レイヤ2のみのVLANでのDHCPのトラブルシューティング：ワイヤレス

内容

- はじめに
- 前提条件
  - 要件
- L2のみの概要
  - 概要
  - L2のみのVLANでのDHCP動作の変更
  - アンダーレイのマルチキャスト
  - アクセストンネルインターフェイス経由のブロードキャスト
- トポロジ
- L2のみのVLAN設定
  - Catalyst CenterからのL2のみのVLANの導入
  - L2のみのVLAN設定：ファブリックエッジ
  - L2のみのVLAN設定：ワイヤレスLANコントローラ
  - L2ハンドオフ設定（ファブリックボーダー）
  - ワイヤレスマルチキャストの有効化
- DHCPトラフィックフロー
  - DHCPの検出と要求 – ワイヤレス側
  - DHCPの検出と要求 – ファブリックエッジ
    - WLC通知を使用したMACラーニング
    - L2フラッディングでブリッジされたDHCPブロードキャスト
    - パケット キャプチャ
  - DHCPの検出と要求 – L2ボーダー
    - パケット キャプチャ
  - DHCPオファーおよびACK – ブロードキャスト – L2ボーダー
    - MACラーニングおよびゲートウェイ登録
    - L2フラッディングでブリッジされたDHCPブロードキャスト
  - DHCPオファーおよびACK – ブロードキャスト – エッジ
  - DHCPオファーおよびACK – ユニキャスト – L2ボーダー
  - DHCPオファーおよびACK – ユニキャスト – エッジ
  - DHCPトランザクション：ワイヤレスの検証

はじめに

このドキュメントでは、SDアクセス(SDA)ファブリックのレイヤ2専用ネットワークのワイヤレスエンドポイントのDHCPをトラブルシューティングする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- インターネットプロトコル(IP)転送
- ロケータ/ID分離プロトコル(LISP)
- Protocol Independent Multicast(PIM)スパースモード
- ファブリック対応ワイヤレス

ハードウェアおよびソフトウェア要件

- Catalyst 9000 シリーズ スイッチ
- Catalyst Centerバージョン2.3.7.9
- Catalyst 9800シリーズワイヤレスLANコントローラ
- Catalyst 9100 シリーズ アクセスポイント
- Cisco IOS® XE 17.12以降

制限事項

- リンクを無効にするFlexLink+やEEMスクリプトなどの堅牢なループ防止メカニズムが適切に設定されていない限り、一意のVLAN/VNIを同時にハンドオフできるのは1つのL2境界だけです。

L2のみの概要

概要

一般的なSD-Accessの導入では、L2/L3境界はファブリックエッジ(FE)に存在し、FEはSVIの形式でクライアントのゲートウェイをホストします。このSVIは「エニーキャストゲートウェイ」とも呼ばれます。 L3 VNI（ルーテッド）はサブネット間トラフィック用に確立され、L2 VNI（スイッチド）はサブネット内トラフィックを管理します。すべてのFEで一貫した設定が可能なため、シームレスなクライアントローミングが可能です。フォワーディングが最適化される：サブネット内(L2)トラフィックはFE間で直接ブリッジされ、サブネット間(L3)トラフィックはFE間またはFEとボーダーノード間でルーティングされます。

SDAファブリック内のエンドポイントのうち、ファブリックの外部に厳密なネットワークエントリポイントを必要とするものについては、SDAファブリックがエッジから外部ゲートウェイへのL2チャネルを提供する必要があります。

この概念は、レイヤ2アクセスネットワークがレイヤ3ルータに接続される従来のイーサネットキャンパスの導入に似ています。VLAN内トラフィックはL2ネットワーク内に留まりますが、VLAN間トラフィックはL3デバイスによってルーティングされ、多くの場合、L2ネットワーク上の別のVLANに戻ります。

LISPコンテキスト内では、サイトコントロールプレーンは主に、従来のARPエントリと同様に、

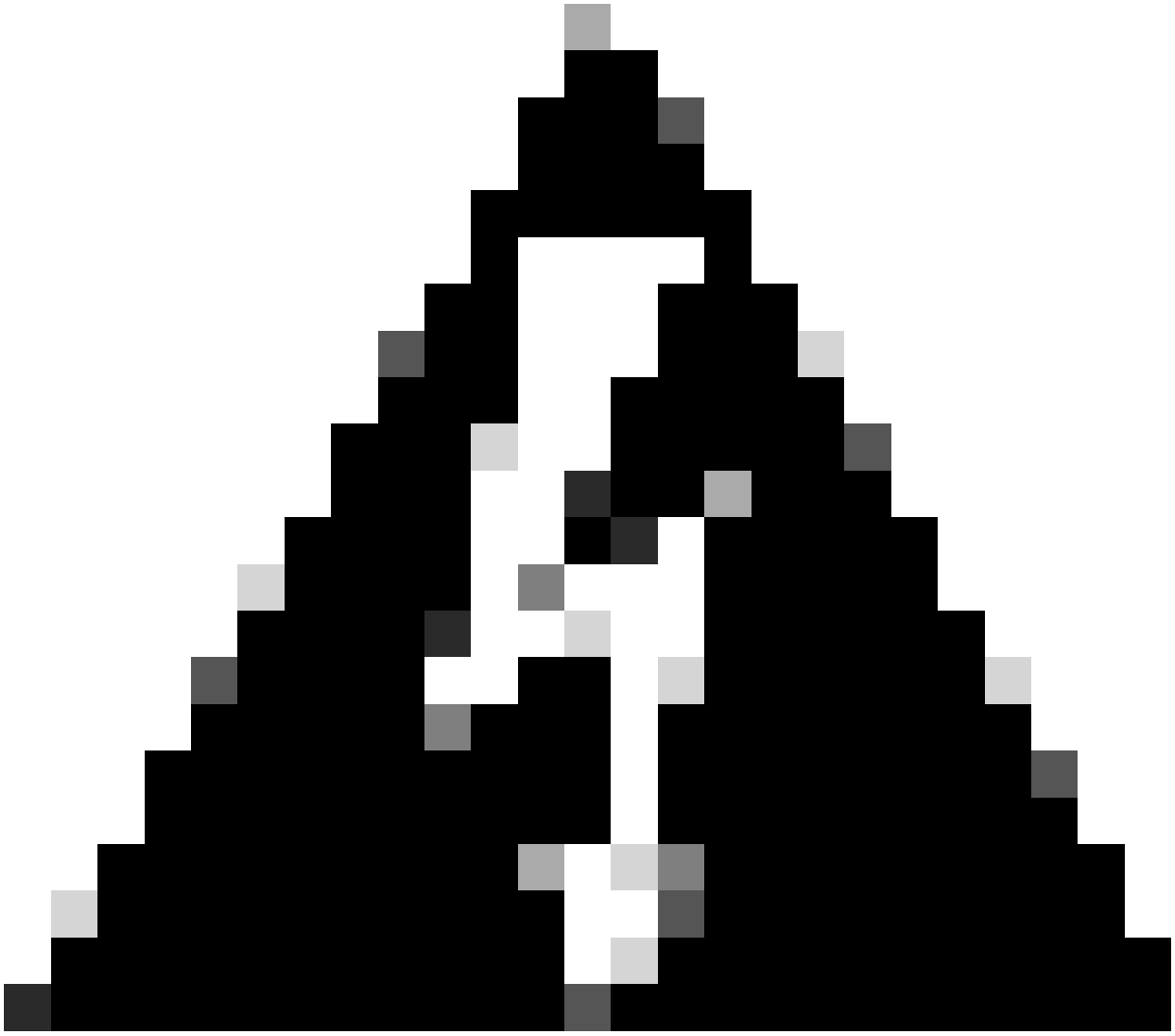
MACアドレスとそれに対応するMAC-to-IPバインディングを追跡します。L2 VNI/L2専用プールは、これら2つのEIDタイプのみに基づいて、登録、解決、転送を容易にするように設計されています。したがって、L2のみの環境でのLISPベースの転送は、MACおよびMAC-to-IP情報のみに依存し、IPv4またはIPv6 EIDを完全に無視します。LISP EIDを補完するため、L2専用プールは、従来のスイッチの動作と同様に、フラッディングおよび学習メカニズムに大きく依存しています。したがって、L2フラッディングは、このソリューション内でブロードキャスト、未知のユニキャスト、およびマルチキャスト(BUM)トラフィックを処理するための重要なコンポーネントとなり、アンダーレイマルチキャストを使用する必要があります。反対に、通常のユニキャストトラフィックは、主にマップキャッシュを介して、標準のLISP転送プロセスを使用して転送されます。

ファブリックエッジ(FEE)と「L2ボーダー」(L2B)の両方がL2　VNIを維持し、ローカルVLANにマッピングします（このマッピングはSDA内でローカルのデバイスで意味を持ち、ノード間で異なるVLANを同じL2 VNIにマッピングできます）。 この特定の使用例では、これらのノードでこれらのVLANにSVIが設定されていません。つまり、対応するL3 VNIはありません。

L2のみのVLANでのDHCP動作の変更

エニーキャストゲートウェイプールでは、すべてのファブリックエッジが直接接続されたエンドポイントのゲートウェイとして機能し、すべてのFEで同じゲートウェイIPを使用するため、DHCPには課題があります。DHCPリレーパケットの元の発信元を正しく特定するには、FEはLISP　RLOC情報を含むDHCPオプション82とそのサブオプションを挿入する必要があります。これは、ファブリックエッジのクライアントVLAN上のDHCPスヌーピングによって実現されます。DHCPスヌーピングは、このコンテキストで2つの目的を果たします。オプション82の挿入を容易にし、重要な点として、ブリッジドメイン(VLAN/VNI)全体でのDHCPブロードキャストパケットのフラッディングを防止します。　エニーキャストゲートウェイでレイヤ2フラッディングが有効になっている場合でも、DHCPスヌーピングにより、ブロードキャストパケットがブロードキャストとしてファブリックエッジから転送されることが効果的に抑制されます。

これに対して、レイヤ2専用VLANにはゲートウェイがないため、DHCPソースの識別が簡単になります。パケットはどのファブリックエッジによってもリレーされないため、送信元を特定するための複雑なメカニズムは不要です。L2　Only　VLANでDHCPスヌーピングを使用しない場合、DHCPパケットのフラッド制御メカニズムは事実上バイパスされます。これにより、L2フラッディングを介して、DHCPブロードキャストを最終宛先に転送できるようになります。最終宛先は、ファブリックノードに直接接続されたDHCPサーバか、DHCPリレー機能を提供するレイヤ3デバイスです。



警告:L2専用プール内の「複数のIPからMAC」機能は、ブリッジVMモードのDHCPスヌーピングを自動的にアクティブ化し、DHCPフラッド制御を実施します。その結果、L2 VNIプールはエンドポイントのDHCPをサポートできなくなります。

アンダーレイのマルチキャスト

DHCPがブロードキャストトラフィックに大きく依存していることを踏まえると、このプロトコルをサポートするには、レイヤ2フラッディングを活用する必要があります。他のL2フラッディング対応プールと同様に、アンダーレイネットワークはマルチキャストトラフィック、特にPIMスパースモードを使用したAny-Source-Multicast用に設定する必要があります。アンダーレイのマルチキャスト設定はLAN自動化ワークフローによって自動化されますが、この手順を省略した場合は、追加の設定（手動またはテンプレート）が必要です。

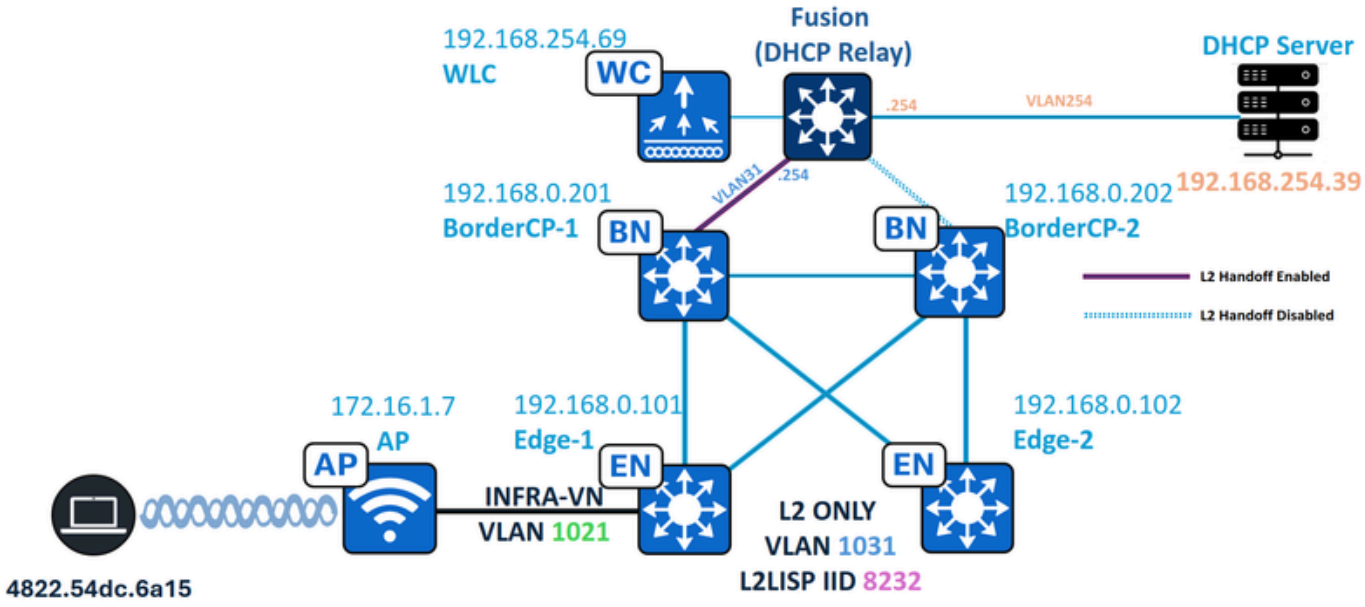
- すべてのノード（ボーダー、エッジ、中間ノードなど）でIPマルチキャストルーティングを有効にします。
- 各ボーダーノードとエッジノードのLoopback0インターフェイスでPIMスパースモードを設定します。

- 各IGP（アンダーレイルーティングプロトコル）インターフェイスでPIMスパースモードを有効にします。
- すべてのノード(Borders、Edges、Intermediate Nodes)でPIM Rendezvous Point(RP)を設定し、BordersにRPを配置することが推奨されます。
- PIMネイバー、PIM RP、およびPIMトンネルステータスを確認します。

アクセストンネルインターフェイス経由のブロードキャスト

Fabric Enabled Wirelessは、APとFEでローカルスイッチングとVTEP機能を採用しています。ただし、IOS-XE 16.10+の制限により、VXLANを介したAPへの出力ブロードキャスト転送が防止されます。L2のみのネットワークでは、DHCPオファー/ACKがワイヤレスクライアントに到達するのをブロックします。「フラッドアクセストンネル」機能は、ファブリックエッジアクセストンネルインターフェイスでブロードキャスト転送を有効にすることによって、これに対処します。

トポロジ



Network Topology

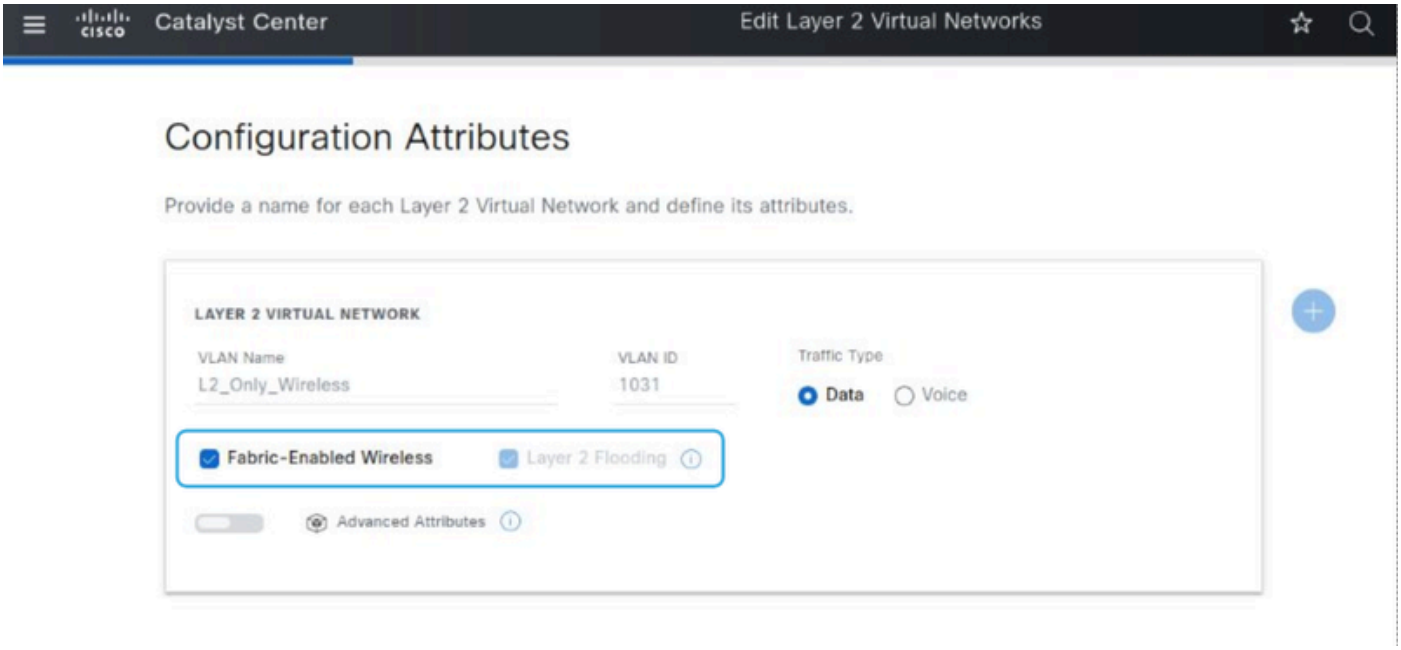
このトポロジでは、次のようになります。

- 192.168.0.201と192.168.0.202はファブリックサイトの境界のコロケートによる分離であり、BorderCP-1はレイヤ2ハンドオフ機能が有効になっている唯一の境界です。
- 192.168.0.101と192.168.0.102はファブリックエッジノード
- 172.16.1.7はVLAN 1021を使用するINFRA-VNのアクセスポイント
- 192.168.254.39はDHCPサーバ
- 192.168.254.69はワイヤレスLANコントローラ
- 4822.54dc.6a15はDHCP対応エンドポイント
- Fusionデバイスは、ファブリックサブネットのDHCPリレーとして機能します。

L2のみのVLAN設定

Catalyst CenterからのL2のみのVLANの導入

パス：Catalyst Center/プロビジョニング/ファブリックサイト/レイヤ2仮想ネットワーク/レイヤ2仮想ネットワークの編集



ファブリック対応ワイヤレスを使用したL2VNI設定

L2のみのVLAN設定：ファブリックエッジ

ファブリックエッジノードには、CTSが有効、IGMPとIPv6 MLDが無効、および必要なL2 LISP設定で設定されたVLANがあります。このL2　Onlyプールはワイヤレスプールです。そのため、L2 Onlyワイヤレスプールに通常見られる機能（RAガード、DHCPGuard、フラッドアクセストンネルなど）が設定されます。ARPフラッディングがワイヤレスプールで有効になっていない。

ファブリックエッジ(192.168.0.101)の設定

<#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

flood-access　tunnelコマンドはマルチキャスト複製バリエーションで設定され、すべてのBUMトラフィックは、BUMトラフィックを転送するためにIGMPスヌーピングによってコンサルテーションされるVLANとしてINFRA-VNアクセスポイントVLANを使用して、Source Specific Multicast(SSM)グループ(232.255.255.1)を使用してAPにカプセル化されます。

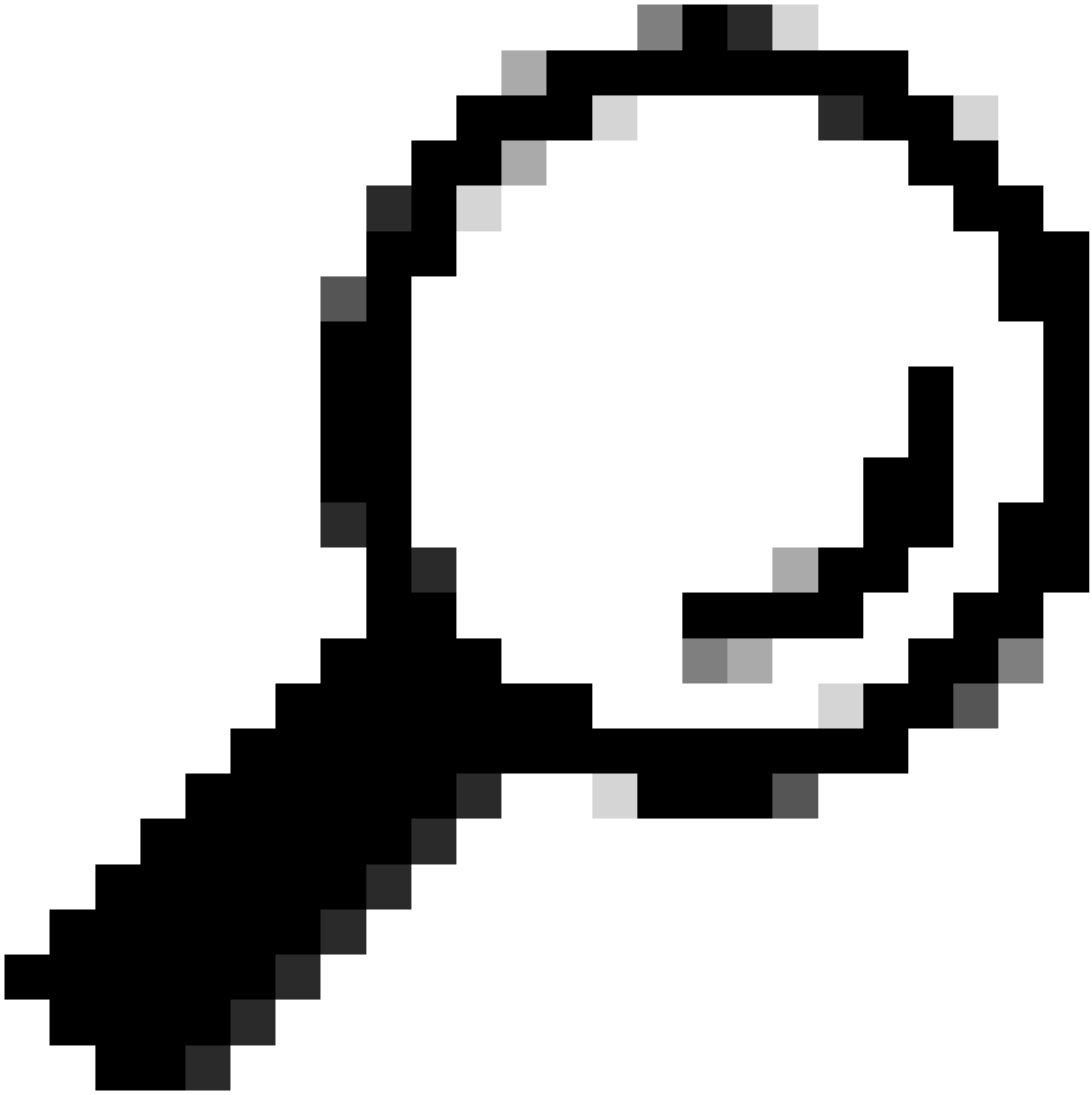
L2のみのVLAN設定：ワイヤレスLANコントローラ

WLC（ワイヤレスLANコントローラ）側で、ファブリックアクセスポイントに関連付けられたサイトタグは、プロキシARP機能を無効にするために「no　fabric　ap-arp-caching」を使用して設定する必要があります。また、「fabric　ap-dhcp-broadcast」を有効にする必要があります。この設定により、DHCPブロードキャストパケットをAPからワイヤレスエンドポイントに転送できます。

ファブリックWLC(192.168.254.69)の設定

<#root>

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

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



ヒント：ワイヤレスマルチキャストグループ232.255.255.1は、すべてのサイトタグで使用されるデフォルトグループです。

<#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

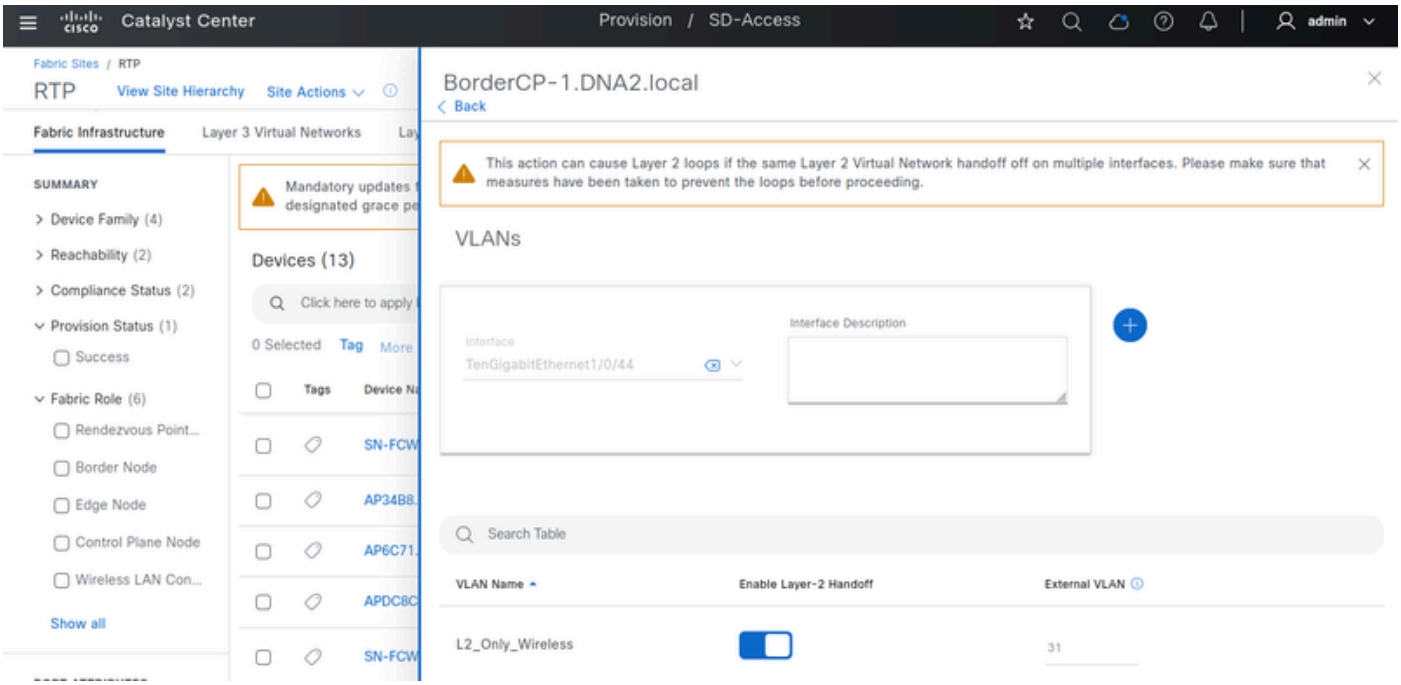
```
RTP-Site-Tag-3 Load : 0
```

L2ハンドオフ設定（ファブリックボーダー）

運用上の観点から、DHCPサーバ（またはルータ/リレー）は、境界と工ッジの両方を含め、任意のファブリックノードに接続できます。

境界ノードを使用したDHCPサーバへの接続は推奨される方法ですが、設計に関しては慎重に検討する必要があります。これは、インターフェイスごとにL2ハンドオフを設定する必要があるためです。これにより、ファブリックプールをファブリック内と同じVLANまたは別のVLANに渡すことができます。ファブリックエッジとボーダーが同じL2 LISPインスタンスIDにマッピングされるため、ファブリックエッジとボーダー間のVLAN　IDの柔軟性が向上します。L2ハンドオフ物理ポートは、SDアクセスネットワーク内のレイヤ2ループを防ぐために、同じVLANで同時に有効にしないでください。冗長性を確保するには、StackWise　Virtual、FlexLink+、またはEEMスクリプトなどの方法が必要です。

一方、DHCPサーバまたはゲートウェイルータをファブリックエッジに接続する場合は、追加の設定は必要ありません。



L2ハンドオフ設定

ファブリック境界/CP(192.168.0.201)の設定

<#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
```

ワイヤレスマルチキャストの有効化

ファブリックエッジは、フラッドアクセストンネルメカニズムを介してアクセスポイントにブロードキャストパケットを転送するように設定されます。これらのパケットは、INFRA-VN VLAN上の232.255.255.1マルチキャストグループにカプセル化されます。アクセスポイントは、このマルチキャストグループを使用するように事前に設定されているため、このマルチキャストグループに自動的に参加します。

```
<#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

アクセスポイントから、ファブリックワイヤレスエンドポイントの関連付けに基づいて、VXLANトンネルが形成されます（AP側では動的、ファブリックエッジ側では常に有効）。 このトンネル内では、CAPWAPファブリックマルチキャストグループは、AP端末からのコマンドを使用して確認されます。

<#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
```

ファブリックエッジ側から、IGMPスヌーピングがINFRA-VN AP VLANに対して有効になっており、アクセスポイントがアクセストンネルインターフェイスを形成し、マルチキャストグループ232.255.255.1に参加していることを確認します

<#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
------------------------------------------------------------------------
```

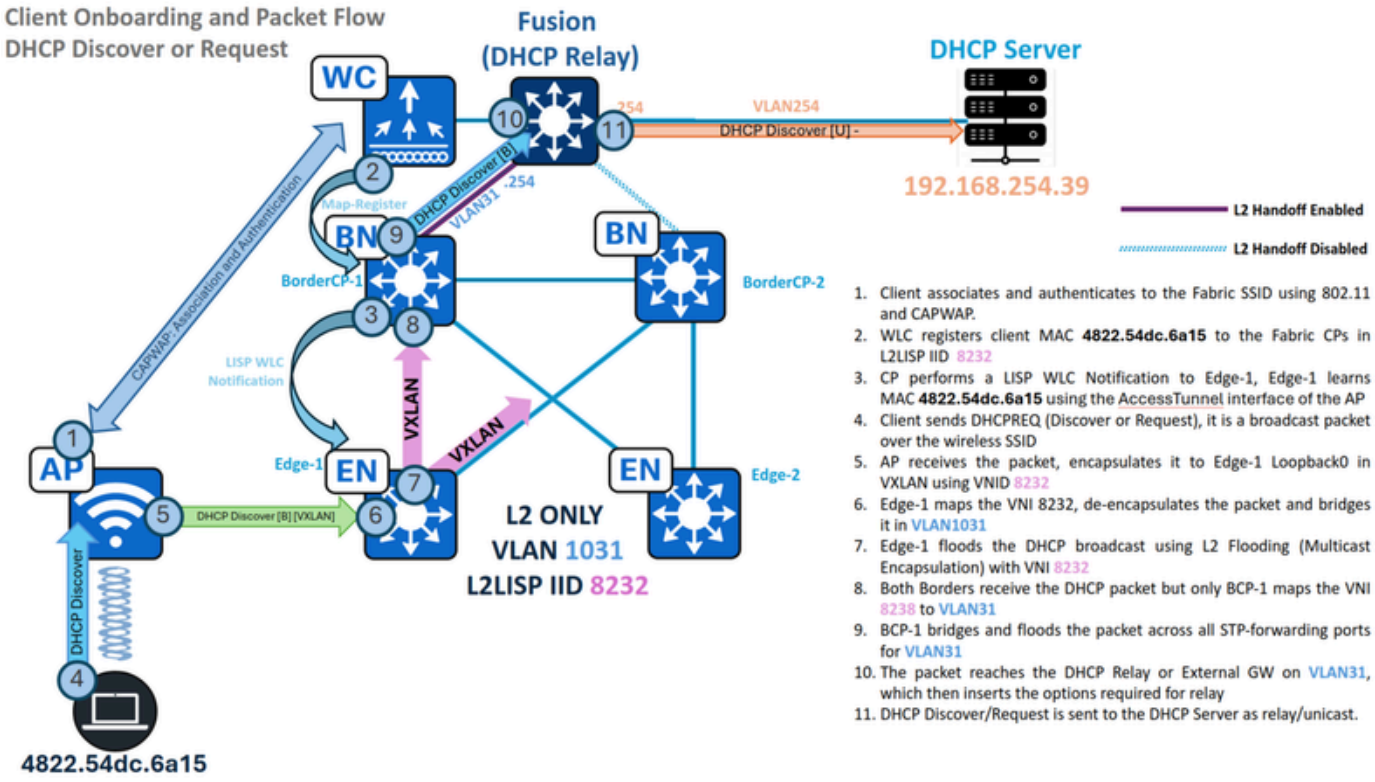
1021 232.255.255.1

```
           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>
```

これらの検証により、アクセスポイント、ファブリックエッジ、およびワイヤレスLANコントローラ全体でワイヤレスマルチキャストが正常に有効化されていることが確認されます。

DHCPトラフィックフロー

DHCPの検出と要求 – ワイヤレス側



トラフィックフロー – DHCPによるL2のみの検出および要求

ワイヤレスエンドポイントの状態、接続されているアクセスポイント、および関連するファブリックプロパティを特定します。

<#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

中央スイッチング機能と中央DHCP機能の両方がポリシープロファイルで無効になっていることを確認することが重要です。コマンド「no central dhcp」および「no central switching」は、SSIDのポリシープロファイルで設定する必要があります。

<#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

これらの検証により、エンドポイントが「AP1」に接続されていることが確認されます。これは、ファブリックエッジRLOC 192.168.0.101に関連付けられています。その結果、そのトラフィックはアクセスポイントからファブリックエッジへの伝送用にVNID 8232を使用してVXLAN経由でカプセル化されます。

DHCPの検出と要求 – ファブリックエッジ

WLC通知を使用したMACラーニング

エンドポイントのオンボーディング時に、WLCはワイヤレスエンドポイントのMACアドレスをファブリックコントロールプレーンに登録します。同時に、コントロールプレーンは、（アクセスポイントが接続されている）ファブリックエッジノードに通知して、アクセスポイントのアクセストンネルインターフェイスを指す特別な「CP_LEARN」MACラーニングエントリを作成します。

<#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

エンドポイントのMACアドレスが、接続されているアクセスポイントに対応するアクセストンネルインターフェイスを介して正しく学習されていれば、この段階は完了したと見なされます。

L2フラッディングでブリッジされたDHCPブロードキャスト

DHCPスヌーピングがディセーブルの場合、DHCPブロードキャストはブロックされず、代わりにレイヤ2フラッディングのためにマルチキャストでカプセル化されます。逆に、DHCPスヌーピングを有効にすると、これらのブロードキャストパケットのフラッディングを防止できます。

<#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>
```

DHCPスヌーピングがディセーブルであるため、DHCPディスカバリ/要求はL2LISP0インターフェイスを使用して、L2フラッディングを介してトラフィックをブリッジします。Catalyst Centerのバージョンおよび適用されるファブリックバナーによっては、L2LISP0インターフェイスに両方向でアクセスリストが設定されている場合があります。そのため、DHCPトラフィック（UDPポート67および68）がアクセスコントロールエントリ(ACE)によって明示的に拒否されないようにする必要があります。

<#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
```

L2LISPインスタンス用に設定されたブロードキャストアンダーレイグループとファブリックエッジのLoopback0のIPアドレスを利用して、このパケットを他のファブリックノードにブリッジするL2フラッディング(S,G)エントリを確認します。mrouteテーブルとmfibテーブルを参照して、着信インターフェイス、発信インターフェイスリスト、転送カウンタなどのパラメータを確認します。

<#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:

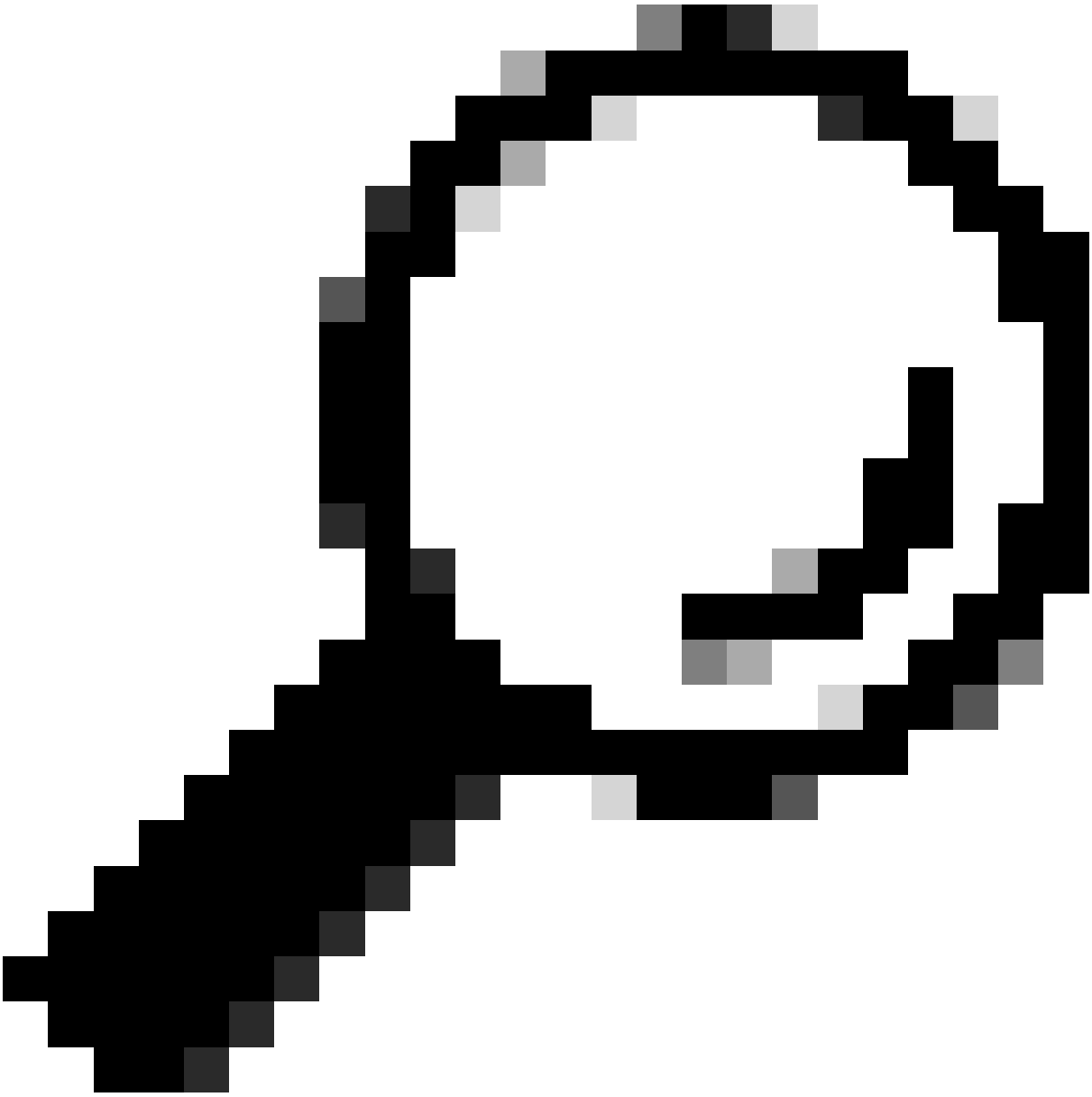
7

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

<--

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

Totals - Source count: 1, Packet count: 8



ヒント: (S,G)エントリが見つからない場合や、発信インターフェイスリスト(OIL)に発信インターフェイス(OIF)が含まれていない場合は、アンダーレイマルチキャストの設定または操作に問題があることを示しています。

パケット キャプチャ

APからの入力DHCPパケットと、L2フラッディングに対応する出力パケットの両方を記録するように、スイッチで同時組み込みパケットキャプチャを設定します。

ファブリックエッジ(192.168.0.101)パケットキャプチャ

<#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
```

パケットキャプチャでは、次の3つの異なるパケットを観察する必要があります。

- DHCPディスカバリ – VXLAN - APからエッジ
- DHCPディスカバリ – CAPWAP - APからWLC
- DHCPディスカバリ – VXLAN – エッジからマルチキャストグループ

```
<#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

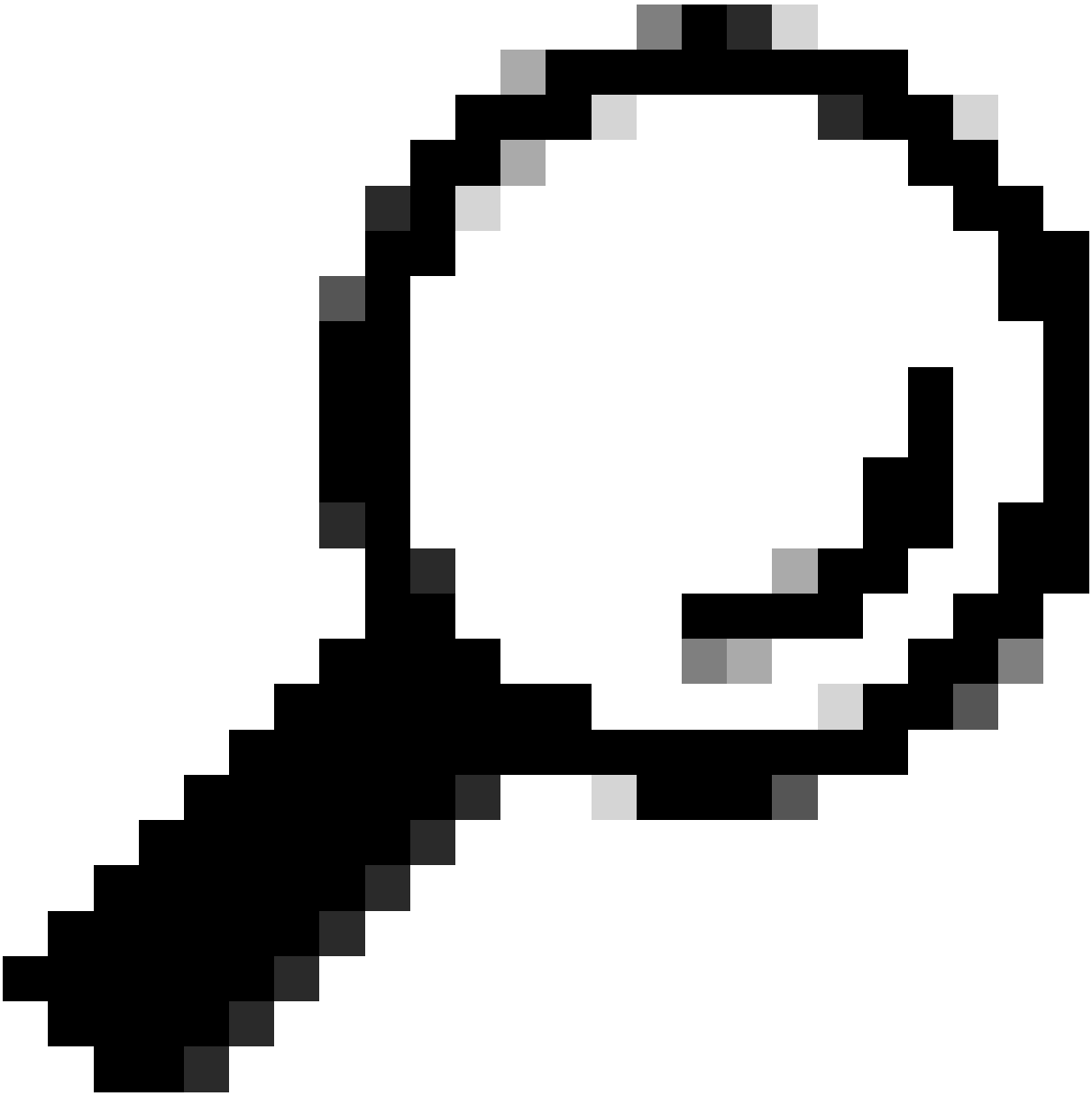
```
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
Internet Protocol Version 4, Src:
```

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



ヒント：ファブリック対応ワイヤレスでは、VXLANカプセル化パケットによってDHCPトラフィックがクライアントまたはサーバに配信されます。ただし、CAPWAPデータ(UDP 5247)でカプセル化されたパケットは、IP Learn状態やWireless Device-Trackingなどの追跡目的のためだけにWLCに送信されます。

DHCPの検出と要求 – L2ボーダー

エッジがブロードキャストアンダーレイグループ239.0.17.1でカプセル化されたレイヤ2フラッディングを介してDHCP　DiscoverおよびRequestパケットを送信すると、これらのパケットはL2ハンドオフ境界、特にこのシナリオではBorder/CP-1で受信されます。

このためには、Border/CP-1がエッジの(S,G)を持つマルチキャストルート(MROUTE)を所有し、その発信インターフェイスリストにL2ハンドオフVLANのL2LISPインスタンスが含まれている必要があります。ハンドオフ用に異なるVLANを使用する場合でも、L2ハンドオフ境界は同じL2LISPインスタンスIDを共有することに注意してください。

<#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,

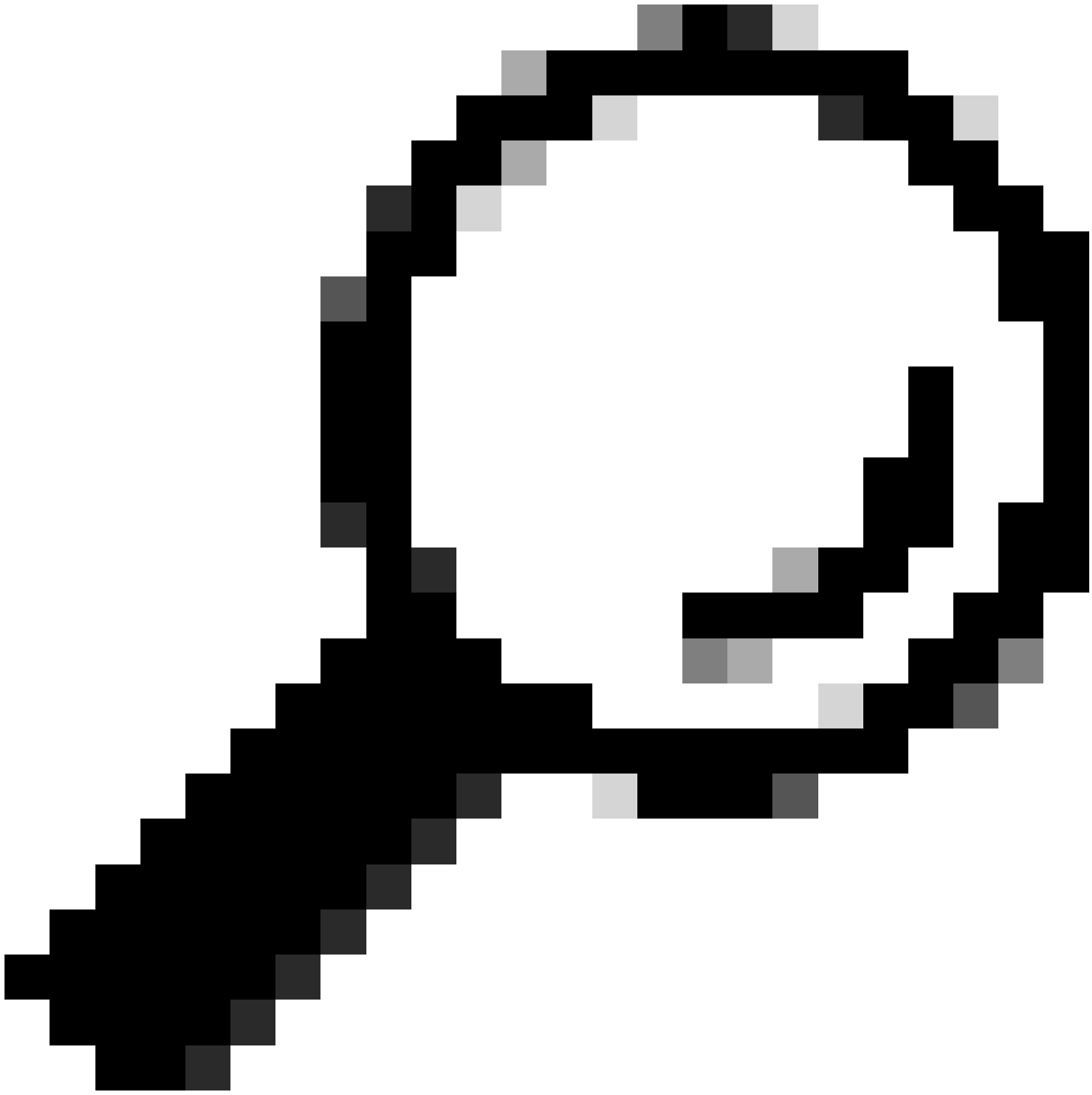
SW Forwarding: 1/0/392/0, Other: 0/0/0
HW Forwarding:

3

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

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

Totals - Source count: 1, Packet count: 4



ヒント: (S,G)エントリが見つからない場合は、アンダーレイマルチキャストの設定または操作に問題があることを示しています。必要なインスタンスのL2LISPがOIFとして存在しない場合は、L2LISPサブインターフェイスのUP/DOWN動作ステータスまたはL2LISPインターフェイスのIGMPイネーブルメントステータスに問題があることを示しています。

ファブリックエッジノードと同様に、アクセスコントロールエントリ(ACE)によってL2LISP0インターフェイスの入力DHCPパケットが拒否されないようにします。

<#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
```

パケットのカプセル化が解除され、VNI　8240に一致するVLANに配置されると、そのブロードキャスト特性により、ハンドオフVLAN　141のすべてのスパニングツリープロトコル(STP)転送ポートからパケットがフラッディングされます。

```
<#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
```

デバイストラッキングテーブルにより、ゲートウェイ/DHCPリレーに接続するインターフェイスTe1/0/44がSTP転送ポートでなければならないことが確認されます。

```
<#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
```

パケット キャプチャ

L2フラッディング（S、G着信インターフェイス）からの着信DHCPパケットと、DHCPリレーへの対応する出力パケットの両方を記録するように、スイッチで同時組み込みパケットキャプチャ(EPC)を設定します。 パケットキャプチャ時には、2つの異なるパケット（Edge-1からのVXLANカプセル化パケットと、DHCPリレーに向かうカプセル化解除パケット）が確認されます。

ファブリックボーダー/CP(192.168.0.201)パケットキャプチャ

<#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

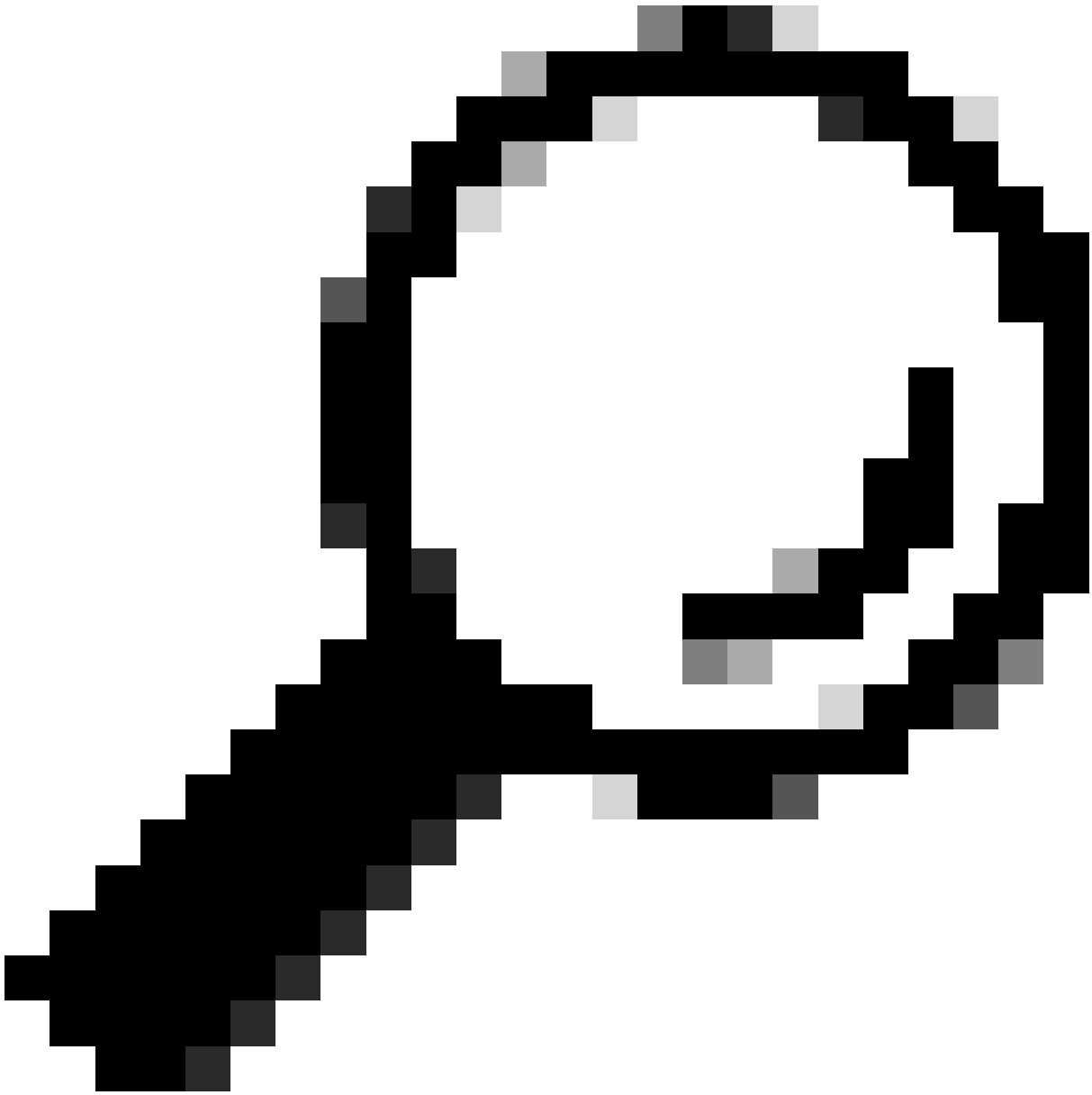
  326 16.695053   0.0.0.0 -> 255.255.255.255 DHCP

```
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
```

この時点で、Discover/RequestパケットによってSD-Accessファブリックが終了し、このセクションは終了しています。ただし、続行する前に、重要なパラメータ（エンドポイント自体によって決定されるDHCPブロードキャストフラグ）によって、後続のOfferパケットまたはACKパケットの転送シナリオが決定されます。このフラグを検査するために、Discoverパケットの1つを調べることができます。

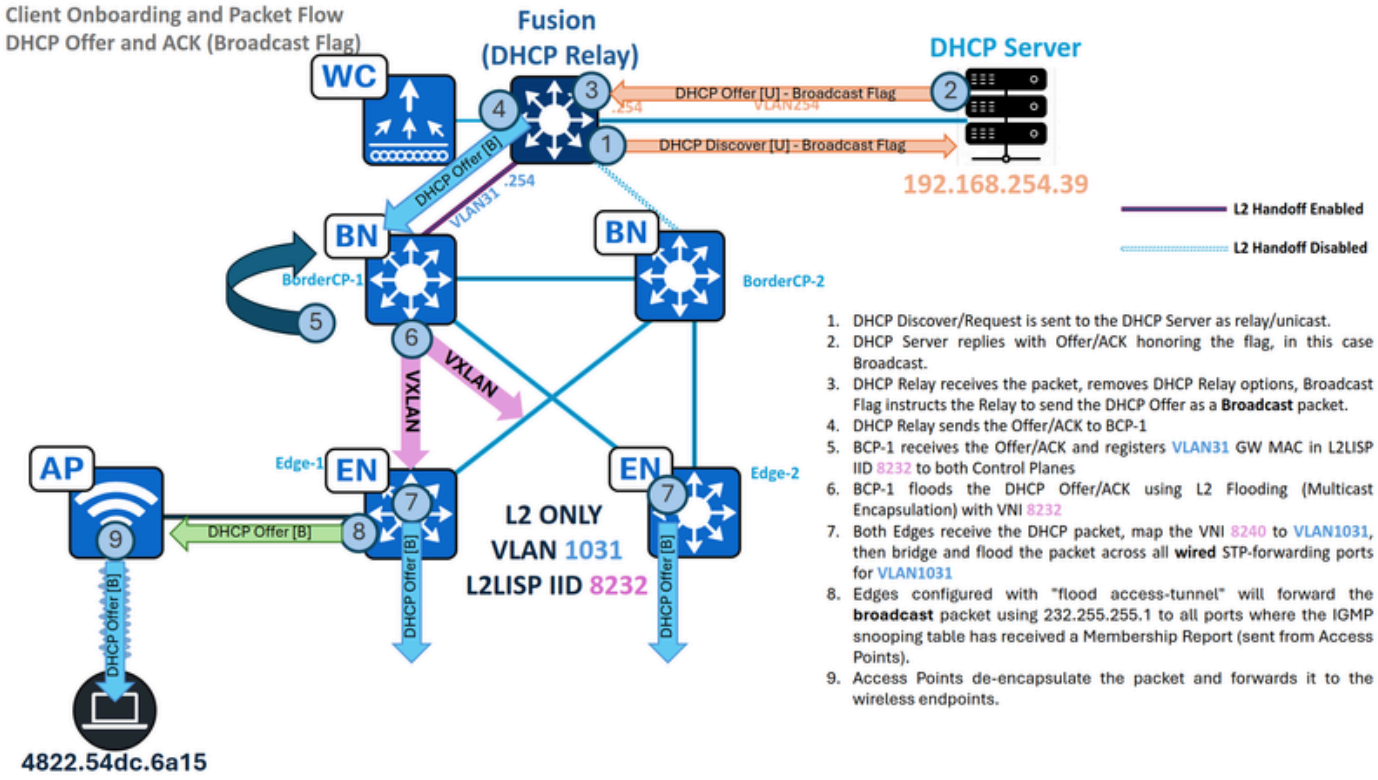
```
<#root>
BorderCP-1#
show monitor capture cap buffer display-filter "bootp.type==1 and dhcp.hw.mac_addr==4822.54dc.6a15
" detailed | sect Dynamic


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
```



ヒント: bootp.type==1を使用すると、DiscoverパケットとRequestパケットのみをフィルタリングできます。

DHCPオファーおよびACK – ブロードキャスト – L2ボーダー



トラフィックフロー – DHCPオファーのブロードキャストとL2のみのACK

DHCP　DiscoverがSD-Accessファブリックを終了したので、DHCPリレーは従来のDHCPリレーオプション（GiAddr/GatewayIPAddressなど）を挿入し、ユニキャスト伝送としてパケットをDHCPサーバに転送します。このフローでは、SDアクセスファブリックは特別なDHCPオプションを付加しません。

DHCPディスカバリ/要求がサーバに到達すると、サーバは組み込みのブロードキャストフラグまたはユニキャストフラグを承認します。このフラグは、DHCPリレーエージェントがDHCPオファーをダウンストリームデバイス（境界）にブロードキャストフレームまたはユニキャストフレームとして転送するかどうかを指定します。このデモンストレーションでは、ブロードキャストシナリオを想定しています。

MACラーニングおよびゲートウェイ登録

DHCPリレーがDHCP　OfferまたはACKを送信すると、L2BNノードはゲートウェイのMACアドレスを学習し、それをMACアドレステーブルに追加してから、L2/MAC SISFテーブルに追加し、最後にL2LISPインスタンス8232にマッピングされたVLAN 141のL2LISPデータベースに追加します。

<#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
```

ゲートウェイのMACアドレスが正しく学習されており、ファブリックコントロールプレーンのACKフラグが「Yes」とマークされている場合は、この段階が完了したと見なされます。

L2フラッディングでブリッジされたDHCPブロードキャスト

DHCPスヌーピングを有効にしないと、DHCPブロードキャストはブロックされず、レイヤ2フラッディングのためにマルチキャストにカプセル化されます。逆に、DHCPスヌーピングが有効な場合、DHCPブロードキャストパケットのフラッディングは防止されます。

<#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

L2BorderではDHCPスヌーピングが有効になっていないため、DHCPスヌーピング信頼設定は必要ありません。

この段階で、L2LISP ACLの検証は両方のデバイスですでに行われています。

L2LISPインスタンス用に設定されたブロードキャストアンダーレイグループとL2Border Loopback0 IPアドレスを利用して、このパケットを他のファブリックノードにブリッジするL2フラッディング(S,G)エントリを確認します。mrouteテーブルとmfibテーブルを参照して、着信インターフェイス、発信インターフェイスリスト、転送カウンタなどのパラメータを確認します。

<#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

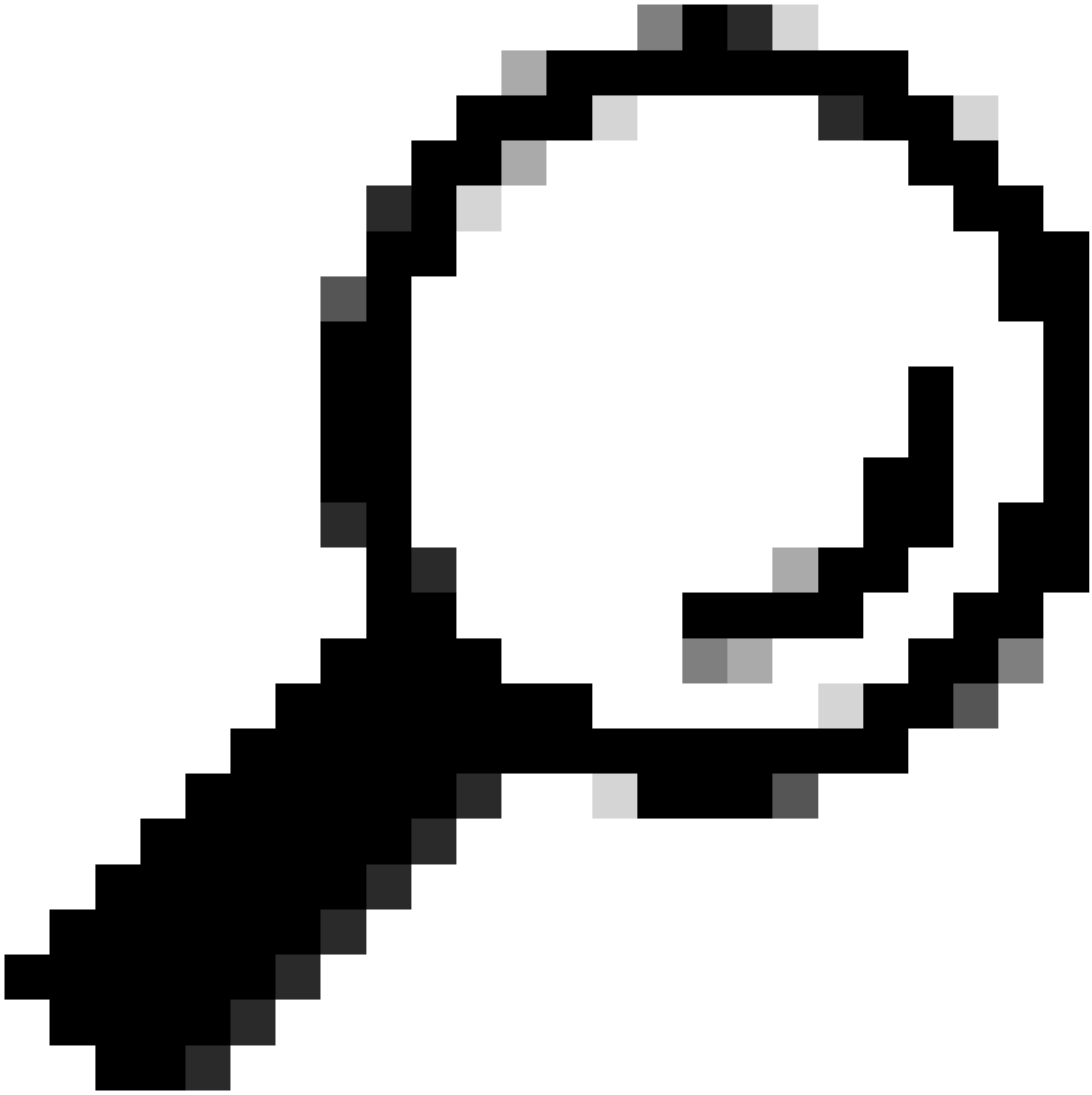
,
   SW Forwarding: 1/0/392/0, Other: 1/1/0
   HW Forwarding:

92071

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

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

  Totals - Source count: 1, Packet count: 92071



ヒント: (S,G)エントリが見つからない場合や、発信インターフェイスリスト(OIL)に発信インターフェイス(OIF)が含まれていない場合は、アンダーレイマルチキャストの設定または操作に問題があることを示しています。

これらの検証により、前述のステップと同様に、パケットキャプチャに沿ってこのセクションを終了します。発信インターフェイスリストの内容(この場合はインターフェイスTenGig1/0/42およびTenGig1/0/43外)を使用してすべてのファブリックエッジへのブロードキャストとしてDHCPオファーが転送されるためです。

DHCPオファーおよびACK – ブロードキャスト – エッジ

前のフローとまったく同様に、ファブリックエッジ内のL2Border S,Gを確認します。ここで、着信インターフェイスはL2BNの方向を指し、OILにはVLAN 1031にマッピングされたL2LISPインスタンスが含まれています。

<#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,

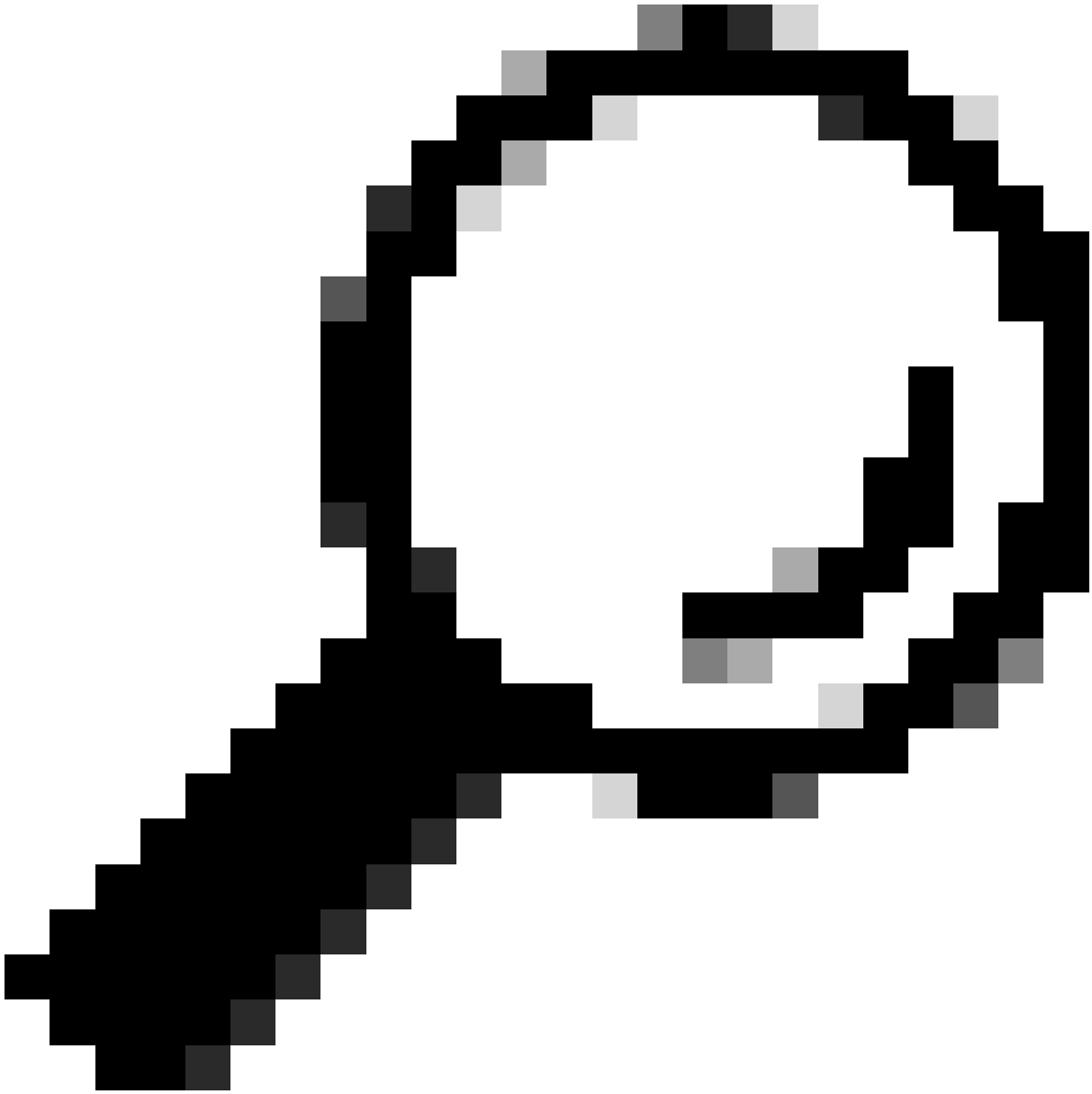
```
   SW Forwarding: 1/0/96/0, Other: 0/0/0
   HW Forwarding:
```

76236

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

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

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



ヒント: (S,G)エントリが見つからない場合は、アンダーレイマルチキャストの設定または

操作に問題があることを示しています。必要なインスタンスのL2LISPがOIFとして存在しない場合は、L2LISPサブインターフェイスのUP/DOWN動作ステータスまたはL2LISPインターフェイスのIGMPイネーブルメントステータスに問題があることを示しています。

L2LISP ACLの検証は、両方のデバイスですでに行われています。

パケットのカプセル化が解除され、VNI　8232に一致するVLANに配置されると、そのブロードキャスト特性により、パケットはVLAN1031のすべての有線スパニングツリープロトコル(STP)転送ポートにフラッディングされます。

<#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
```

ただし、DHCPオファーをブロードキャストするために探しているインターフェイスは、アクセスポイントに関連付けられたアクセストンネルインターフェイスです。これが可能なのは、「フラッドアクセストンネル」がL2LISP IID 8232で有効になっているためです。それ以外の場合、このパケットはAccessTunnelインターフェイスに転送されるのをブロックされます。

<#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
```

マルチキャストフラッディンググループのIGMPスヌーピングエントリにより、DHCPオファーとACKがAPの物理ポートに転送されます。

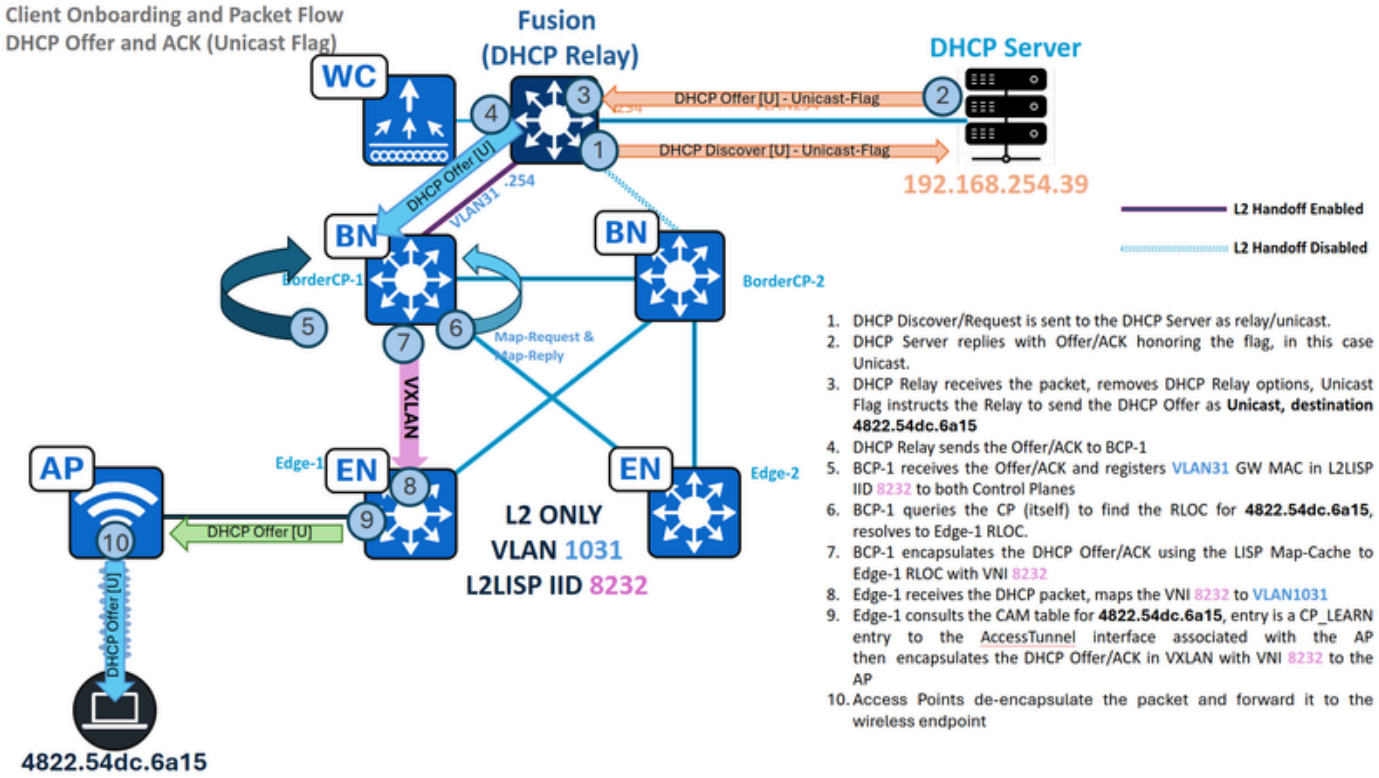
DHCPオファーおよびACKプロセスは一貫しています。DHCPスヌーピングがイネーブルにされていないと、DHCPスヌーピングテーブルにエントリは作成されません。その結果、DHCP対応エンドポイントのデバイストラッキングエントリは、収集されたARPパケットによって生成されます。また、DHCPスヌーピングがディセーブルになっているため、「show platform dhcpsnooping client stats」のようなコマンドではデータが表示されないことが予想されます。

<#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
```

DHCPオファーおよびACK – ユニキャスト – L2ボーダー



トラフィックフロー – ユニキャストDHCPオファーおよびL2のみのACK

このシナリオは少し異なります。エンドポイントはDHCPブロードキャストフラグをunsetまたは「0」に設定します。

DHCPリレーはDHCP Offer/ACKをブロードキャストとして送信せず、代わりにユニキャストパケットとして送信します。ユニキャストパケットには、DHCPペイロード内のクライアントハード

ウェアアドレスから派生した宛先MACアドレスが使用されます。これにより、SDアクセスファブリックでのパケットの処理方法が大幅に変更され、レイヤ2フラッディングマルチキャストカプセル化方式ではなく、L2LISPマップキャッシュを使用してトラフィックが転送されます。

ファブリックBorder/CP(192.168.0.201)パケットCatPURE：入力DHCPオファー

```
<#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)
```

このシナリオでは、L2フラッディングは検出/要求のみに使用され、オファー/ACKはL2LISPマップキャッシュ経由で転送されるため、操作全体が簡素化されます。ユニキャスト転送の原則に従って、L2境界は宛先MACアドレスをコントロールプレーンに照会します。ファブリックエッジで「MACラーニングおよびWLC通知」が正常に行われると仮定して、コントロールプレーンにはこのエンドポイントID(EID)が登録されています。

```
<#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
```

コントロールプレーン（ローカルまたはリモート）に対するBorderのクエリーの後、LISP解決はエンドポイントのMACアドレスのマップキャッシュエントリを確立します。

```
<#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        -
```

RLOCが解決されると、DHCPオファー(Offer)がユニキャストでカプセル化され、192.168.0.101のEdge-1にVNI 8240で直接送信されます。

```
<#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
```

前のセクションと同じ方法で、DHCPリレーからの入力とRLOC出力インターフェイスへの入力の両方のトラフィックをキャプチャし、エッジRLOCへのユニキャストのVXLANカプセル化を確認します。

DHCPオファーおよびACK – ユニキャスト – エッジ

エッジは境界からユニキャストDHCP　Offer/ACKを受信し、トラフィックのカプセル化を解除し、MACアドレステーブルを参照して正しい出力ポートを決定します。ブロードキャストOffer/ACKとは異なり、エッジノードは、エンドポイントが接続されている特定のアクセストンネルにのみパケットを転送し、すべてのポートにパケットをフラッディングしません。

MACアドレステーブルは、ポートAccessTunnel2をAP1に関連付けられた仮想ポートとして識別します。

<#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
```

DHCPオファーおよびACKプロセスは一貫しています。DHCPスヌーピングがイネーブルにされていないと、DHCPスヌーピングテーブルにエントリが作成されません。その結果、DHCP対応エンドポイントのデバイストラッキングエントリは、DHCPではなく、収集されたARPパケットによって生成されます。また、DHCPスヌーピングがディセーブルになっているため、「show platform dhcpsnooping client stats」のようなコマンドではデータが表示されないことが予想されます。

<#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
```

SDアクセスファブリックはエンドポイントの動作のみであるため、ユニキャストまたはブロードキャストフラグの使用に影響を与えないことに注意することが重要です。この機能はDHCPリレーまたはDHCPサーバ自体によって上書きされる可能性がありますが、L2専用環境でのシームレスなDHCP運用には、両方のメカニズムが不可欠です。ブロードキャストOffer/ACKに対するアンダーレイマルチキャストによるL2フラッディング、ユニキャストOffer/ACKに対するコントロールプレーンでの適切なエンドポイント登録です。

DHCPトランザクション：ワイヤレスの検証

WLCから、RAトレースを使用してDHCPトランザクションが監視されます。

<#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
```

トランザクションの終了時に、エンドポイントはワイヤレスLANコントローラのデバイストラッキングデータベースに追加されます。

<#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
```

DHCPトランザクション全体が、アクセスポイント自体でデバッグされます。

<#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**

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。