Risoluzione dei problemi di DHCP nella VLAN di solo layer 2 - Cablata

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi a DHCP per endpoint con cavo in una rete di solo livello 2 in un'infrastruttura SDA (SD-Access).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Inoltro IP (Internet Protocol)
- Locator/ID Separation Protocol (LISP)
- PIM (Protocol Independent Multicast) in modalità sparse

Requisiti hardware e software

- Switch Catalyst serie 9000
- Catalyst Center versione 2.3.7.9
- Cisco IOS® XE 17.12 e versioni successive

Limitazioni

- Un solo bordo L2 può gestire una VLAN/VNI univoca contemporaneamente, a meno che non siano configurati correttamente meccanismi affidabili di prevenzione dei loop, come FlexLink+ o script EEM per disabilitare i collegamenti.

Panoramica solo L2

Panoramica

Nelle tipiche implementazioni ad accesso SD, il limite L2/L3 risiede sul Fabric Edge (FE), dove il FE ospita il gateway del client sotto forma di SVI, spesso chiamato "Anycast Gateway". I VNI L3 (routing) vengono stabiliti per il traffico tra subnet, mentre i VNI L2 (switching) gestiscono il traffico all'interno della subnet. La configurazione coerente tra tutti gli FE consente il roaming dei client senza problemi. Inoltro ottimizzato: il traffico all'interno della subnet (L2) è collegato direttamente tra FE e il traffico all'interno della subnet (L3) è indirizzato tra FE o tra FE e un nodo di confine.

Per gli endpoint nei fabric SDA che richiedono un punto di ingresso di rete rigoroso all'esterno del fabric, il fabric SDA deve fornire un canale L2 dal perimetro a un gateway esterno.

Questo concetto è analogo alle tradizionali implementazioni Ethernet nei campus in cui una rete di accesso di layer 2 si connette a un router di layer 3. Il traffico tra VLAN rimane all'interno della rete L2, mentre il traffico tra VLAN viene instradato dal dispositivo L3, spesso torna a una VLAN diversa sulla rete L2.

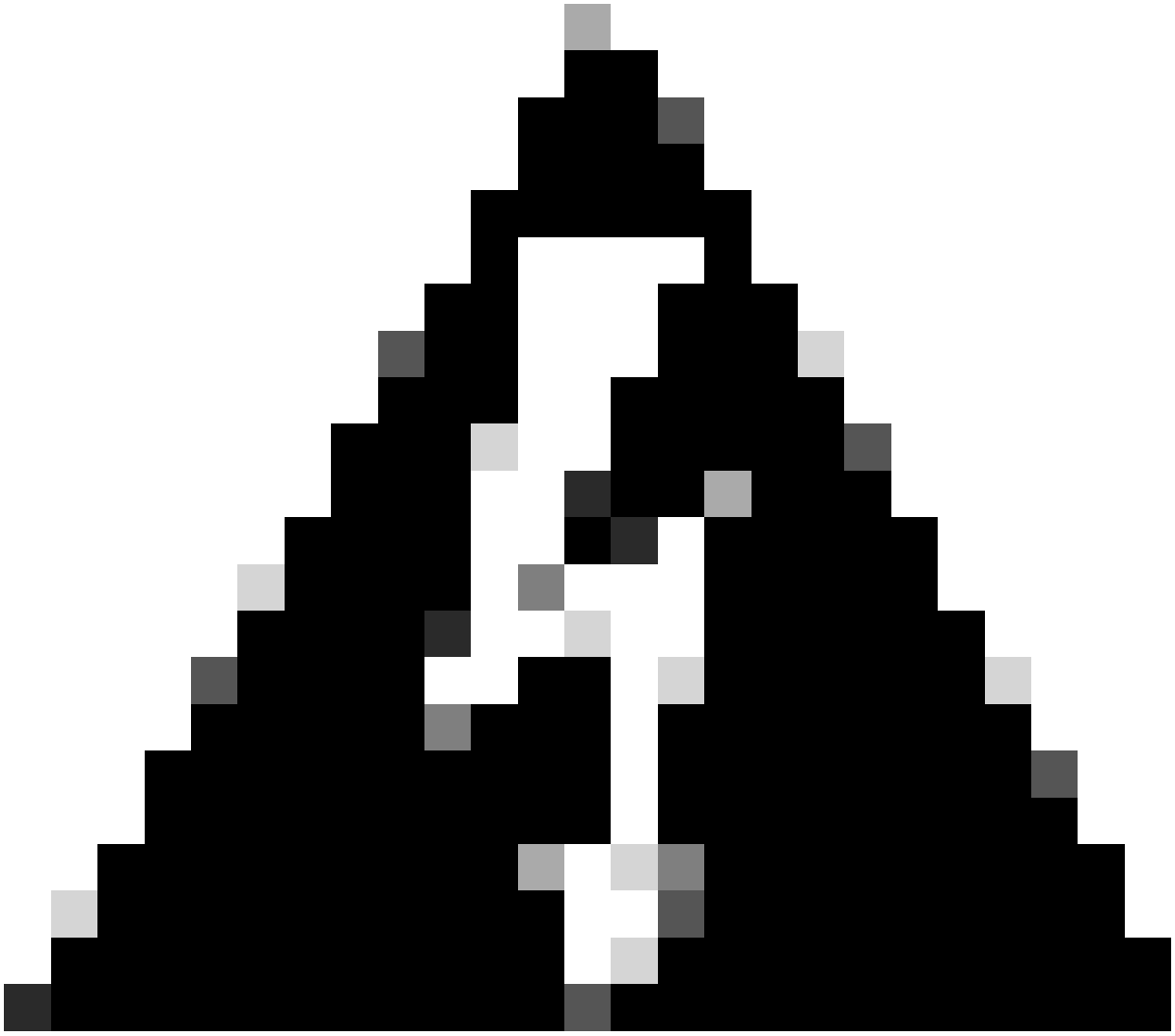
All'interno di un contesto LISP, il Piano di controllo del sito tiene traccia principalmente degli indirizzi MAC e delle corrispondenti associazioni da MAC a IP, analogamente alle voci ARP tradizionali. I pool L2 VNI/L2 Only sono progettati per facilitare la registrazione, la risoluzione e l'inoltro esclusivamente in base a questi due tipi di EID. Pertanto, qualsiasi inoltro basato su LISP in un ambiente L2-only si basa esclusivamente sulle informazioni MAC e MAC-to-IP, ignorando completamente gli EID IPv4 o IPv6. A complemento degli EID dei LISP, i pool solo L2 dipendono in modo significativo dai meccanismi di apprendimento e di gestione delle inondazioni, analogamente al comportamento degli switch tradizionali. Di conseguenza, L2 Flooding diventa un componente critico per la gestione del traffico broadcast, unicast sconosciuto e multicast (BUM) all'interno di questa soluzione, e richiede l'uso di Underlay Multicast. Al contrario, il normale traffico unicast viene inoltrato utilizzando processi di inoltro LISP standard, principalmente tramite Map-Caches.

Sia i bordi del fabric che il "bordo L2" (L2B) mantengono le VNI L2, che eseguono il mapping alle VLAN locali (questa mappatura è significativa per i dispositivi locali all'interno dell'SDA, consentendo a VLAN diverse di eseguire il mapping alla stessa VNI L2 sui nodi). In questo caso di utilizzo specifico, sulle VLAN non è configurata alcuna SVI in questi nodi, ossia non esiste una VNI L3 corrispondente.

Modifica del comportamento DHCP nelle VLAN solo L2

Nei pool di gateway Anycast, il DHCP rappresenta una sfida perché ogni Fabric Edge agisce come gateway per i suoi endpoint con connessione diretta, con lo stesso IP gateway in tutti i FE. Per identificare correttamente l'origine di un pacchetto DHCP inoltrato, i FE devono inserire l'opzione DHCP 82 e le relative opzioni secondarie, incluse le informazioni LISP RLOC. A tale scopo, lo snooping DHCP viene eseguito sulla VLAN client sul perimetro del fabric. Lo snooping DHCP ha un duplice scopo in questo contesto: facilita l'inserimento dell'opzione 82 e, aspetto cruciale, impedisce il flusso di pacchetti di trasmissione DHCP attraverso il dominio-ponte (VLAN/VNI). Anche quando il layer 2 Flooding è abilitato per un gateway Anycast, lo snooping DHCP elimina efficacemente il pacchetto di broadcast da inoltrare dal fabric Edge come broadcast.

Al contrario, una VLAN di solo layer 2 non dispone di un gateway, il che semplifica l'identificazione dell'origine DHCP. Poiché i pacchetti non vengono inoltrati da nessun spigolo di fabric, non sono necessari meccanismi complessi per l'identificazione dell'origine. Senza lo snooping DHCP sulla VLAN L2 Only, il meccanismo di controllo dell'inondazione per i pacchetti DHCP viene efficacemente ignorato. In questo modo, le trasmissioni DHCP possono essere inoltrate tramite Flooding L2 alla destinazione finale, ossia un server DHCP connesso direttamente a un nodo fabric o un dispositivo di livello 3 che fornisce la funzionalità di inoltro DHCP.



Avviso: La funzionalità "IP multiplo a MAC" all'interno di un pool L2 Only attiva automaticamente lo snooping DHCP in modalità Bridge VM, che impone il controllo di flood DHCP. Di conseguenza, il pool VNI L2 non sarà in grado di supportare DHCP per i relativi endpoint.

Multicast underlay

Dato che DHCP si basa fortemente sul traffico broadcast, il layer 2 del protocollo deve essere sfruttato per supportare questo protocollo. Come per qualsiasi altro pool L2 abilitato per il flooding, la rete sottostante deve essere configurata per il traffico multicast, in particolare per Any-Source-Multicast che utilizza PIM Sparse-Mode. mentre la configurazione multicast di base è automatizzata tramite il flusso di lavoro di automazione LAN, se questo passaggio è stato omesso, è necessaria una configurazione aggiuntiva (manuale o modello).

- Abilitare il routing multicast IP su tutti i nodi (bordi, bordi, nodi intermedi, ecc.).
- Configurare PIM Sparse-Mode sull'interfaccia Loopback0 di ciascun nodo Border and Edge.
- Abilitare PIM Sparse-Mode su ciascuna interfaccia IGP (underlay routing protocol).

- Configurare il PIM Rendezvous Point (RP) su tutti i nodi (Bordi, Bordi, Nodi intermedi); è consigliabile posizionare RP sui bordi.
- Verificare lo stato dei vicini PIM, PIM RP e del tunnel PIM.

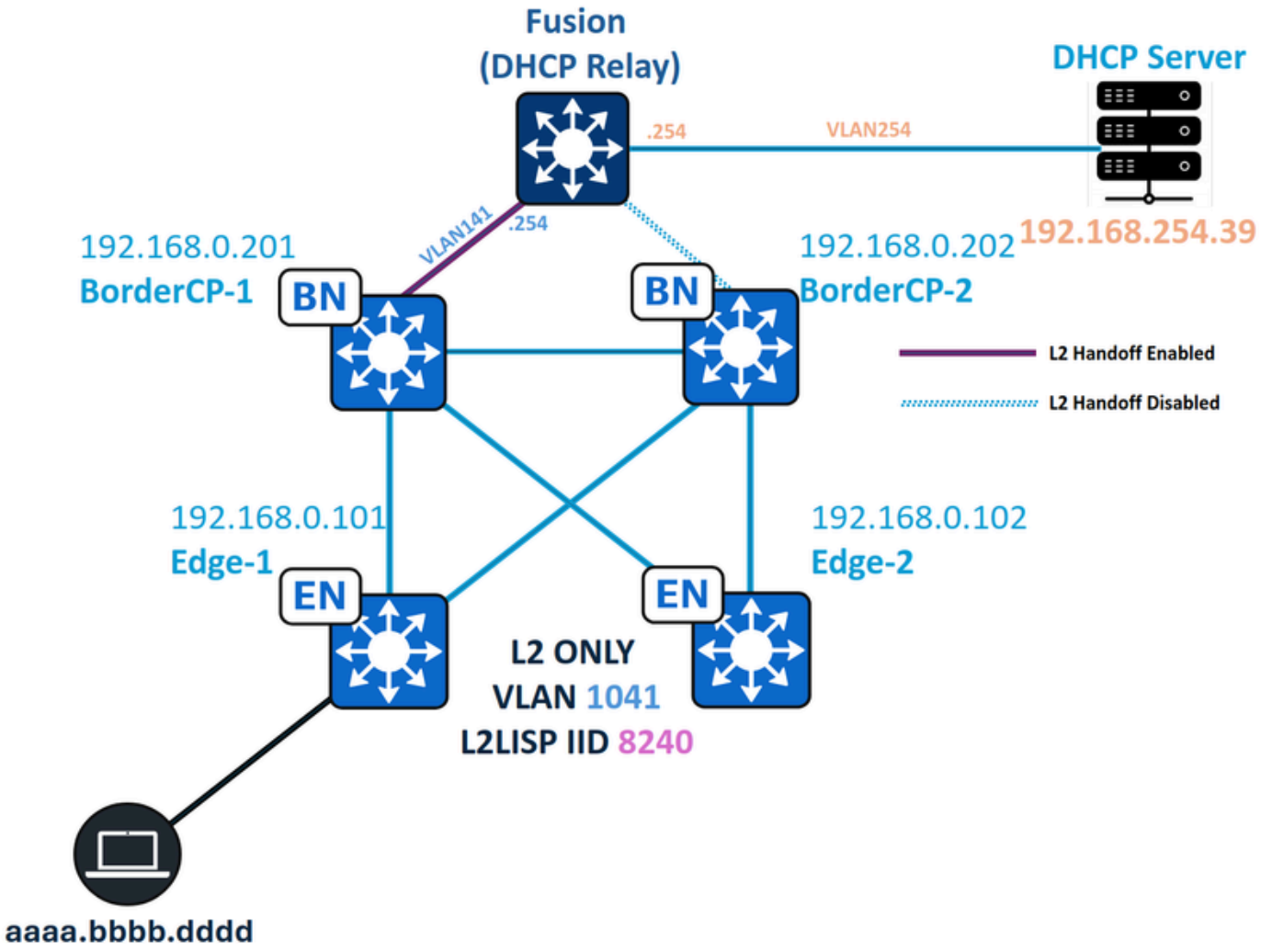
Server DHCP all'interno del fabric ad accesso SD

Una domanda di progettazione comune è se un server DHCP può essere distribuito all'interno di una struttura ad accesso SD. La risposta, in sostanza, è sia sì che no.

Il progetto ufficiale Cisco Validated consiglia di posizionare il server DHCP all'esterno dell'infrastruttura, in genere all'interno del blocco Shared Services. Tuttavia, se le circostanze richiedono il collegamento fisico del server DHCP a un nodo fabric (ad esempio, un bordo o un bordo), l'unico metodo supportato è tramite una rete L2 Only. Ciò è dovuto al comportamento intrinseco dei pool di Anycast Gateway, dove lo snooping DHCP è abilitato per impostazione predefinita. In questo modo, non solo si bloccano le offerte e le conferme DHCP provenienti dal server, ma si impedisce anche l'inoltro dei pacchetti DHCP Discover e Request, anche quando sono incapsulati nella VXLAN. Mentre lo "Snooping Trust DHCP" sulle porte del server DHCP consente offerte e conferme, i pacchetti Discover e Request non vengono inoltrati con lo stesso metodo. Inoltre, la rimozione dello snooping DHCP in un pool di gateway Anycast non è un'opzione supportata, in quanto Catalyst Center contrassegna una deviazione di configurazione di questo tipo durante la convalida della conformità.

Al contrario, quando il server DHCP viene posizionato all'interno di una rete L2 Only, lo snooping DHCP non viene applicato, consentendo il passaggio di tutti i pacchetti DHCP senza ispezione basata su criteri o blocco. Il dispositivo di rete a monte del fabric SD-Access (ad esempio, un router Fusion) è configurato come gateway per la rete L2 Only, consentendo al traffico proveniente da più VRF di accedere allo stesso server DHCP all'interno di tale segmento L2 Only.

Topologia



Topologia della rete

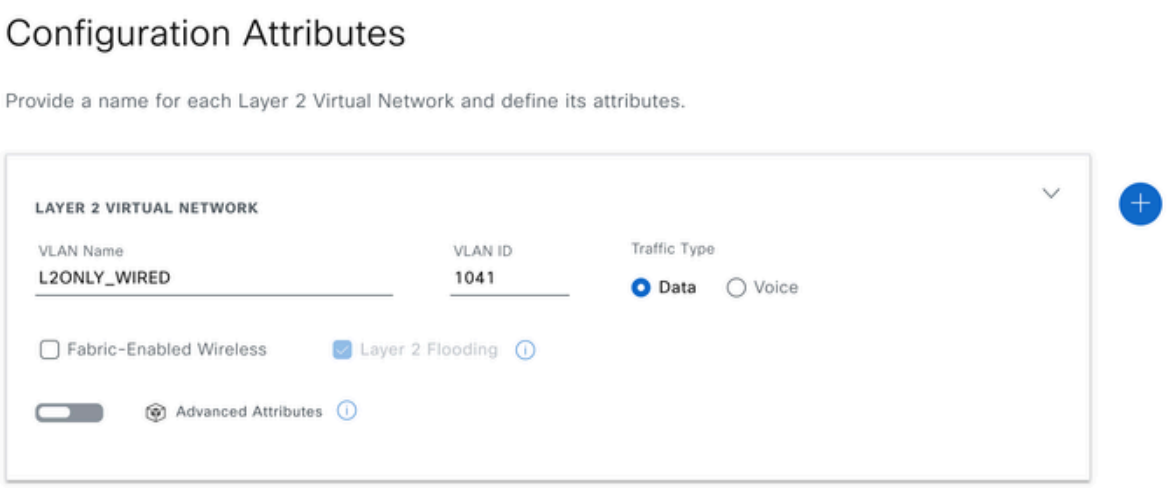
In questa topologia:

- 192.168.0.201 e 192.168.0.202 sono bordi rilocati per il sito fabric, BorderCP-1 è l'unico bordo con la funzione di handoff di layer 2 abilitata.
- 192.168.0.101 e 192.168.0.102 sono nodi Fabric Edge
- 192.168.254.39 è il server DHCP
- aaaa.bbbb.ddd è l'endpoint abilitato per DHCP
- Il dispositivo Fusion funge da inoltro DHCP per le subnet dell'infrastruttura.

Configurazione VLAN solo L2

Implementazione VLAN solo L2 da Catalyst Center

Percorso: Catalyst Center / Provisioning / Sito fabric / Reti virtuali di layer 2 / Modifica reti virtuali di layer 2



Configurazione L2VNI

Configurazione VLAN solo L2 - Spigoli fabric

Sui nodi Fabric Edge la VLAN è configurata con CTS abilitato, IGMP e MLD IPv6 disabilitati e la configurazione LISP L2 richiesta. Questo pool L2 Only non è un pool wireless; pertanto, le funzionalità tipiche dei pool wireless L2 Only, ad esempio RA-Guard, DHCPGuard e Flood Access Tunnel, non sono configurate. Al contrario, il flooding dei pacchetti ARP è esplicitamente abilitato con "flood arp-end"

Configurazione di Fabric Edge (192.168.0.101)

<#root>

```
cts role-based enforcement vlan-list
1041


vlan
1041


name L2ONLY_WIRED


no ip igmp snooping vlan 1041 querier


no ip igmp snooping vlan 1041


no ipv6 mld snooping vlan 1041
```

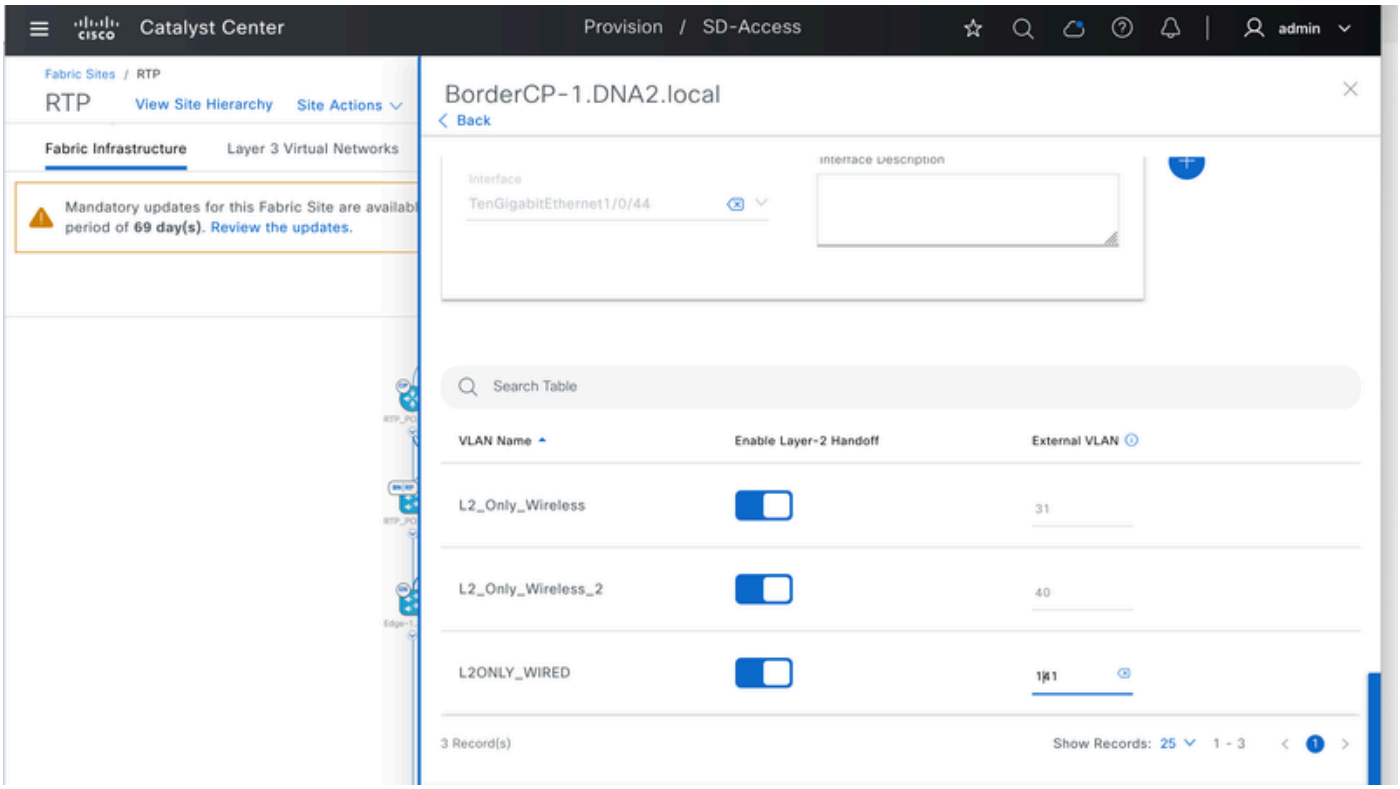
```
router lisp
 instance-id
8240
  remote-rloc-probe on-route-change
  service ethernet
eid-table vlan
1041
   broadcast-underlay
239.0.17.1
flood arp-nd
 flood unknown-unicast
   database-mapping mac locator-set rloc_91947dad-3621-42bd-ab6b-379ecebb5a2b
   exit-service-ethernet
```

Configurazione handoff L2 - Bordo fabric

Da una prospettiva operativa, il server DHCP (o router/relay) può essere connesso a qualsiasi nodo fabric, inclusi i bordi e i bordi.

L'utilizzo di nodi di bordo per connettere il server DHCP è l'approccio consigliato, ma richiede un'attenta valutazione a livello di progettazione. Infatti, il bordo deve essere configurato per l'handoff L2 per singola interfaccia. In questo modo, il pool di infrastrutture può essere consegnato alla stessa VLAN in cui si trova il fabric o a una VLAN diversa. Questa flessibilità negli ID VLAN tra i bordi dell'infrastruttura e i bordi è possibile perché entrambi sono mappati allo stesso Instance-ID L2 LISP. Per evitare loop di layer 2 nella rete di accesso SD, le porte fisiche lato L2 non devono essere abilitate contemporaneamente alla stessa VLAN. Per la ridondanza, sono necessari metodi quali gli script StackWise Virtual, FlexLink+ o EEM.

Al contrario, la connessione del server DHCP o del router gateway a un Fabric Edge non richiede alcuna configurazione aggiuntiva.



Configurazione handoff L2

Configurazione del bordo del fabric (192.168.0.201)

<#root>

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

141

```
vlan
```

141

name L2ONLY_WIRED

no ip igmp snooping vlan 141 querier

no ip igmp snooping vlan 141

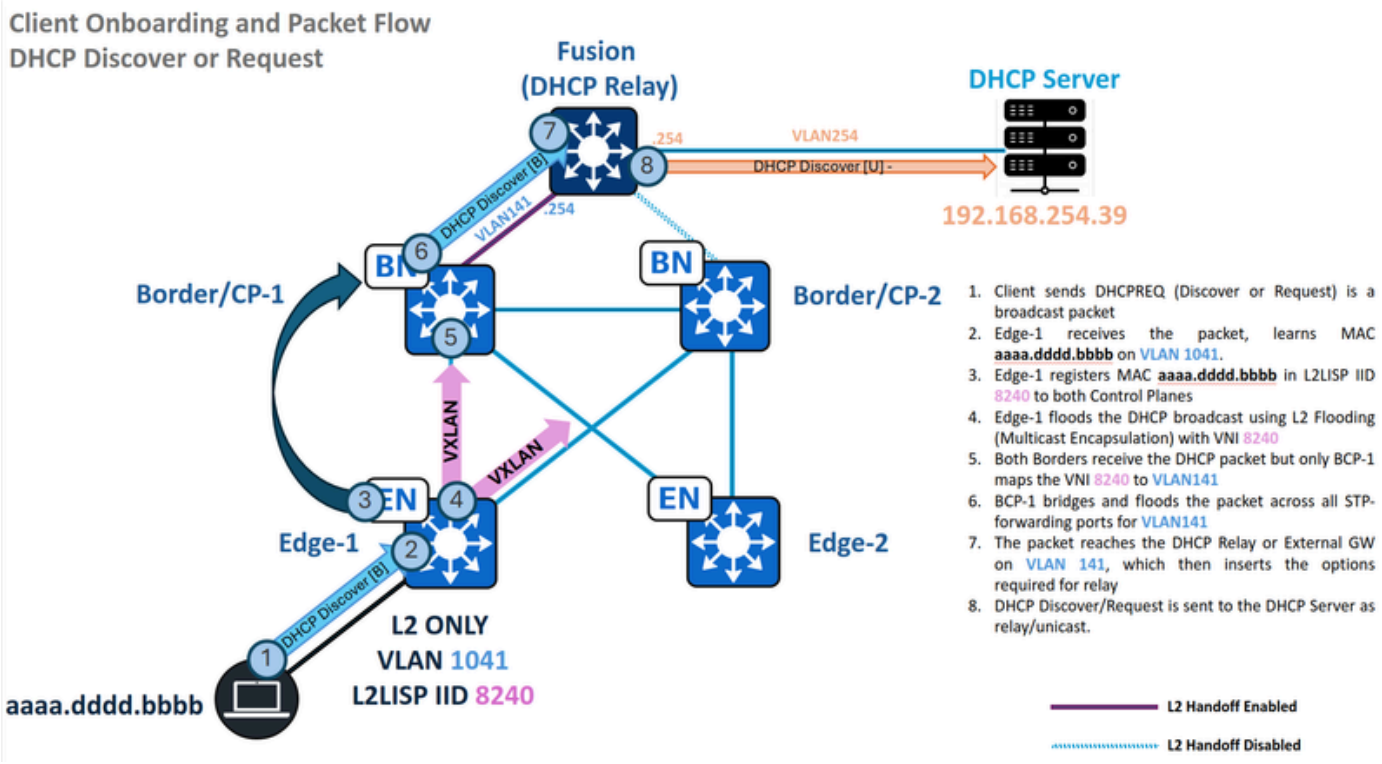
no ipv6 mld snooping vlan 141

```
router lisp
 instance-id
```

```
8240

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

eid-table


vlan 141



 broadcast-underlay 239.0.17.1


   flood arp-nd


   flood unknown-unicast


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

interface TenGigabitEthernet1/0/44


  switchport mode trunk
```

Flusso traffico DHCP

Rilevamento e richiesta DHCP - Edge



Flusso di traffico - Rilevamento DHCP e richiesta solo in L2

Apprendimento degli indirizzi MAC e registrazione degli endpoint

Quando l'endpoint aaaa.ddd.bbbb invia una richiesta o un'individuazione DHCP (un pacchetto di trasmissione), il nodo Edge deve conoscere l'indirizzo MAC dell'endpoint, aggiungerlo alla relativa tabella degli indirizzi MAC, quindi alla tabella L2/MAC SISF e infine al database L2LISP per la VLAN 1041, mappato all'istanza L2LISP 8240.

<#root>

Edge-1#

show mac address-table interface te1/0/2

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

1041

aaaa.dddd.bbbb

DYNAMIC

Te1/0/2

Edge-1#

show vlan id 1041

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

1041 L2ONLY_WIRED



active

    L2LI0:

8240

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

Edge-1#

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


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

Edge-1#

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


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

8240



aaaa.dddd.bbbb

   N/A           6d04h     never

0



Edge-1#

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


LISP ETR MAC Mapping Database for LISP 0 EID-table

Vlan 1041 (IID 8240)

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

aaaa.dddd.bbbb/48

,

dynamic-eid Auto-L2-group-8240

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

 192.168.0.101
```

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

  192.168.0.201

  6d04h

Yes

  0

  192.168.0.202

 6d04h

Yes

  0
```

Se l'indirizzo MAC dell'endpoint è stato appreso correttamente e il flag ACK è stato contrassegnato come "Yes" (Sì) per i piani di controllo dell'infrastruttura, questa fase viene considerata completata.

Trasmissione DHCP con bridging L2

Quando lo snooping DHCP è disabilitato, i broadcast DHCP non vengono bloccati; al contrario, sono incapsulati in multicast per il layer 2 Flooding. Al contrario, abilitando lo snooping DHCP si impedisce il flooding di questi pacchetti di broadcast.

<#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>
```

Poiché lo snooping DHCP è disabilitato, il comando DHCP Discover/Request utilizza l'interfaccia L2LISP0, creando un bridging del traffico tramite L2 Flooding. A seconda della versione di Catalyst Center e dei banner fabric applicati, l'interfaccia L2LISP0 può avere elenchi degli accessi configurati in entrambe le direzioni; pertanto, verificare che il traffico DHCP (porte UDP 67 e 68) non venga negato esplicitamente da alcuna voce di controllo di accesso (ACE, Access Control Entries).

<#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

Utilizzare il gruppo broadcast-underlay configurato per l'istanza L2LISP e l'indirizzo IP Loopback0 del server perimetrale dell'infrastruttura per verificare la voce L2 Flooding (S,G) che collega questo pacchetto ad altri nodi dell'infrastruttura. Consultare le tabelle mroute e mfib per convalidare parametri quali l'interfaccia in ingresso, l'elenco delle interfacce in uscita e i contatori di inoltro.

<#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:

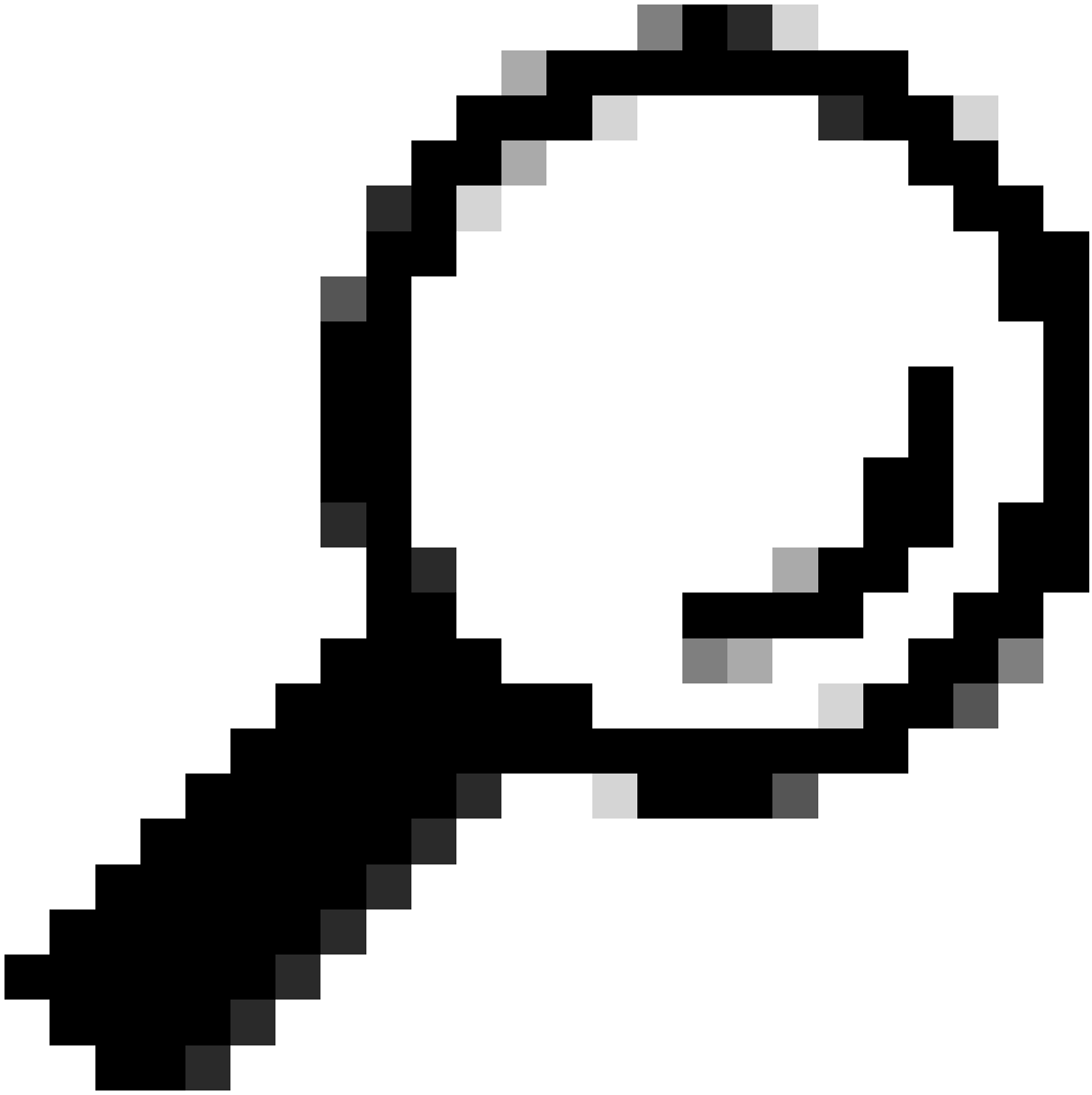
7

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

<--

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

Totals - Source count: 1, Packet count: 8



Suggerimento: Se non viene trovata una voce (S,G) o l'elenco delle interfacce in uscita (OIL) non contiene interfacce in uscita (OIF), indica un problema con la configurazione o l'operazione multicast sottostante.

Acquisizioni pacchetti

Configurare un'acquisizione simultanea di pacchetti incorporati sullo switch per registrare sia il pacchetto DHCP in ingresso dall'endpoint che il pacchetto in uscita corrispondente per L2 Flooding. Durante l'acquisizione del pacchetto, è necessario osservare due pacchetti distinti: la richiesta/individuazione DHCP originale e la controparte incapsulata VXLAN, destinata al gruppo Underlay (239.0.17.1).

Acquisizione pacchetti Fabric Edge (192.168.0.101)

<#root>

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

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

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

Edge-1#

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

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

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

356 DHCP Discover

 - Transaction ID 0xf8e

<--

356 is the Length of the original packet

   23   2.487037   0.0.0.0 -> 255.255.255.255 DHCP

406 DHCP Discover

 - Transaction ID 0xf8e

<--

406 is the Length of the VXLAN encapsulated packet

Edge-1#

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

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

406 DHCP Discover

 - Transaction ID 0xf8e

Edge-1#

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

```
Internet Protocol Version 4, Src:
192.168.0.101, Dst: 239.0.17.1  <-- DHCP Discover is encapsulated for Layer 2 Flooding

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

Rilevamento e richiesta DHCP - Bordo L2

Dopo che il server Edge ha inviato i pacchetti DHCP Discover e Request tramite Flooding di layer 2, incapsulati con il gruppo Broadcast-Underlay 239.0.17.1, questi pacchetti vengono ricevuti dal Border L2 handoff, in particolare dal Border/CP-1 in questo scenario.

A tal fine, Border/CP-1 deve possedere una route multicast con il router (S,G) del perimetro e il relativo elenco di interfacce in uscita deve includere l'istanza L2LISP della VLAN dell'handoff L2. È importante notare che i bordi handoff L2 condividono lo stesso Instance-ID L2LISP, anche se utilizzano VLAN diverse per lo handoff.

```
<#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

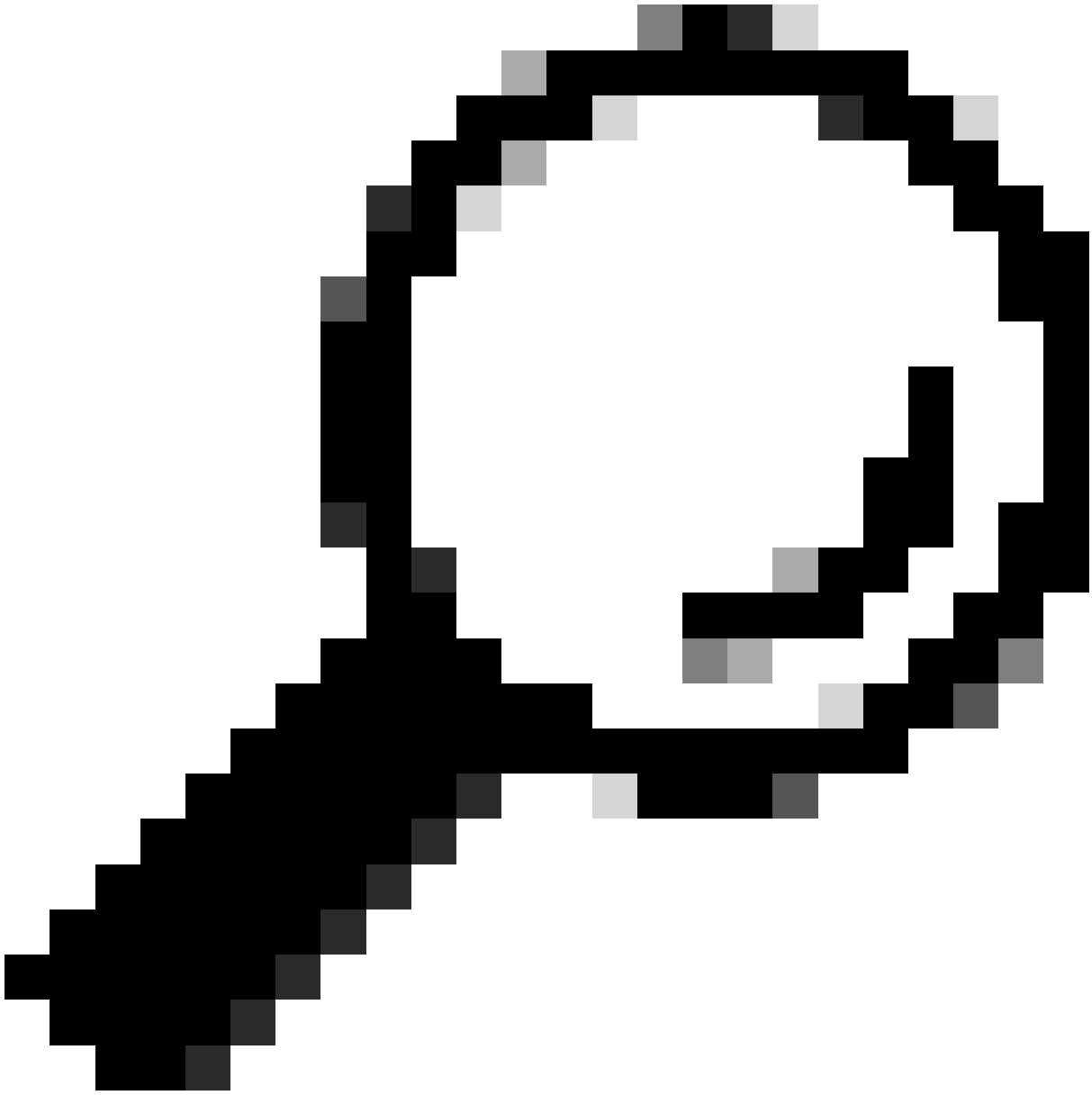
,
   SW Forwarding: 1/0/392/0, Other: 0/0/0
   HW Forwarding:

3

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

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

  Totals - Source count: 1, Packet count: 4



Suggerimento: Se non viene trovata una voce (S,G), indica un problema con la configurazione o l'operazione multicast sottostante. Se l'opzione L2LISP per l'istanza richiesta non è presente come OIF, indica un problema con lo stato operazione SU/GIÙ della sottointerfaccia L2LISP o lo stato abilitazione IGMP dell'interfaccia L2LISP.

Analogamente al nodo Fabric Edge, verificare che nessuna voce di controllo dell'accesso neghi il pacchetto DHCP incorporato sull'interfaccia L2LISP0.

<#root>

```
BorderCP-1#
```

show access-list SDA-FABRIC-LISP

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

40 permit ip any any
```

Dopo aver decapsulato il pacchetto e averlo inserito sulla VLAN corrispondente allo VNI 8240, per natura del broadcast il pacchetto viene inviato a tutte le porte di inoltro dello Spanning Tree Protocol per la VLAN 141 handoff.

<#root>

```
BorderCP-1#

show spanning-tree vlan 141 | be Interface

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

Te1/0/44

          Desg

FWD

 2000      128.56   P2p
```

La tabella Device-Tracking conferma che l'interfaccia Te1/0/44, che si connette al gateway/inoltro DHCP, deve essere una porta di inoltro STP.

<#root>

```
BorderCP-1#

show device-tracking database address 172.16.141.254 | be Network

   Network Layer Address                  Link Layer Address     Interface  vlan       prlvl      age
ARP

172.16.141.254

f87b.2003.7fc0

Te1/0/44

 141
```

```
       0005       133s       REACHABLE  112 s try 0
```

Acquisizioni pacchetti

Configurare un'acquisizione simultanea di pacchetti incorporata sullo switch per registrare sia il pacchetto DHCP in arrivo da L2 Flooding (interfaccia S,G in entrata) che il pacchetto in uscita corrispondente sul relay DHCP. Durante l'acquisizione del pacchetto, è necessario osservare due pacchetti distinti: il pacchetto incapsulato VXLAN dal perimetro 1 e il pacchetto decapsulato che va al relay DHCP.

Fabric Border/CP (192.168.0.201) cattura pacchetti

<#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

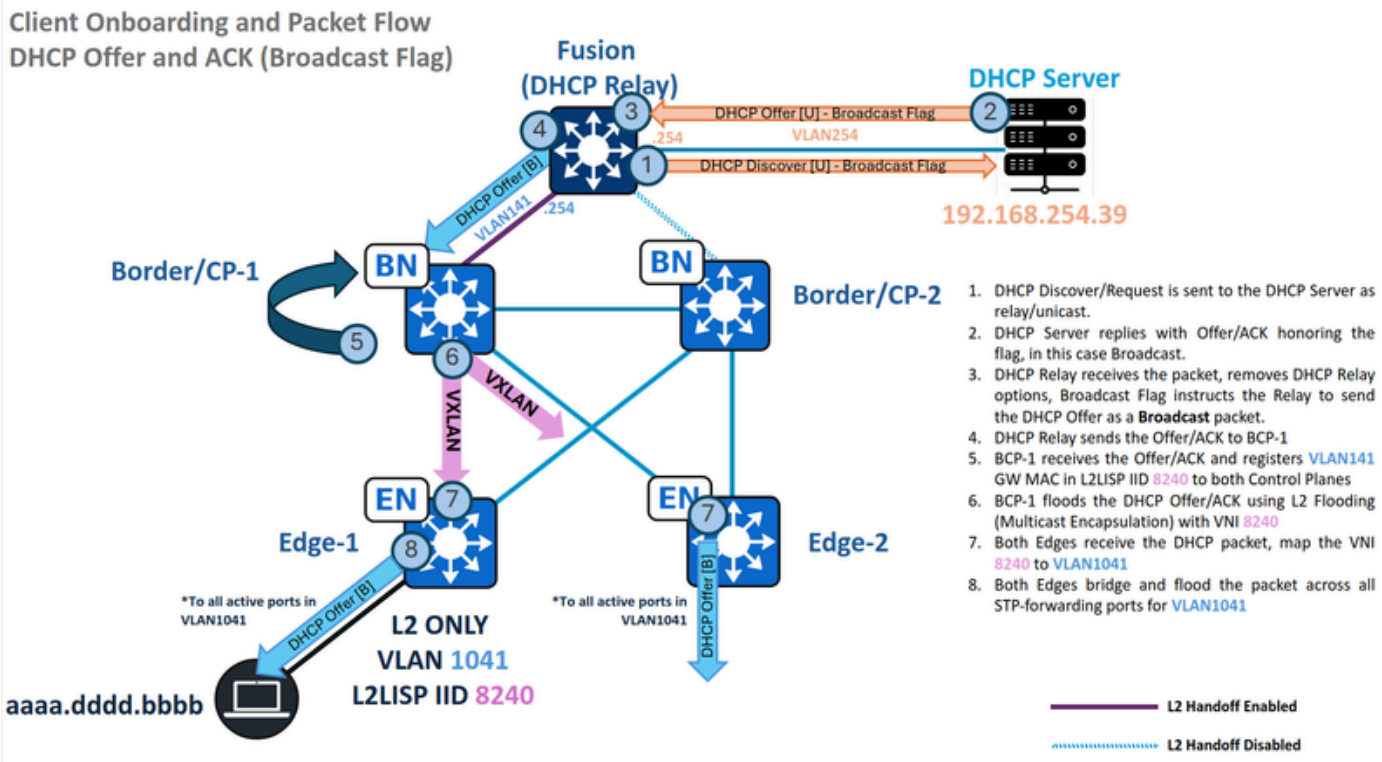
Packet 428: Plain (dot1Q cannot be captured at egress direction)

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

Offerta e ACK DHCP - Broadcast - Bordo L2



Flusso del traffico - Offerta DHCP broadcast e ACK solo in L2

Ora che il comando DHCP Discover ha chiuso il fabric SD-Access, il relay DHCP inserisce le opzioni di inoltro DHCP tradizionali (ad esempio GiAddr/GatewayIPAddress) e inoltra il pacchetto come trasmissione unicast al server DHCP. In questo flusso, il fabric SD-Access non aggiunge opzioni DHCP speciali.

All'arrivo di una richiesta di individuazione/individuazione DHCP al server, il server rispetta il flag Broadcast o Unicast incorporato. Questo flag determina se l'agente di inoltro DHCP inoltra l'offerta DHCP al dispositivo a valle (i nostri bordi) come frame broadcast o unicast. Per questa dimostrazione, si presuppone uno scenario di trasmissione.

Apprendimento degli indirizzi MAC e registrazione dei gateway

Quando il relay DHCP invia un'offerta DHCP o un ACK, il nodo L2BN deve conoscere l'indirizzo MAC del gateway, aggiungerlo alla relativa tabella degli indirizzi MAC, quindi alla tabella L2/MAC SISF e infine al database L2LISP per la VLAN 141, mappato all'istanza L2LISP 8240.

<#root>

BorderCP-1#

show mac address-table interface te1/0/44

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

141

f87b.2003.7fc0

    DYNAMIC

Te1/0/44
```

BorderCP-1#

show vlan id 141

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

141

L2ONLY_WIRED

               active    L2LI0:
```

8240

,

Te1/0/44

BorderCP-1#

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

MAC Interface vlan prlvl state Time left Policy

f87b.2003.7fc0

Te1/0/44 141

NO TRUST

MAC-REACHABLE

61 s LISP-DT-GLEAN-VLAN 64

BorderCP-1#

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

Dyn-EID Name Dynamic-EID Interface Uptime Last Pending

Auto-L2-group-8240

f87b.2003.7fc0

N/A 6d06h never

0

BorderCP-1#

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

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

141

(IID

8240

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

f87b.2003.7fc0/48

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

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


 192.168.0.201

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


192.168.0.201

 6d06h

Yes

  0


192.168.0.202

  6d06h

Yes

  0
```

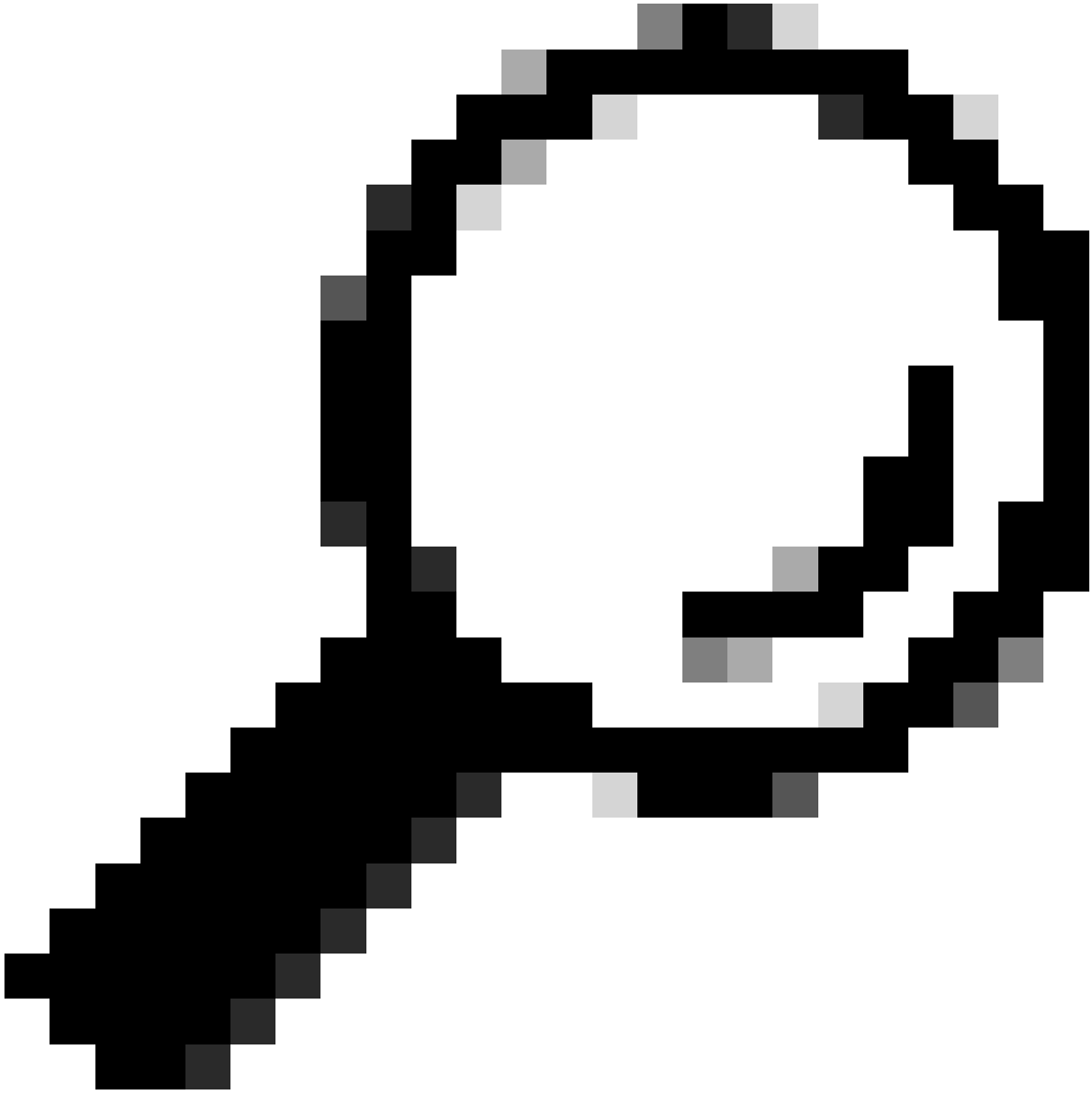
Se l'indirizzo MAC del gateway è stato appreso correttamente e il flag ACK è stato contrassegnato come "Yes" (Sì) per i piani di controllo dell'infrastruttura, questa fase viene considerata completata.

Trasmissione DHCP con bridging L2

Senza lo snooping DHCP abilitato, i broadcast DHCP non vengono bloccati e vengono incapsulati in multicast per il layer 2 Flooding. Al contrario, se lo snooping DHCP è abilitato, il flusso dei pacchetti broadcast DHCP viene impedito.

<#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
```



Suggerimento: Poiché lo snooping DHCP non è abilitato in L2Border, la configurazione del trust dello snooping DHCP non è necessaria.

In questa fase, la convalida dell'ACL L2LISP è già stata eseguita su entrambi i dispositivi.

Utilizzare il gruppo broadcast-underlay configurato per l'istanza L2LISP e l'indirizzo IP L2Border Loopback0 per verificare la voce L2 Flooding (S,G) che collega questo pacchetto ad altri nodi fabric. Consultare le tabelle mroute e mfib per convalidare parametri quali l'interfaccia in ingresso, l'elenco delle interfacce in uscita e i contatori di inoltro.

<#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

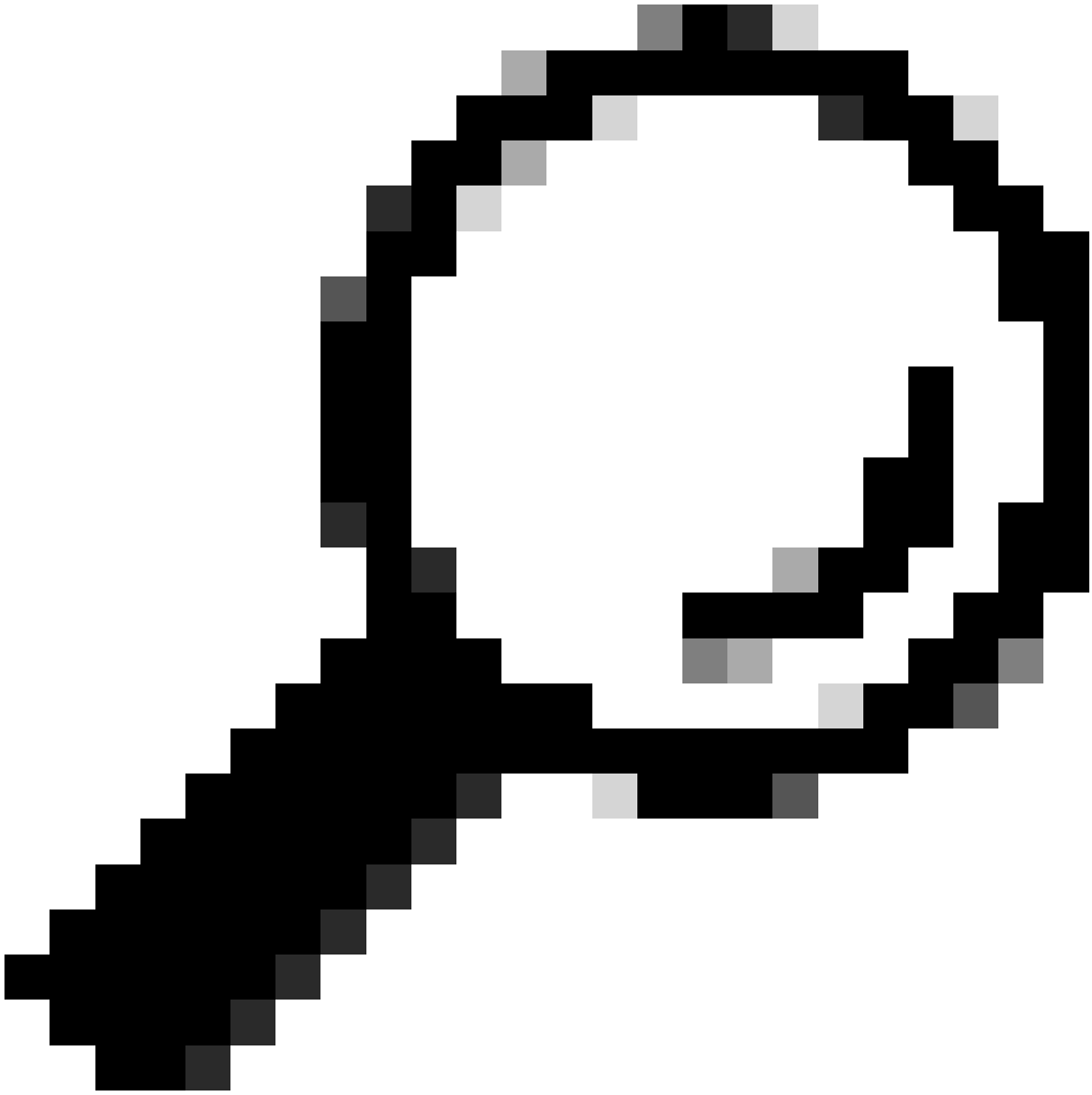
,
   SW Forwarding: 1/0/392/0, Other: 1/1/0
   HW Forwarding:

  92071

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

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

  Totals - Source count: 1, Packet count: 92071



Suggerimento: Se non viene trovata una voce (S,G) o l'elenco delle interfacce in uscita (OIL) non contiene interfacce in uscita (OIF), indica un problema con la configurazione o l'operazione multicast sottostante.

Con queste convalide, insieme alle acquisizioni dei pacchetti simili ai passaggi precedenti, questa sezione si conclude, poiché l'offerta DHCP viene inoltrata come trasmissione a tutti i Fabric Edge che usano il contenuto dell'elenco di interfacce in uscita, in questo caso fuori dall'interfaccia TenGig1/0/42 e TenGig1/0/43.

Offerta DHCP e ACK - Broadcast - Edge

Esattamente come il flusso precedente, verificare il valore L2Border S,G nel Fabric Edge, dove l'interfaccia in entrata punta verso L2BN e il valore OIL contiene l'istanza L2LISP mappata alla VLAN 1041.

<#root>

Edge-1#

show vlan id 1041

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

1041

L2ONLY_WIRED

active

    L2LIO:

8240

,

Te1/0/2

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

Edge-1#

show ip mroute 239.0.17.1 192.168.0.201 | be \(

(

192.168.0.201

,

239.0.17.1

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

TenGigabitEthernet1/1/2

, RPF nbr 192.168.98.2

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

  Outgoing interface list:

L2LISP0.8240,

Forward/Sparse-Dense

,

 1w3d/00:02:23, flags:

Edge-1#

show ip mfib 239.0.17.1 192.168.0.201 count

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

239.0.17.1

  Source:

192.168.0.201,

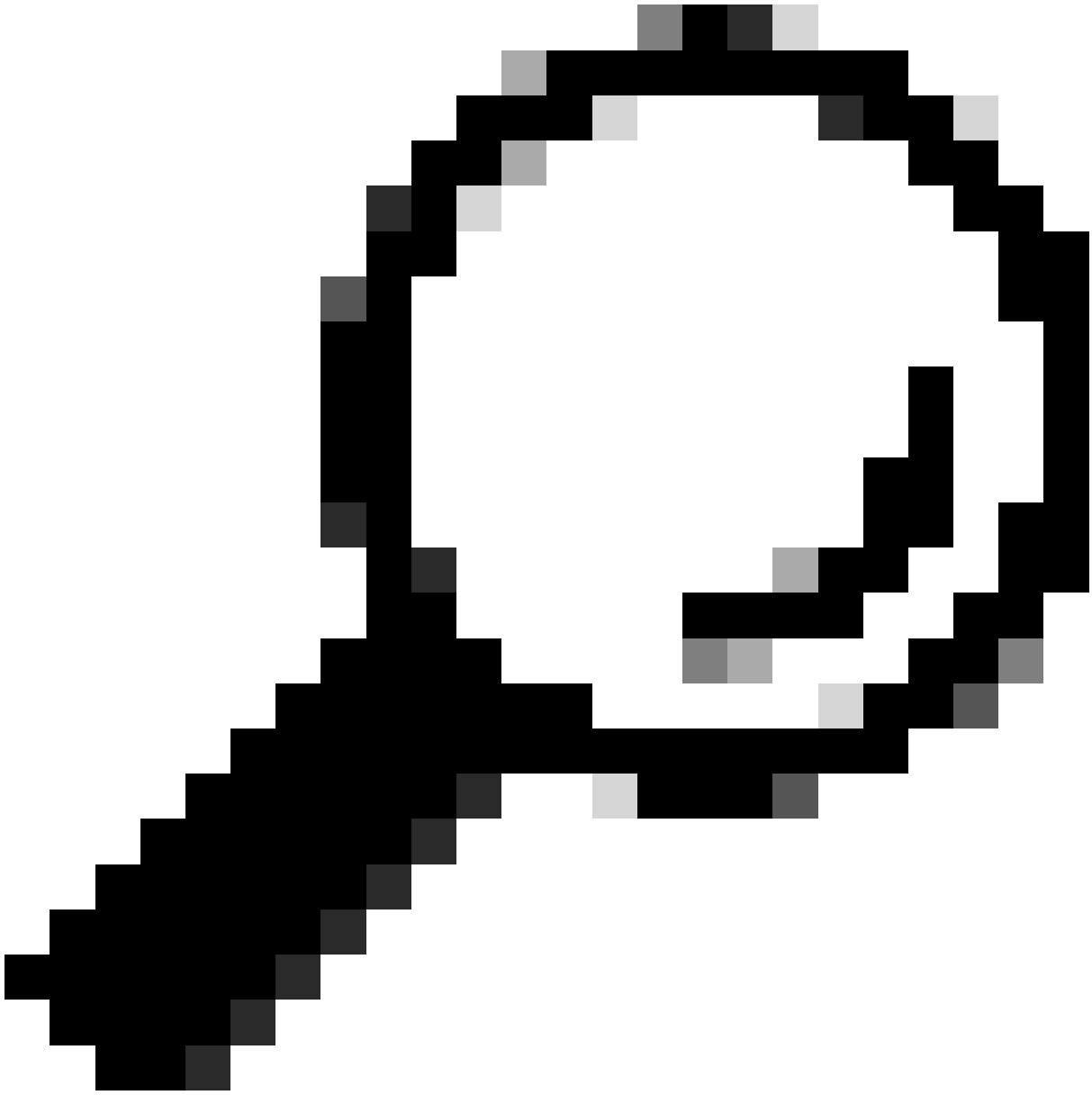
   SW Forwarding: 1/0/96/0, Other: 0/0/0
   HW Forwarding:

76236

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

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

  Totals - Source count: 1, Packet count: 4



Suggerimento: Se non viene trovata una voce (S,G), indica un problema con la configurazione o l'operazione multicast sottostante. Se l'opzione L2LISP per l'istanza richiesta non è presente come OIF, indica un problema con lo stato operazione SU/GIÙ della sottointerfaccia L2LISP o lo stato abilitazione IGMP dell'interfaccia L2LISP.

La convalida dell'ACL L2LISP è già stata eseguita su entrambi i dispositivi.

Dopo aver decapsulato il pacchetto e averlo inserito sulla VLAN corrispondente allo VNI 8240, per natura del broadcast il pacchetto viene inviato a tutte le porte di inoltro dello Spanning Tree Protocol per la VLAN 1041.

<#root>

```
Edge-1#
```

show spanning-tree vlan 1041 | be Interface

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

Te1/0/2

```
         Desg
```

FWD

```
 20000     128.2    P2p Edge
Te1/0/17            Desg
```

FWD

```
 2000      128.17   P2p
Te1/0/18            Back
```

BLK

```
 2000      128.18   P2p
Te1/0/19            Desg
```

FWD

```
 2000      128.19   P2p
Te1/0/20            Back
```

BLK

```
 2000      128.20   P2p
```

La tabella degli indirizzi MAC identifica la porta Te1/0/2 come porta dell'endpoint, che è in stato FWD da STP, il pacchetto viene inviato all'endpoint.

<#root>

Edge-1#

show mac address-table interface te1/0/2

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

1041

aaaa.dddd.bbbb

```
    DYNAMIC
```

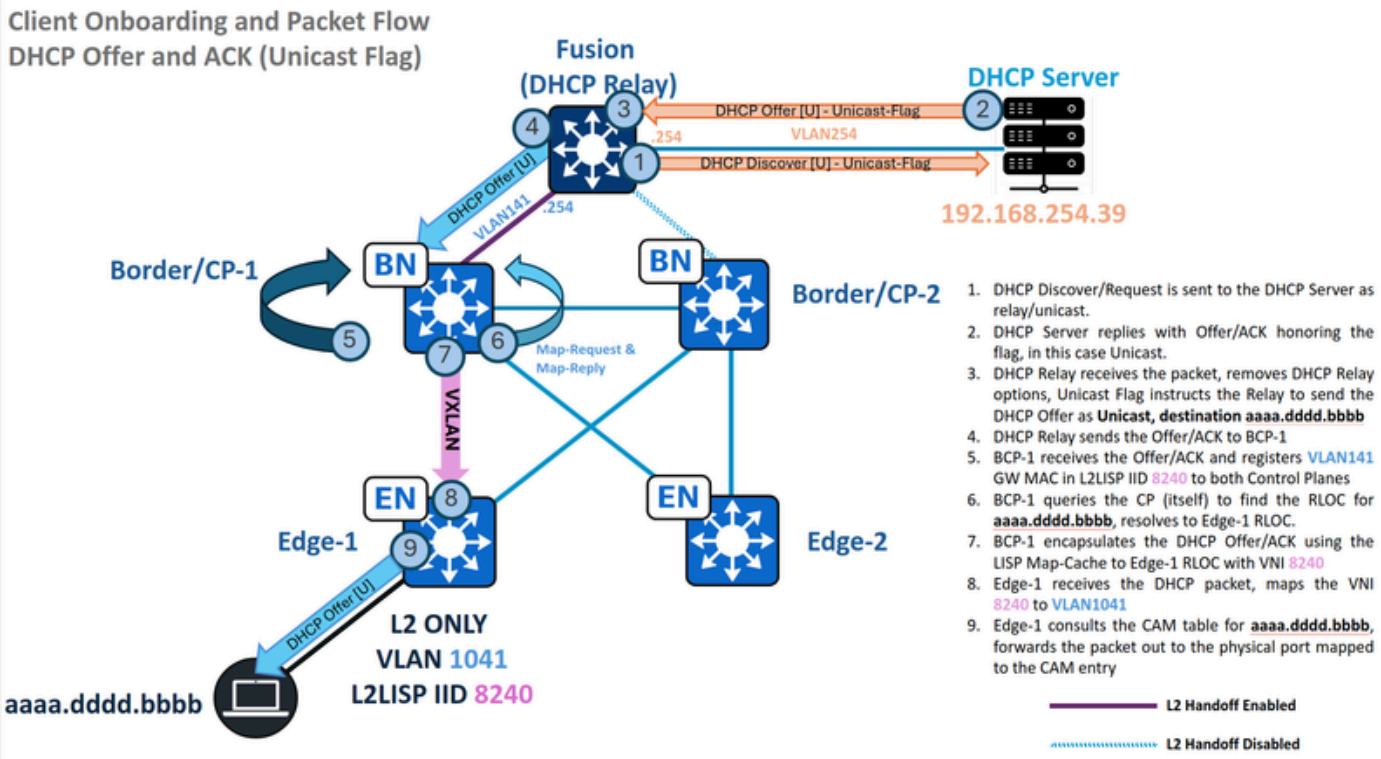
Te1/0/2

Il processo di offerta e ACK DHCP rimane coerente. Se lo snooping DHCP non è abilitato, nella tabella Snooping DHCP non verrà creata alcuna voce. Di conseguenza, la voce Device Tracking per l'endpoint abilitato per DHCP viene generata dalla pulitura dei pacchetti ARP. Si prevede inoltre che comandi quali "show platform dhcpsnooping client status" non visualizzino dati, poiché lo snooping DHCP è disabilitato.

<#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
```

Offerta e ACK DHCP - Unicast - Bordo L2



Flusso del traffico - Offerta DHCP unicast e ACK solo in L2

In questo caso, lo scenario è leggermente diverso e l'endpoint imposta il flag di trasmissione DHCP su unset o "0".

L'inoltro DHCP non invia l'offerta/ACK DHCP come broadcast, ma come pacchetto unicast, con un indirizzo MAC di destinazione derivato dall'indirizzo hardware del client all'interno del payload DHCP. Questo modifica drasticamente il modo in cui il pacchetto viene gestito dalla struttura SD-Access, utilizza la Map-Cache L2LISP per inoltrare il traffico, non il metodo di incapsulamento multicast Layer 2 Flooding.

Fabric Border/CP (192.168.0.201) acquisizione pacchetti: Offerta DHCP in ingresso

<#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)
```

In questo scenario, L2 Flooding viene utilizzato esclusivamente per le operazioni di individuazione/richiesta, mentre le offerte/ACK vengono inoltrate tramite le cache di mapping L2LISP, semplificando il funzionamento complessivo. In base ai principi di inoltro unicast, il bordo L2 esegue una query sul piano di controllo per l'indirizzo MAC di destinazione (aaaa.ddd.bbb). Presupponendo che "MAC Learning and Endpoint Registration" sia riuscito sul perimetro della struttura, il Control Plane ha registrato questo ID endpoint (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
```

Dopo la query di Border sul Control Plane (locale o remoto), la risoluzione LISP stabilisce una voce Map-Cache per l'indirizzo MAC dell'endpoint.

```
<#root>

BorderCP-1#

show lisp instance-id 8240 ethernet map-cache aaaa.dddd.bbbb


LISP MAC Mapping Cache for LISP 0 EID-table Vlan

141

 (IID

8240

), 1 entries


aaaa.dddd.bbbb/48

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

via map-reply

,

complete

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

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

Con il RLOC risolto, l'offerta DHCP viene incapsulata in unicast e inviata direttamente al perimetro 1 a 192.168.0.101, utilizzando il VNI 8240.

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

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

141

 aaaa.dddd.bbbb

CP_LEARN

L2LI0

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

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

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

Routing entry for 192.168.0.101/32
```

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


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

Con la stessa metodologia delle sezioni precedenti, acquisire il traffico in entrata sia dal relay DHCP sia verso l'interfaccia di uscita RLOC per osservare l'incapsulamento VXLAN in modalità unicast al edge RLOC.

Offerta e ACK DHCP - Unicast - Edge

Il perimetro riceve l'offerta DHCP/ACK unicast dal bordo, incapsula il traffico e consulta la relativa tabella degli indirizzi MAC per determinare la porta di uscita corretta. A differenza delle offerte broadcast/ACK, il nodo Edge inoltra il pacchetto solo alla porta specifica a cui è connesso l'endpoint, anziché inviarlo a tutte le porte.

La tabella degli indirizzi MAC identifica la porta Te1/0/2 come porta client, che è in stato FWD da STP, il pacchetto viene inoltrato all'endpoint.

```
<#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
```

Il processo di offerta e ACK DHCP rimane coerente. Se lo snooping DHCP non è abilitato, nella

tabella Snooping DHCP non verrà creata alcuna voce. Di conseguenza, la voce Device Tracking per l'endpoint abilitato per DHCP viene generata dai pacchetti ARP puliti. Si prevede inoltre che comandi quali "show platform dhcpsnooping client status" non visualizzino dati, poiché lo snooping DHCP è disabilitato.

<#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

È importante notare che il fabric SD-Access non influenza l'uso del flag Unicast o Broadcast, in quanto si tratta solo di un comportamento dell'endpoint. Anche se questa funzionalità può essere ignorata dall'inoltro DHCP o dal server DHCP stesso, entrambi i meccanismi sono essenziali per il funzionamento ininterrotto di DHCP in un ambiente L2 Only: Inondazione L2 con multicast inferiore per offerte/ACK broadcast e corretta registrazione dell'endpoint nel Control Plane per offerte/ACK unicast.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).