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

Contents

Introdução

Este documento descreve como solucionar problemas de DHCP para terminais com 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

Requisitos de hardware e software

- Catalyst 9000 Series Switches
- Catalyst Center Versão 2.3.7.9
- 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

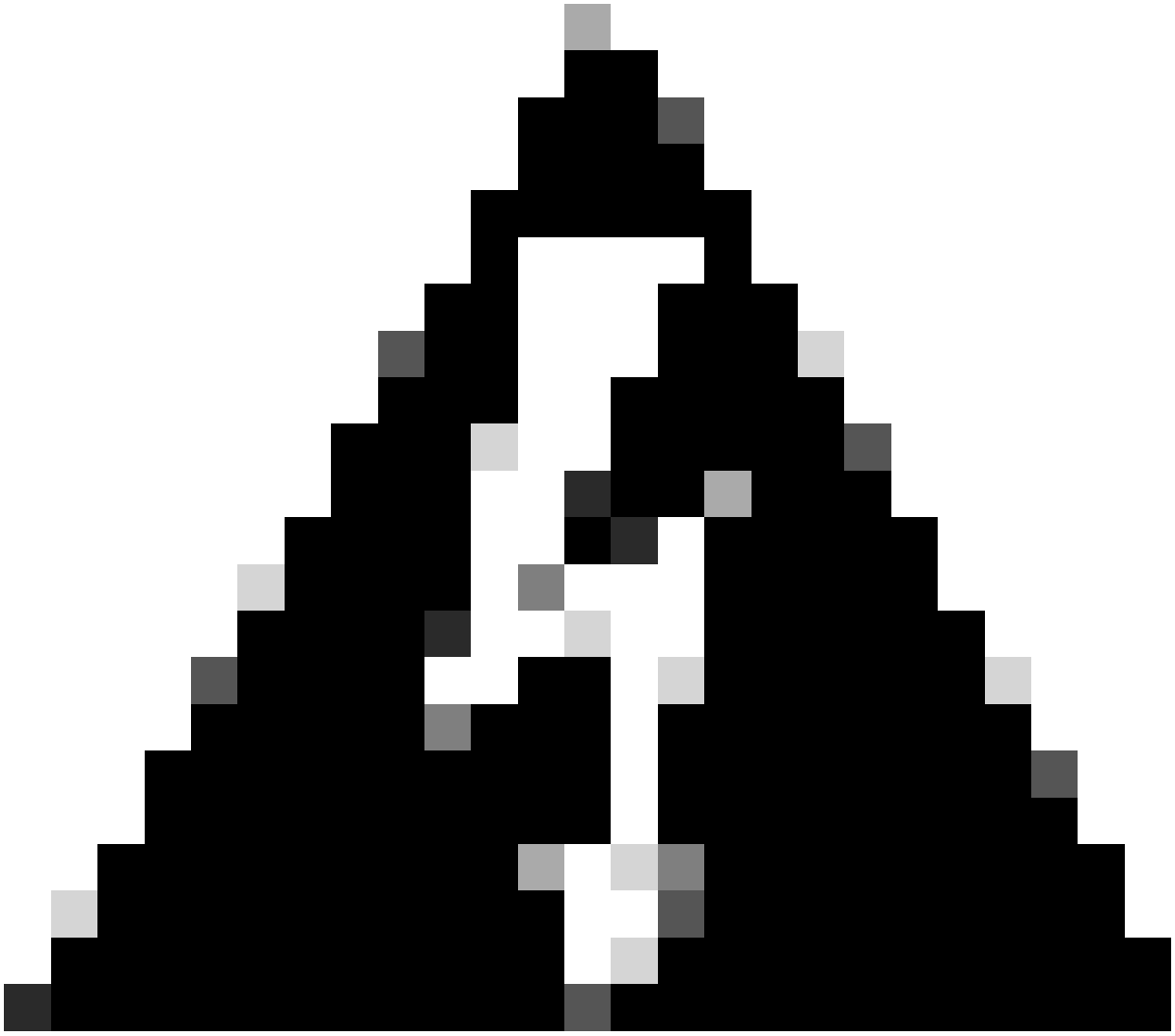
padrão, principalmente através de Caches de Mapa.

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.

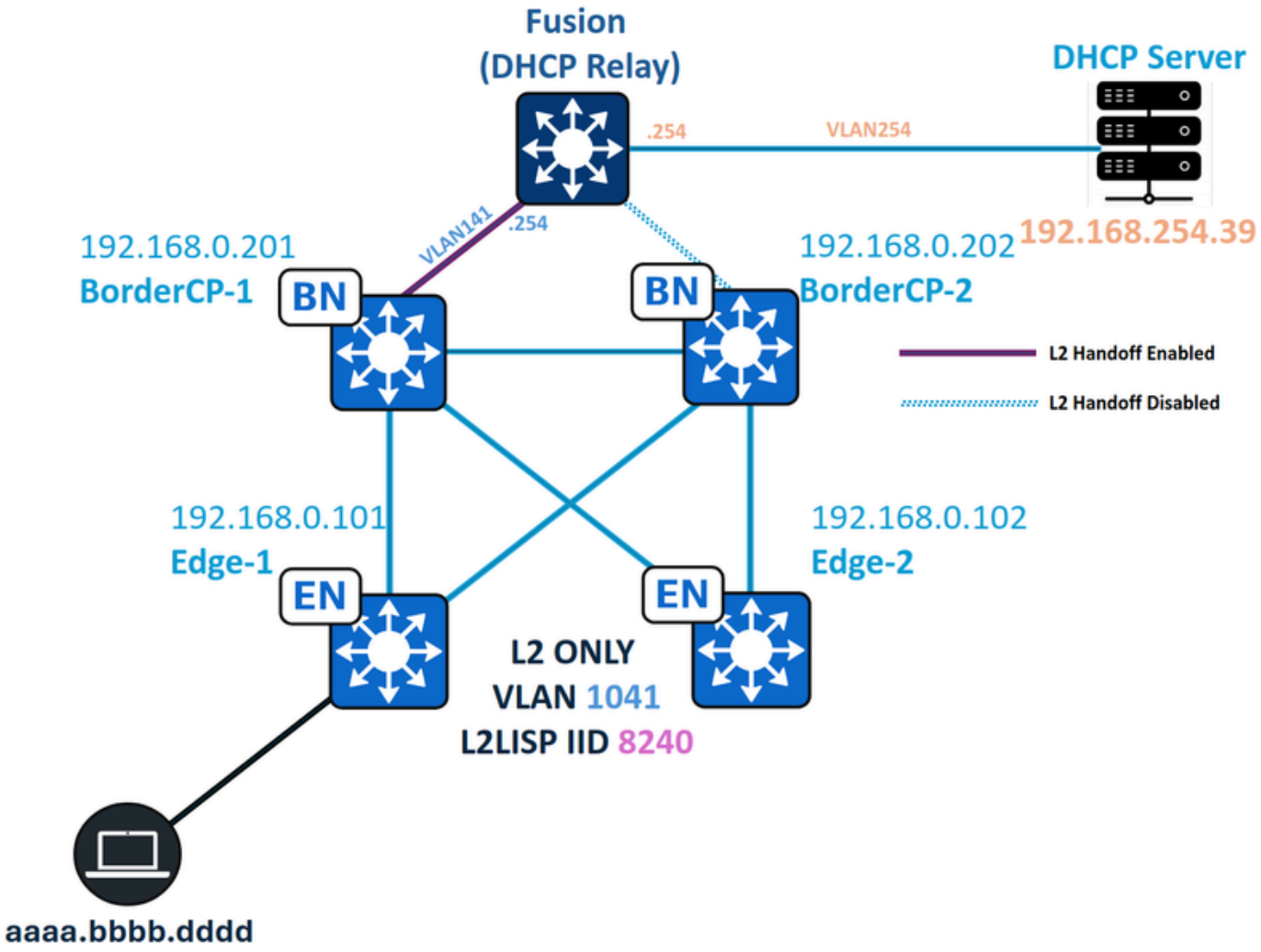
Servidor DHCP dentro da malha de acesso SD

Uma questão de design comum é se um servidor DHCP pode ser implantado em uma malha SD-Access. A resposta, no essencial, é sim e não.

O Cisco Validated Design oficial recomenda que o servidor DHCP seja colocado fora da estrutura, normalmente dentro do bloco Shared Services. No entanto, se as circunstâncias exigirem a conexão física do servidor DHCP a um nó de estrutura (por exemplo, uma borda ou borda), o único método suportado é através de uma rede L2 Only. Isso se deve ao comportamento inerente dos pools de Gateway Anycast, onde o rastreamento de DHCP é habilitado por padrão. Isso não apenas bloqueia as ofertas e confirmações DHCP do servidor, mas também impede que os pacotes de descoberta e solicitação DHCP, mesmo quando encapsulados em VXLAN, sejam encaminhados. Embora a "DHCP Snooping Trust" nas portas do servidor DHCP permita Ofertas e Confirmações, os pacotes de Descoberta e Solicitação não são encaminhados usando o mesmo método. Além disso, a remoção de rastreamento de DHCP em um pool de gateway Anycast não é uma opção suportada, pois o Catalyst Center sinaliza tal desvio de configuração durante a validação de conformidade.

Por outro lado, quando o servidor DHCP é colocado dentro de uma rede L2 Only, o DHCP Snooping não é imposto, permitindo que todos os pacotes DHCP passem sem inspeção ou bloqueio baseado em política. O dispositivo de rede upstream da estrutura SD-Access (por exemplo, um roteador Fusion) é configurado como o gateway para a rede L2 Only, permitindo que o tráfego de vários VRFs acesse o mesmo servidor DHCP dentro desse segmento L2 Only.

Topologia



Topologia de rede

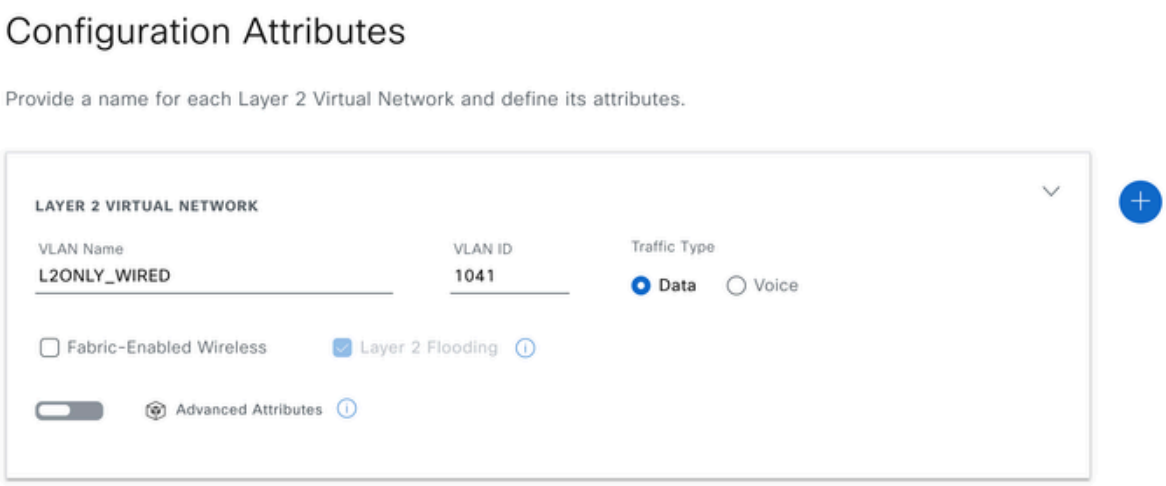
Nesta topologia:

- 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
- 192.168.254.39 é o servidor DHCP
- aaaa.bbbb.dddd é o ponto de extremidade 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

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 não é um pool Wireless; portanto, os recursos normalmente encontrados em pools sem fio somente L2, como RA-Guard, DHCPGuard e Flood Access Tunnel, não são configurados. Em vez disso, a inundação de pacotes ARP é explicitamente habilitada com "flood arp-nd"

Configuração da borda da malha (192.168.0.101)

<#root>

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


vlan
1041


name L2ONLY_WIRED


no ip igmp snooping vlan 1041 querier


no ip igmp snooping vlan 1041


no ipv6 mld snooping vlan 1041
```

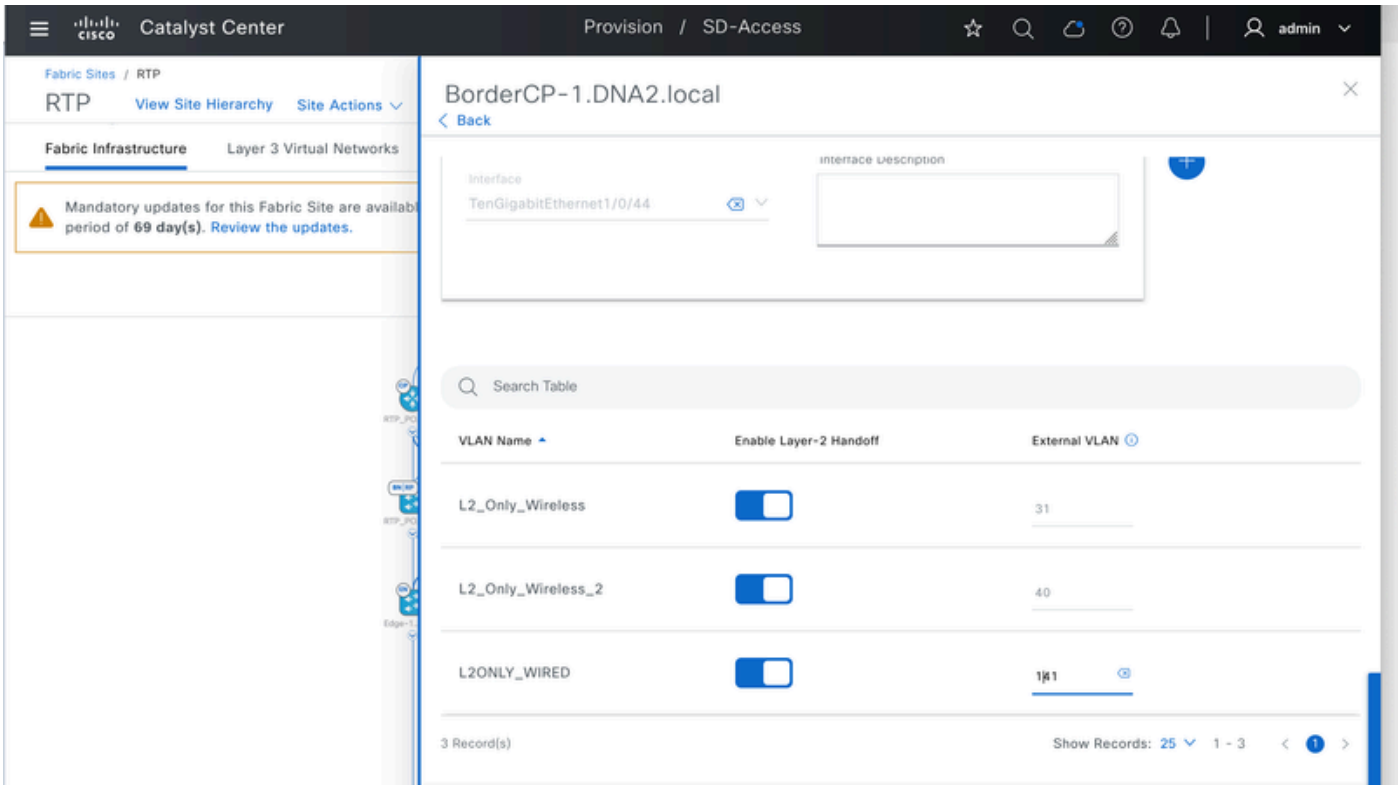
```
router lisp
 instance-id
8240

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

eid-table vlan

1041

   broadcast-underlay
239.0.17.1

flood arp-nd

 flood unknown-unicast

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

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 (192.168.0.201)

<#root>

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

141

```
vlan
```

141

name L2ONLY_WIRED

no ip igmp snooping vlan 141 querier

no ip igmp snooping vlan 141

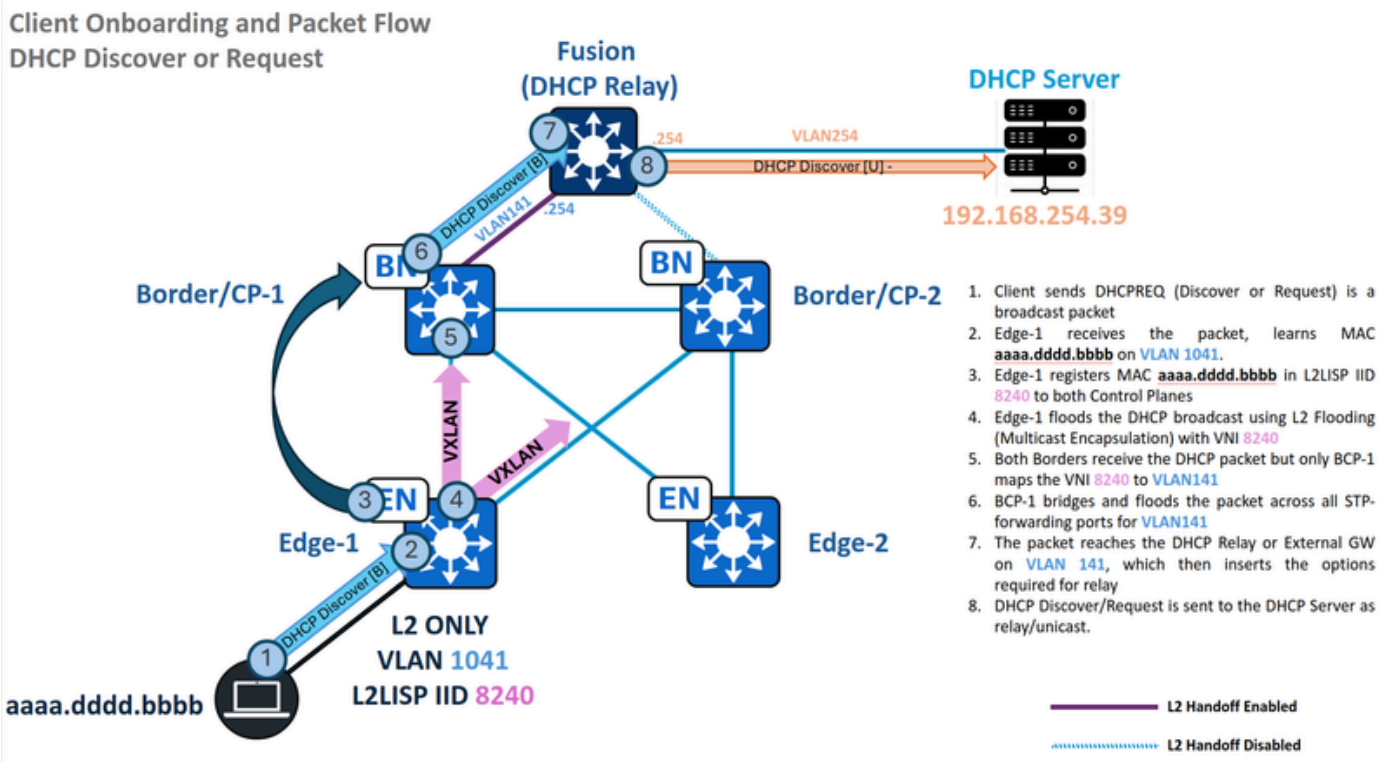
no ipv6 mld snooping vlan 141

```
router lisp
 instance-id
```

```
8240

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

eid-table


vlan 141



 broadcast-underlay 239.0.17.1


   flood arp-nd


   flood unknown-unicast


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

interface TenGigabitEthernet1/0/44


  switchport mode trunk
```

Fluxo de tráfego DHCP

Descoberta e solicitação DHCP - Borda



Fluxo de tráfego - Descoberta e solicitação de DHCP somente em L2

Aprendizado MAC e registro de endpoint

Quando o endpoint aaaa.dddd.bbbb envia uma Descoberta ou Solicitação DHCP (um pacote de broadcast), o nó de borda deve aprender o endereço MAC do endpoint, adicioná-lo à sua tabela de endereços MAC, depois à tabela SISF L2/MAC e, finalmente, ao Banco de Dados L2LISP para a VLAN 1041, mapeado para a Instância L2LISP 8240.

<#root>

Edge-1#

show mac address-table interface te1/0/2

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

1041

aaaa.dddd.bbbb

DYNAMIC

Te1/0/2

Edge-1#

show vlan id 1041

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

1041 L2ONLY_WIRED



active

    L2LI0:

8240

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

Edge-1#

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


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

Edge-1#

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


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

8240



aaaa.dddd.bbbb

   N/A           6d04h     never

0



Edge-1#

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


LISP ETR MAC Mapping Database for LISP 0 EID-table

Vlan 1041 (IID 8240)

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

aaaa.dddd.bbbb/48

,

dynamic-eid Auto-L2-group-8240

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

 192.168.0.101
```

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

  192.168.0.201

  6d04h

Yes

  0

  192.168.0.202

 6d04h

Yes

  0
```

Se o endereço MAC do ponto final for aprendido corretamente e a flag ACK tiver sido marcada como "Sim" para os planos de Controle de estrutura, esse estágio será considerado concluído.

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 is enabled


Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
12-13,50,52-53,333,1021-1026
DHCP snooping is operational on following VLANs:

12-13,50,52-53,333,1021-1026


<--

VLAN1041 should not be listed, as DHCP snooping must be disabled in L2 Only pools.


 Proxy bridge is configured on following VLANs:
1024
 Proxy bridge is operational on following VLANs:
1024
<snip>
```

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 8240

interface L2LISP0.8240

instance-id 8240

  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 1041

 broadcast-underlay 239.0.17.1

Edge-1#

show ip mroute 239.0.17.1 192.168.0.101 | be \(

(192.168.0.101, 239.0.17.1)

, 00:00:19/00:03:17, flags: FT
  Incoming interface:

Null0

, RPF nbr 0.0.0.0

<--

Local S,G IIF must be Null0

  Outgoing interface list:

 TenGigabitEthernet1/1/2

,

Forward

/Sparse, 00:00:19/00:03:10, flags:

<--

1st OIF = Te1/1/2 = Border2 Uplink

 TenGigabitEthernet1/1/1

,

Forward

/Sparse, 00:00:19/00:03:13, flags:

<--

2nd OIF = Te1/1/1 = Border1 Uplink

Edge-1#

show ip mfib 239.0.17.1 192.168.0.101 count

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

239.0.17.1

  Source:

192.168.0.101

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

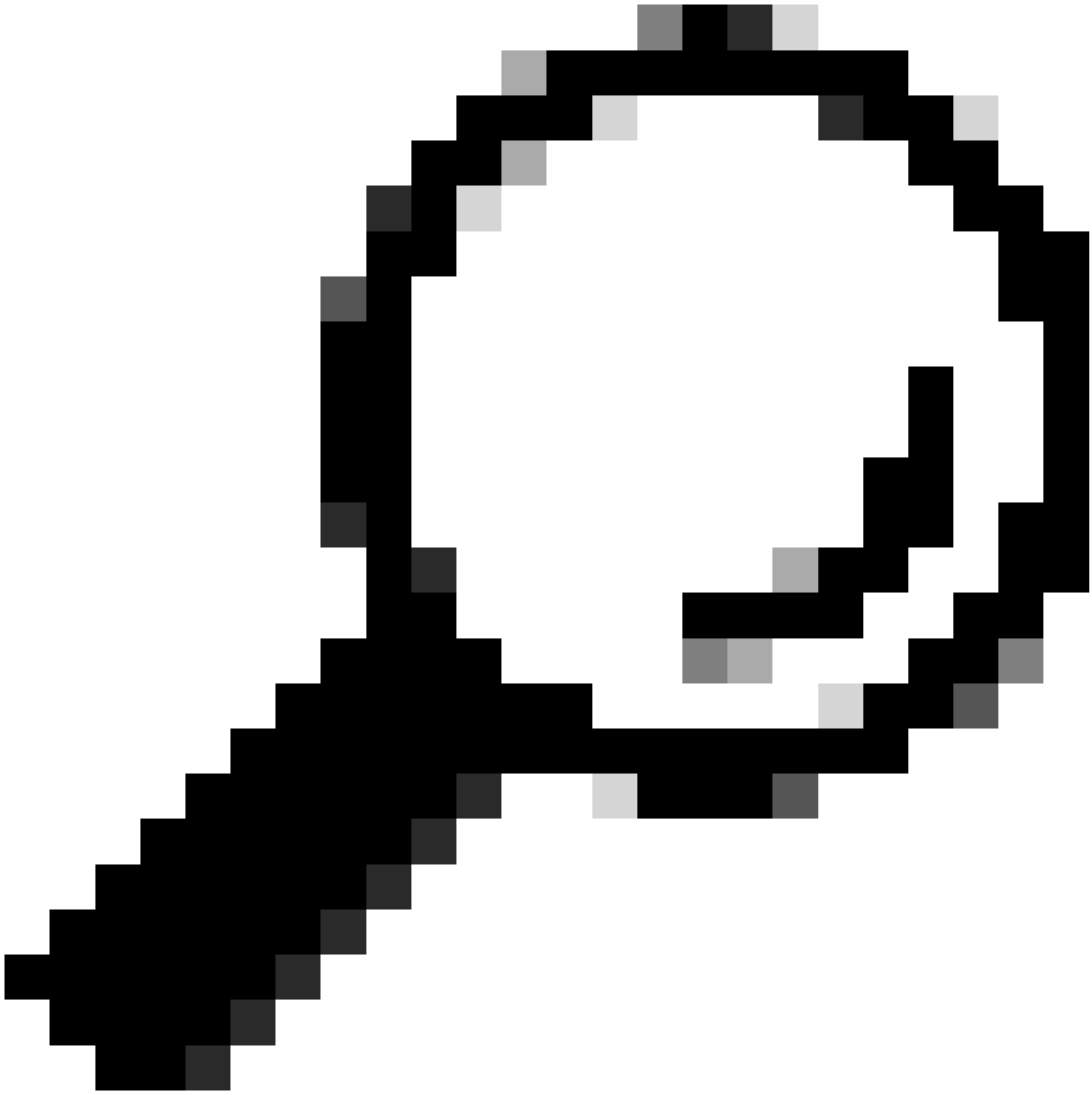
 7

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

<--

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

  Totals - Source count: 1, Packet count: 8



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 de pacote incorporada simultânea no switch para registrar o pacote DHCP recebido do ponto final e o pacote de saída correspondente para Inundação de L2. Na captura de pacote, dois pacotes distintos devem ser observados: o DHCP Discover/Request original e seu equivalente encapsulado em VXLAN, destinado ao Underlay Group (239.0.17.1).

Capturas de pacotes Fabric Edge (192.168.0.101)

<#root>

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

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

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

Edge-1#

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

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

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

356 DHCP Discover

 - Transaction ID 0xf8e

<--

356 is the Length of the original packet

   23   2.487037   0.0.0.0 -> 255.255.255.255 DHCP

406 DHCP Discover

 - Transaction ID 0xf8e

<--

406 is the Length of the VXLAN encapsulated packet

Edge-1#

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

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

406 DHCP Discover

 - Transaction ID 0xf8e

Edge-1#

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

Internet Protocol Version 4, Src:

192.168.0.101, Dst: 239.0.17.1 <-- DHCP Discover is encapsulated for Layer 2 Flooding

Internet Protocol Version 4, Src:

0.0.0.0, Dst: 255.255.255.255

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 transferência L2 compartilham a mesma Instance-ID L2LISP, mesmo que utilizem VLANs diferentes para a transferência.

<#root>

BorderCP-1#

show vlan id 141

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

141 L2ONLY_WIRED

active

L2LI0:

8240

, Te1/0/44

BorderCP-1#

show ip mroute 239.0.17.1 192.168.0.101 | be \(

(192.168.0.101, 239.0.17.1)

, 00:03:20/00:00:48, flags: MTA
Incoming interface:

TenGigabitEthernet1/0/42

, RPF nbr 192.168.98.3

<--

Incoming Interface Te1/0/42 is the RPF interface for 192.168.0.101 (Edge RLOC)

```
  Outgoing interface list:
   TenGigabitEthernet1/0/26, Forward/Sparse, 00:03:20/00:03:24, flags:
    L2LISP0.
```

8240

```
, Forward/Sparse-Dense, 00:03:20/00:02:39, flags:

BorderCP-1#
```

show ip mfib 239.0.17.1 192.168.0.101 count

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

239.0.17.1

```
  Source:
```

192.168.0.101

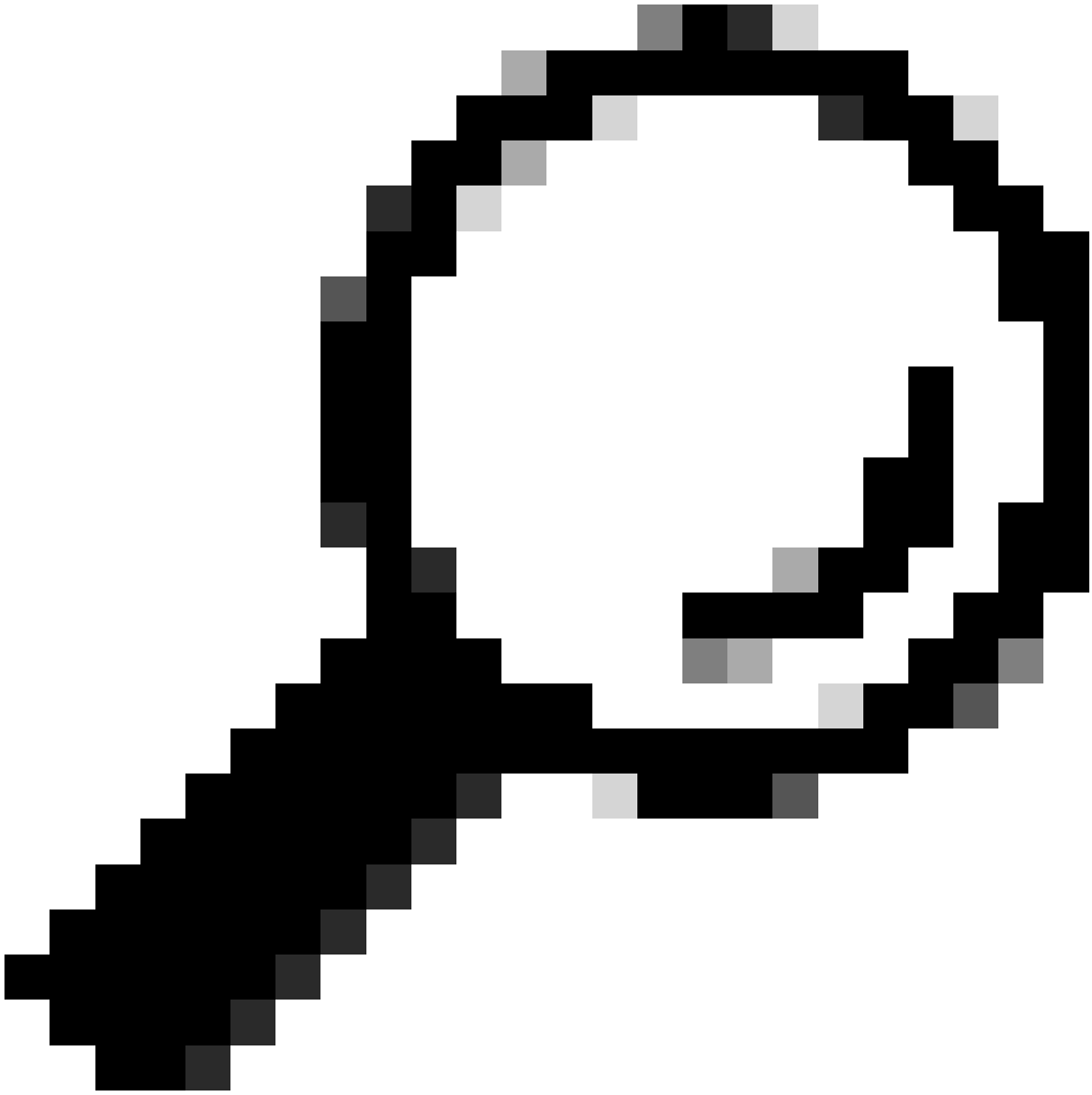
```
,
   SW Forwarding: 1/0/392/0, Other: 0/0/0
   HW Forwarding:
```

3

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

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

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



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 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
```

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 141 | 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
ARP

172.16.141.254


f87b.2003.7fc0


Te1/0/44


 141
```

```
       0005       133s       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    <-- Incoming interface for Edge's S,G Mrout

monitor capture cap interface TenGigabitEthernet1/0/44 OUT   <-- Interface that connects to the DHCP Rel

monitor capture cap match any

monitor capture cap buffer size 100

monitor capture cap start

monitor capture cap stop


BorderCP-1#
show monitor capture cap buffer display-filter "bootp and dhcp.hw.mac_addr==aaaa.dddd.bbbb"

Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  427  16.695022      0.0.0.0 -> 255.255.255.255 DHCP
406
 DHCP Discover - Transaction ID 0x2030
<-- 406 is the Lenght of the VXLAN encapsulated packet

  428  16.695053      0.0.0.0 -> 255.255.255.255 DHCP
364
 DHCP Discover - Transaction ID 0x2030
<-- 364 is the Lenght of the VXLAN encapsulated packet
```

Packet 427: VXLAN Encapsulated

BorderCP-1#

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

Internet Protocol Version 4, Src:

192.168.0.101, Dst: 239.0.17.1

Internet Protocol Version 4, Src:

0.0.0.0, Dst: 255.255.255.255

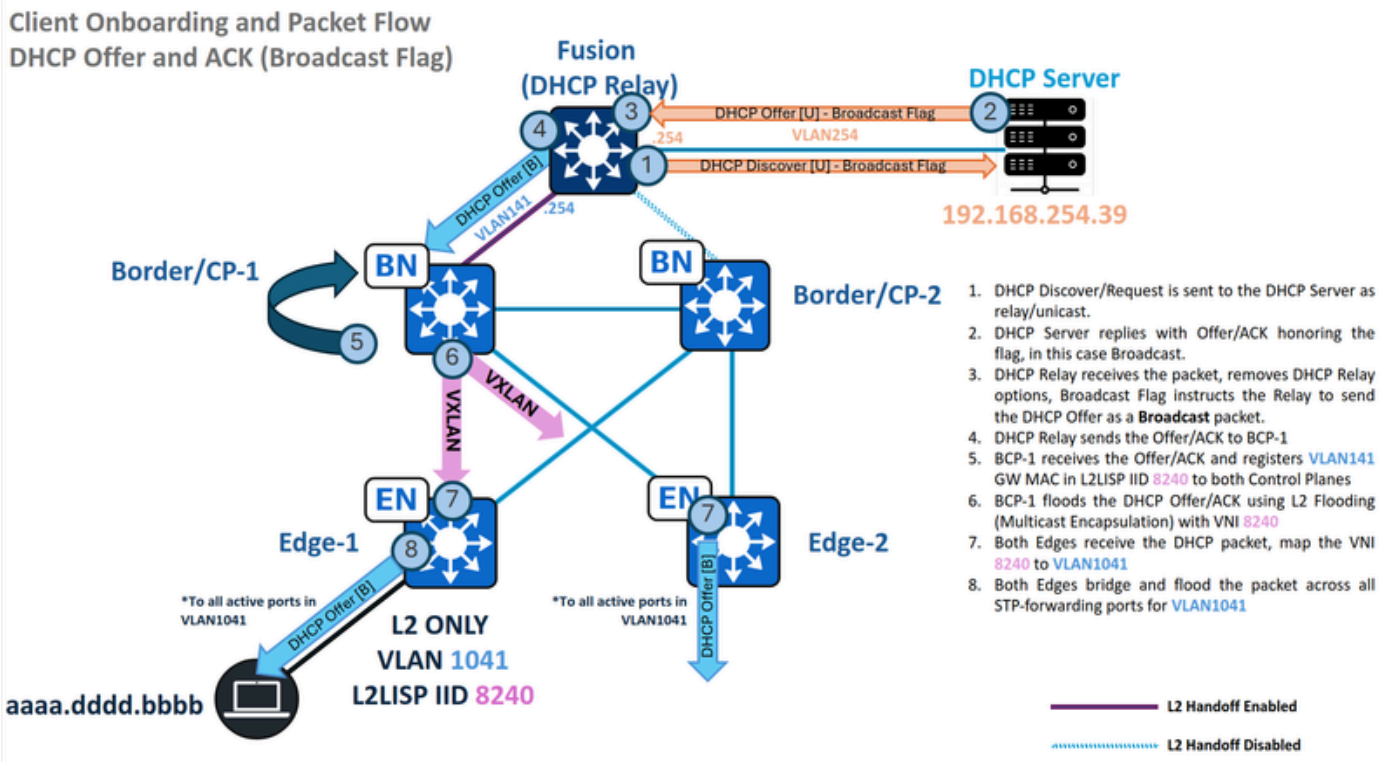
Packet 428: Plain (dot1Q cannot be captured at egress direction)

BorderCP-1#

show monitor capture cap buffer display-filter "bootp and dhcp.hw.mac_addr==aaaa.dddd.bbbb and not vxlan

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

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 insere as opções tradicionais de retransmissão de DHCP (por exemplo, GiAddr/GatewayIPAddress) e encaminha 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 8240.

<#root>

```
BorderCP-1#
show mac address-table interface te1/0/44

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

141

f87b.2003.7fc0
    DYNAMIC
Te1/0/44



BorderCP-1#
show vlan id 141

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

141

L2ONLY_WIRED
               active    L2LI0:
```

8240

,

Te1/0/44

BorderCP-1#

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

MAC Interface vlan prlvl state Time left Policy

f87b.2003.7fc0

Te1/0/44 141

NO TRUST

MAC-REACHABLE

61 s LISP-DT-GLEAN-VLAN 64

BorderCP-1#

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

Dyn-EID Name Dynamic-EID Interface Uptime Last Pending

Auto-L2-group-8240

f87b.2003.7fc0

N/A 6d06h never

0

BorderCP-1#

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

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

141

(IID

8240

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

f87b.2003.7fc0/48

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

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


 192.168.0.201

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


192.168.0.201

 6d06h

Yes

  0


192.168.0.202

  6d06h

Yes

  0
```

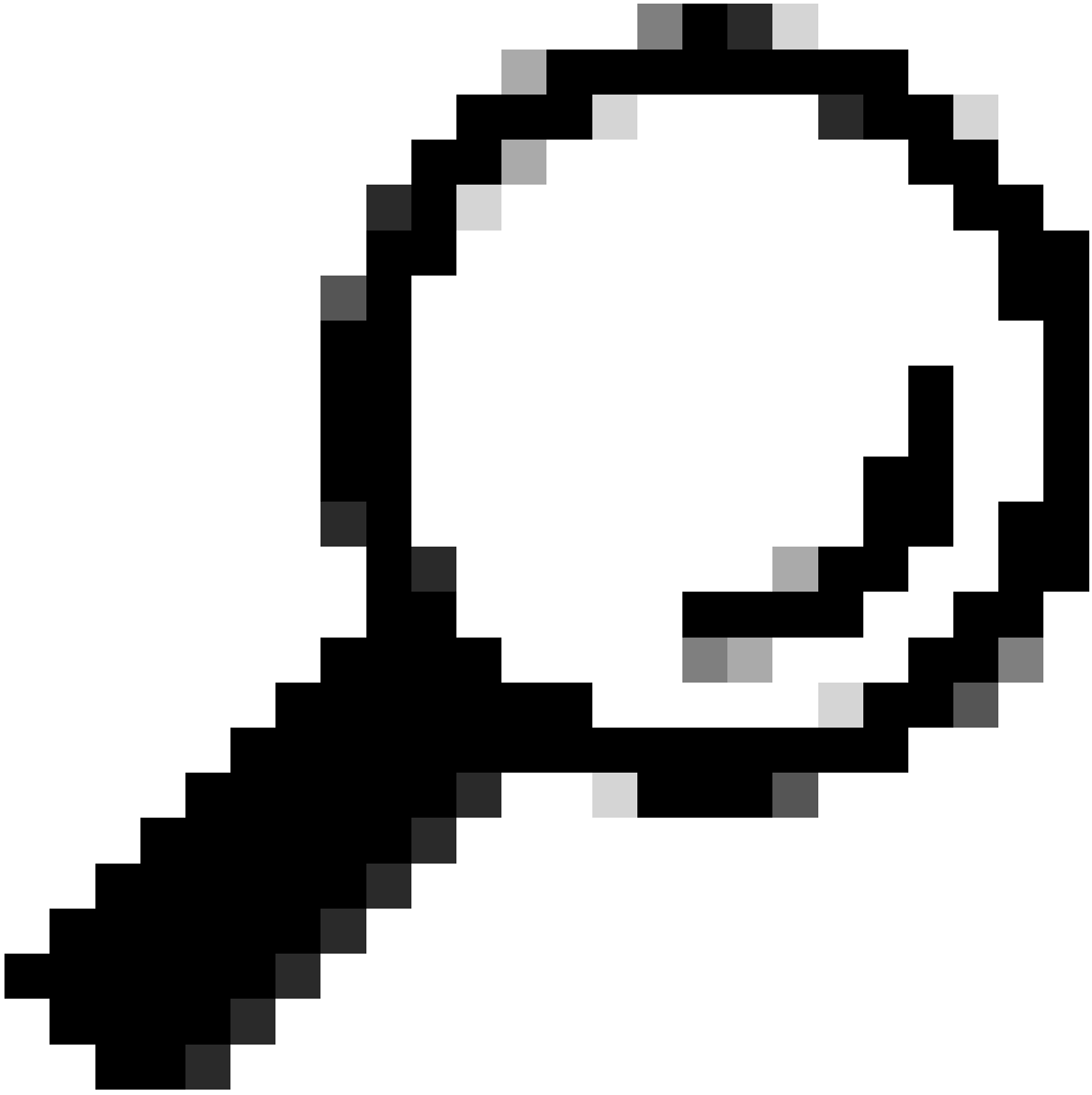
Se o endereço MAC do gateway for aprendido corretamente e a flag ACK tiver sido marcada como "Sim" para os planos de Controle de estrutura, essa etapa será considerada concluída.

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     <-- VLAN141 should not be listed, as DHCP snooping must be disabled in L2 Only pools.


 Proxy bridge is configured on following VLANs:
none
 Proxy bridge is operational on following VLANs:
none
```



Tip: 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 conecta 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 8240

interface L2LISP0.8240

instance-id 8240

  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 1041

broadcast-underlay 239.0.17.1

BorderCP-1#

show ip mroute 239.0.17.1 192.168.0.201 | be \(

(

192.168.0.201, 239.0.17.1

), 1w5d/00:02:52, flags: FTA
  Incoming interface:

Null0

, RPF nbr 0.0.0.0

<-- Local S,G IIF must be Null0

  Outgoing interface list:

TenGigabitEthernet1/0/42

, Forward/Sparse, 1w3d/00:02:52, flags:

<-- Edge1 Downlink

TenGigabitEthernet1/0/43

, Forward/Sparse, 1w3d/00:02:52, flags:

<-- Edge2 Downlink

BorderCP-1#

show ip mfib 239.0.17.1 192.168.0.201 count

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

239.0.17.1

  Source:

192.168.0.201

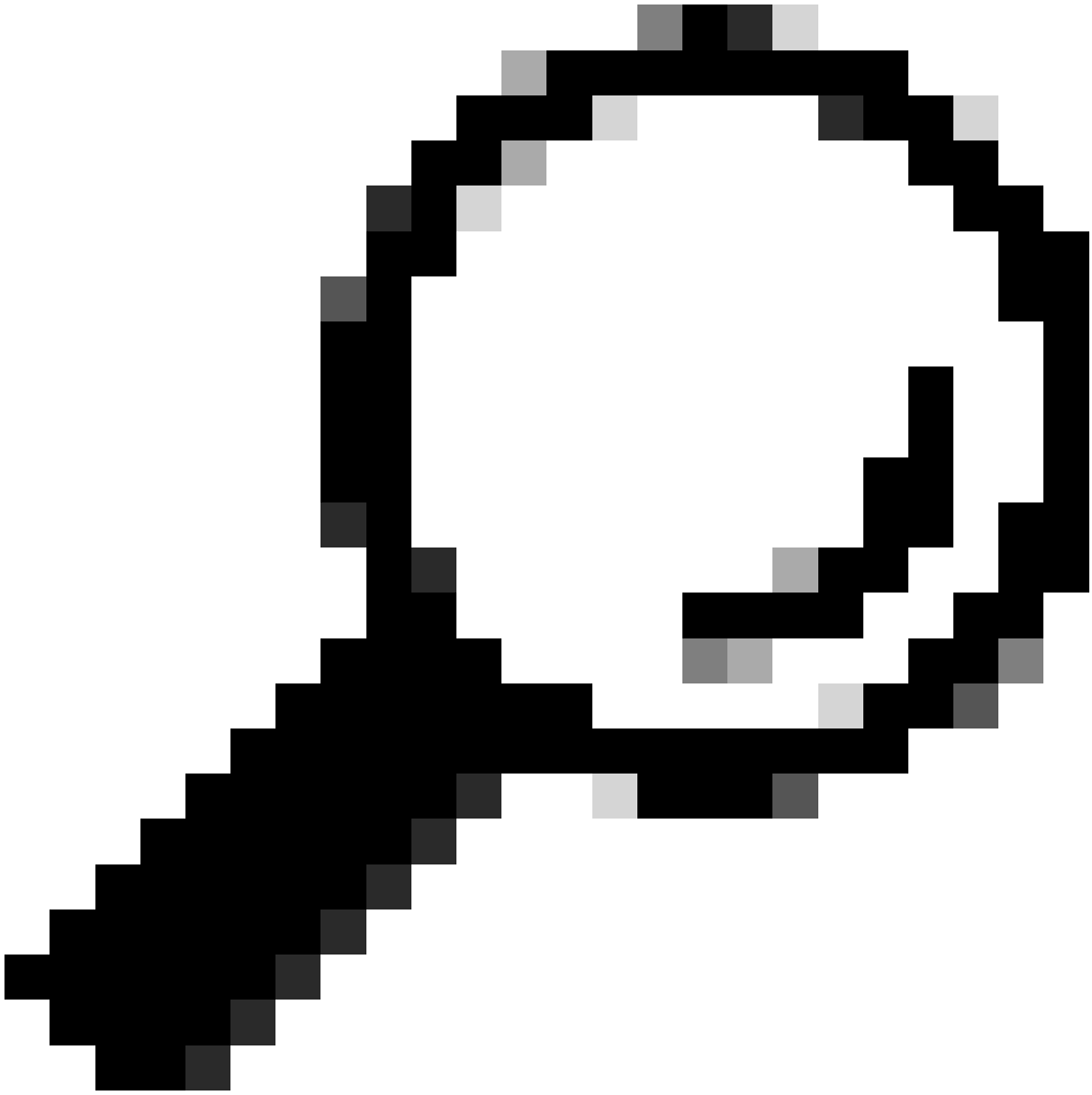
,
   SW Forwarding: 1/0/392/0, Other: 1/1/0
   HW Forwarding:

  92071

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

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

  Totals - Source count: 1, Packet count: 92071



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, esta seção é concluída, pois a oferta DHCP é encaminhada como um broadcast para todas as Bordas de estrutura usando o conteúdo da lista de interface 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, verifique o L2Border S,G na Borda da Estrutura, onde a interface de entrada aponta para o L2BN e o OIL contém a instância L2LISP mapeada para a VLAN 1041.

<#root>

Edge-1#

show vlan id 1041

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

1041

L2ONLY_WIRED

active

    L2LIO:

8240

,

Te1/0/2

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

Edge-1#

show ip mroute 239.0.17.1 192.168.0.201 | be \(

(

192.168.0.201

,

239.0.17.1

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

TenGigabitEthernet1/1/2

, RPF nbr 192.168.98.2

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

  Outgoing interface list:

L2LISP0.8240,

Forward/Sparse-Dense

,

 1w3d/00:02:23, flags:

Edge-1#

show ip mfib 239.0.17.1 192.168.0.201 count

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

239.0.17.1

  Source:

192.168.0.201,

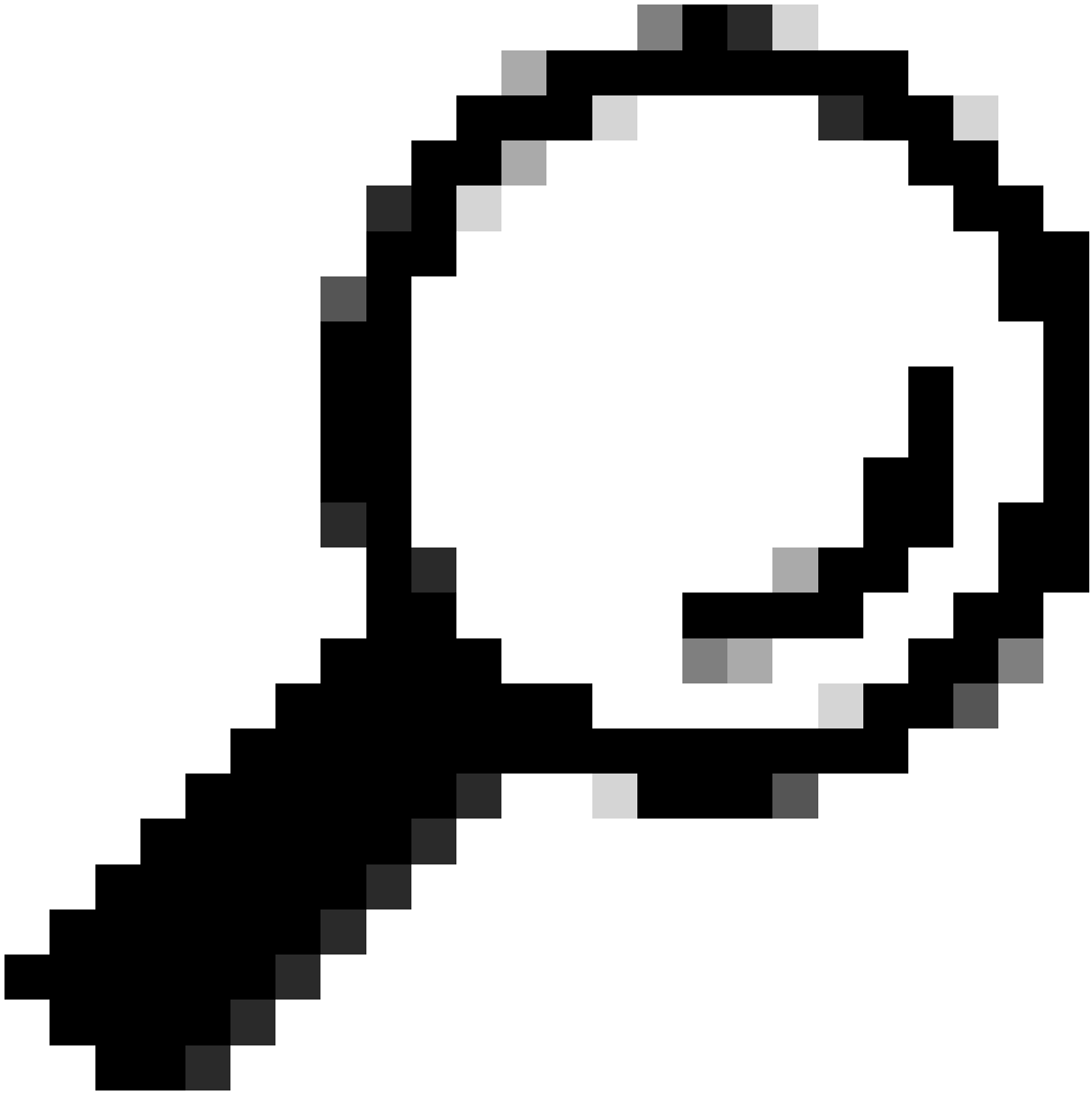
   SW Forwarding: 1/0/96/0, Other: 0/0/0
   HW Forwarding:

76236

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

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

  Totals - Source count: 1, Packet count: 4



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 8240, sua natureza de broadcast determina que ele é inundado por todas as portas de encaminhamento do Spanning Tree Protocol para VLAN1041.

<#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
```

A tabela de endereços MAC identifica a porta Te1/0/2 como a porta do ponto final, que está no estado FWD pelo STP, o pacote é enviado para o ponto final.

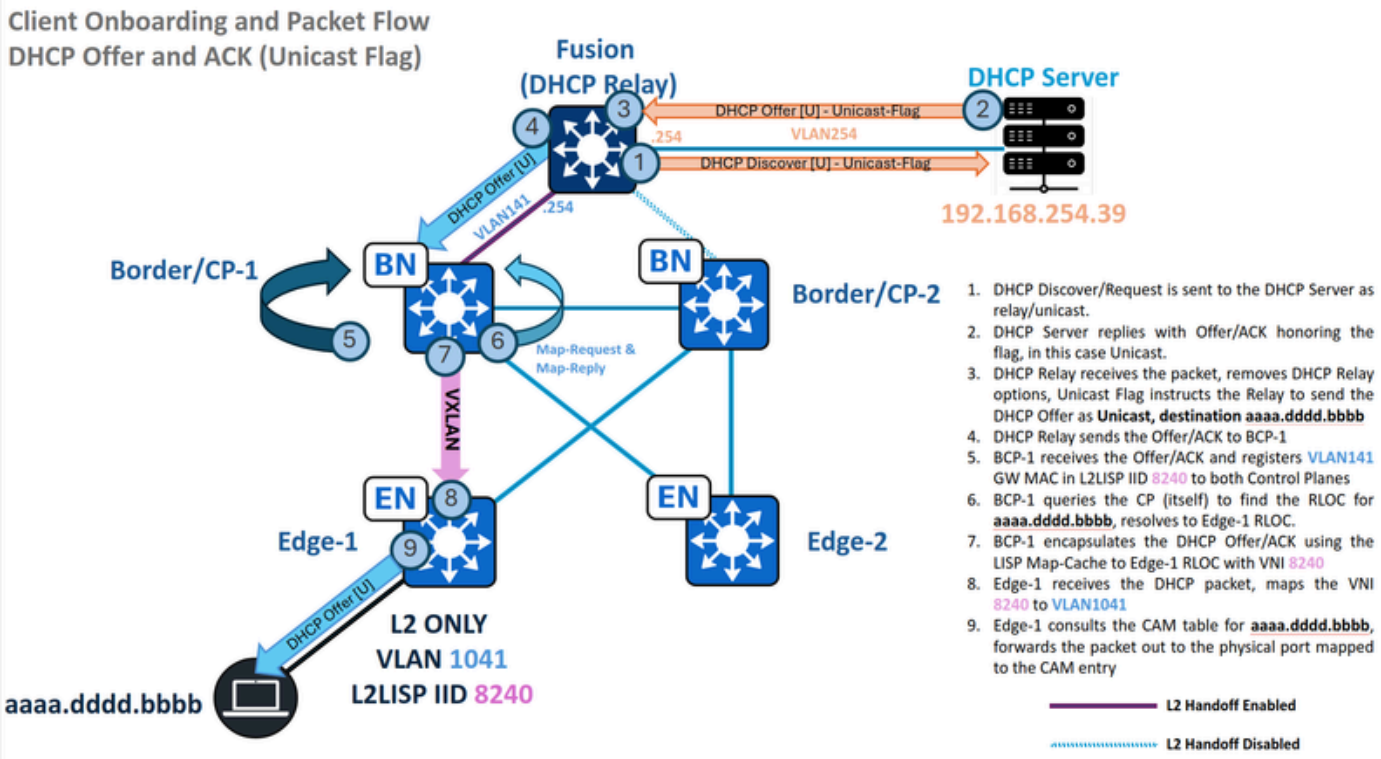
<#root>

```
Edge-1#
show mac address-table interface te1/0/2

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

1041

aaaa.dddd.bbbb

    DYNAMIC

Te1/0/2
```

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 de Rastreamento de dispositivo para o ponto final habilitado por DHCP é gerada pelo conjunto de pacotes ARP. 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      ag

ARP

172.16.141.1

 aaaa.dddd.bbbb

       Te1/0/2

1041

       0005       45s        REACHABLE  207 s try 0

Edge-1#

show ip dhcp snooping  binding vlan 1041

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

Total number of bindings: 0
```

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==aaaa.dddd.bbbb" deta


Dynamic Host Configuration Protocol (

Discover

)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00002030
    Seconds elapsed: 0

    Bootp flags: 0x0000, Broadcast flag (Unicast)
```

```
        0... .... .... .... = Broadcast flag: Unicast


        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0


Client MAC address: aa:aa:dd:dd:bb:bb (aa:aa:dd:dd:bb:bb)
```

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 (aaaa.dddd.bbb). Supondo que o "Aprendizado MAC e registro de endpoint" tenha sido bem-sucedido na borda da malha, o plano de controle tem essa ID de endpoint (EID) registrada.

<#root>

```
BorderCP-1#

show

 lisp instance-id 8240 ethernet server aaaa.dddd.bbbb


LISP Site Registration Information
Site name: site_uci
Description: map-server configured from Catalyst Center
Allowed configured locators: any
Requested EID-prefix:
  EID-prefix:

aaaa.dddd.bbbb/48

 instance-id

8240


    First registered:     00:36:37
    Last registered:      00:36:37
    Routing table tag:    0
    Origin:               Dynamic, more specific of any-mac
    Merge active:         No
    Proxy reply:          Yes
    Skip Publication:     No
    Force Withdraw:       No
    TTL:                  1d00h
    State:                complete
    Extranet IID:         Unspecified

    Registration errors:
```

```
      Authentication failures:   0


      Allowed locators mismatch: 0



 ETR 192.168.0.101:51328

, last registered 00:36:37, proxy-reply, map-notify
                             TTL 1d00h, no merge, hash-function sha1
                             state complete, no security-capability
                             nonce 0x1BF33879-0x707E9307
                             xTR-ID 0xDEF44F0B-0xA801409E-0x29F87978-0xB865BF0D
                             site-ID unspecified
                             Domain-ID 1712573701
                             Multihoming-ID unspecified
                             sourced by reliable transport
      Locator        Local  State      Pri/Wgt  Scope

 192.168.0.101  yes    up          10/10   IPv4 none
```

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 8240 ethernet map-cache aaaa.dddd.bbbb


LISP MAC Mapping Cache for LISP 0 EID-table Vlan

141

 (IID

8240

), 1 entries


aaaa.dddd.bbbb/48

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

via map-reply

,

complete

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

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

Com o RLOC resolvido, a oferta DHCP é encapsulada em unicast e enviada diretamente para Edge-1 em 192.168.0.101, utilizando o VNI 8240.

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

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

141

 aaaa.dddd.bbbb

CP_LEARN

L2LI0

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

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

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

Routing entry for 192.168.0.101/32
```

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


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

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 encaminha o pacote somente para a porta específica onde o endpoint está conectado, em vez de inundá-lo para todas as portas.

A tabela de endereços MAC identifica a porta Te1/0/2 como a porta do nosso cliente, que está no estado FWD pelo STP, o pacote é encaminhado para o ponto final.

```
<#root>

Edge-1#
show mac address-table interface te1/0/2


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


1041


aaaa.dddd.bbbb
    DYNAMIC
Te1/0/2
```

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 pelos pacotes ARP de limpeza. 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 ag

ARP

172.16.141.1

aaaa.dddd.bbbb

Te1/0/2

1041

0005 45s REACHABLE 207 s try 0

Edge-1#

show ip dhcp snooping binding vlan 1041

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

Total number of bindings: 0

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.

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.