Identificar e Solucionar Problemas do DHCP na VLAN Somente da Camada 2 - Sem Fio

Contents

Introdução

Este documento descreve como solucionar problemas de DHCP para terminais sem fio em uma rede somente de camada 2 na estrutura de acesso SD (SDA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Encaminhamento de Internet Protocol (IP)
- Protocolo de separação de localizador/ID (LISP)
- Protocol Independent Multicast (PIM) Modo escasso
- Rede sem fio habilitada para malha

Requisitos de hardware e software

- Catalyst 9000 Series Switches
- Catalyst Center Versão 2.3.7.9
- Controladores de LAN sem fio Catalyst 9800 Series
- Pontos de acesso Catalyst 9100 Series
- Cisco IOS® XE 17.12 e posterior

Limitações

- Apenas uma borda L2 pode transferir uma VLAN/VNI exclusiva simultaneamente, a menos que mecanismos robustos de prevenção de loop, como scripts FlexLink+ ou EEM para desativar links, estejam configurados corretamente.

Visão geral somente de L2

Overview

Em implantações SD-Access típicas, o limite L2/L3 reside no Fabric Edge (FE), onde o FE hospeda o gateway do cliente na forma de um SVI, que é frequentemente chamado de "Anycast Gateway". As VNIs L3 (roteadas) são estabelecidas para o tráfego entre sub-redes, enquanto as VNIs L2 (comutadas) gerenciam o tráfego entre sub-redes. A configuração consistente em todos os FEs permite roaming transparente de clientes. O encaminhamento é otimizado: o tráfego intra-sub-rede (L2) é diretamente ligado entre os FEs e o tráfego inter-sub-rede (L3) é roteado entre os FEs ou entre um FE e um nó de borda.

Para endpoints em estruturas SDA que exigem um ponto de entrada de rede rígido fora da estrutura, a estrutura SDA deve fornecer um canal L2 da borda para um gateway externo.

Esse conceito é análogo às implantações de campus Ethernet tradicionais, onde uma rede de acesso de Camada 2 se conecta a um roteador de Camada 3. O tráfego entre VLANs permanece dentro da rede L2, enquanto o tráfego entre VLANs é roteado pelo dispositivo L3, geralmente retorna para uma VLAN diferente na rede L2.

Dentro de um contexto LISP, o plano de controle de site rastreia principalmente endereços MAC e suas vinculações MAC-para-IP correspondentes, muito parecido com as entradas ARP

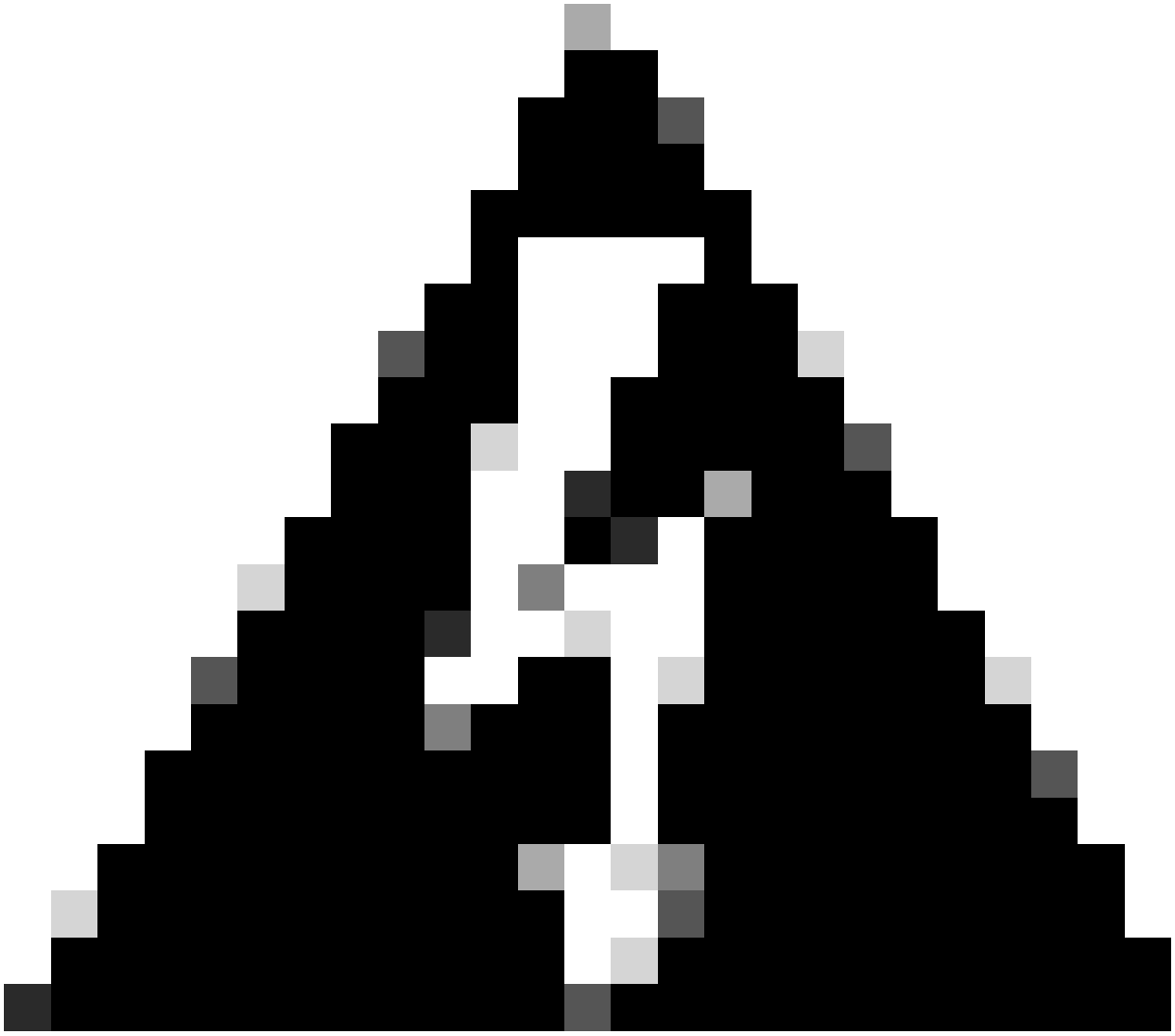
tradicionais. Os pools somente de L2 VNI/L2 são projetados para facilitar o registro, a resolução e o encaminhamento exclusivamente com base nesses dois tipos de EID. Portanto, qualquer encaminhamento baseado em LISP em um ambiente somente L2 depende exclusivamente de informações MAC e MAC-para-IP, ele ignora completamente EIDs IPv4 ou IPv6. Para complementar os LISP EIDs, os pools somente L2 dependem muito dos mecanismos flood-and-learn, semelhantes ao comportamento dos switches tradicionais. Consequentemente, a inundação de L2 se torna um componente crítico para lidar com o tráfego de broadcast, unicast desconhecido e multicast (BUM) dentro dessa solução, requer o uso de multicast subjacente. Por outro lado, o tráfego unicast normal é encaminhado usando processos de encaminhamento LISP padrão, principalmente através de Caches de Mapa.

Tanto as Bordas de Estrutura quanto a "Borda L2" (L2B) mantêm VNIs L2, que mapeiam para VLANs locais (esse mapeamento é significativo localmente para dispositivos dentro do SDA, permitindo que VLANs diferentes mapeiem para o mesmo VNI L2 entre os nós). Neste caso de uso específico, nenhum SVI é configurado nessas VLANs nesses nós, o que significa que não há nenhuma VNI de L3 correspondente.

Alteração do comportamento do DHCP nas VLANs L2 somente

Nos pools de Gateway Anycast, o DHCP apresenta um desafio, pois cada Borda de estrutura atua como o gateway para seus endpoints diretamente conectados, com o mesmo IP de gateway em todos os FEs. Para identificar corretamente a origem original de um pacote DHCP retransmitido, os FEs devem inserir a Opção de DHCP 82 e suas subopções, incluindo as informações de LISP RLOC. Isso é obtido com o rastreamento de DHCP na VLAN do cliente na borda da estrutura. O DHCP Snooping tem duas finalidades neste contexto: facilita a inserção da Opção 82 e, fundamentalmente, evita a inundação de pacotes de broadcast DHCP através do domínio de bridge (VLAN/VNI). Mesmo quando a inundação de Camada 2 está habilitada para um gateway Anycast, o DHCP Snooping efetivamente suprime o pacote de broadcast a ser encaminhado para fora da Borda da Estrutura como um broadcast.

Em contraste, uma VLAN somente de camada 2 não tem um gateway, o que simplifica a identificação da origem DHCP. Como os pacotes não são retransmitidos por nenhuma Borda de estrutura, os mecanismos complexos para identificação de origem são desnecessários. Sem o rastreamento de DHCP na VLAN Somente L2, o mecanismo de controle de inundação para pacotes DHCP é efetivamente ignorado. Isso permite que os broadcasts DHCP sejam encaminhados por meio da Inundação de L2 para seu destino final, que pode ser um servidor DHCP conectado diretamente a um Nó de estrutura ou a um dispositivo de Camada 3 que forneça a funcionalidade de retransmissão de DHCP.



aviso: A funcionalidade "Vários IP para MAC" dentro de um pool Somente L2 ativa automaticamente o rastreamento de DHCP no modo Bridge VM, que reforça o controle de inundação de DHCP. Consequentemente, isso torna o pool VNI L2 incapaz de suportar DHCP para seus endpoints.

Multicast Subjacente

Dada a forte dependência do DHCP no tráfego de broadcast, a inundação da Camada 2 deve ser aproveitada para suportar esse protocolo. Como com qualquer outro pool habilitado para inundação de L2, a rede subjacente deve ser configurada para tráfego multicast, especificamente Any-Source-Multicast utilizando PIM Sparse-Mode. Enquanto a configuração multicast subjacente é automatizada através do fluxo de trabalho de automação de LAN, se esta etapa foi omitida, é necessária configuração adicional (manual ou modelo).

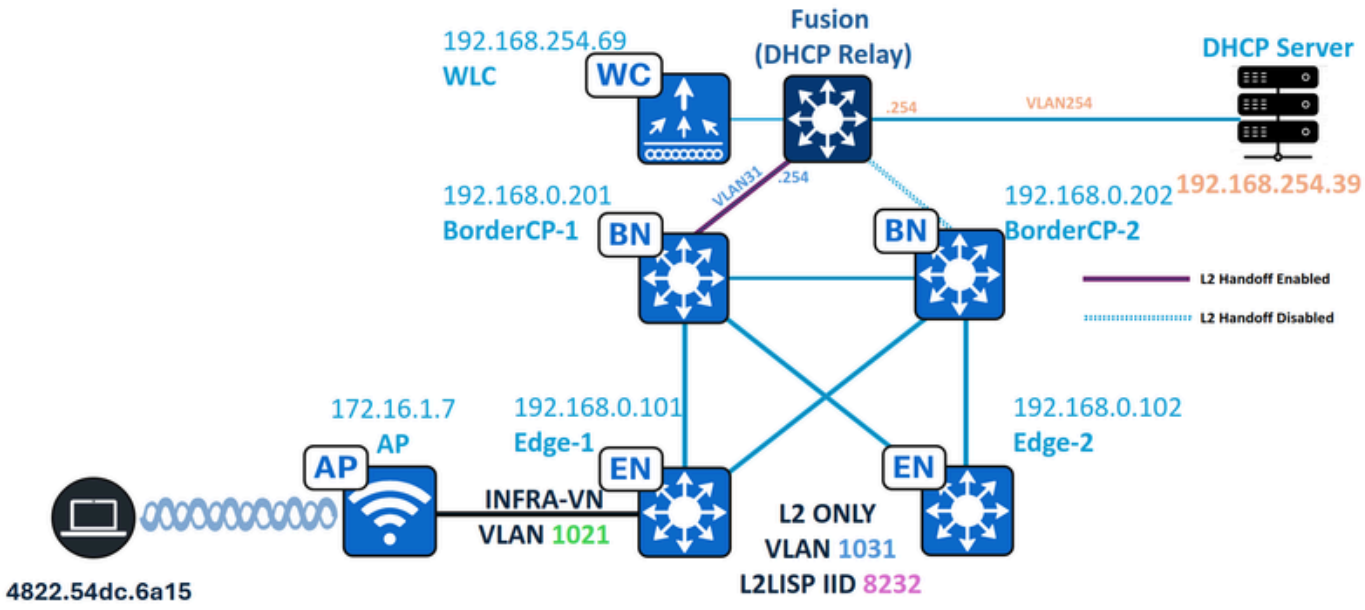
- Ative o roteamento multicast IP em todos os nós (bordas, bordas, nós intermediários etc.).
- Configure o modo escasso do PIM na interface Loopback0 de cada nó de borda e borda.
- Ative o modo escasso PIM em cada interface IGP (protocolo de roteamento de base).

- Configure o PIM Rendezvous Point (RP) em todos os nós (Bordas, Bordas, Nós Intermediários); a colocação do RP em Bordas é recomendada.
- Verifique os vizinhos PIM, PIM RP e o status do túnel PIM.

Interfaces de Broadcast sobre Túnel de Acesso

A rede sem fio habilitada para malha emprega switching local e funcionalidade VTEP no AP e FE. No entanto, uma limitação do IOS-XE 16.10+ impede o encaminhamento de broadcast de saída sobre VXLAN para APs. Em redes Somente L2, isso impede que Ofertas/ACKs DHCP alcancem clientes sem fio. O recurso de "túnel de acesso de inundação" aborda isso ativando o encaminhamento de broadcast nas interfaces de túnel de acesso de borda de malha.

Topologia



Topologia de rede

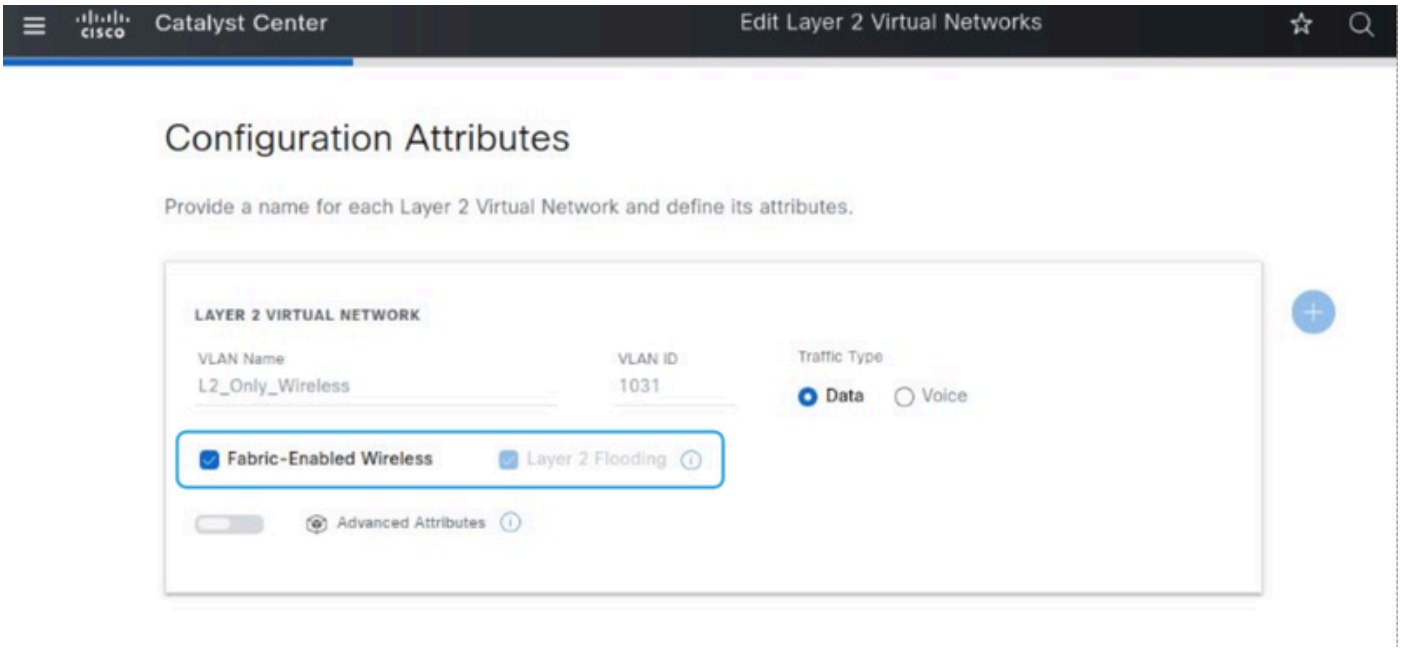
Nesta topologia:

- 192.168.0.201 e 192.168.0.202 são Bordas Alocadas para o Site de Malha, BorderCP-1 é a única Borda com o recurso de Entrega da Camada 2 habilitado.
- 192.168.0.101 e 192.168.0.102 são nós de borda de malha
- 172.16.1.7 é o ponto de acesso em INFRA-VN com VLAN 1021
- 192.168.254.39 é o servidor DHCP
- 192.168.254.69 é a controladora Wireless LAN
- 4822.54dc.6a15 é o endpoint habilitado para DHCP
- O dispositivo Fusion atua como DHCP Relay para as sub-redes de estrutura.

Configuração VLAN Somente L2

Implantação de VLAN somente L2 do Catalyst Center

Caminho: Centro Catalyst / Provisionamento / Site de estrutura / Redes virtuais de Camada 2 / Editar redes virtuais de Camada 2



Configuração L2VNI com rede sem fio habilitada para malha

Configuração VLAN Somente L2 - Bordas de Estrutura

Os nós de borda de malha têm a VLAN configurada com CTS habilitado, IGMP e IPv6 MLD desabilitado e a configuração L2 LISP necessária. Este pool L2 Only é um pool Wireless; portanto, recursos normalmente encontrados em pools sem fio somente L2, como RA-Guard, DHCPGuard e Flood Access Tunnel, são configurados. A Inundação ARP não está habilitada em um pool sem fio.

Configuração da borda da malha (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
```

O comando flood-access tunnel é configurado em sua variação de replicação multicast, em que todo o tráfego de BUM é encapsulado em APs usando o grupo multicast específico da origem (232.255.255.1) usando a VLAN do Ponto de Acesso INFRA-VN como a VLAN que é consultada pela espionagem de IGMP para encaminhar o tráfego de BUM.

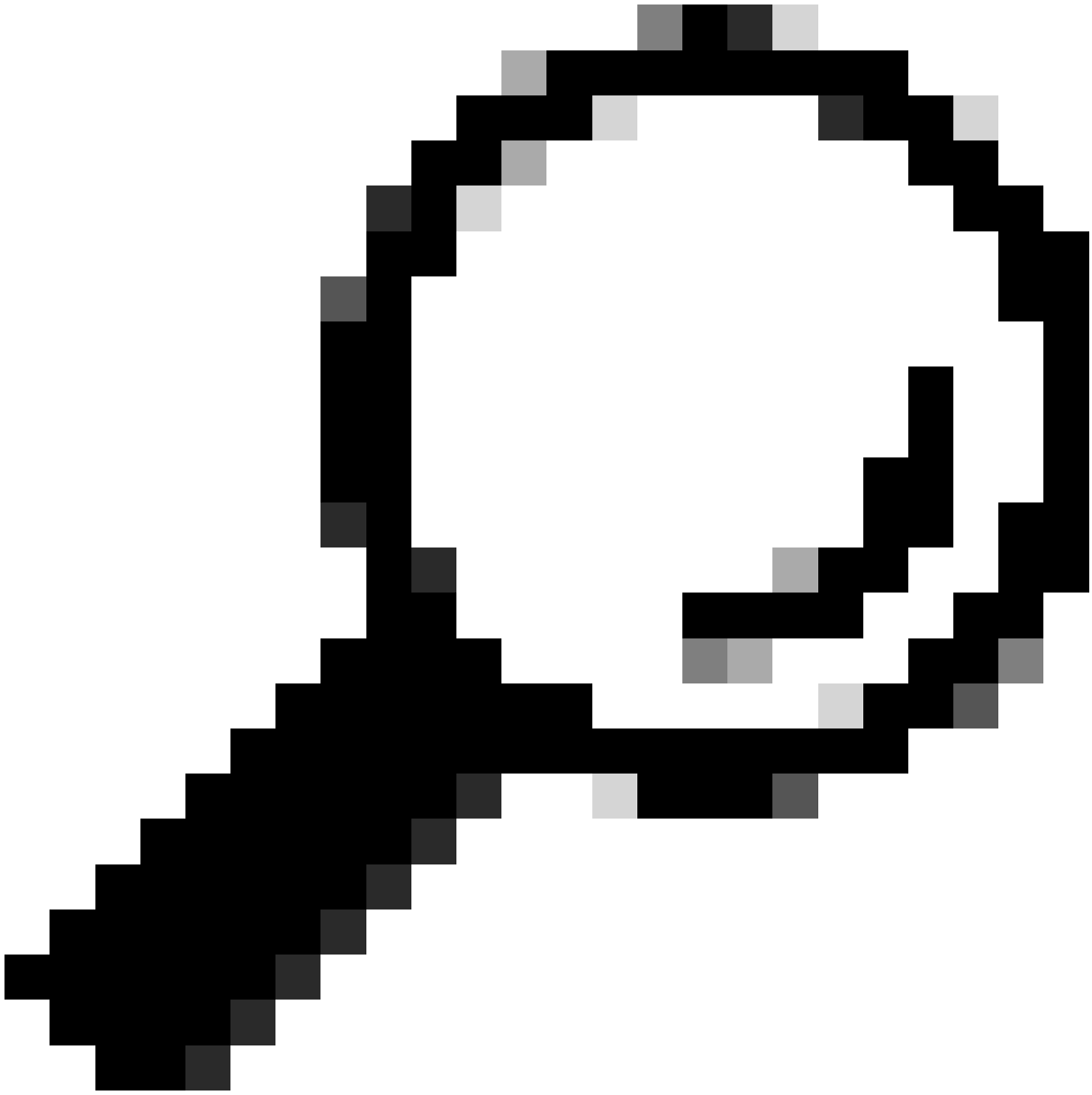
Configuração VLAN Somente L2 - Controlador LAN Sem Fio

No lado da WLC (Wireless LAN Controller), as marcas de site associadas aos pontos de acesso de estrutura devem ser configuradas com "no fabric ap-arp-caching" para desabilitar a funcionalidade proxy-ARP. Além disso, a "estrutura ap-dhcp-broadcast" deve ser habilitada, essa configuração permite que os pacotes de transmissão DHCP sejam encaminhados do AP para os terminais sem fio.

Configuração de WLC de estrutura (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
```



Tip: O grupo multicast sem fio 232.255.255.1 é o grupo padrão usado por todas as marcas de site.

<#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

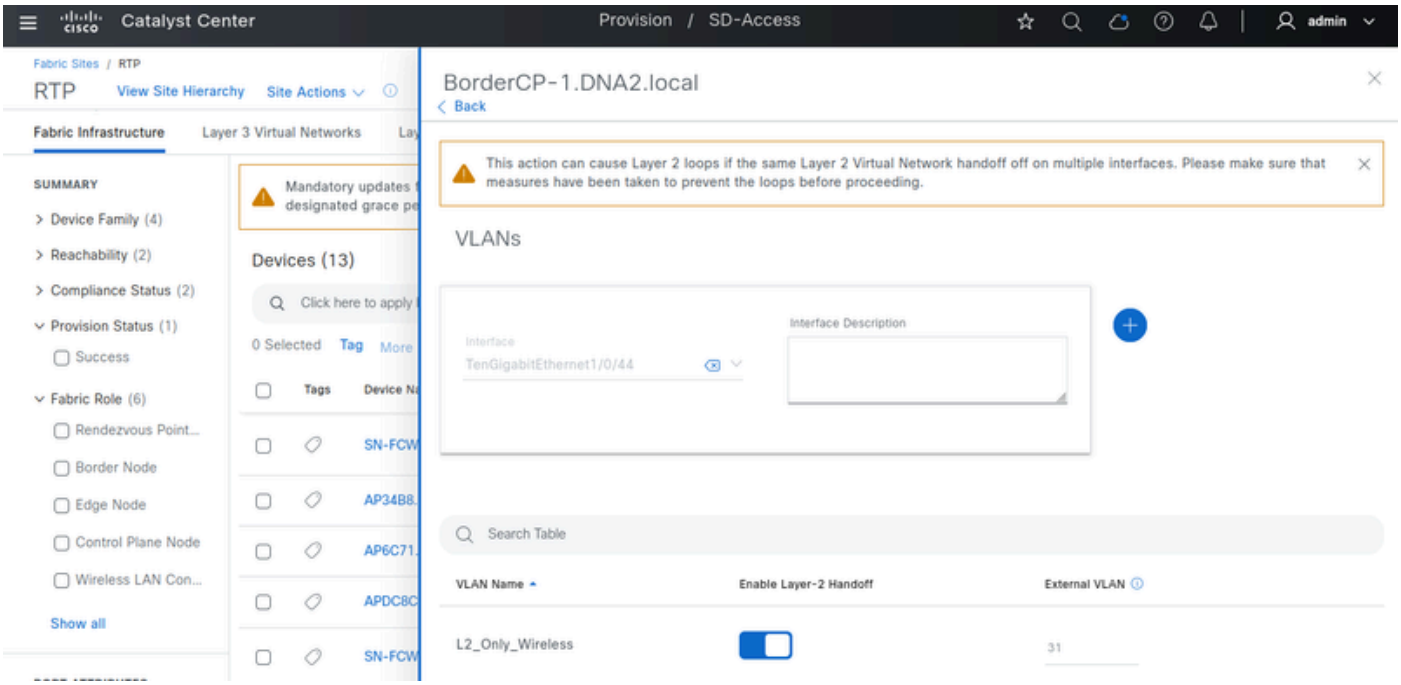
```
RTP-Site-Tag-3 Load : 0
```

Configuração de hand-off de camada 2 (borda da malha)

De uma perspectiva operacional, o servidor DHCP (ou Roteador/Retransmissão) pode ser conectado a qualquer nó de estrutura, incluindo bordas e bordas.

O uso de nós de borda para conectar o servidor DHCP é a abordagem recomendada, no entanto, requer consideração cuidadosa no projeto. Isso ocorre porque a Borda deve ser configurada para Transmissão L2 em uma base por interface. Isso permite que o Pool de Malha seja entregue à mesma VLAN da Malha ou a uma diferente. Essa flexibilidade em IDs de VLAN entre bordas de estrutura e bordas é possível porque ambas são mapeadas para o mesmo ID de instância L2 LISP. As portas físicas L2 de hand-off não devem ser ativadas simultaneamente com a mesma VLAN para evitar loops de Camada 2 dentro da rede de acesso SD. Para redundância, são necessários métodos como os scripts StackWise Virtual, FlexLink+ ou EEM.

Por outro lado, a conexão do servidor DHCP ou do roteador gateway a uma borda de malha não requer configuração adicional.



Configuração de hand-off de L2

Configuração da borda da estrutura/CP (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
```

Capacitação Multicast Sem Fio

As bordas de estrutura são configuradas para encaminhar pacotes de broadcast para pontos de acesso por meio do mecanismo flood access-tunnel. esses pacotes são encapsulados no grupo multicast 232.255.255.1 na VLAN INFRA-VN. Os pontos de acesso se unem automaticamente a esse grupo de multicast, pois sua marca de site é pré-configurada para utilizá-lo.

```
<#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
```

A partir do ponto de acesso, mediante a associação de um endpoint sem fio de estrutura, um túnel VXLAN é formado (dinâmico no lado do AP, sempre ativo no lado da borda da estrutura). Nesse túnel, o grupo multicast de estrutura CAPWAP é verificado com comandos do terminal 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
```

Do lado da borda da estrutura, confirme se o rastreamento de IGMP está habilitado para a VLAN do AP INFRA-VN, se os pontos de acesso formaram uma interface de túnel de acesso e se juntaram ao grupo 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

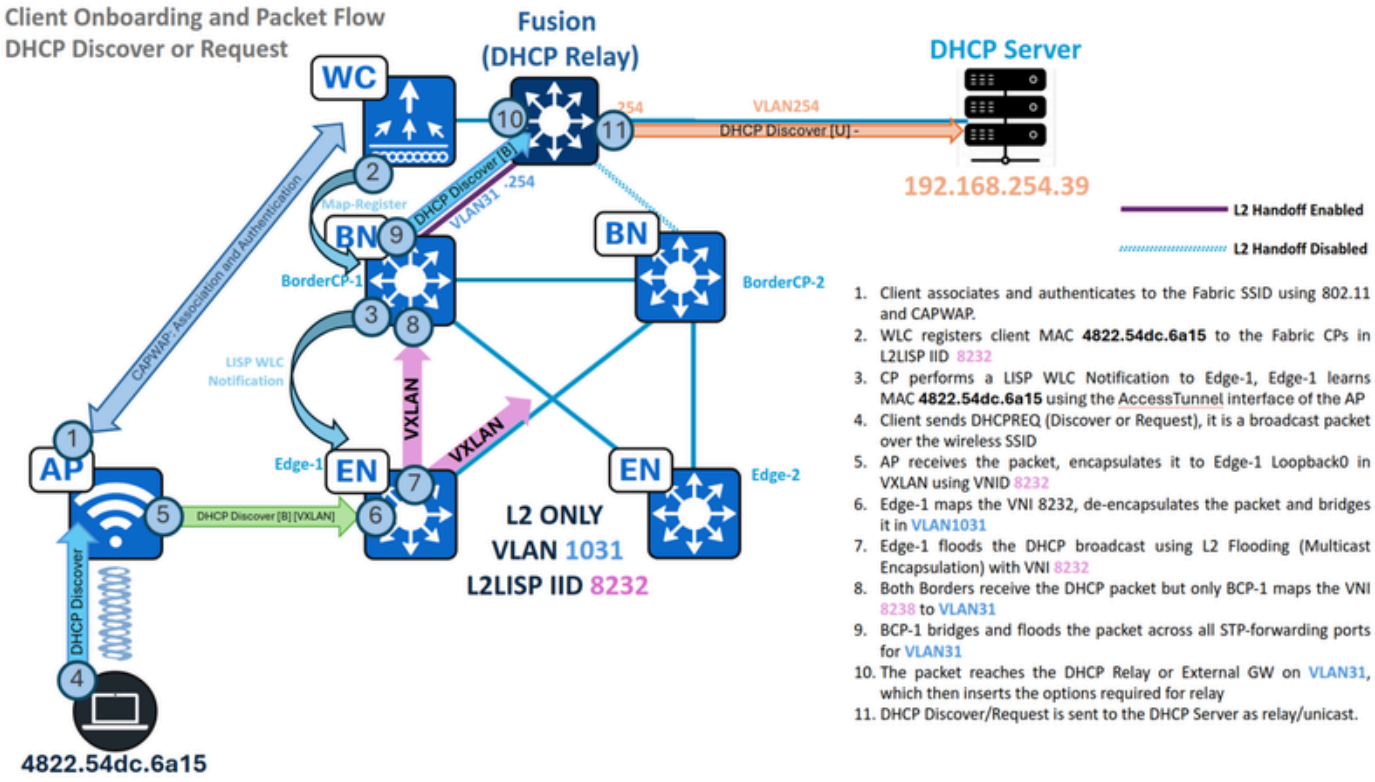
```
           igmp        v2
```

```
 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>
```

Essas verificações confirmam a habilitação bem-sucedida do multicast sem fio pelo Ponto de acesso, Borda da malha e Controlador LAN sem fio.

Fluxo de tráfego DHCP

Descoberta e solicitação DHCP - Lado sem fio



Fluxo de tráfego - Descoberta e solicitação DHCP somente em L2

identifique o estado do ponto de extremidade sem fio, seu ponto de acesso conectado e as propriedades de malha associadas.

<#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
```

É importante confirmar que os recursos de switching central e de dhcp central estão desativados no perfil de política. Os comandos "no central dhcp" e "no central switching" devem ser configurados no perfil de política para o 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
```

Essas verificações confirmam que o endpoint está conectado ao "AP1", que está associado ao Fabric Edge RLOC 192.168.0.101. Consequentemente, seu tráfego é encapsulado via VXLAN com VNID 8232 para transmissão do Access Point para o Fabric Edge.

Descoberta e solicitação DHCP - Borda da malha

Aprendizado de MAC usando Notificação de WLC

Durante a integração do endpoint, a WLC registra o endereço MAC do endpoint sem fio com o plano de controle de estrutura. Simultaneamente, o plano de controle notifica o nó da borda da estrutura (ao qual o ponto de acesso está conectado) para criar uma entrada de aprendizagem MAC "CP_LEARN" especial, apontando para a interface de túnel de acesso do ponto de acesso.

<#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 o endereço MAC do ponto final for aprendido corretamente através da interface de túnel de acesso correspondente ao seu ponto de acesso conectado, esse estágio é considerado completo.

Transmissão DHCP ligada em inundação de L2

Quando o rastreamento de DHCP está desativado, os broadcasts de DHCP não são bloqueados; em vez disso, eles são encapsulados em multicast para inundação de Camada 2. Por outro lado, a habilitação do DHCP Snooping impede a inundação desses pacotes de 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>
```

Como o rastreamento de DHCP está desabilitado, a descoberta/solicitação de DHCP utiliza a interface L2LISP0, fazendo a ponte do tráfego por meio da inundação de L2. Dependendo da versão do Catalyst Center e dos Banners de estrutura aplicados, a interface L2LISP0 pode ter listas de acesso configuradas em ambas as direções; portanto, certifique-se de que o tráfego DHCP (portas UDP 67 e 68) não seja negado explicitamente por nenhuma entrada de controle de acesso (ACEs).

<#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

Utilize o grupo de broadcast-underlay configurado para a instância L2LISP e o endereço IP Loopback0 do Fabric Edge para verificar a entrada L2 Flooding (S,G) que conecta esse pacote a outros Fabric Nodes. Consulte as tabelas mroute e mfib para validar parâmetros como a interface de entrada, a lista de interfaces de saída e os contadores de encaminhamento.

<#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:

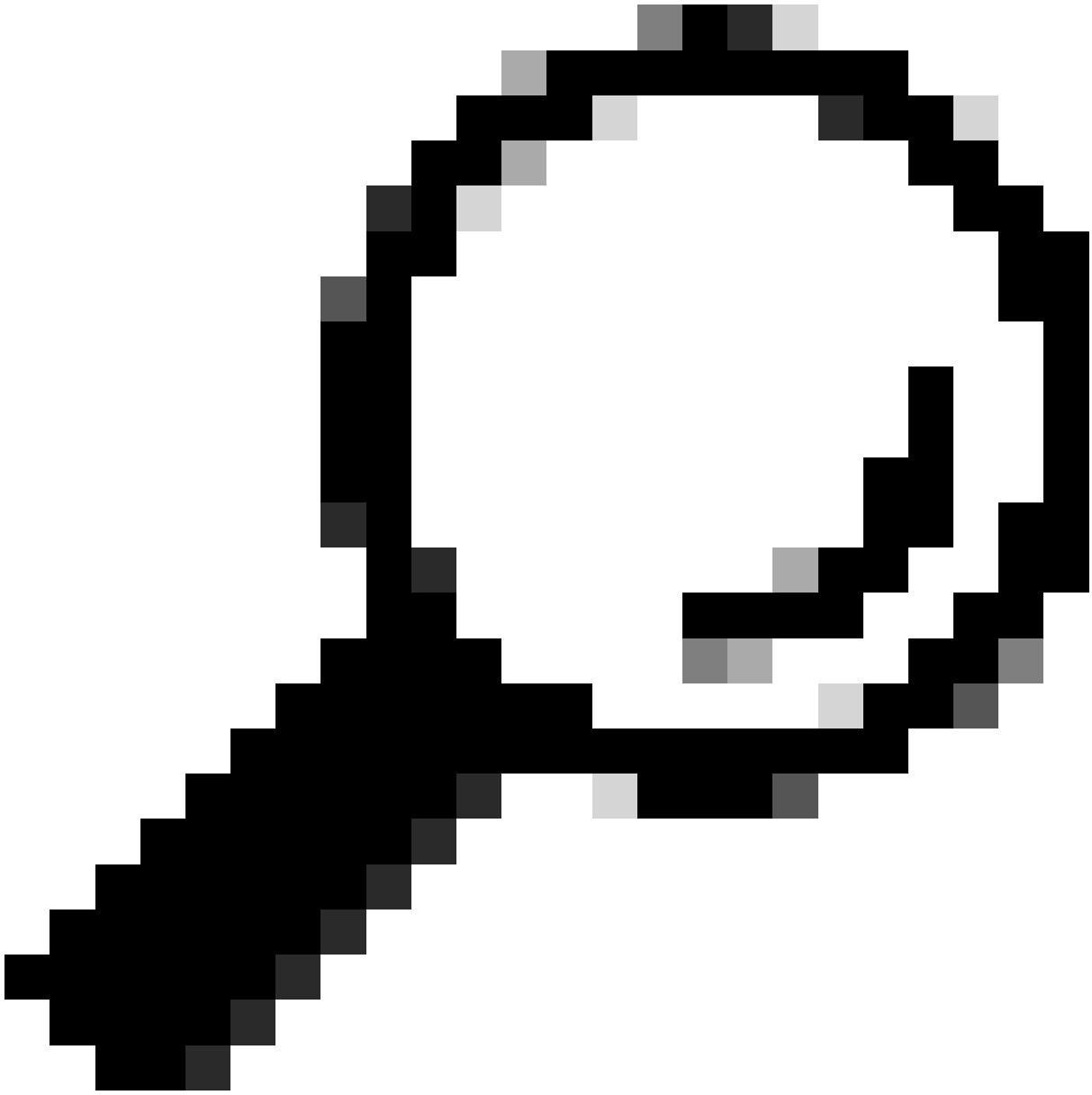
7

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

<--

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

  Totals - Source count: 1, Packet count: 8



Tip: Tip: Se uma entrada (S,G) não for encontrada ou se a Outgoing Interface List (OIL) não contiver interfaces de saída (OIFs), isso indica um problema com a configuração ou operação multicast subjacente.

Capturas de pacotes

Configure uma captura simultânea de pacotes incorporada no switch para registrar o pacote DHCP de entrada do AP e o pacote de saída correspondente para a inundação de L2.

Capturas de pacotes 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
```

Na captura de pacotes, três pacotes distintos devem ser observados:

- Descoberta de DHCP - VXLAN - AP para borda
- Descoberta de DHCP - CAPWAP - AP para WLC
- Descoberta de DHCP - VXLAN - Edge para grupo 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

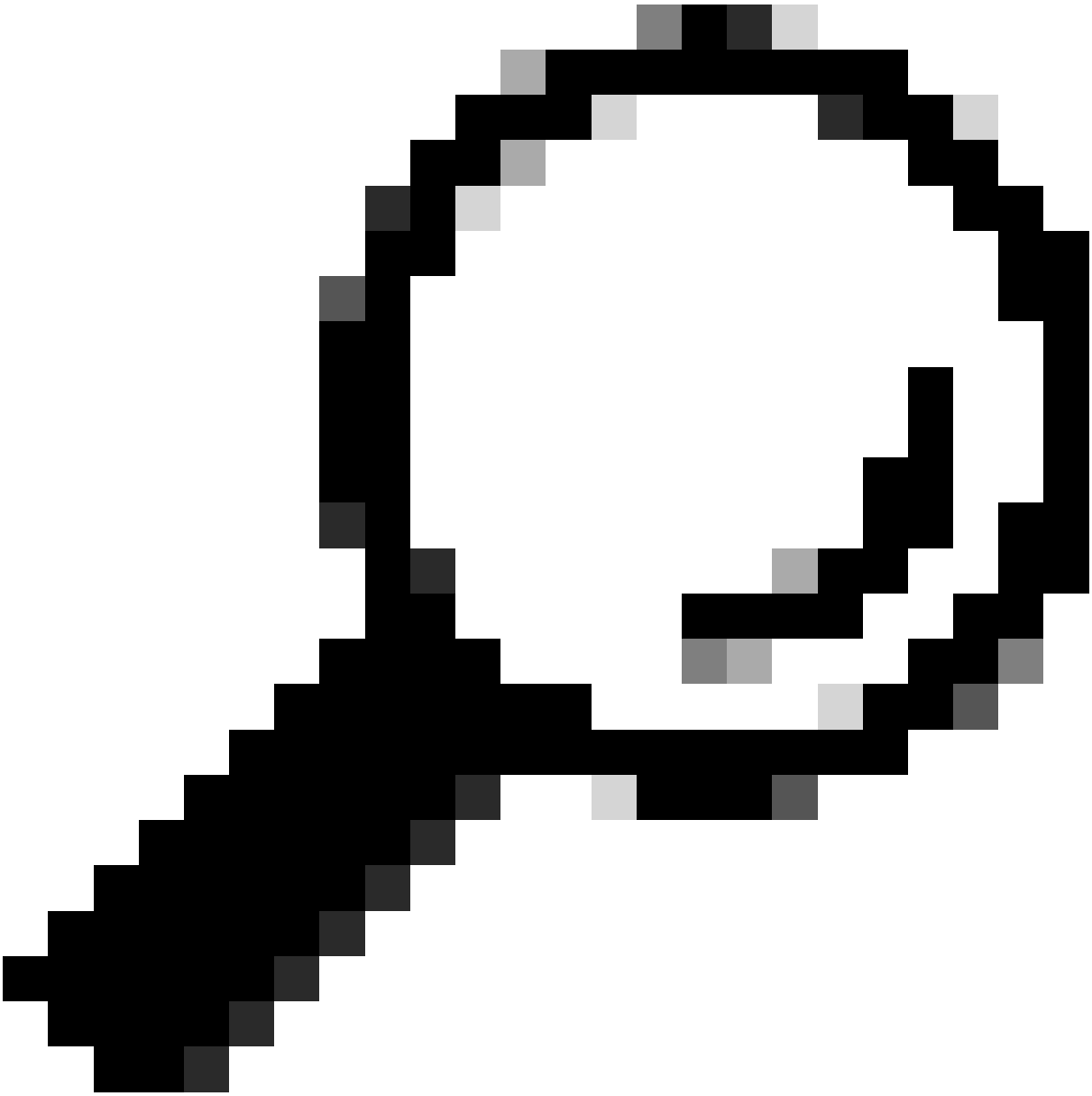
```
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
Internet Protocol Version 4, Src:
```

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



Tip: Na rede sem fio habilitada para matriz, os pacotes encapsulados de VXLAN fornecem o tráfego DHCP aos clientes ou servidores. Os pacotes encapsulados CAPWAP DATA (UDP 5247), no entanto, transmitem para a WLC somente para fins de rastreamento, como o estado IP Learn ou Wireless Device-Tracking.

Descoberta e solicitação DHCP - Borda L2

Depois que a borda envia os pacotes de descoberta e solicitação de DHCP através da inundação da camada 2, encapsulada com o grupo de transmissão subjacente 239.0.17.1, esses pacotes são recebidos pela borda de hand-off de L2, especificamente a borda/CP-1 neste cenário.

Para que isso ocorra, o Border/CP-1 deve possuir uma rota multicast com o (S,G) do Edge, e sua lista de interface de saída deve incluir a instância L2LISP da VLAN de Handoff L2. É importante observar que as Bordas de Transmissão L2 compartilham o mesmo L2LISP Instance-ID, mesmo que utilizem VLANs diferentes para a Transmissão.

<#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,

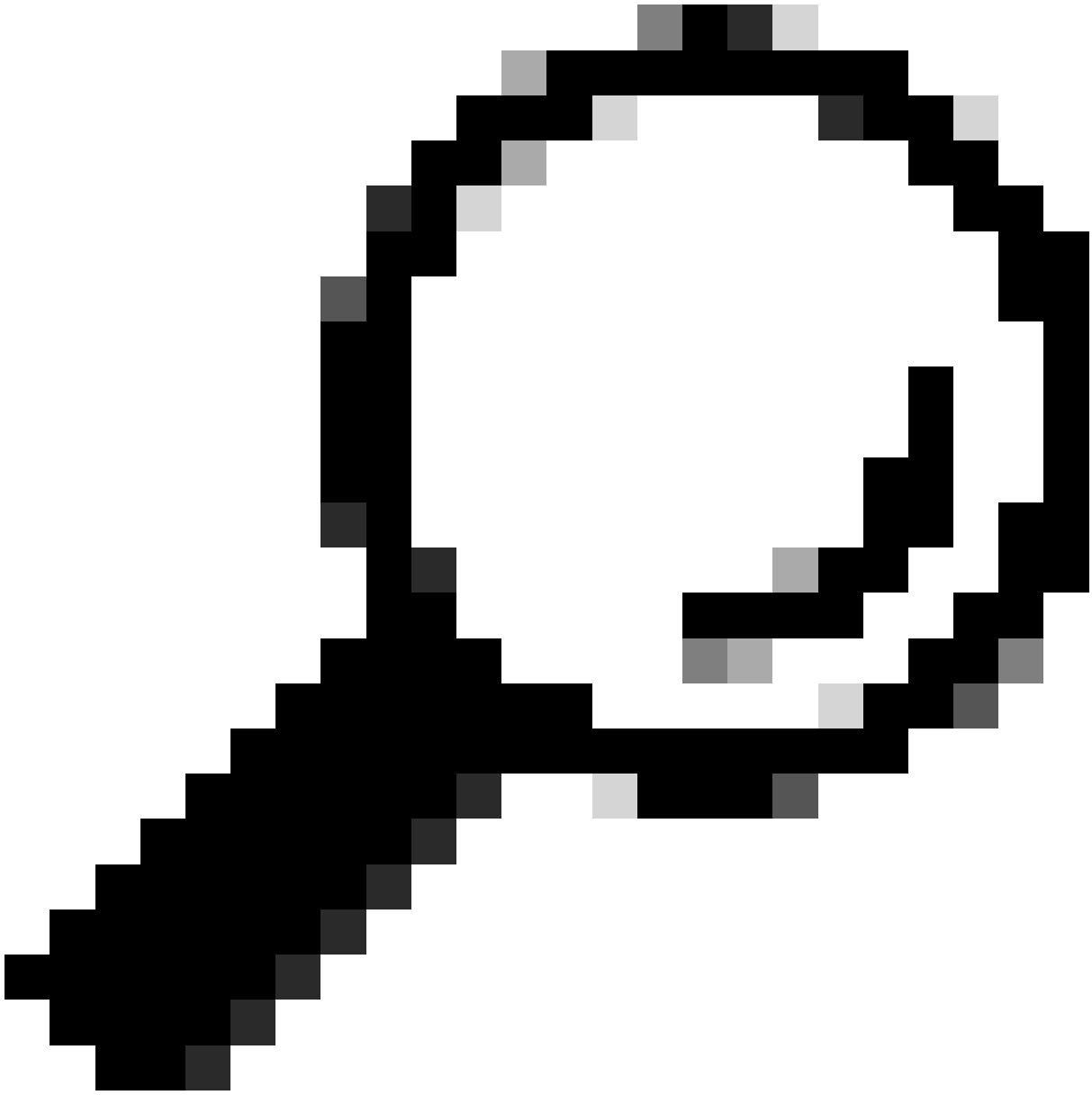
SW Forwarding: 1/0/392/0, Other: 0/0/0
HW Forwarding:

3

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

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

Totals - Source count: 1, Packet count: 4



Tip: Se uma entrada (S,G) não for encontrada, isso indica um problema com a configuração ou operação multicast subjacente. Se o L2LISP para a instância necessária não estiver presente como OIF, ele indicará um problema com o status de operação UP/DOWN da subinterface L2LISP ou o status de habilitação de IGMP da interface L2LISP.

Semelhante ao nó Fabric Edge, certifique-se de que nenhuma entrada de controle de acesso negue o pacote DHCP de entrada na interface 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
```

Depois que o pacote é desencapsulado e colocado na VLAN correspondente ao VNI 8240, sua natureza de broadcast determina que ele é inundado por todas as portas de encaminhamento do Spanning Tree Protocol para a VLAN 141 de entrega.

<#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
```

A tabela Rastreamento de Dispositivo confirma que a interface Te1/0/44, que se conecta ao Gateway/Retransmissão DHCP, deve ser uma porta de encaminhamento 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
```

Capturas de pacotes

Configure uma captura de pacote incorporada simultânea no switch para registrar o pacote DHCP recebido da inundação de L2 (interface de entrada S,G) e o pacote de saída correspondente para o relé DHCP. Na captura do pacote, dois pacotes distintos devem ser observados: o pacote encapsulado de VXLAN de Edge-1 e o pacote desencapsulado que vai para o DHCP Relay.

Capturas de pacotes Fabric Border/CP (192.168.0.201)

<#root>

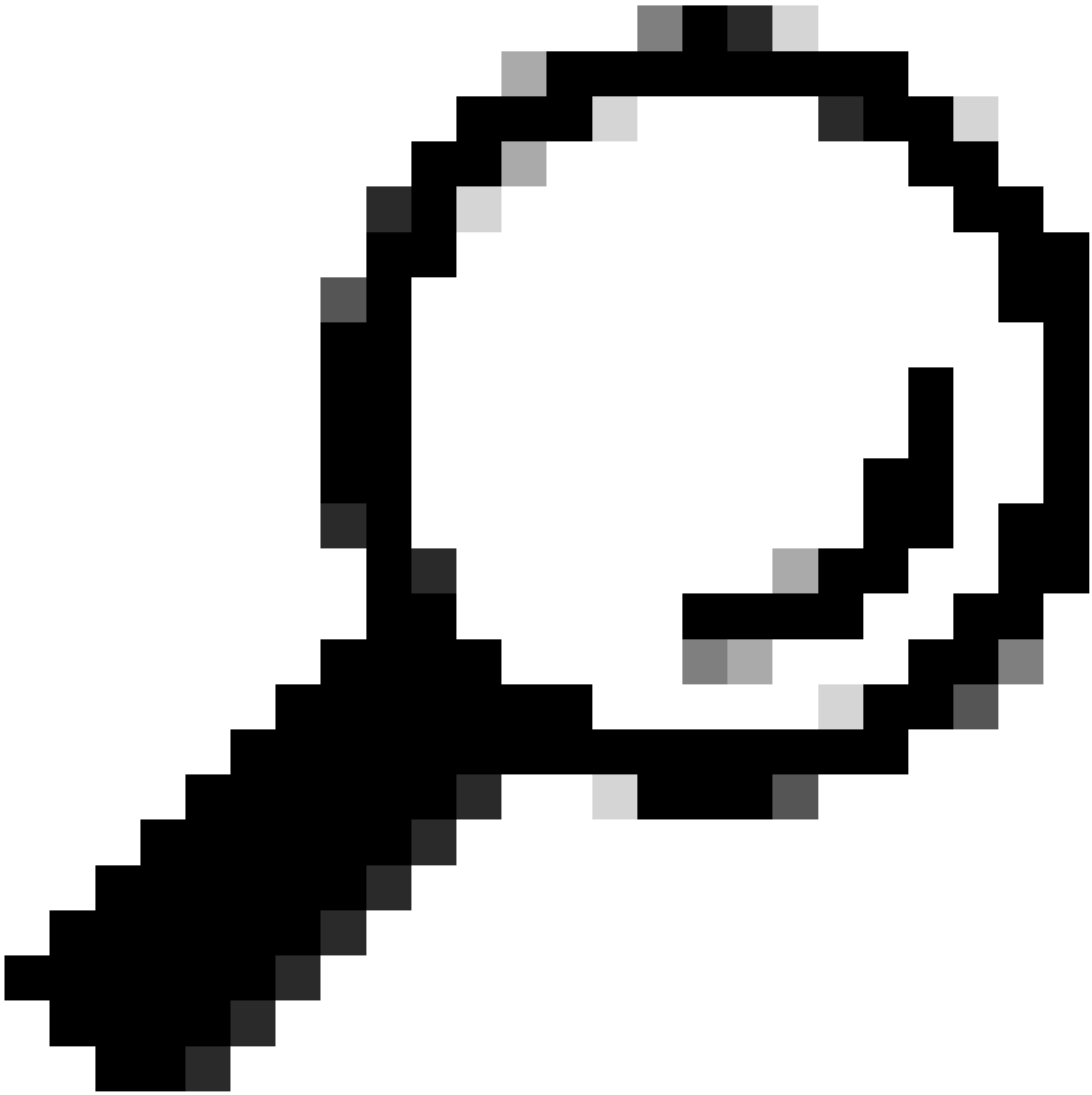
```
monitor capture cap interface TenGigabitEthernet1/0/42 IN

<--

 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
```

Neste ponto, o pacote Discover/Request saiu da estrutura SD-Access, concluindo esta seção. No entanto, antes de continuar, um parâmetro crucial — o Sinalizador de Broadcast DHCP, determinado pelo próprio ponto final — ditará o cenário de encaminhamento para pacotes Offer ou ACK subsequentes. Podemos examinar um de nossos pacotes Discover para inspecionar essa flag.

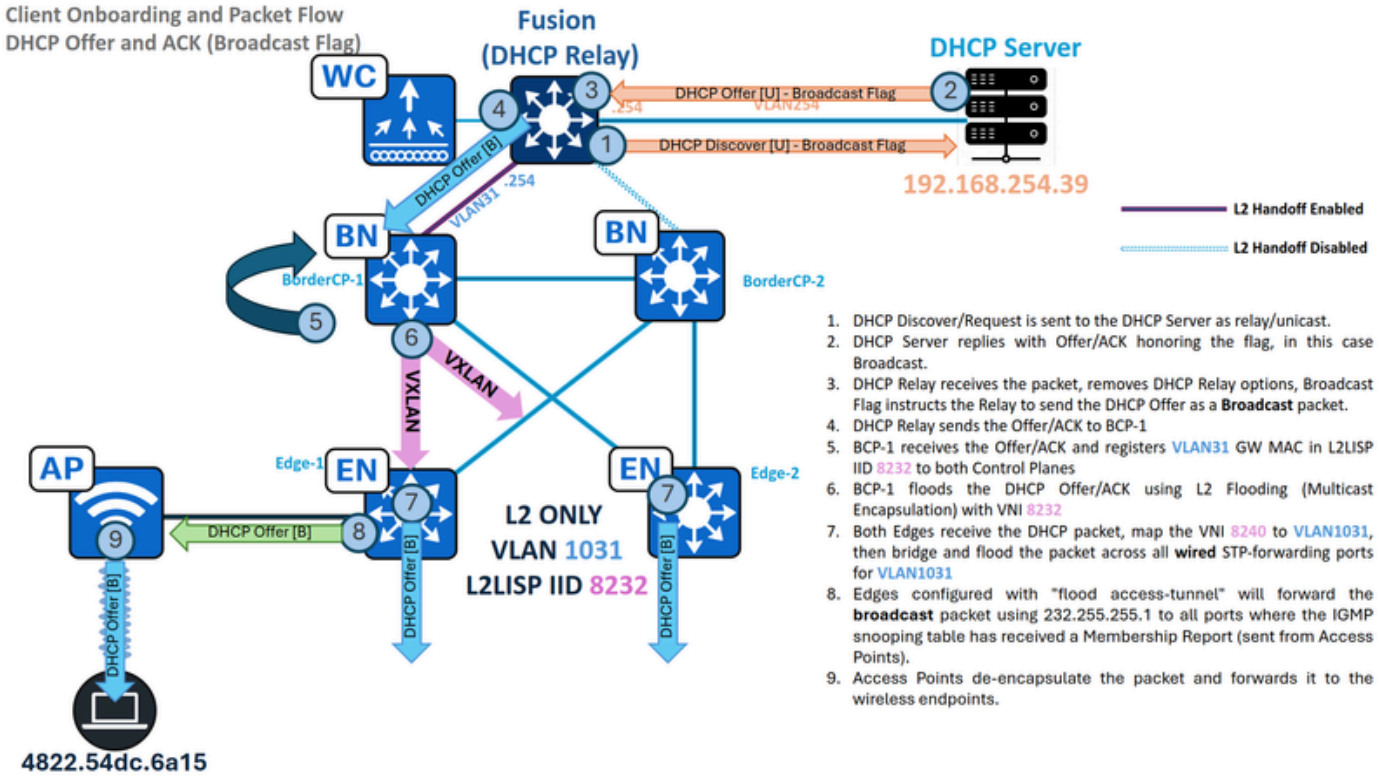
```
<#root>
BorderCP-1#
show monitor capture cap buffer display-filter "bootp.type==1 and dhcp.hw.mac_addr==4822.54dc.6a15
" detailed | sect Dynamic


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
```



Tip: O bootp.type==1 pode ser usado para filtrar apenas pacotes Discover e Request.

Oferta DHCP e ACK - Broadcast - Borda L2



Fluxo de tráfego - oferta de broadcast DHCP e ACK somente em L2

Agora que a Descoberta de DHCP saiu da malha de Acesso SD, a retransmissão de DHCP inserirá as Opções tradicionais de Retransmissão de DHCP (por exemplo, GiAddr/GatewayIPAddress) e encaminhará o pacote como uma transmissão unicast para o Servidor DHCP. Nesse fluxo, a estrutura de acesso SD não anexa nenhuma opção especial de DHCP.

Após a chegada de uma descoberta/solicitação de DHCP ao servidor, o servidor honra o sinalizador Broadcast ou Unicast incorporado. Essa flag determina se o Agente de Retransmissão DHCP encaminha a Oferta DHCP para o dispositivo downstream (nossas Bordas) como um quadro de broadcast ou unicast. Para esta demonstração, presume-se um cenário de broadcast.

Aprendizado MAC e registro de gateway

Quando o relé DHCP envia uma oferta DHCP ou ACK, o nó L2BN deve aprender o endereço MAC do gateway, adicioná-lo à sua tabela de endereços MAC, depois à tabela SISF L2/MAC e, finalmente, ao banco de dados L2LISP para a VLAN 141, mapeada para a instância 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 o endereço MAC do gateway for aprendido corretamente e a flag ACK tiver sido marcada como "Sim" para os planos de Controle de estrutura, essa etapa será considerada concluída.

Transmissão DHCP ligada em inundação de L2

Sem o rastreamento de DHCP habilitado, os broadcasts de DHCP não são bloqueados e são encapsulados em multicast para a inundação da camada 2. Por outro lado, se o rastreamento de DHCP estiver habilitado, a inundação de pacotes de broadcast de DHCP será impedida.

```
<#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
```

Como o DHCP Snooping não está habilitado na L2Border, a configuração DHCP Snooping Trust não é necessária.

Neste estágio, a validação da ACL L2LISP já é feita em ambos os dispositivos.

Utilize o grupo de broadcast-underlay configurado para a instância L2LISP e o endereço IP L2Border Loopback0 para verificar a entrada L2 Flooding (S,G) que conectará esse pacote a outros nós de estrutura. Consulte as tabelas mroute e mfib para validar parâmetros como a interface de entrada, a lista de interfaces de saída e os contadores de encaminhamento.

```
<#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

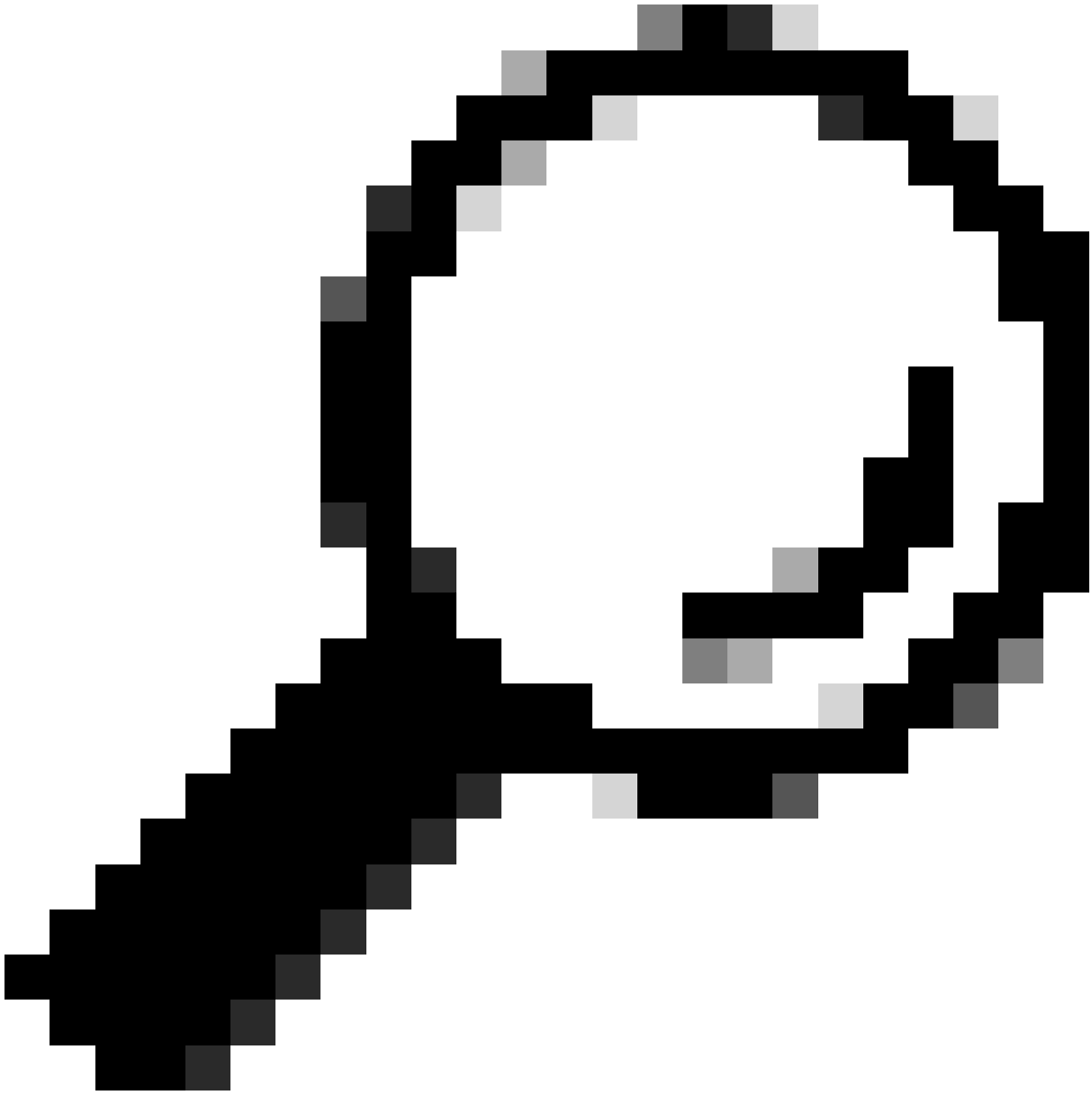
,
   SW Forwarding: 1/0/392/0, Other: 1/1/0
   HW Forwarding:

92071

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

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

  Totals - Source count: 1, Packet count: 92071



Tip: Se uma entrada (S,G) não for encontrada ou se a Outgoing Interface List (OIL) não contiver interfaces de saída (OIFs), isso indica um problema com a configuração ou operação multicast subjacente.

Com essas validações, junto com capturas de pacotes semelhantes às etapas anteriores, concluímos esta seção, pois a oferta DHCP será encaminhada como um broadcast para todas as Bordas de estrutura usando o conteúdo da lista de interfaces de saída, neste caso, fora da interface TenGig1/0/42 e TenGig1/0/43.

Oferta DHCP e ACK - Broadcast - Borda

Exatamente como no fluxo anterior, agora verificamos o L2Border S,G no Fabric Edge, onde a interface de entrada aponta para o L2BN e o OIL contém a instância L2LISP mapeada para a 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,

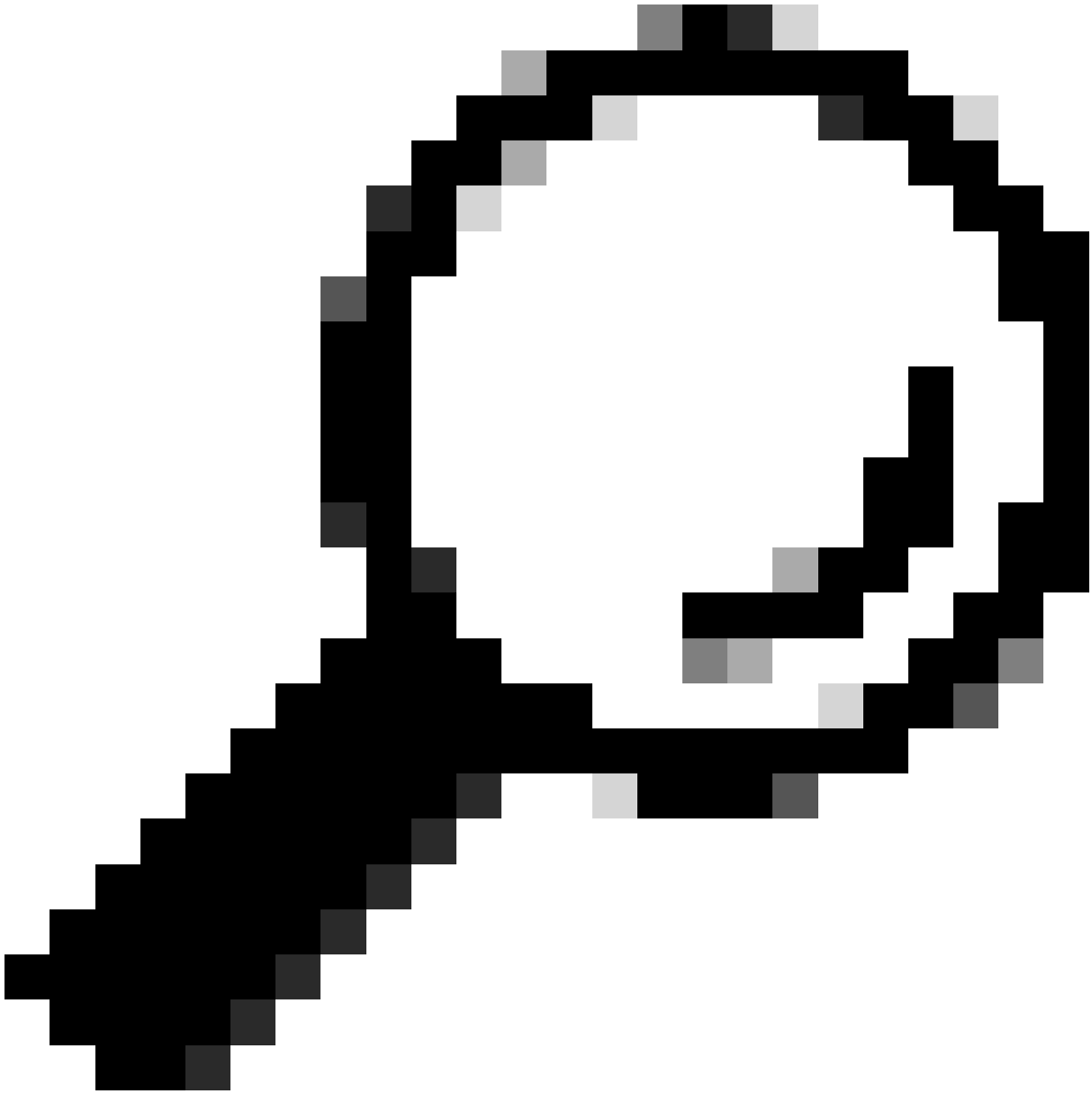
```
   SW Forwarding: 1/0/96/0, Other: 0/0/0
   HW Forwarding:
```

76236

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

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

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



Tip: Se uma entrada (S,G) não for encontrada, isso indica um problema com a

---

configuração ou operação multicast subjacente. Se o L2LISP para a instância necessária não estiver presente como OIF, ele indicará um problema com o status de operação UP/DOWN da subinterface L2LISP ou o status de habilitação de IGMP da interface L2LISP.

A validação da ACL L2LISP já foi feita em ambos os dispositivos.

Depois que o pacote é desencapsulado e colocado na VLAN correspondente ao VNI 8232, sua natureza de broadcast determina que ele é inundado por todas as portas de encaminhamento de protocolo de árvore de abrangência com fio para 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
```

No entanto, a interface que estamos procurando para transmitir a oferta DHCP é a interface de túnel de acesso associada ao ponto de acesso. Isso só é possível porque "flood access-tunnel" está habilitado no L2LISP IID 8232, caso contrário esse pacote será bloqueado para ser encaminhado para a interface 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
```

Com a entrada de rastreamento IGMP para o grupo de inundação de multicast, as ofertas e ACKs DHCP são encaminhadas à porta física do AP.

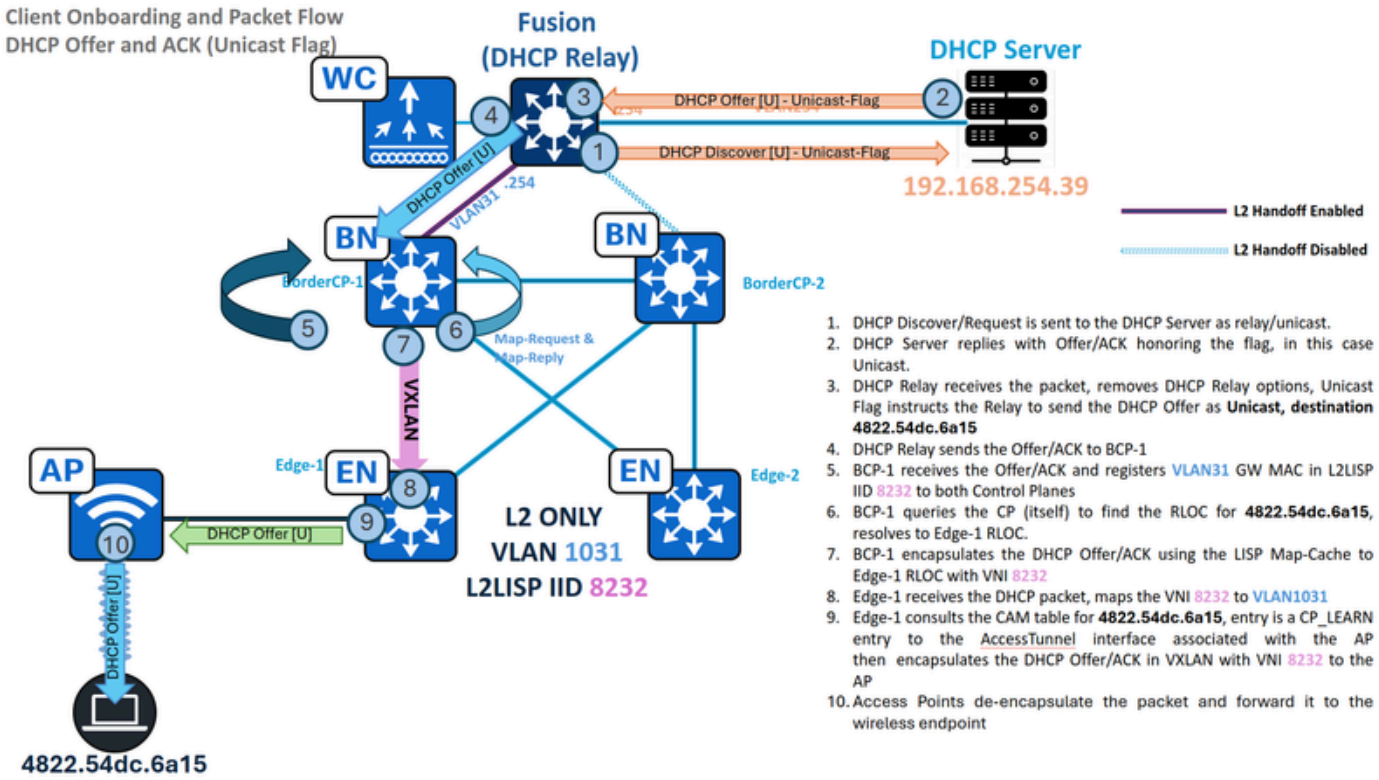
O processo DHCP Offer e ACK permanece consistente. Sem o rastreamento de DHCP habilitado, nenhuma entrada é criada na tabela de rastreamento de DHCP. Consequentemente, a entrada Device-Tracking para o ponto final habilitado por DHCP é gerada por pacotes ARP coletados. Também é esperado que comandos como "show platform dhcpsnooping client stats" não exibam dados, pois o rastreamento de DHCP está desabilitado.

<#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
```

Oferta DHCP e ACK - Unicast - Borda L2



Fluxo de tráfego - Oferta DHCP Unicast e ACK somente em L2

Aqui o cenário é um pouco diferente, o ponto final define o Sinalizador de broadcast DHCP como desdefinido ou "0".

O DHCP Relay não envia a oferta/ACK de DHCP como broadcast, mas como um pacote unicast, com um endereço MAC de destino derivado do endereço de hardware do cliente dentro do

payload de DHCP. Isso modifica drasticamente a maneira como o pacote é tratado pela estrutura de acesso SD, ele usa o L2LISP Map-Cache para encaminhar o tráfego, não o método de encapsulamento multicast de inundação de camada 2.

Captura de pacote Fabric Border/CP (192.168.0.201): Oferta DHCP de entrada

```
<#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)
```

Neste cenário, a Inundação de L2 é usada exclusivamente para Descoberta/Solicitações, enquanto Ofertas/ACKs são encaminhadas através de Caches de Mapa de L2LISP, simplificando a operação geral. Seguindo os princípios de encaminhamento unicast, a borda L2 consulta o plano de controle para obter o endereço MAC de destino. Supondo que a "Aprendizagem de MAC e Notificação de WLC" tenha sido bem-sucedida na Borda da Estrutura, o Plano de Controle tem essa ID de Endpoint (EID) registrada.

```
<#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
```

Após a consulta da borda ao plano de controle (local ou remoto), a resolução LISP estabelece uma entrada Map-Cache para o endereço MAC do ponto final.

```
<#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        -
```

Com o RLOC resolvido, a oferta DHCP é encapsulada em unicast e enviada diretamente para Edge-1 em 192.168.0.101, com 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
```

Com a mesma metodologia das seções anteriores, capture o tráfego de entrada do Relé DHCP e da interface de saída RLOC para observar o encapsulamento de VXLAN em unicast para o RLOC de Borda.

Oferta DHCP e ACK - Unicast - Borda

A borda recebe a oferta/ACK DHCP unicast da borda, desencapsula o tráfego e consulta sua tabela de endereços MAC para determinar a porta de saída correta. Diferentemente da oferta/ACKs de broadcast, o nó de borda encaminhará o pacote somente ao túnel de acesso específico onde o endpoint está conectado, em vez de inundá-lo para todas as portas.

A tabela de endereços MAC identifica a porta AccessTunnel2 como nossa porta virtual associada ao 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

O processo DHCP Offer e ACK permanece consistente. Sem o rastreamento de DHCP habilitado, nenhuma entrada será criada na tabela de rastreamento de DHCP. Consequentemente, a entrada de Rastreamento de dispositivo para o ponto final habilitado por DHCP é gerada por pacotes ARP obtidos, não por DHCP. Também é esperado que comandos como "show platform dhcpsnooping client stats" não exibam dados, pois o rastreamento de DHCP está desabilitado.

<#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
```

É importante observar que a estrutura de acesso SD não influencia o uso do sinalizador Unicast ou Broadcast, pois isso é apenas um comportamento de endpoint. Embora essa funcionalidade possa ser substituída pelo Relé DHCP ou pelo próprio Servidor DHCP, ambos os mecanismos são essenciais para a operação DHCP transparente em um ambiente Somente L2: Inundação de L2 com multicast subjacente para ofertas de broadcast/ACKs e registro de endpoint apropriado no plano de controle para oferta de unicast/ACKs.

Transação DHCP - Verificação sem fio

A partir da WLC, a transação DHCP é monitorada através de 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

No final da transação, o ponto final é adicionado ao banco de dados de rastreamento de dispositivo no controlador de LAN sem fio.

<#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

Toda a transação DHCP é depurada no próprio Ponto de acesso.

<#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**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.