僅第2層VLAN中的DHCP故障排除 — 有線

目錄

簡介

必要條件

- 需求

僅第2層概述

- 概觀
- 僅L2 VLAN中的DHCP行為更改
- 底層多點傳送
- SD訪問交換矩陣內部的DHCP伺服器

拓撲

僅L2 VLAN配置

- 從Catalyst Center僅部署L2 VLAN

僅L2 VLAN配置 — 交換矩陣邊緣

第2層轉接配置 — 交換矩陣邊界

DHCP流量流

- DHCP探索和請求 — 邊緣
  - MAC學習和終端註冊
  - L2泛洪中的DHCP廣播橋接
  - 封包擷取
- DHCP發現和請求 — L2邊框
  - 封包擷取
- DHCP提供和ACK — 廣播 — L2邊框
  - MAC學習和網關註冊
  - L2泛洪中的DHCP廣播橋接
- DHCP提供和ACK — 廣播 — 邊緣
- DHCP提供和ACK — 單播 — L2邊界
- DHCP提供和ACK — 單播 — 邊緣

簡介

本文說明如何在SD-Access(SDA)交換矩陣中的第2層專用網路中排除有線終端的DHCP故障。

必要條件

需求

思科建議您瞭解以下主題：

- 網際網路通訊協定(IP)轉送
- Locator/ID Separation Protocol(LISP)

- 通訊協定無關多點傳送(PIM)稀疏模式

硬體和軟體要求

- Catalyst 9000 系列交換器
- Catalyst中心版本2.3.7.9
- Cisco IOS® XE 17.12及更高版本

限制

- 只有一個L2邊界可以同時切換唯一的VLAN/VNI，除非正確配置了強大的環路防止機制（如用於禁用鏈路的FlexLink+或EEM指令碼）。

僅第2層概述

概觀

在典型的SD-Access部署中，L2/L3邊界位於交換矩陣邊緣(FE)，其中FE以SVI的形式承載客戶端網關，通常稱為「任播網關」。第3層VNI（路由）針對子網間流量建立，而第2層VNI（交換）管理子網內流量。跨所有FE的一致配置可實現無縫客戶端漫遊。轉發已最佳化：子網內(L2)流量直接橋接在FE之間，而子網間(L3)流量則在FE之間或FE與邊界節點之間路由。

對於SDA交換矩陣中需要交換矩陣外部的嚴格網路入口點的終端，SDA交換矩陣必須提供從邊緣到外部網關的L2通道。

此概念類似於傳統的乙太網園區部署，其中第2層接入網路連線到第3層路由器。VLAN內流量保留在L2網路中，而VLAN間流量由L3裝置路由，通常會返回到L2網路上的不同VLAN。

在LISP上下文中，站點控制平面主要跟蹤MAC地址及其相應的MAC到IP繫結，非常類似於傳統的ARP條目。僅L2 VNI/L2池專門用於促進基於這兩種EID型別的註冊、解析和轉發。因此，在僅使用L2的環境中，任何基於LISP的轉發僅依賴於MAC和MAC到IP資訊，它完全忽略IPv4或IPv6 EID。為了補充LISP EID，僅第2層池嚴重依賴泛洪和學習機制，與傳統交換機的行為類似。因此，L2泛洪成為此解決方案中處理廣播、未知單播和多播(BUM)流量的關鍵元件，需要使用底層多播。相反，通常的單點傳播流量使用標準LISP轉發流程轉發，主要通過對映快取轉發。

交換矩陣邊緣和「L2邊界」(L2B)都維護對映到本地VLAN的第2層VNI（此對映在SDA內對本地裝置有效，允許不同的VLAN跨節點對映到相同的L2 VNI）。 在此特定使用案例中，在這些節點的這些VLAN上未配置SVI，這意味著沒有對應的第3層VNI。

僅L2 VLAN中的DHCP行為更改

在任播網關池中，DHCP帶來了挑戰，因為每個交換矩陣邊緣都充當其直連端點的網關，所有FE上使用相同的網關IP。要正確識別DHCP中繼資料包的原始源，FE必須插入DHCP選項82及其子選項，包括LISP RLOC資訊。這是通過在交換矩陣邊緣的客戶端VLAN上執行DHCP監聽實現的。DHCP監聽在此環境中具有雙重作用：它方便了選項82的插入，而且關鍵的是，防止了DHCP廣播資料包通過橋接域(VLAN/VNI)泛洪。 即使為任播網關啟用第2層泛洪，DHCP監聽也會有效地抑制廣播資料包，使其作為廣播從交換矩陣邊緣轉發出去。

相比之下，僅第2層VLAN缺少網關，從而簡化了DHCP源識別。由於資料包不通過任何交換矩陣邊緣中繼，因此不需要複雜的源識別機制。如果L2 Only VLAN上沒有DHCP監聽，則有效地繞過DHCP資料包的泛洪控制機制。這允許通過L2泛洪將DHCP廣播轉發到其最終目的地，該目的地可以是直接連線到交換矩陣節點的DHCP伺服器，或提供DHCP中繼功能的第3層裝置。

警告：L2 Only池中的「多個IP到MAC」功能在網橋VM模式下自動啟用DHCP監聽，從而實施DHCP泛洪控制。因此，這會導致L2 VNI池無法支援其終端的DHCP。

底層多點傳送

由於DHCP嚴重依賴廣播流量，因此必須利用第2層泛洪來支援此協定。與任何其他啟用第2層泛洪的池一樣，底層網路必須配置為組播流量，尤其是使用PIM稀疏模式的Any-Source-Multicast。雖然底層組播配置是通過LAN自動化工作流程自動執行的，但如果省略此步驟，則需要額外的配置（手動或模板）。

- 在所有節點（邊界、邊緣、中間節點等）上啟用IP組播路由。
- 在每個Border和Edge節點的Loopback0介面上配置PIM稀疏模式。

- 在每個IGP（底層路由協定）介面上啟用PIM稀疏模式。
- 在所有節點（邊界、邊緣、中間節點）上配置PIM集結點(RP)，建議將RP放置在邊界上。
- 驗證PIM鄰居、PIM RP和PIM隧道狀態。

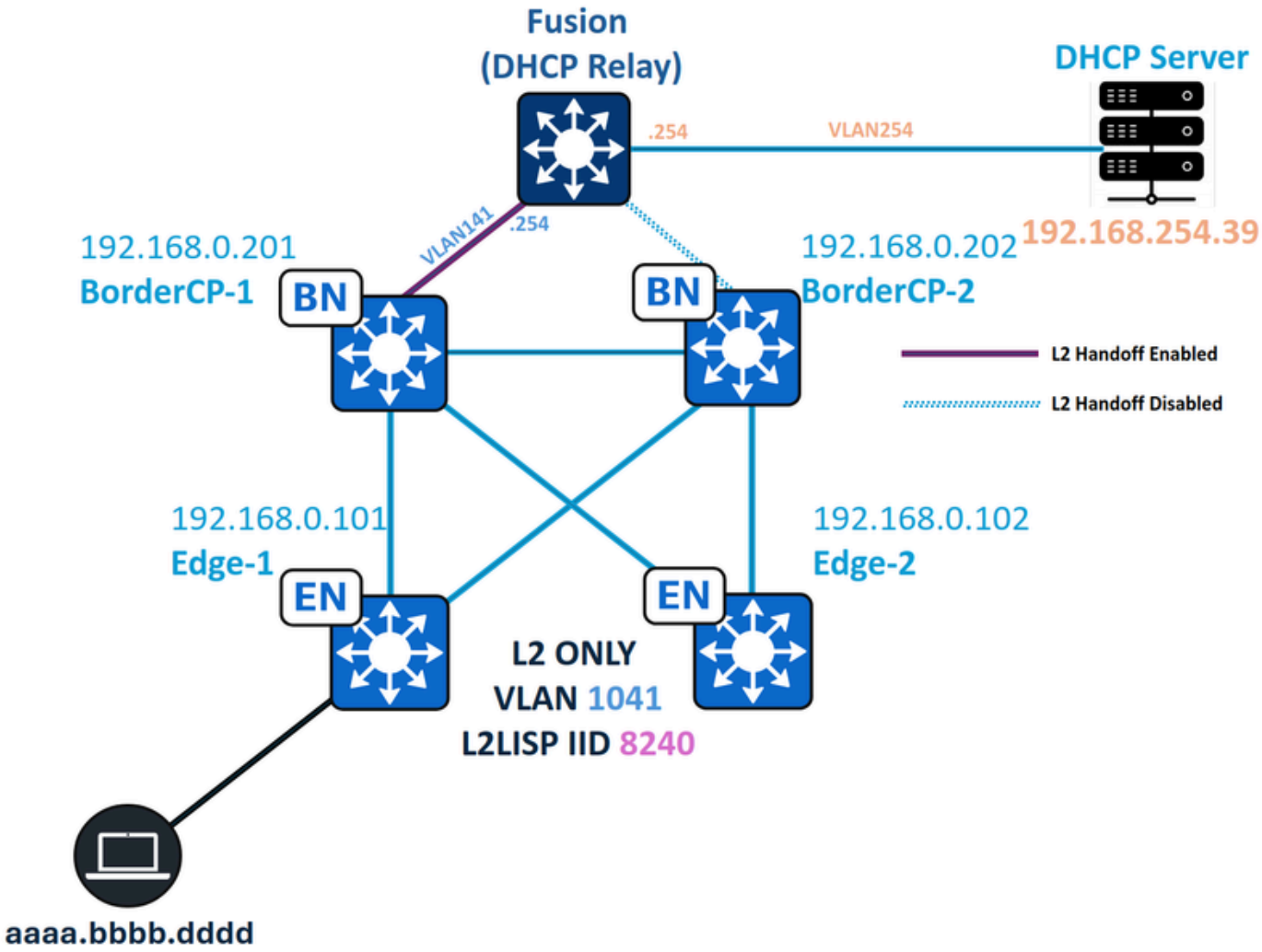
SD訪問交換矩陣內部的DHCP伺服器

一個常見的設計問題是是否可在SD-Access交換矩陣中部署DHCP伺服器。從本質上講，答案既是肯定的，也是否定的。

官方Cisco Validated Design建議將DHCP伺服器放置在交換矩陣之外，通常放在Shared Services塊中。但是，如果情況需要DHCP伺服器物理連線到交換矩陣節點（例如邊緣或邊界），則唯一支援的方法是通過僅第2層網路。這是因為任播網關池的固有行為，其中預設啟用DHCP監聽。這不僅會阻塞來自伺服器的DHCP提供和確認，而且會阻止DHCP發現和請求資料包（即使封裝在VXLAN中）被轉發。雖然DHCP伺服器連線埠上的「DHCP窺探信任」允許提供和確認，但探索和請求封包不會使用相同的方法轉送。此外，不支援刪除任播網關池中的DHCP監聽，因為Catalyst　Center會在合規性驗證期間標籤這樣的配置偏差。

反之，當DHCP伺服器放置在L2　Only網路中時，不會實施DHCP監聽，從而允許所有DHCP資料包通過，而無需基於策略的檢查或阻止。SD-Access交換矩陣上游的網路裝置（例如，Fusion Router）被配置為僅第2層網路的網關，使來自多個VRF的流量能夠訪問該L2　　Only網段內的同一DHCP伺服器。

拓撲



網路拓撲

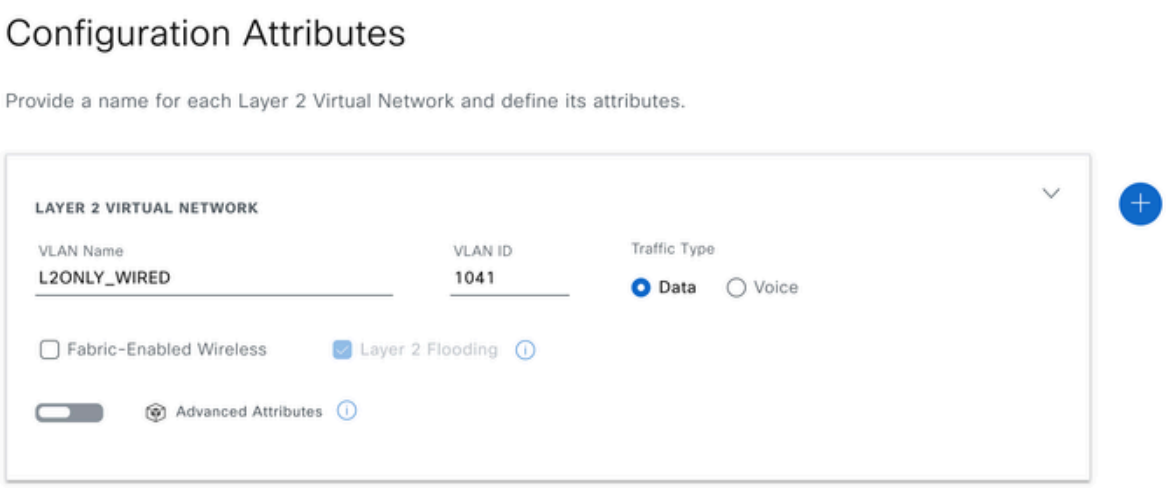
在此拓撲中：

- 192.168.0.201和192.168.0.202是交換矩陣站點的並置邊界，BorderCP-1是啟用第2層傳遞功能的唯一邊界。
- 192.168.0.101和192.168.0.102是交換矩陣邊緣節點
- 192.168.254.39是DHCP伺服器
- aaaa.bbb.dddd是啟用DHCP的端點
- Fusion裝置充當交換矩陣子網的DHCP中繼。

僅L2 VLAN配置

從Catalyst Center僅部署L2 VLAN

路徑：Catalyst中心/調配/交換矩陣站點/第2層虛擬網路/編輯第2層虛擬網路



L2VNI組態

僅L2 VLAN配置 — 交換矩陣邊緣

交換矩陣邊緣節點的VLAN配置為啟用CTS、禁用IGMP和IPv6 MLD以及所需的L2 LISP配置。此L2 Only池不是無線池；因此，未配置L2 Only Wireless Pools中通常存在的功能，如RA-Guard、DHCPGuard和泛洪接入隧道。相反，ARP資料包的泛洪是使用「flood arp-nd」顯式啟用的

交換矩陣邊緣(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
```

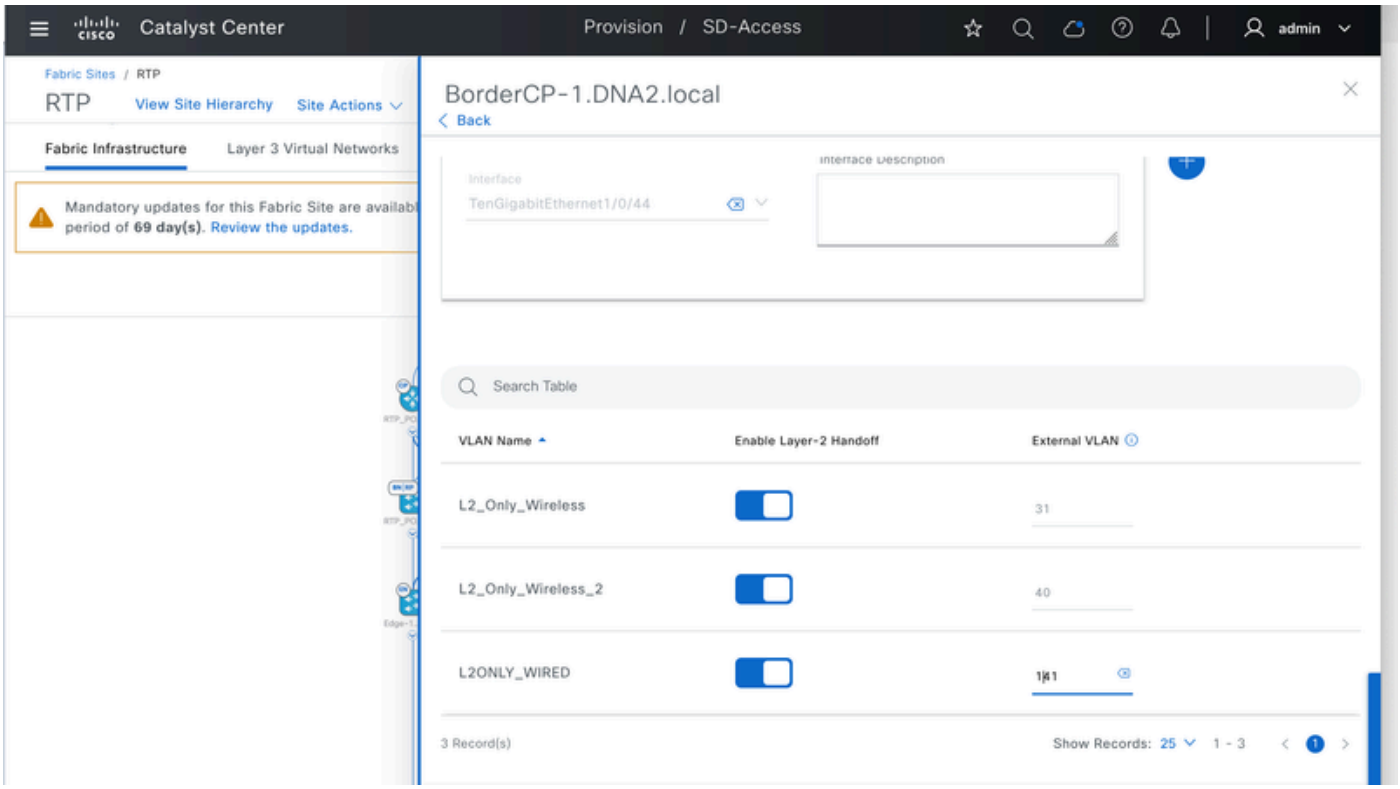
```
 instance-id
8240

  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
```

第2層轉接配置 — 交換矩陣邊界

從操作角度來看，允許DHCP伺服器（或路由器/中繼）連線到任何交換矩陣節點，包括邊界和邊緣。

使用Border節點連線DHCP伺服器是推薦的方法，但需要仔細設計考慮。這是因為必須在每個介面上為第2層傳遞配置邊框。這允許將交換矩陣池傳遞給交換矩陣內相同的VLAN或不同的VLAN。交換矩陣邊緣和邊界之間的VLAN ID具有這種靈活性，因為兩者都對映到相同的L2 LISP例項ID。不能使用同一個VLAN同時啟用L2切換物理埠，以防止SD-Access網路出現第2層環路。若要實現冗餘，需要使用StackWise Virtual、FlexLink+或EEM指令碼等方法。

相反，將DHCP伺服器或網關路由器連線到交換矩陣邊緣不需要額外的配置。



L2轉接配置

交換矩陣邊界(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

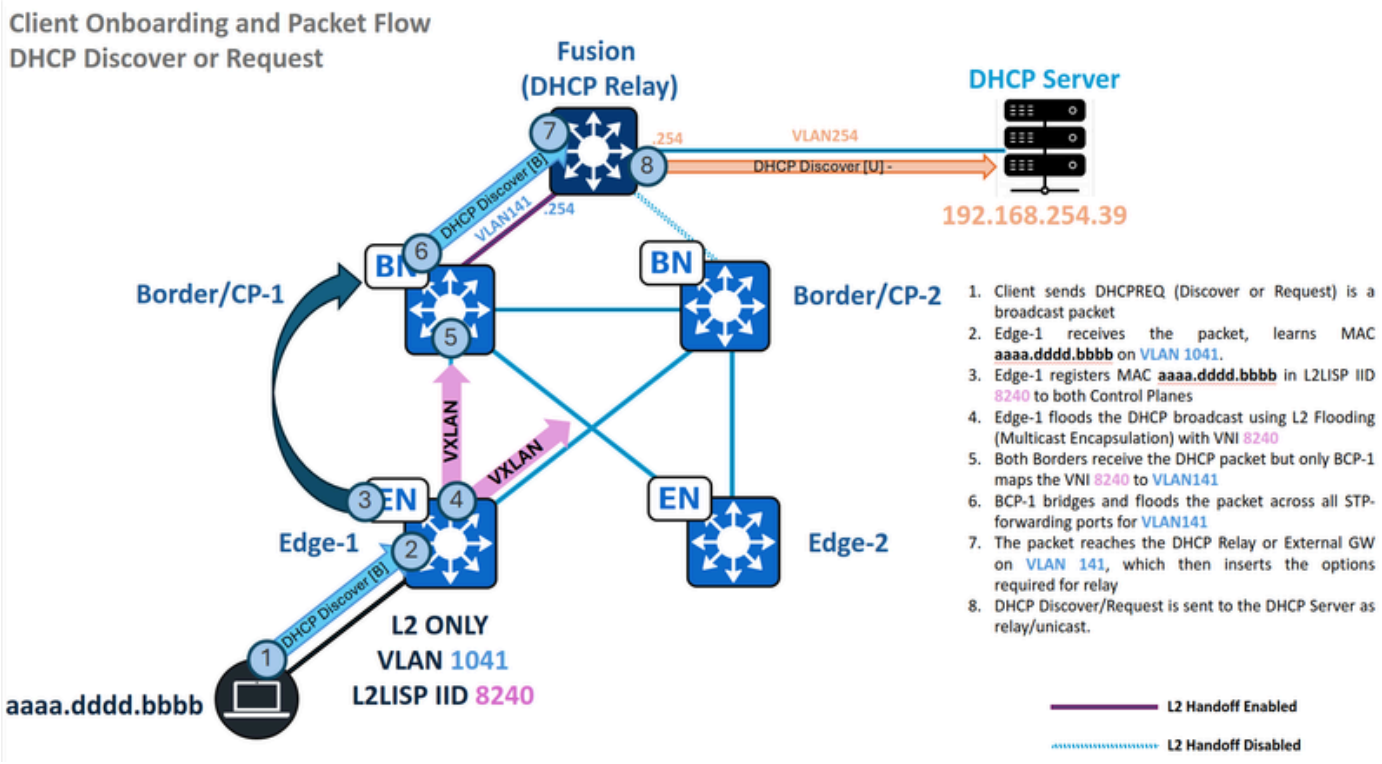
no ipv6 mld snooping vlan 141

```
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流量流

DHCP探索和請求 — 邊緣



通訊流 — 僅L2中的DHCP發現和請求

MAC學習和終端註冊

當終端aaaa.dddd.bbb傳送DHCP發現或請求（廣播資料包）時，邊緣節點必須獲取終端的MAC地址，將其新增到其MAC地址表，然後新增到L2/MAC SISF表，最後到VLAN 1041的L2LISP資料庫，對映到L2LISP例項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
```

如果終端的MAC地址已正確獲知，並且交換矩陣控制平面的ACK標誌已標籤為「Yes」，則此階段視為已完成。

L2泛洪中的DHCP廣播橋接

禁用DHCP監聽時，不會阻止DHCP廣播；相反，它們會封裝在組播中，以便進行第2層泛洪。反之，啟用DHCP監聽可以防止這些廣播資料包泛洪。

<#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>
```

由於DHCP監聽已禁用，因此DHCP發現/請求利用L2LISP0介面，通過L2泛洪橋接流量。根據Catalyst Center版本和應用的Fabric Banner，L2LISP0介面可能具有雙向配置的訪問清單；因此

，請確保任何存取控制專案(ACE)都沒有明確拒絕DHCP流量（UDP連線埠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
```

利用為L2LISP例項配置的廣播底層組和交換矩陣邊緣的Loopback0 IP地址來檢驗將該資料包橋接至其他交換矩陣節點的L2泛洪(S，G)條目。請參閱mroute和mfib表以驗證引數，如傳入介面、傳出介面清單和轉發計數器。

```
<#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:

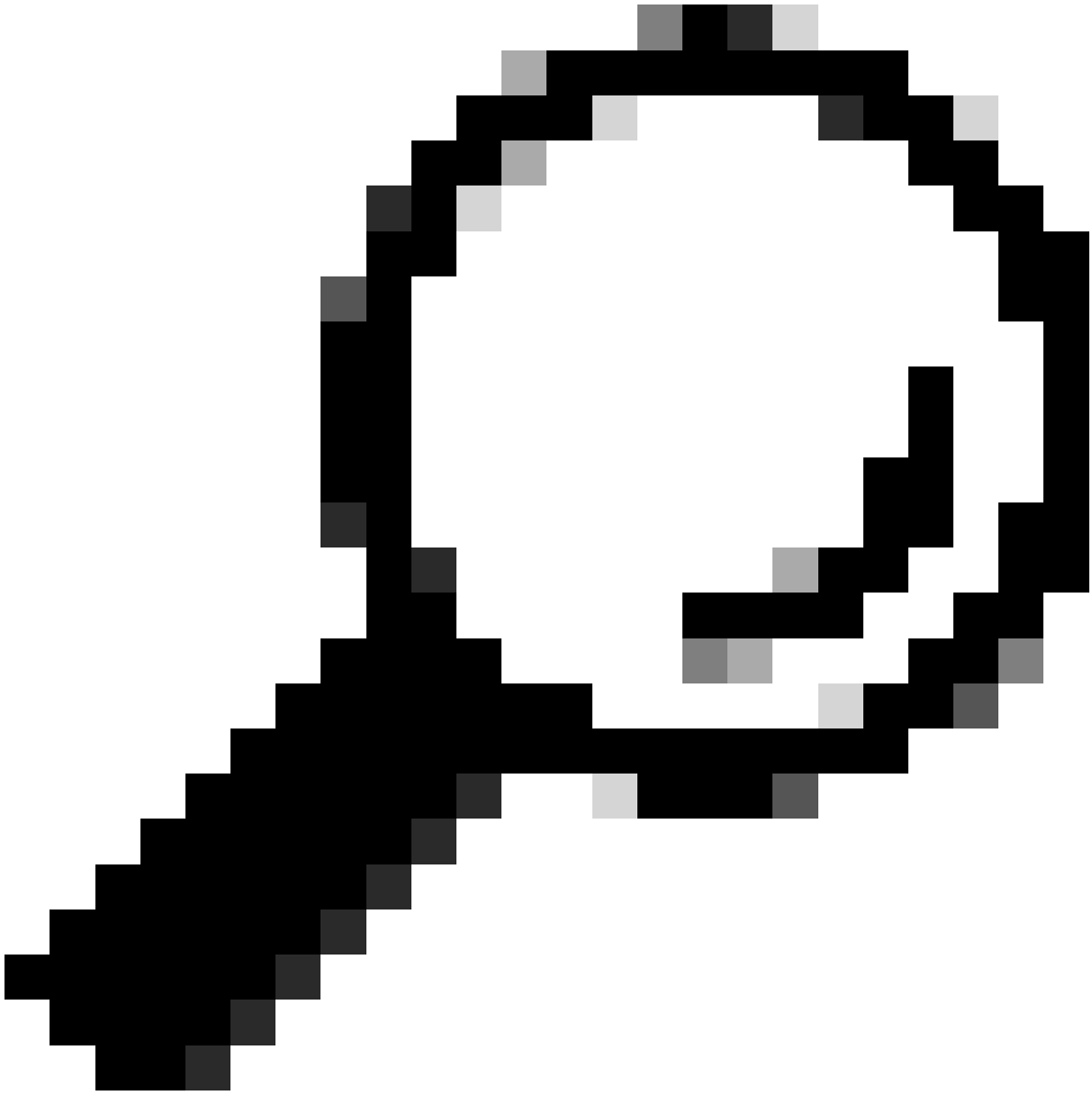
 7

/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：如果找不到(S，G)條目或傳出介面清單(OIL)不包含傳出介面(OIF)，則表明底層組播配置或操作有問題。

封包擷取

在交換機上配置同時嵌入式資料包捕獲，以記錄來自終端的傳入DHCP資料包和相應的輸出資料包，以進行L2泛洪。捕獲資料包時，應觀察兩個不同的資料包：原始DHCP探索/要求及其VXLAN封裝的對應項，目的地為底層組(239.0.17.1)。

光纖邊緣(192.168.0.101)封包擷取

<#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發現和請求 — L2邊框

邊緣通過第2層泛洪傳送DHCP發現和請求資料包後（封裝了Broadcast-Underlay組239.0.17.1），這些資料包將由L2轉發邊界接收，在本場景中具體是Border/CP-1。

為此，Border/CP-1必須擁有與邊緣(S，G)的組播路由，其傳出介面清單必須包括L2切換VLAN的L2LISP例項。必須注意的是，L2轉接邊界共用相同的L2LISP例項ID，即使它們為轉接使用不同的VLAN。

<#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

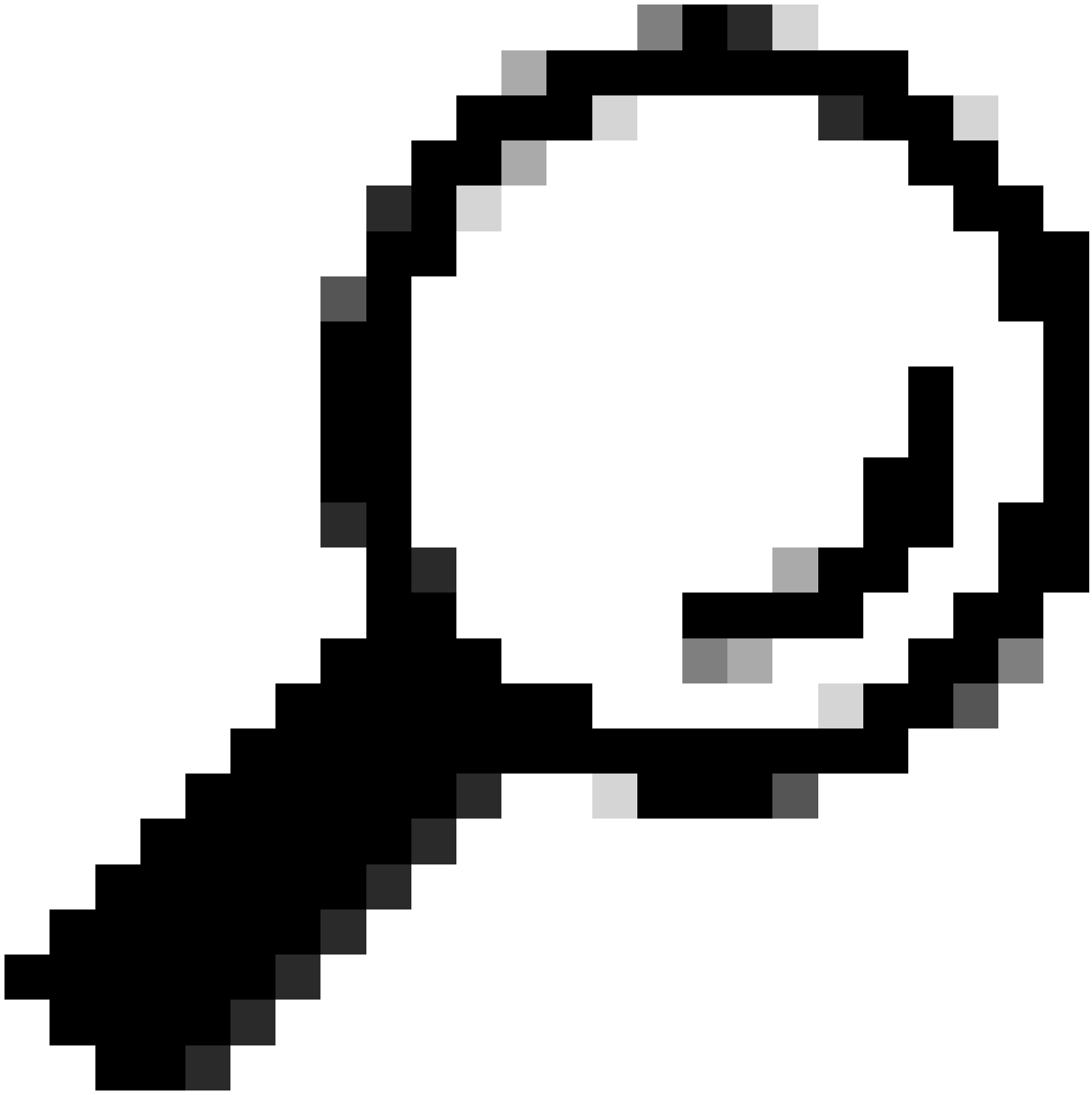
,
   SW Forwarding: 1/0/392/0, Other: 0/0/0
   HW Forwarding:

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)條目，則表示底層組播配置或操作有問題。如果所需例項的L2LISP未作為OIF存在，則表明L2LISP子介面的操作UP/DOWN狀態或L2LISP介面的IGMP啟用狀態存在問題。

與交換矩陣邊緣節點類似，請確保沒有訪問控制項會拒絕L2LISP0介面上的輸入DHCP資料包。

<#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
```

將封包解除封裝並放置在與VNI 8240相符的VLAN上後，其廣播性質表示封包已泛洪到轉送的VLAN 141的所有跨距樹狀目錄通訊協定轉送連線埠。

```
<#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
```

Device-Tracking表確認連線到網關/DHCP中繼的介面Te1/0/44必須是STP轉發埠。

```
<#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
```

封包擷取

在交換機上配置同時嵌入式資料包捕獲，以記錄來自L2泛洪（S，G傳入介面）的傳入DHCP資料包和到DHCP中繼的相應輸出資料包。捕獲資料包時，應觀察兩個不同的資料包：來自Edge-1的VXLAN封裝資料包，以及到達DHCP中繼的解封裝資料包。

光纖邊界/CP(192.168.0.201)封包擷取器

<#root>

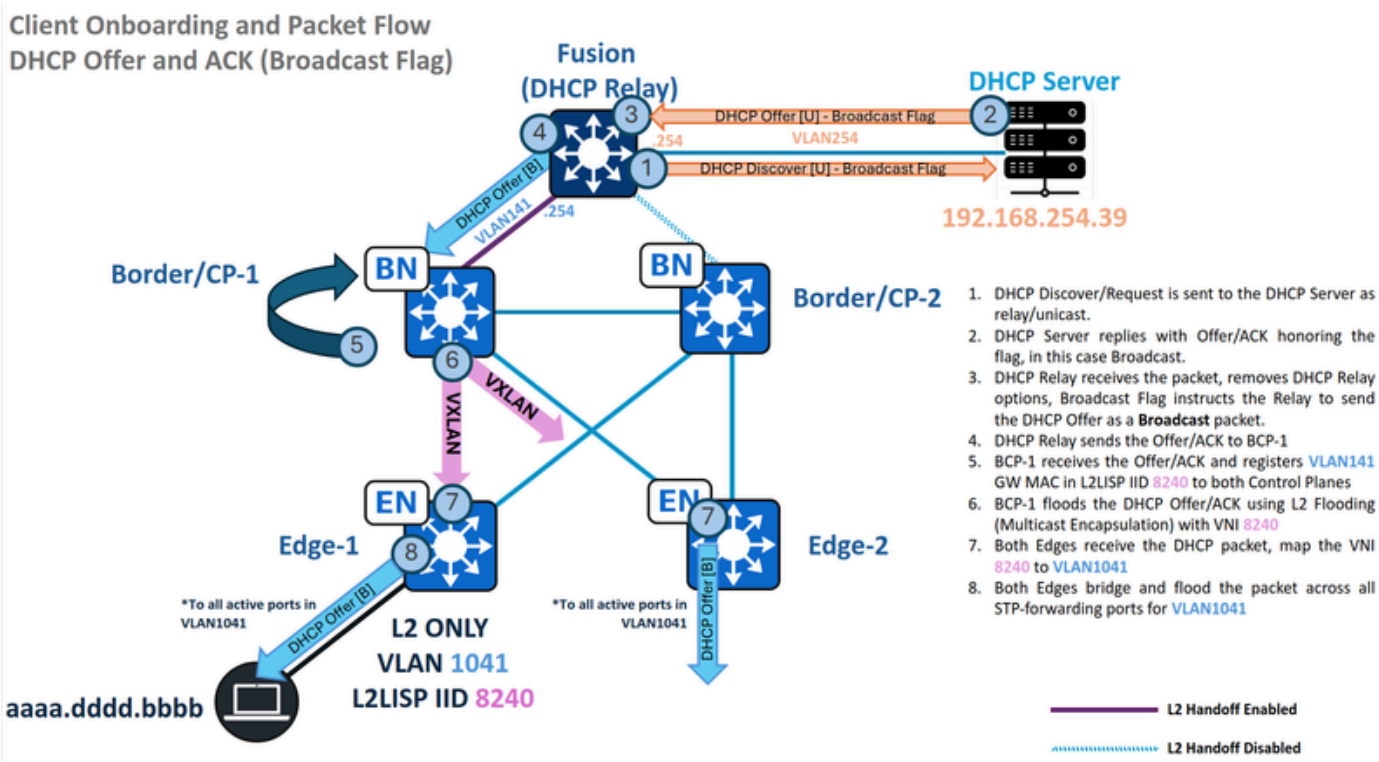
```
monitor capture cap interface TenGigabitEthernet1/0/42 IN    <-- Incoming interface for Edge's S,G Mrout

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 — 廣播 — L2邊框



通訊流 — 僅在第2層廣播DHCP提供和ACK

現在DHCP發現已退出SD-Access交換矩陣，DHCP中繼將插入傳統的DHCP中繼選項（例如GiAddr/GatewayIPAddress），並將資料包作為單播傳輸轉發到DHCP伺服器。在此流程中，SD-Access交換矩陣不附加任何特殊的DHCP選項。

在伺服器收到DHCP發現/請求後，伺服器會執行嵌入的廣播或單播標誌。此標籤指示DHCP中繼代理是否將DHCP提供作為廣播幀或單播幀轉發到下游裝置（我們的邊界）。在本演示中，假設存在廣播場景。

MAC學習和網關註冊

當DHCP中繼傳送DHCP提供或ACK時，L2BN節點必須獲取網關的MAC地址，將其新增到其MAC地址表中，然後到L2/MAC　SISF表，最後到VLAN　141的L2LISP資料庫，對映到L2LISP例項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

如果網關的MAC地址已正確獲知，並且交換矩陣控制平面的ACK標誌已標籤為「Yes」，則此階段視為已完成。

L2泛洪中的DHCP廣播橋接

如果沒有啟用DHCP監聽，DHCP廣播不會受到阻止，而是封裝在組播中，以實現第2層泛洪。反之，如果啟用DHCP監聽，則會阻止DHCP廣播資料包泛洪。

<#root>

BorderCP-1#

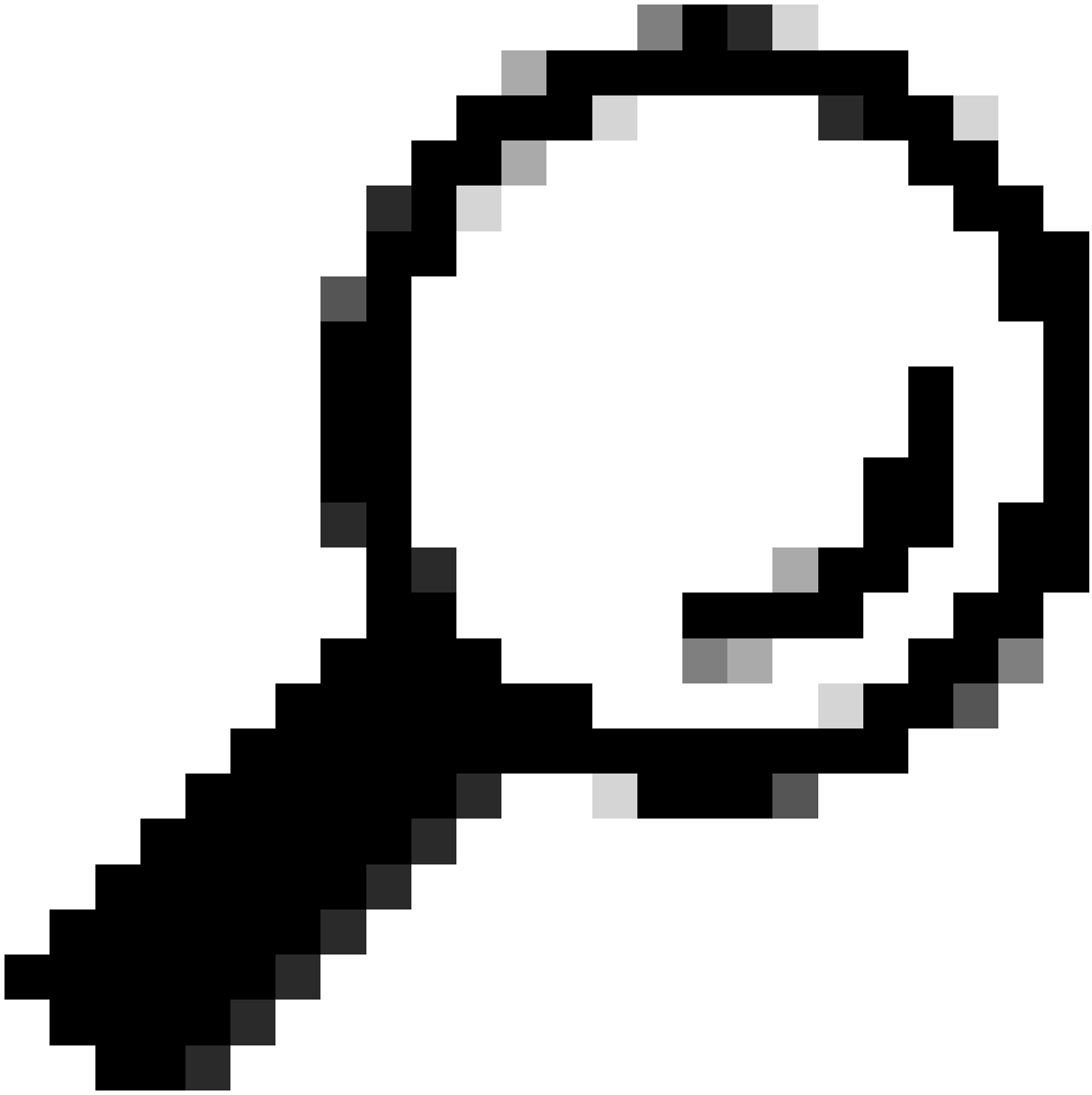
show ip dhcp snooping

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：由於L2Border中未啟用DHCP監聽，因此不需要配置DHCP監聽信任。

在這個階段，兩台裝置都已完成L2LISP ACL驗證。

利用為L2LISP例項配置的廣播底層組和L2Border Loopback0 IP地址來檢驗將該資料包橋接到其他交換矩陣節點的L2泛洪(S，G)條目。請參閱mroute和mfib表以驗證引數，如傳入介面、傳出介面清單和轉發計數器。

<#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

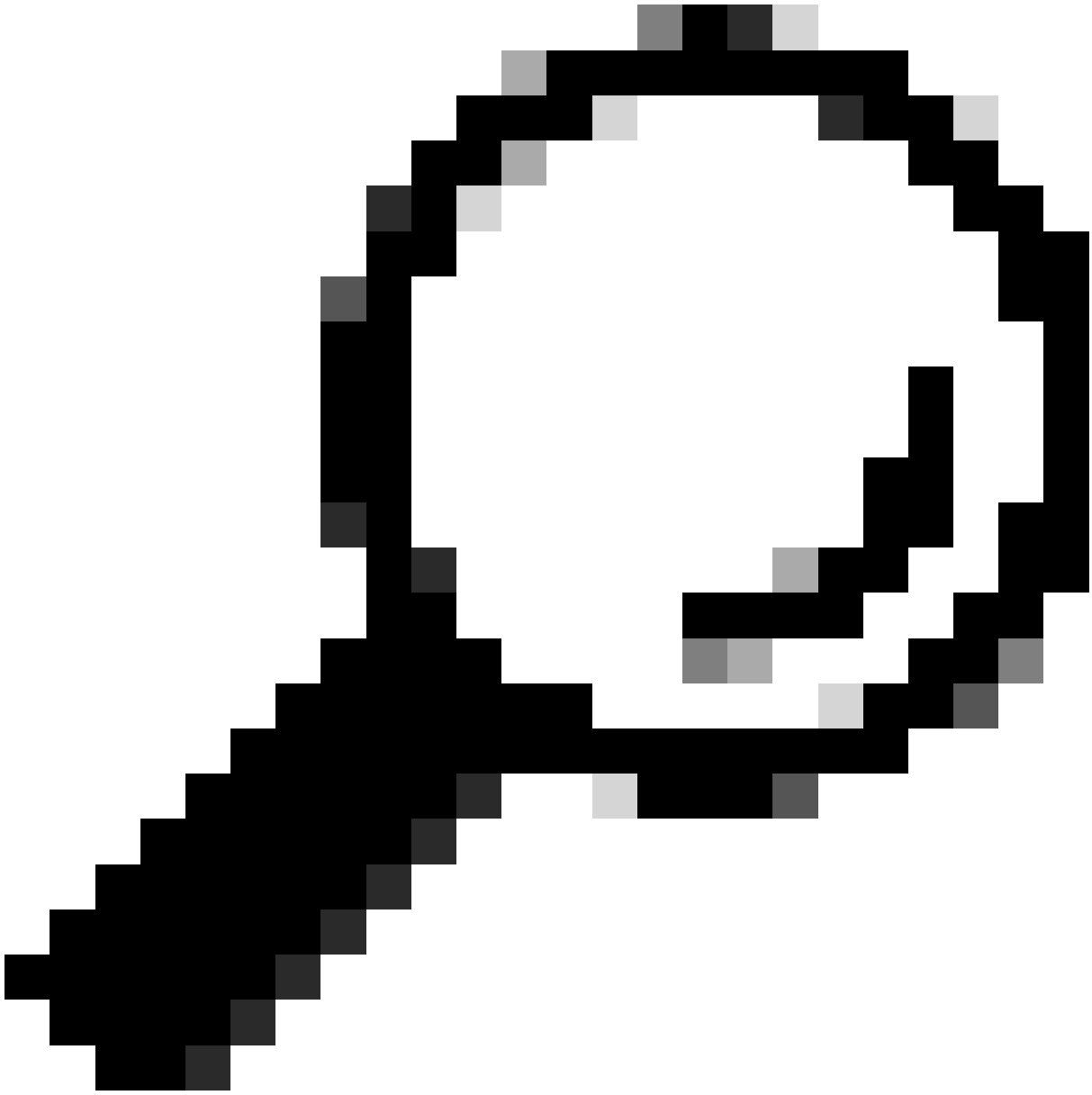
,
   SW Forwarding: 1/0/392/0, Other: 1/1/0
   HW Forwarding:

  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：如果找不到(S，G)條目或傳出介面清單(OIL)不包含傳出介面(OIF)，則表明底層組播配置或操作有問題。

通過這些驗證，沿資料包捕獲（類似於前面的步驟），本節將結束，因為DHCP提供會使用傳出介面清單內容（在本例中是介面TenGig1/0/42和TenGig1/0/43之外）以廣播形式轉發到所有交換矩陣邊緣。

DHCP提供和ACK — 廣播 — 邊緣

與上一個流完全相同，在交換矩陣邊緣驗證L2Border S、G，其中傳入介面指向L2BN，並且OIL包含對映到VLAN 1041的L2LISP例項。

```
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,

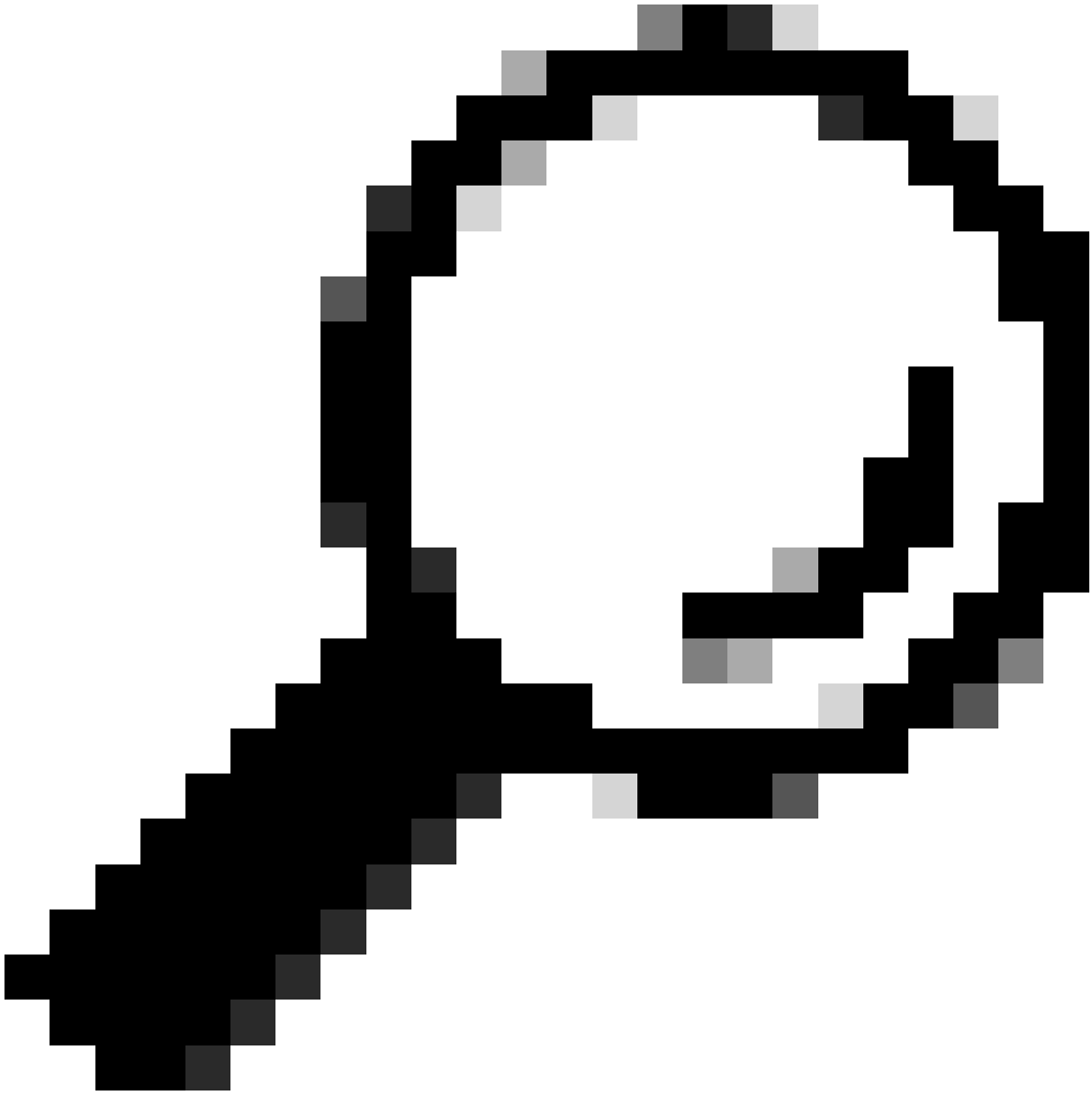
   SW Forwarding: 1/0/96/0, Other: 0/0/0
   HW Forwarding:

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)條目，則表示底層組播配置或操作有問題。如果所需例項的L2LISP未作為OIF存在，則表明L2LISP子介面的操作UP/DOWN狀態或L2LISP介面的IGMP啟用狀態存在問題。

兩台裝置中都已完成L2LISP ACL驗證。

將封包解除封裝並放在與VNI 8240相符的VLAN上後，其廣播性質表示其已泛洪出去，從VLAN1041的所有跨距樹狀目錄通訊協定轉送連線埠中轉出。

<#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地址表將埠Te1/0/2標識為終端埠，該埠通過STP處於FWD狀態，資料包被泛洪到終端。

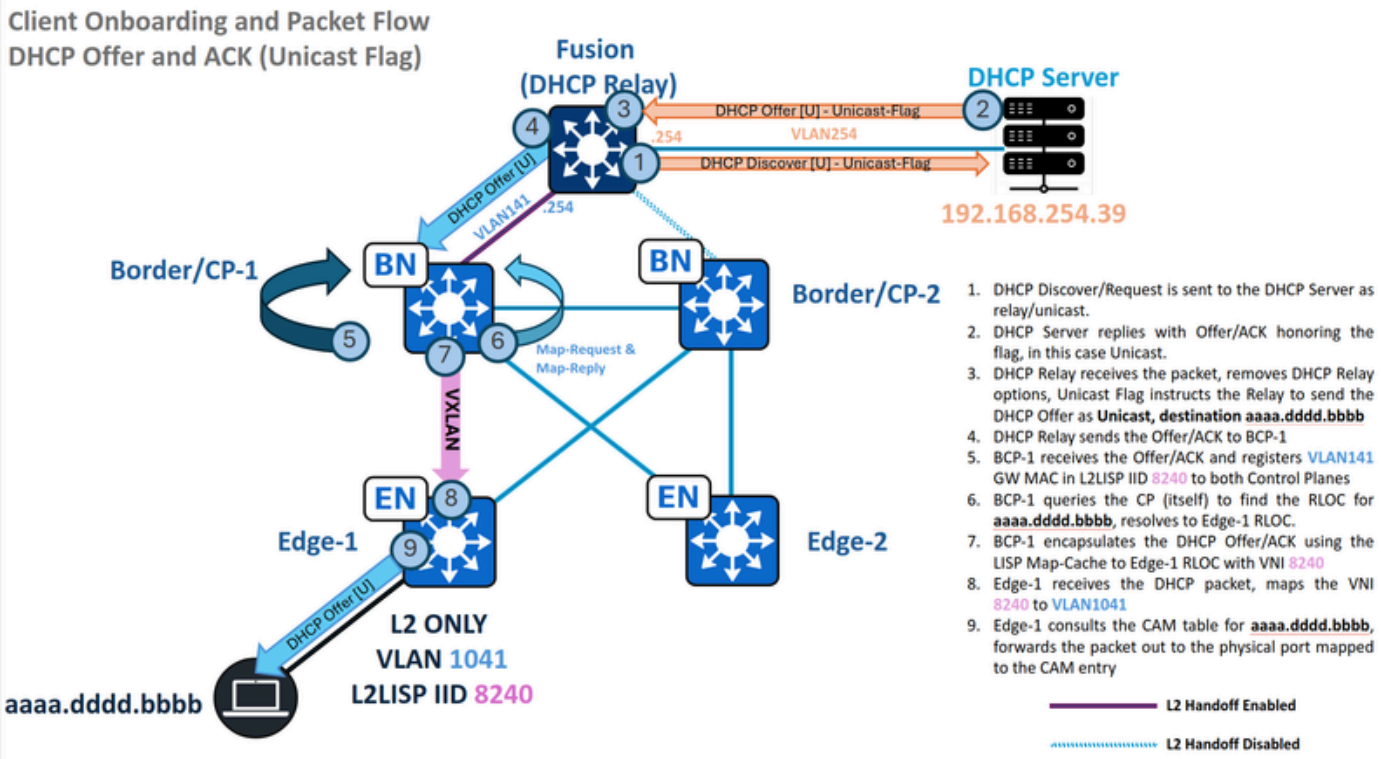
```
<#root>

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過程始終保持一致。如果未啟用DHCP監聽，則不會在DHCP監聽表中建立任何條目。因此，啟用DHCP的終端的裝置跟蹤條目通過收集ARP資料包生成。由於DHCP監聽已禁用

，因此「show platform dhcpsnooping client stats」等命令預計不會顯示任何資料。

```
<#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 — 單播 — L2邊界



通訊流 — 單播DHCP提供和ACK（僅限第2層）

在此場景略有不同，終端將DHCP廣播標誌設定為unset或「0」。

DHCP中繼不會將DHCP提供/ACK作為廣播傳送，而是作為單播資料包傳送，其目的MAC地址從DHCP負載內的客戶端硬體地址派生。這顯著地修改了SD-Access交換矩陣處理資料包的方式，它使用L2LISP對映快取來轉發流量，而不是第2層泛洪組播封裝方法。

交換矩陣邊界/CP(192.168.0.201)資料包catpure:輸入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)
```

在此場景中，L2泛洪專門用於發現/請求，而提供/ACK則通過L2LISP對映快取轉發，從而簡化了整體操作。根據單播轉發原則，L2邊界向控制平面查詢目的MAC地址(aaaa.dddd.bbb)。 假設在交換矩陣邊緣上成功「MAC學習和終端註冊」，則控制平面已註冊此終端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
```

在邊界向控制平面（本地或遠端）查詢後，LISP解析為終端的MAC地址建立對映快取條目。

```
<#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        -
```

解決RLOC後，DHCP提供將封裝為單播，並使用VNI 8240直接傳送到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
```

使用與前面部分相同的方法，捕獲從DHCP中繼和RLOC輸出介面的輸入流量，以觀察單播到邊緣RLOC的VXLAN封裝。

DHCP提供和ACK — 單播 — 邊緣

邊緣從邊界接收單播DHCP提供/ACK，解封裝流量並查詢其MAC地址表以確定正確的出口埠。與廣播Offer/ACK不同，邊緣節點僅將資料包轉發到終端所連線的特定埠，而不是將其泛洪到所有埠。

MAC地址表將埠Te1/0/2標識為我們的客戶端埠，該埠通過STP處於FWD狀態，資料包將被轉發到終端。

```
<#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過程始終保持一致。如果未啟用DHCP監聽，則不會在DHCP監聽表中建立任何條目。因此，啟用DHCP的終端的裝置跟蹤條目由收集ARP資料包生成。由於DHCP監聽已禁用，因此「show platform dhcpsnooping client stats」等命令預計不會顯示任何資料。

```
<#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
```

必須注意的是，SD-Access交換矩陣不影響單播或廣播標誌的使用，因為這只是端點行為。雖然此功能可能被DHCP中繼或DHCP伺服器本身所覆蓋，但兩種機制對於在L2 Only環境中無縫DHCP操作都至關重要：使用廣播提供/ACK的底層組播進行第2層泛洪，並在控制平面中為單播提供/ACK進行正確的端點註冊。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。