Risoluzione dei problemi relativi al DHCP nella VLAN di solo layer 2 - Wireless

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi a DHCP per endpoint wireless 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
- Wireless abilitato per fabric

Requisiti hardware e software

- Switch Catalyst serie 9000
- Catalyst Center versione 2.3.7.9
- Catalyst serie 9800 wireless LAN Controller
- Access point Catalyst serie 9100
- 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

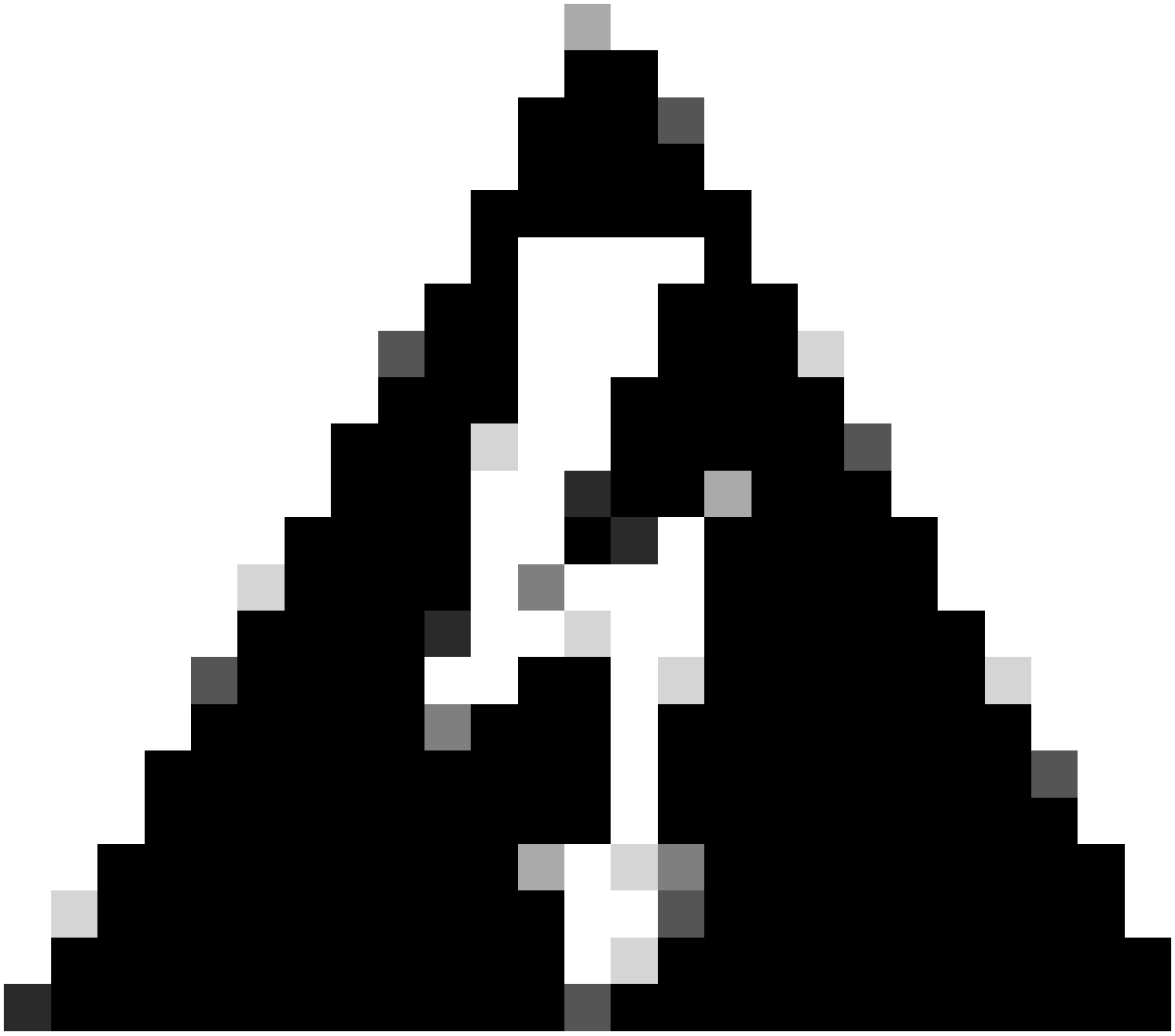
l'inoltro esclusivamente in base a questi due tipi di EID. Pertanto, qualsiasi inoltro basato su LISP in un ambiente L2-only si basa esclusivamente sulle informazioni MAC e MAC-to-IP, ignorando completamente gli EID IPv4 o IPv6. A complemento degli EID dei LISP, i pool solo L2 dipendono in modo significativo 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).

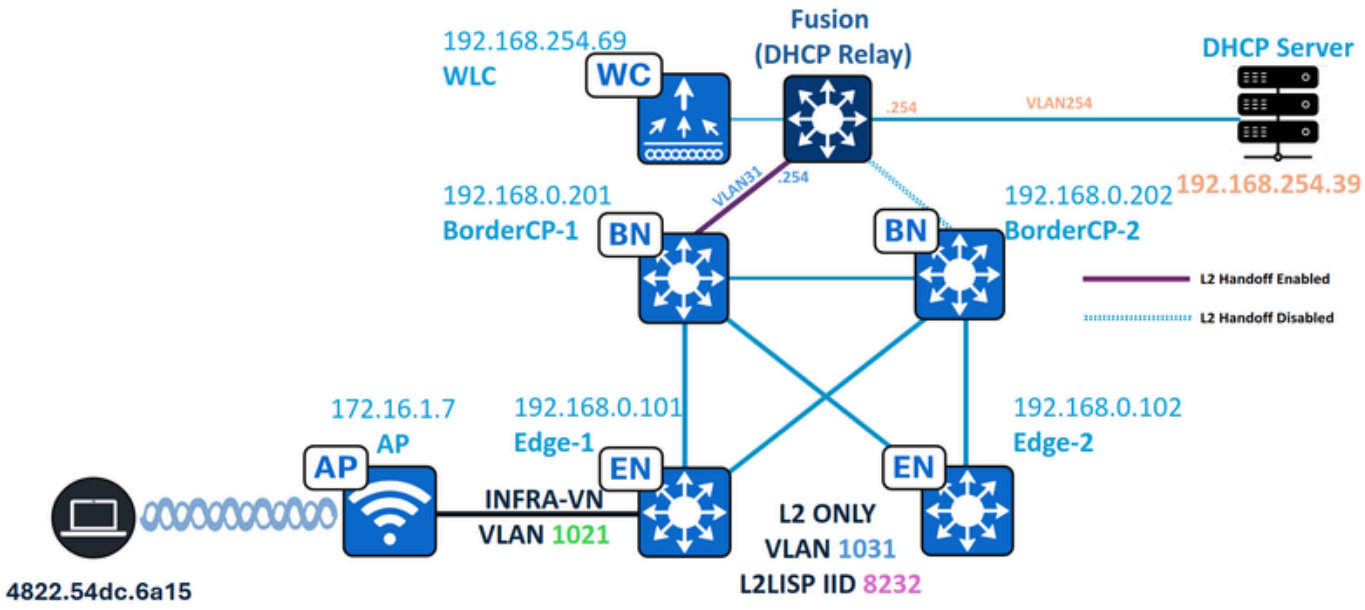
- Abilitare il routing multicast IP su tutti i nodi (bordi, bordi, nodi intermedi, ecc.).
- Configurare PIM Sparse-Mode sull'interfaccia Loopback0 di ciascun nodo Border and Edge.
- Abilitare PIM Sparse-Mode su ciascuna interfaccia IGP (underlay routing protocol).

- 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.

Interfacce Broadcast Over Access-Tunnel

Fabric Enabled Wireless utilizza la commutazione locale e la funzionalità VTEP nell'access point e in FE. Tuttavia, una limitazione IOS-XE 16.10+ impedisce l'inoltro di broadcast in uscita su VXLAN agli access point. Nelle reti solo L2, impedisce alle offerte DHCP/ACK di raggiungere i client wireless. La funzionalità "flood access-tunnel" permette di risolvere questo problema, abilitando l'inoltro di broadcast sulle interfacce del tunnel di accesso Fabric Edge.

Topologia



Topologia della rete

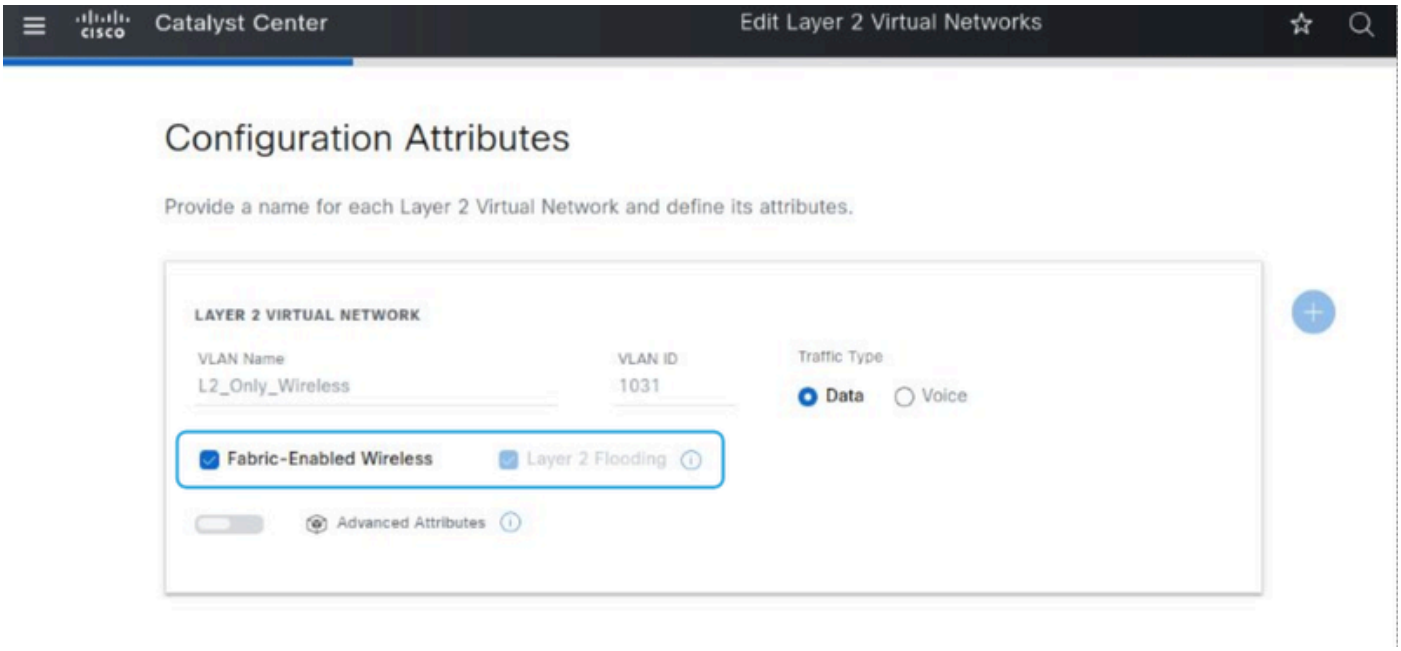
In questa topologia:

- 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
- 172.16.1.7 è il punto di accesso nell'INFRA-VN con VLAN 1021
- 192.168.254.39 è il server DHCP
- 192.168.254.69 è il controller LAN wireless
- 482.54dc.6a15 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 con wireless abilitato per fabric

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 è un pool wireless; pertanto, vengono configurate le funzionalità tipiche dei pool wireless L2 Only, ad esempio RA-Guard, DHCPGuard e Flood Access Tunnel. Il flooding ARP non è abilitato in un pool wireless.

Configurazione di Fabric Edge (192.168.0.101)

<#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
```

Il comando flood-access tunnel è configurato nella sua variante di replica multicast, in cui tutto il traffico BUM viene incapsulato ai punti di accesso usando il gruppo multicast specifico dell'origine (232.255.255.1) e la VLAN del punto di accesso INFRA-VN come VLAN consultata dallo snooping IGMP per inoltrare il traffico BUM.

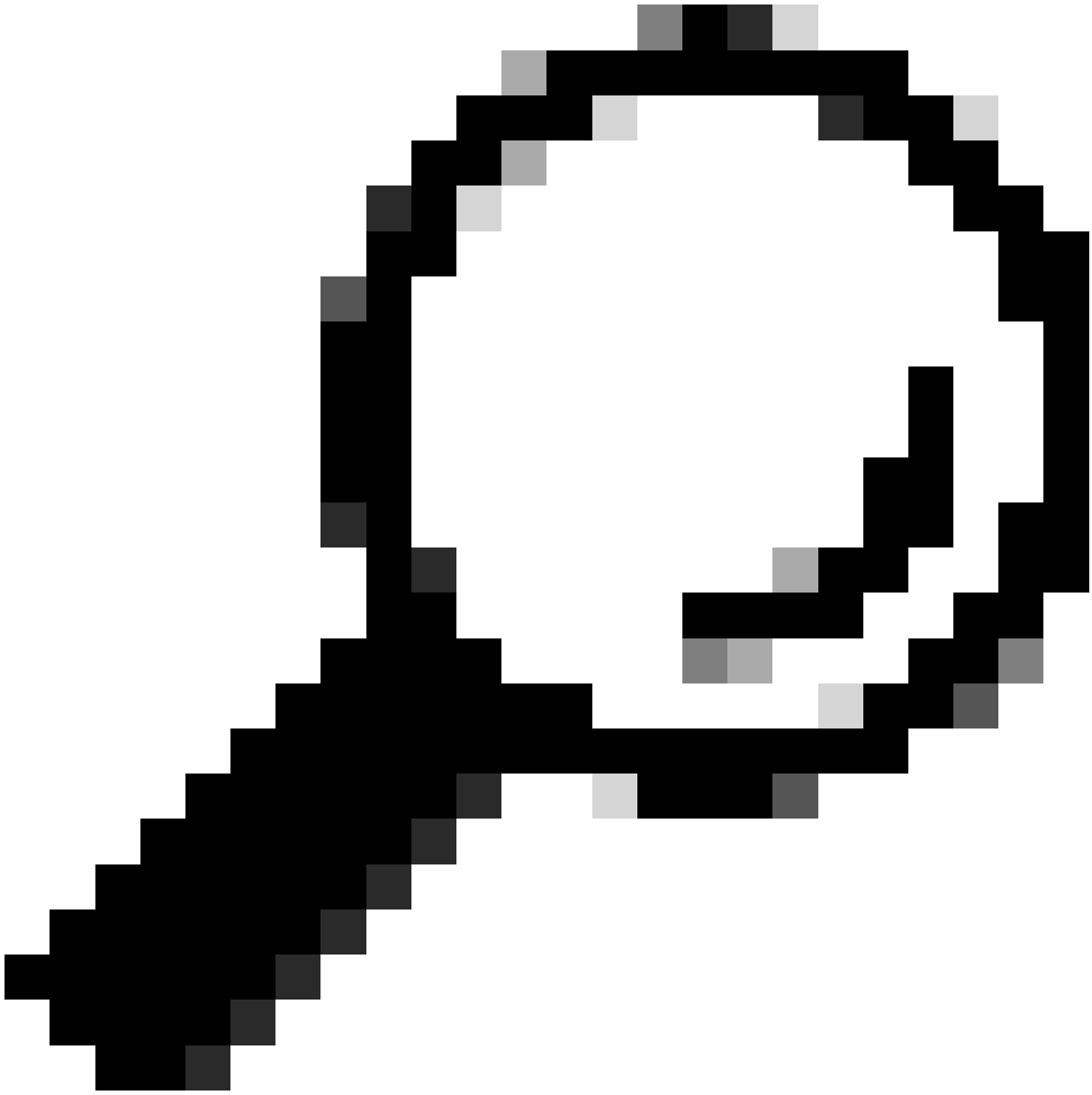
Configurazione VLAN solo L2 - Controller LAN wireless

Sul lato WLC (Wireless LAN Controller), i tag del sito associati ai punti di accesso all'infrastruttura devono essere configurati con "no fabric ap-arp-caching" per disabilitare la funzionalità proxy-ARP. Inoltre, è necessario abilitare "fabric ap-dhcp-broadcast". Questa configurazione consente l'inoltro dei pacchetti di trasmissione DHCP dall'access point agli endpoint wireless.

Configurazione Fabric WLC (192.168.254.69)

<#root>

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

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



Suggerimento: Il gruppo multicast wireless 232.255.255.1 è il gruppo predefinito utilizzato da tutti i tag del sito.

<#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

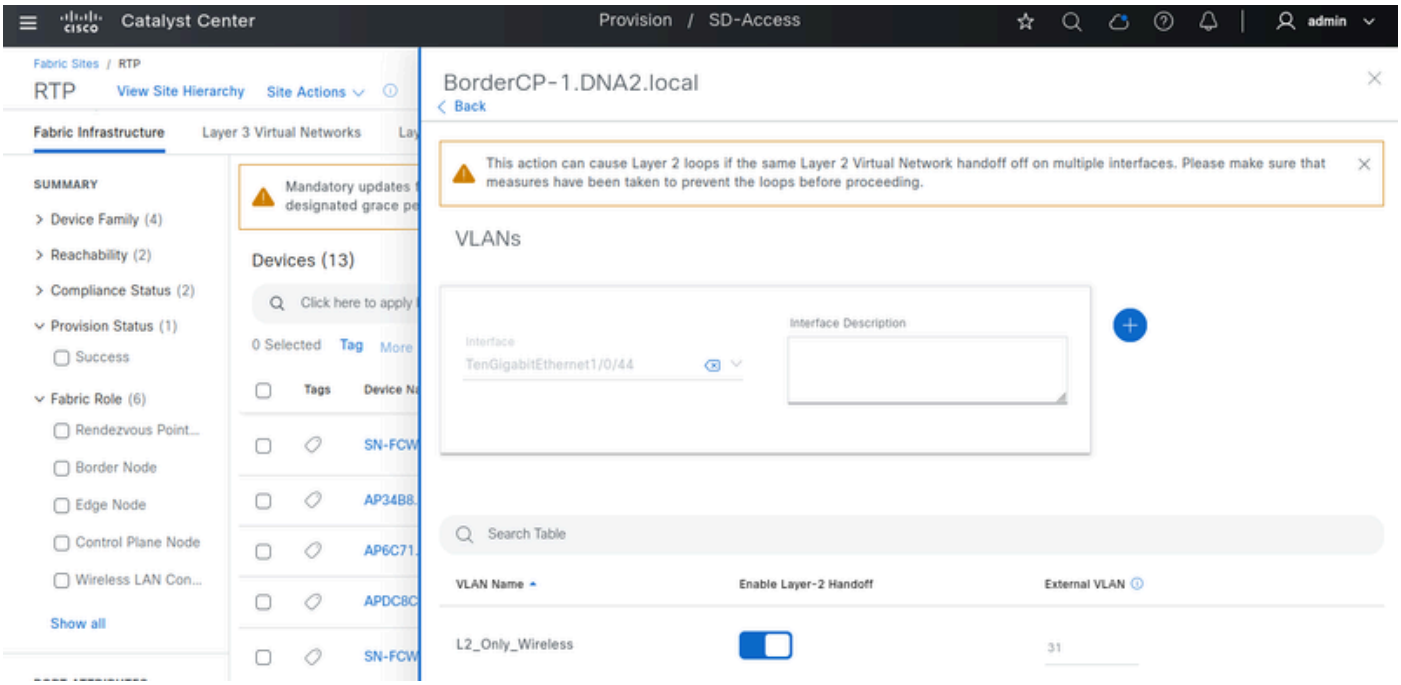
```
RTP-Site-Tag-3 Load : 0
```

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 border/CP fabric (192.168.0.201)

<#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
```

Abilitazione multicast wireless

I fabric edge sono configurati in modo da inoltrare i pacchetti broadcast ai punti di accesso tramite il meccanismo del tunnel di accesso in caso di inondazione. questi pacchetti sono incapsulati nel gruppo multicast 232.255.255.1 sulla VLAN INFRA-VN. I punti di accesso vengono aggiunti automaticamente a questo gruppo multicast, poiché il relativo tag del sito è preconfigurato per utilizzarlo.

```
<#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
```

Dal punto di accesso, in base all'associazione di un endpoint wireless dell'infrastruttura, viene formato un tunnel VXLAN (dinamico sul lato AP, sempre attivo sul lato Fabric Edge). All'interno di questo tunnel, il gruppo multicast dell'infrastruttura CAPWAP viene verificato con i comandi del terminale AP.

```
<#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
```

Dal lato Fabric Edge, verificare che lo snooping IGMP sia abilitato per la VLAN AP INFRA-VN, che i punti di accesso abbiano formato un'interfaccia del tunnel di accesso e che si siano uniti al gruppo multicast 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
------------------------------------------------------------------------
```

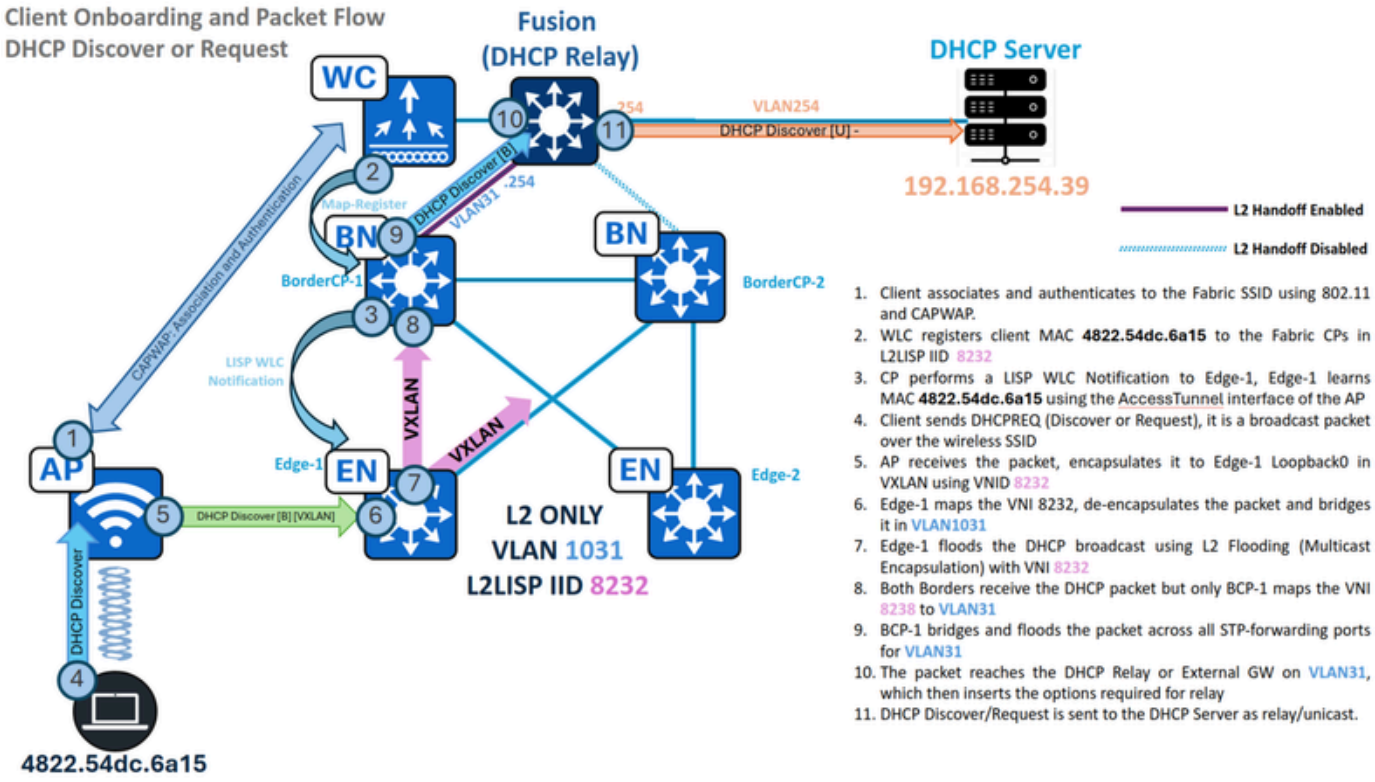
1021   232.255.255.1

```
           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>
```

Queste verifiche confermano l'abilitazione del multicast wireless su Access Point, Fabric Edge e Wireless LAN Controller.

Flusso traffico DHCP

Rilevamento e richiesta DHCP - Lato wireless



Flusso di traffico - Rilevamento e richiesta DHCP solo in L2

identificare lo stato dell'endpoint wireless, il relativo punto di accesso connesso e le proprietà dell'infrastruttura associate.

<#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

È importante verificare che le funzionalità di commutazione centrale e dhcp centrale siano disabilitate nel profilo della policy. I comandi "no central dhcp" e "no central switching" devono essere configurati sul profilo dei criteri per l'SSID.

<#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

Queste verifiche confermano che l'endpoint è connesso a "AP1", associato alla RLOC 192.168.0.101 del perimetro della struttura. Di conseguenza, il suo traffico viene incapsulato tramite VXLAN con VNID 8232 per la trasmissione dal punto di accesso al perimetro della struttura.

Rilevamento e richiesta DHCP - Fabric Edge

Apprendimento MAC con notifica WLC

Durante l'onboarding, il WLC registra l'indirizzo MAC dell'endpoint wireless con il Fabric Control Plane. Contemporaneamente, il Control Plane notifica al nodo Fabric Edge (al quale è connesso il punto di accesso) di creare una speciale voce di apprendimento MAC "CP_LEARN", che punta all'interfaccia del tunnel di accesso del punto di accesso.

<#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
```

Se l'indirizzo MAC dell'endpoint viene appreso correttamente tramite l'interfaccia del tunnel di accesso corrispondente al relativo punto di accesso connesso, 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 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>
```

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 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:

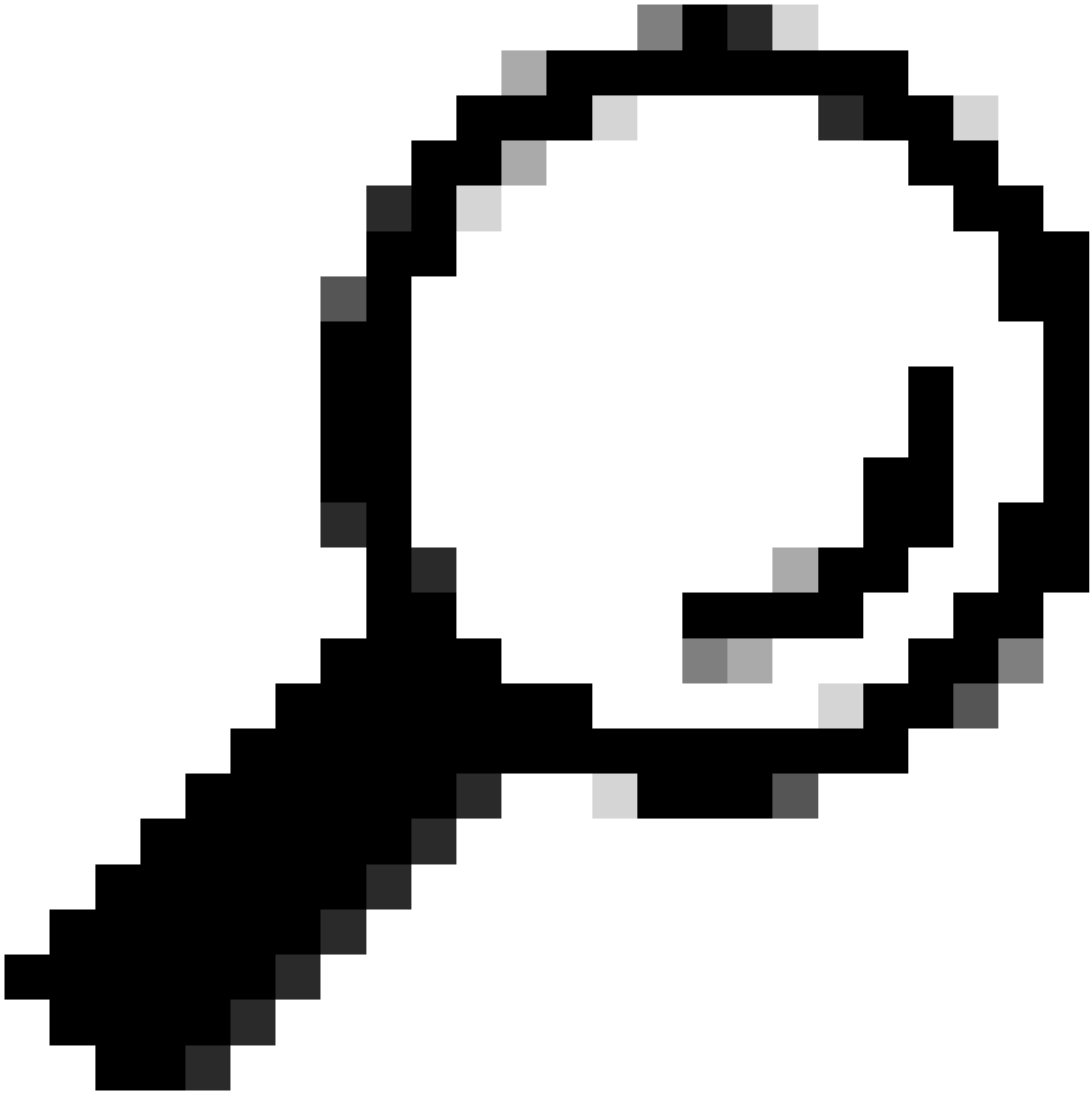
7

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

<--

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

  Totals - Source count: 1, Packet count: 8



Suggerimento: 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 entrata dal punto di accesso che il pacchetto in uscita corrispondente per L2 Flooding.

Acquisizione pacchetti Fabric Edge (192.168.0.101)

<#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
```

Durante l'acquisizione dei pacchetti, è necessario osservare tre pacchetti distinti:

- Individuazione DHCP - VXLAN - AP-Edge
- Individuazione DHCP - CAPWAP - Da AP a WLC
- Rilevamento DHCP - VXLAN - da perimetro a gruppo multicast

<#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

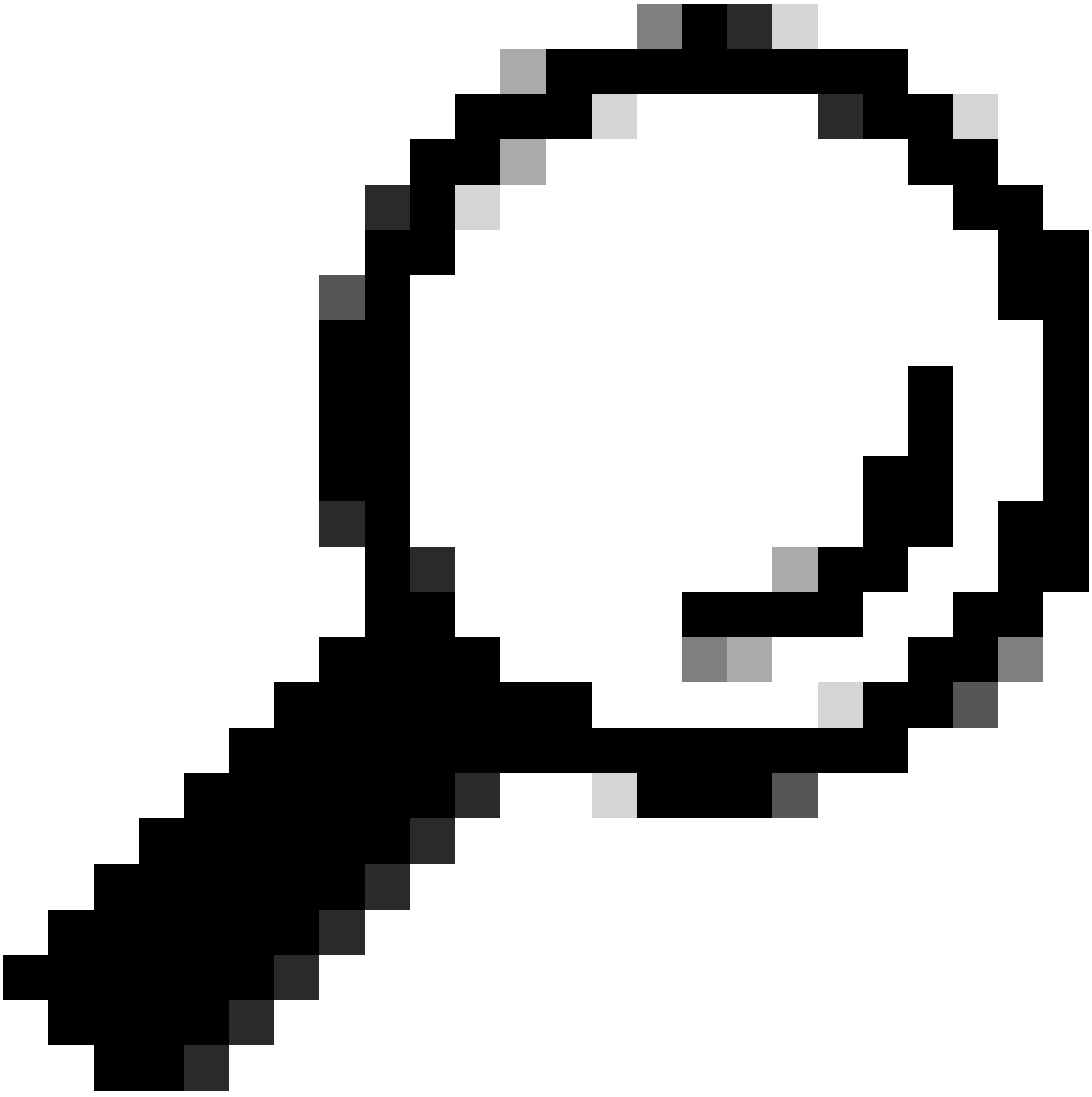
```
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
Internet Protocol Version 4, Src:
```

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



Suggerimento: Sui pacchetti wireless fabric abilitati, i pacchetti incapsulati VXLAN consegnano il traffico DHCP ai client o ai server. I pacchetti incapsulati CAPWAP DATA (UDP 5247), tuttavia, vengono trasmessi al WLC solo per scopi di rilevamento, come lo stato di apprendimento IP o il rilevamento dei dispositivi wireless.

Rilevamento e richiesta DHCP - Bordo L2

Dopo che il server Edge ha inviato i pacchetti DHCP Discover e Request tramite il layer 2 Flooding, incapsulato con il gruppo Broadcast-Underlay 239.0.17.1, questi pacchetti vengono ricevuti dal L2 Hand-Off Border, 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 31

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

31


L2_Only_Wireless


active
    L2LI0:
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,

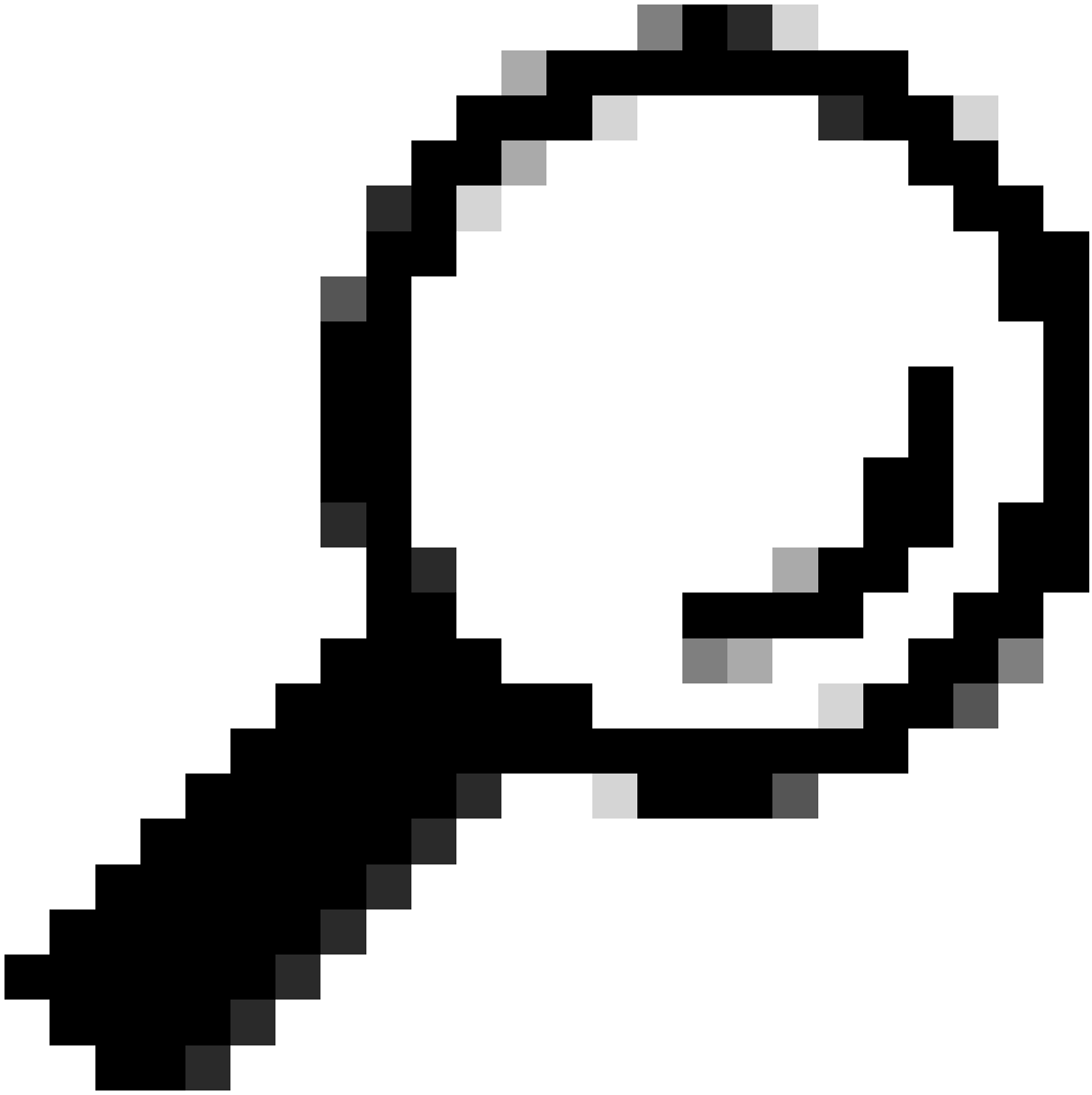
SW Forwarding: 1/0/392/0, Other: 0/0/0
HW Forwarding:

3

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

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

Totals - Source count: 1, Packet count: 4



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 in entrata sull'interfaccia L2LISP0.

<#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
```

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 31 | 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        state      Time left
ARP
172.16.131.254
                        f87b.2003.7fd5
Te1/0/44

 31
       0005       34s       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

<--

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

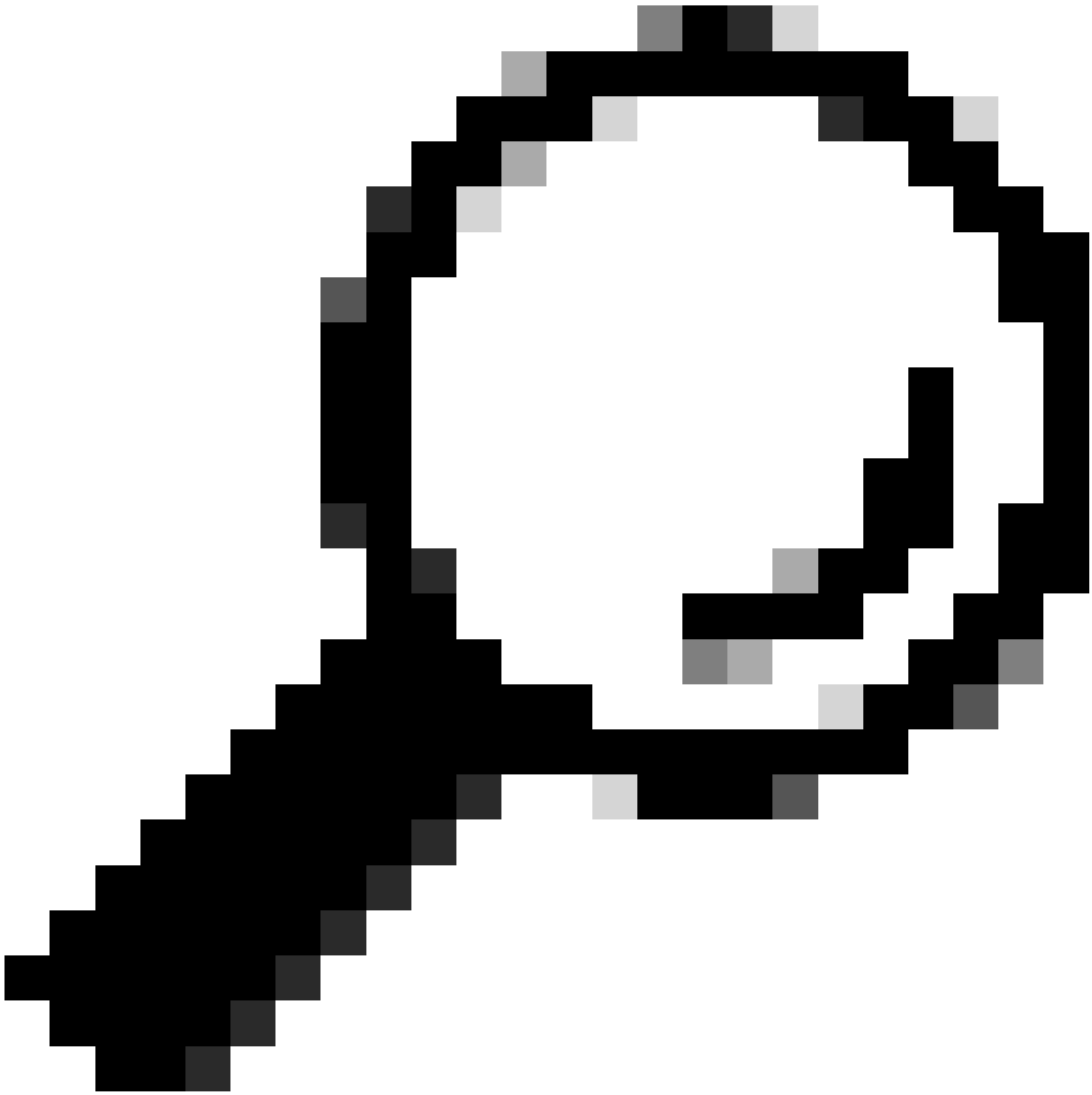
  326 16.695053   0.0.0.0 -> 255.255.255.255 DHCP

```
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
```

A questo punto, il pacchetto Discover/Request è uscito dalla struttura SD-Access, concludendo questa sezione. Tuttavia, prima di procedere, un parametro cruciale (il flag di trasmissione DHCP, determinato dall'endpoint stesso) determina lo scenario di inoltro per i pacchetti dell'offerta o della conferma. Possiamo esaminare uno dei nostri pacchetti Discover per ispezionare questa bandiera.

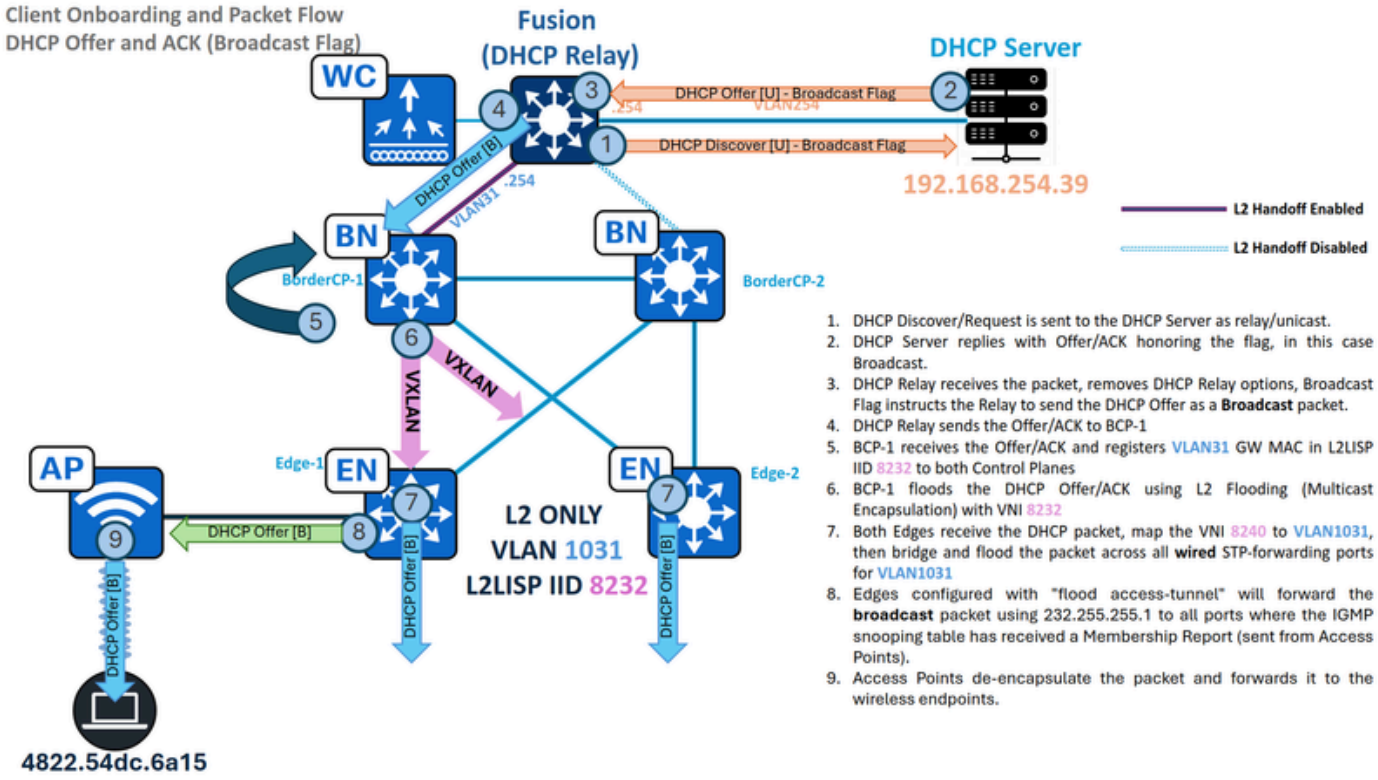
```
<#root>
BorderCP-1#
show monitor capture cap buffer display-filter "bootp.type==1 and dhcp.hw.mac_addr==4822.54dc.6a15
" detailed | sect Dynamic


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
```



Suggerimento: Il bootp.type==1 può essere utilizzato per filtrare solo i pacchetti Discover e Request.

Offerta e ACK DHCP - Broadcast - Bordo L2



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

Ora che il comando DHCP Discover è uscito dal fabric SD-Access, il relay DHCP inserirà le opzioni di inoltro DHCP tradizionali (ad esempio GiAddr/GatewayIPAddress) e inoltrerà 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 8232.

<#root>

```
BorderCP-1#
```

show mac address-table interface te1/0/44

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

```
----    -----------       --------    -----

31


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
```

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 <-- 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

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 collegherà 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 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

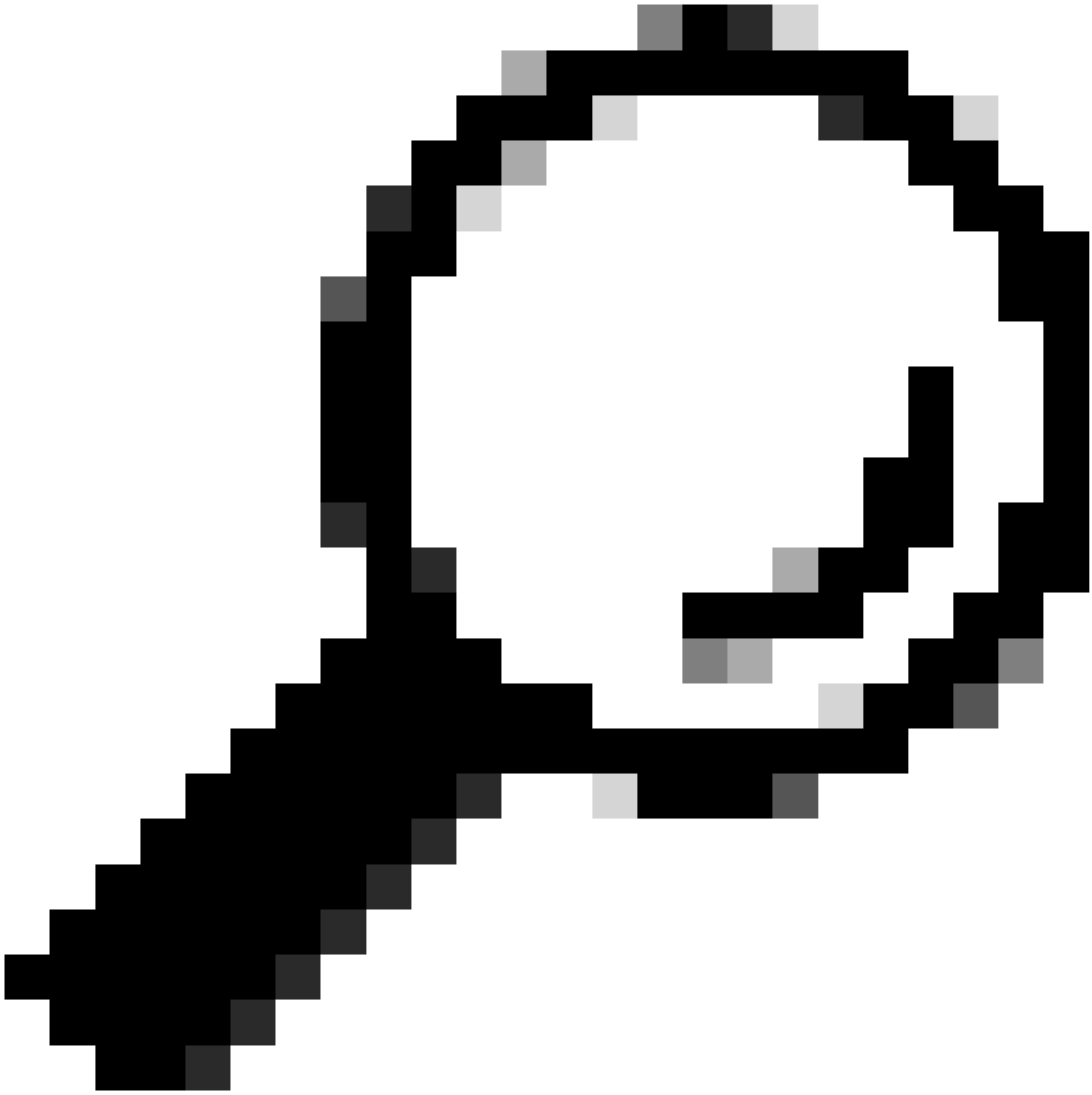
,
   SW Forwarding: 1/0/392/0, Other: 1/1/0
   HW Forwarding:

92071

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

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

  Totals - Source count: 1, Packet count: 92071



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, concludiamo questa sezione, poiché l'offerta DHCP verrà 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, ora controlliamo il L2Border S,G nel Fabric Edge, dove l'interfaccia in entrata punta verso L2BN e l'OIL contiene l'istanza L2LISP mappata alla VLAN 1031.

<#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,

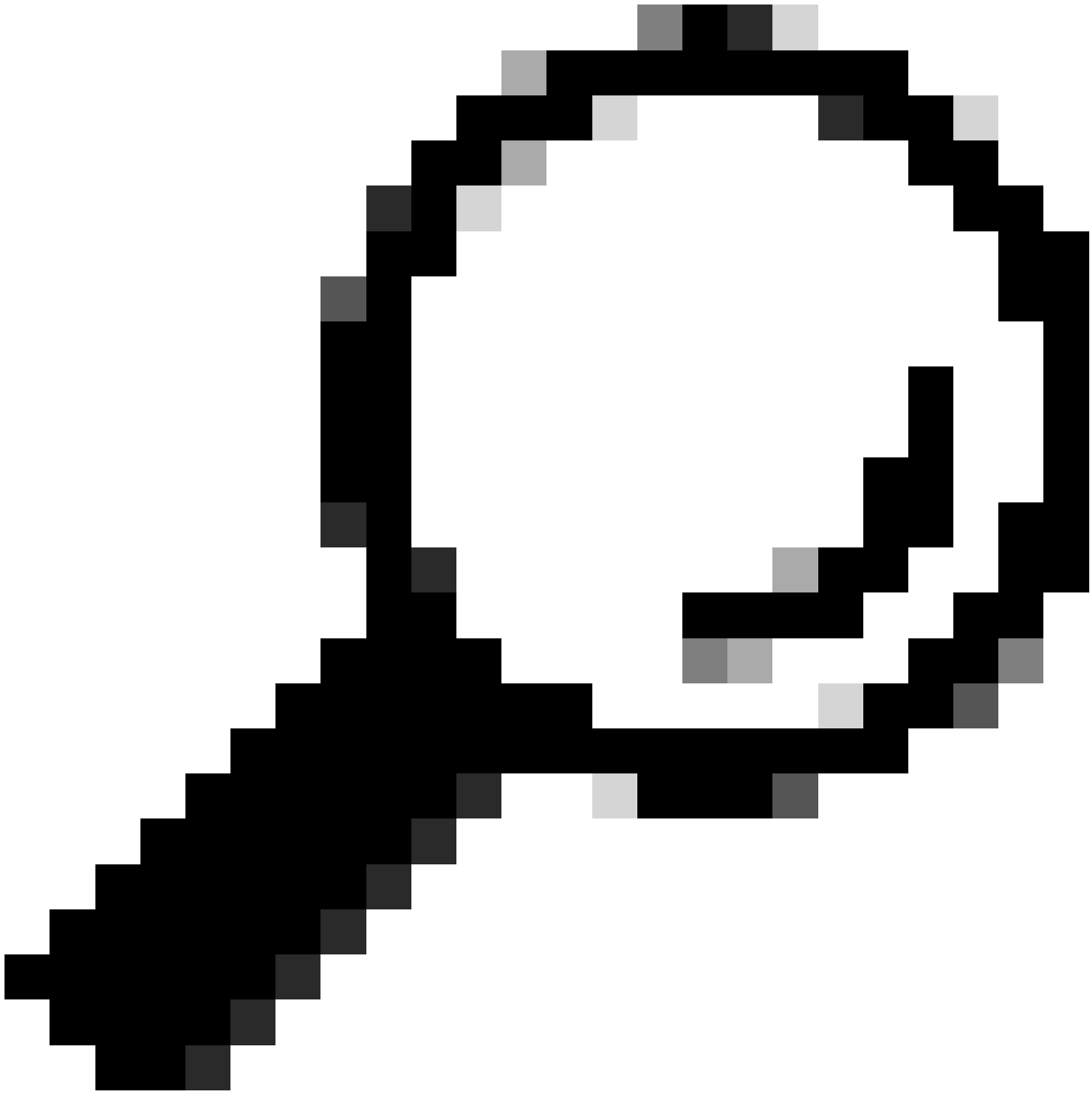
```
   SW Forwarding: 1/0/96/0, Other: 0/0/0
   HW Forwarding:
```

76236

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

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

```
  Totals - Source count: 1, Packet count: 4
```



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 posizionato sulla VLAN corrispondente al VNI 8232, per natura del broadcast il pacchetto viene inviato a tutte le porte di inoltro cablate dello Spanning Tree Protocol per VLAN1031.

<#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
```

Tuttavia, l'interfaccia che stiamo cercando per trasmettere l'offerta DHCP è l'interfaccia del tunnel di accesso associata al punto di accesso. Ciò è possibile solo perché "flood access-tunnel" è abilitato sull'ID L2LISP 8232, altrimenti il pacchetto viene bloccato e inoltrato all'interfaccia AccessTunnel.

<#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
```

Con la voce Snooping IGMP per il gruppo di flooding multicast, le offerte DHCP e gli ACK vengono inoltrati alla porta fisica dell'access point.

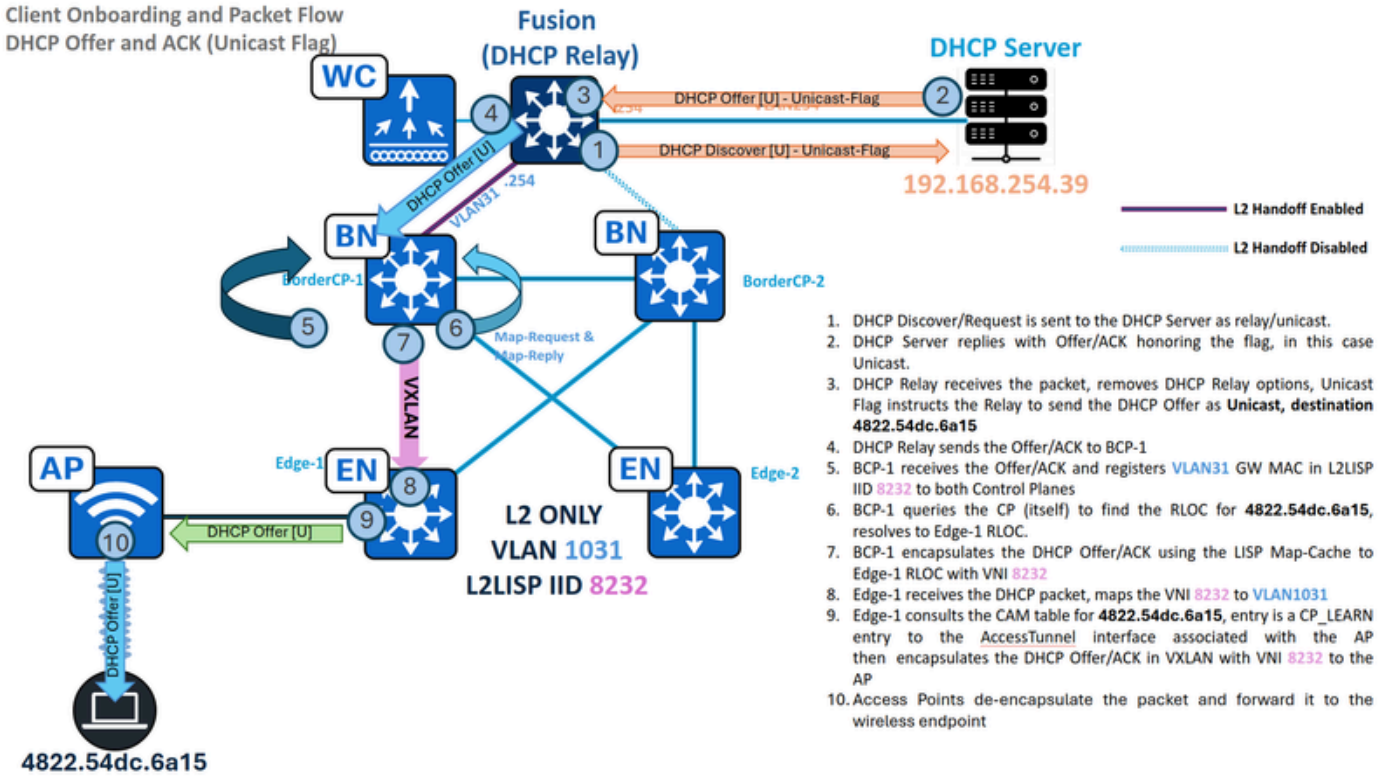
Il processo di offerta e ACK DHCP rimane coerente. Se lo snooping DHCP non è abilitato, nella tabella Snooping DHCP non verrà creata alcuna voce. Di conseguenza, la voce Device Tracking per l'endpoint abilitato per DHCP viene generata dai pacchetti ARP acquisiti. Si prevede inoltre che comandi quali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

<#root>

```
Edge-1#
show device-tracking database interface 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
```

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==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)
```

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 individuare l'indirizzo MAC di destinazione. Presupponendo che l'"apprendimento MAC e la notifica WLC" sul perimetro della struttura abbia esito positivo, il Control Plane ha registrato questo ID endpoint (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
```

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 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        -
```

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

```
<#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
```

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 al tunnel di accesso specifico a cui è connesso l'endpoint, anziché inviarlo a tutte le porte.

La tabella degli indirizzi MAC identifica la porta AccessTunnel2 come porta virtuale associata a AP1.

<#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

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 acquisiti, non da DHCP. 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 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
```

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.

Transazione DHCP - Verifica wireless

Dal WLC, la transazione DHCP viene monitorata tramite RA-Traces.

<#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

Al termine della transazione, l'endpoint viene aggiunto al database Device-Tracking sul controller LAN wireless.

<#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

L'intera transazione DHCP viene sottoposta a debug sul punto di accesso stesso.

<#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:

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:
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: 1754890669.36
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**

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).