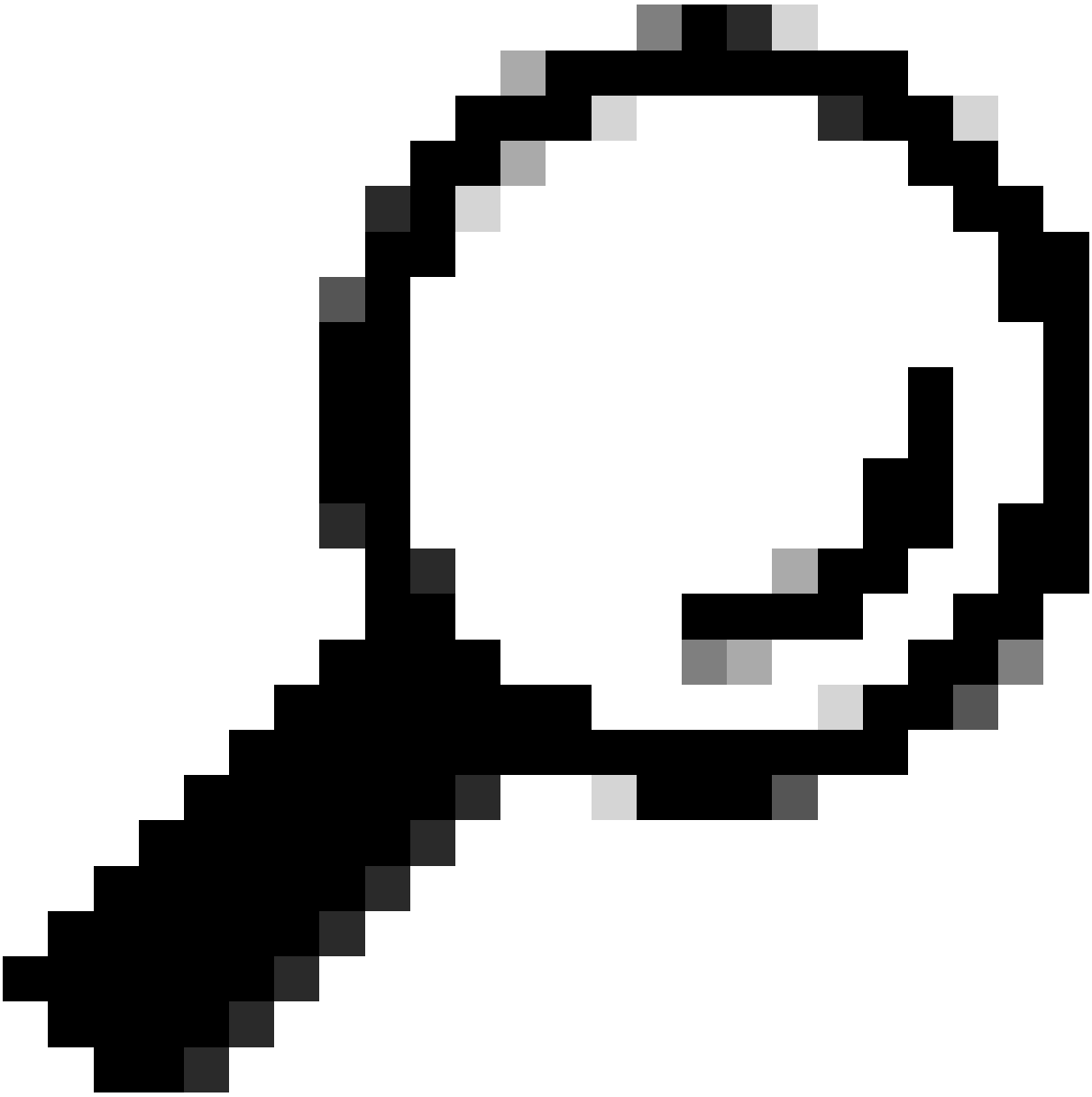
   SW Forwarding: 1/0/96/0, Other: 0/0/0
   HW Forwarding:

76236

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

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

  Totals - Source count: 1, Packet count: 4



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 8232匹配的VLAN上之后，其广播性质表明它被泛洪到VLAN1031的所有有线生成树协议转发端口。

<#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
```

但是，我们寻求广播DHCP提供的接口是与接入点关联的接入隧道接口。只有在L2LISP ID 8232上启用了“泛洪接入隧道”，才能实现此目的，否则此数据包将被阻止转发到AccessTunnel接口。

```
<#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
```

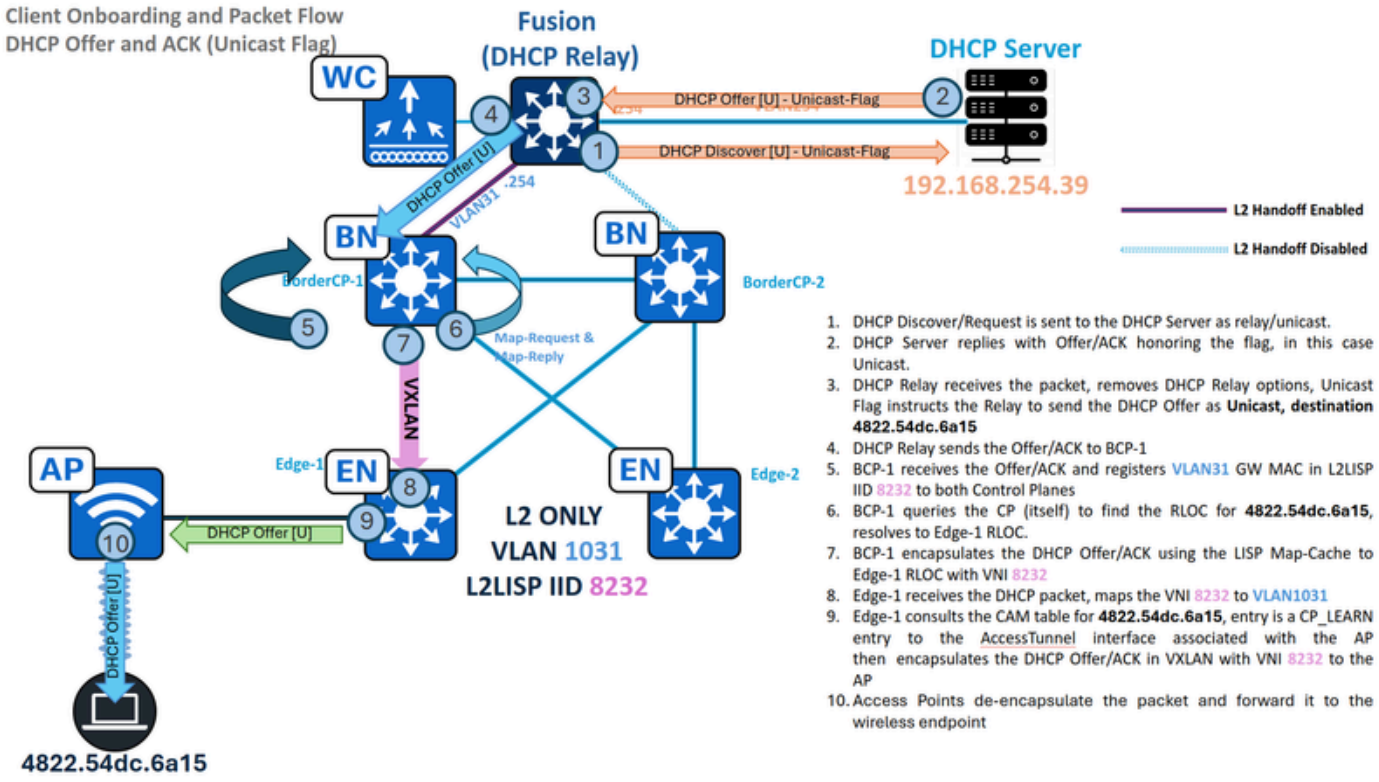
使用组播泛洪组的IGMP监听条目，DHCP提供和ACK将转发到AP的物理端口。

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的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 Ac2 | be Network

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

ARP

172.16.131.4

 4822.54dc.6a15

Ac2

1031

       0005       45s        REACHABLE  207 s try 0

Edge-1#show ip dhcp snooping  binding vlan 1041

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

Total number of bindings: 0
```

DHCP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==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)

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。根据单播转发原则，L2边界向控制平面查询目的MAC地址。假设在交换矩阵边缘上成功“MAC Learning and WLC Notification”（MAC学习和WLC通知），则控制平面已注册此终端ID(EID)。

<#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

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 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   -

解决RLOC后，DHCP提供以单播方式封装，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
----   -----------   --------   -----

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
```

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，边缘节点随后将仅将数据包转发到终端连接的特定接入隧道，而不是将其泛洪到所有端口。

MAC地址表将端口AccessTunnel2标识为与AP1关联的虚拟端口。

```
<#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
```

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的ARP数据包（而不是DHCP）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      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

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。

DHCP事务 — 无线验证

从WLC，通过RA-Trace监控DHCP事务。

<#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
```

在事务结束时，终端会添加到无线LAN控制器上的设备跟踪数据库。

<#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
```

整个DHCP事务在接入点本身进行调试。

<#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: 0
Aug 11 05:37:47 AP1 kernel: [*08/11/2025 05:37:47.3533] chatter: dhcp_reply_nonat: 1754890667.353287600
Aug 11 05:37:49 AP1 kernel: [*08/11/2025 05:37:49.3587] chatter: dhcp_from_inet: 1754890669.358709760: 1
Aug 11 05:37:49 AP1 kernel: [*08/11/2025 05:37:49.3588] chatter: dhcp_reply_nonat: 1754890669.358709760
Aug 11 05:37:49 AP1 kernel: [*08/11/2025 05:37:49.3589] [1754890669:358910] [AP1] [48:22:54:dc:6a:15]
```

[D:W]

DHCP_OFFER

```
 : TransId 0x76281006 tag:534

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

[U:W] DHCP_REQUEST

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

[D:W]

DHCP_ACK

```
 : TransId 0x76281006 tag:536

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

[D:A] DHCP_OFFER

```
 : TransId 0x76281006 [
```

Tx Success

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

[D:A]

DHCP_ACK

 : TransId 0x76281006 [

Tx Success

] tag:53

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

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

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

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）。