

レイヤ2専用VLANのDHCPのトラブルシューティング：有線

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](#)

[SDアクセスファブリック内のDHCPサーバ](#)

[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ハンドオフ設定：ファブリックボーダー](#)

[DHCPトラフィックフロー](#)

[DHCPの検出と要求－エッジ](#)

[MACラーニングおよびエンドポイント登録](#)

[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](#)

[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オフアーおよび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オフアーおよびACK－ブロードキャスト－エッジ](#)

[DHCPオフアーおよびACK－ユニキャスト－L2ボーダー](#)

[DHCPオフアーおよびACK－ユニキャスト－エッジ](#)

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有線エンドポイントの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)スパスモード

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
- 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「ユニ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が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チャン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。

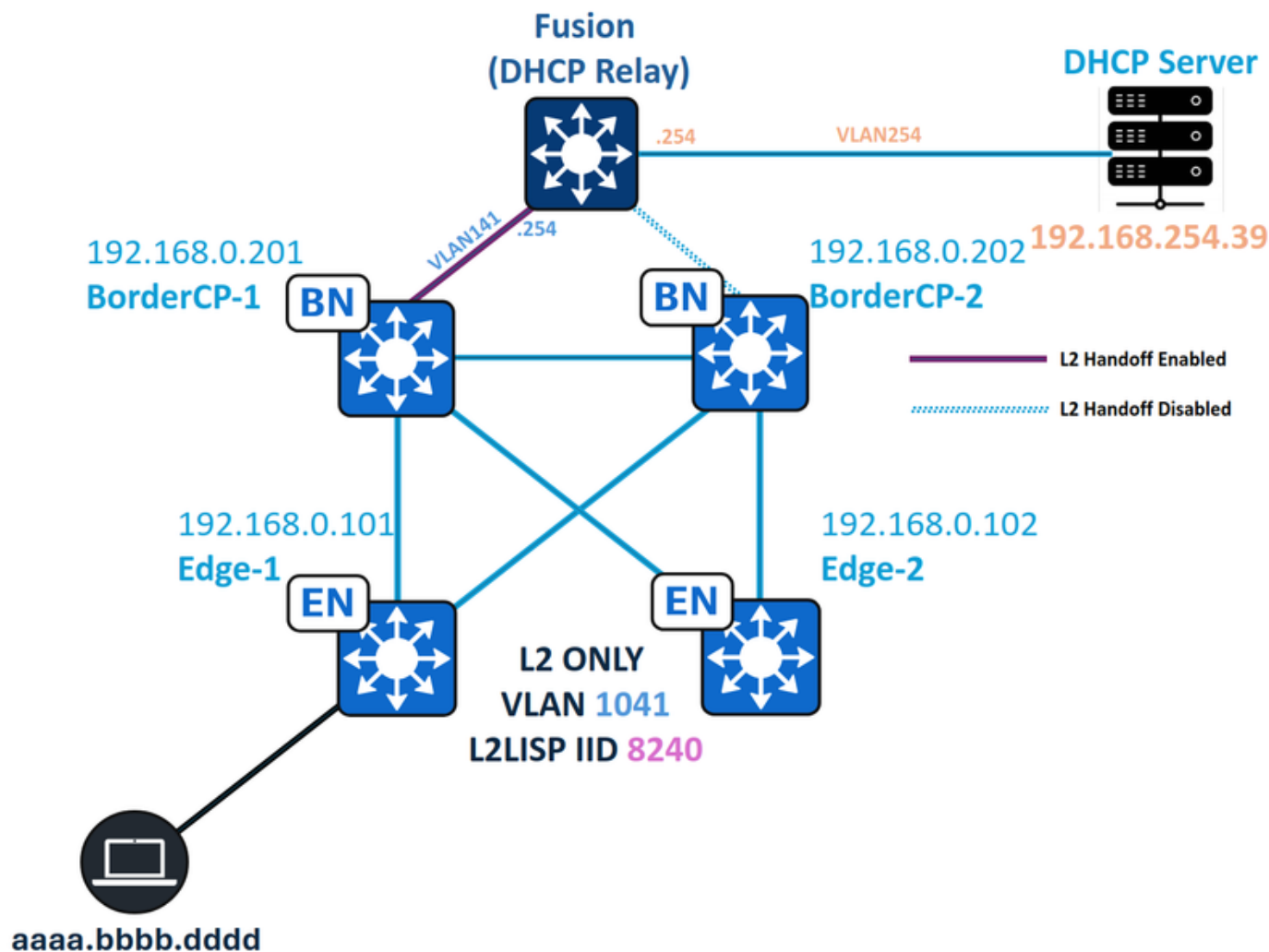
SDアクセスファブリック内のDHCPサーバ

設計に関する一般的な質問は、SDアクセスファブリック内にDHCPサーバを導入できるかどうかです。答えは本質的にイエスとノーの両方です。

公式の[Cisco Validated Design](#)では、DHCPサーバをファブリックの外部 (通常はShared Servicesブロックの内部) に配置することを推奨しています。ただし、DHCPサーバのファブリックノードへの物理的な接続 (エッジや境界など) が必要な場合は、L2 Onlyネットワークを介する方法だけがサポートされます。これは、DHCPスヌーピングがデフォルトで有効になっているエニーキャストゲートウェイプールに固有の動作が原因です。これにより、サーバからのDHCPオファーと確認応答がブロックされるだけでなく、VXLANにカプセル化されている場合でも、DHCPディスカバリおよび要求パケットの転送が阻止されます。DHCPサーバポートの「DHCPスヌーピング信頼」ではオファーと確認応答が可能ですが、ディスカバリと要求のパケットは同じ方法で転送されません。さらに、Catalyst Centerではコンプライアンス検証中に設定の変更にフラグが付けられるため、エニーキャストゲートウェイプールでのDHCPスヌーピングの削除はサポートされていません。

逆に、DHCPサーバがL2のみのネットワーク内に配置されている場合、DHCPスヌーピングは適用されず、ポリシーベースのインスペクションやブロックを行わずにすべてのDHCPパケットを通過させることができます。SDアクセスファブリックのアップストリームのネットワークデバイス (Fusionルータなど) は、L2専用ネットワークのゲートウェイとして設定され、複数のVRFからのトラフィックが、そのL2専用セグメント内の同じDHCPサーバにアクセスできるようにします。

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
- 192.168.254.39はDHCPサーバ
- aaaa.bbbb.ddddはDHCP対応エンドポイントです
- 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。

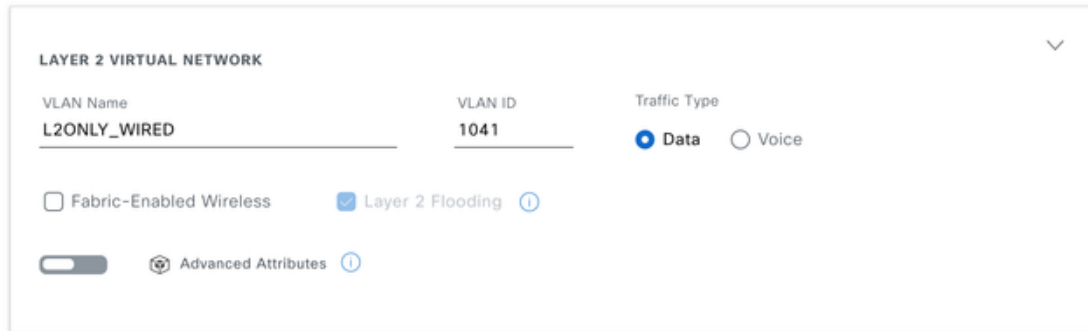
L2のみのVLAN設定

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

Configuration Attributes

Provide a name for each Layer 2 Virtual Network and define its attributes.



L2VNIの設定

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はありません。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) は設定されません。代わりに、ARPパケットのフラッディングは「flood arp-nd」で明示的に有効になります。

ファブリックエッジ(192.168.0.101)の設定

<#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
```

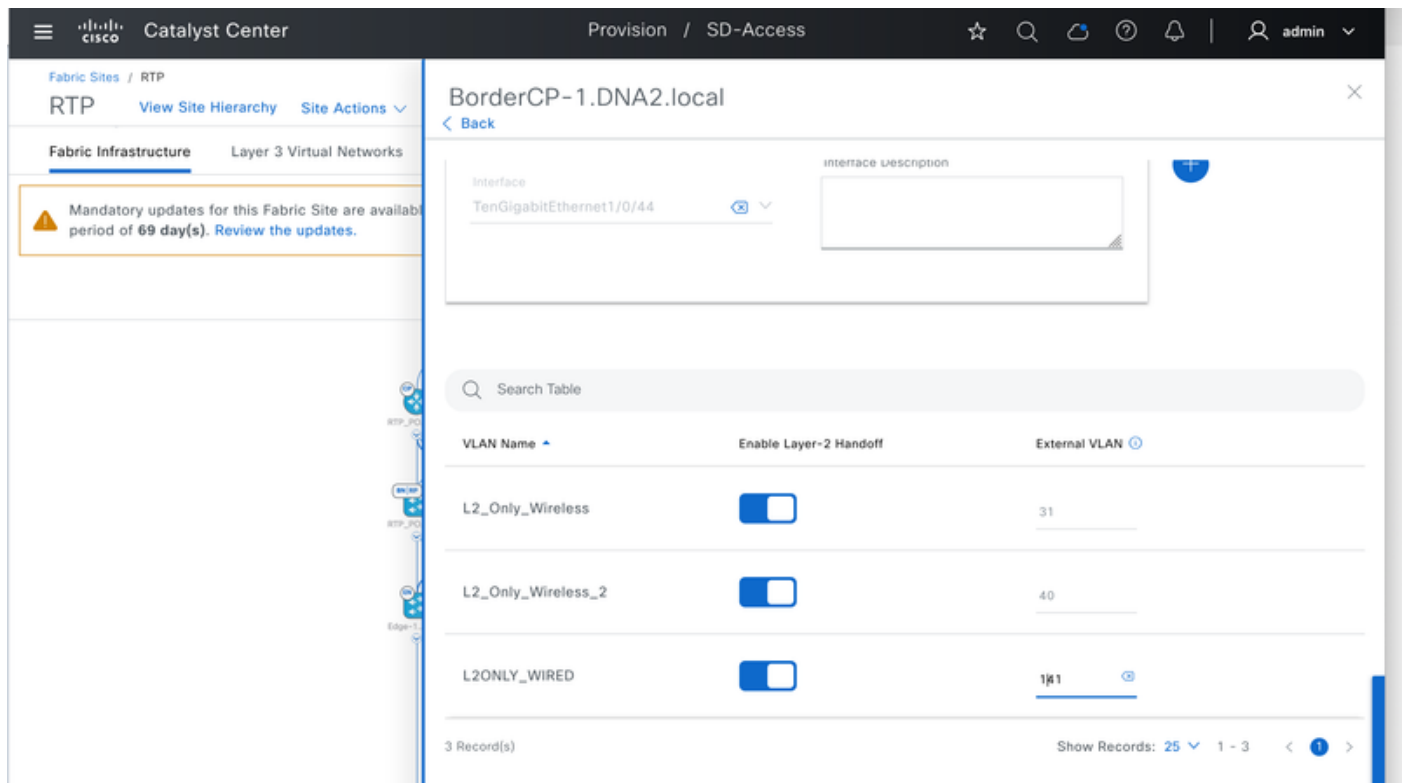
```
database-mapping mac locator-set rloc_91947dad-3621-42bd-ab6b-379ecebb5a2b
exit-service-ethernet
```

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、境界とエッジの両方を含め、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

ファブリックボーダー(192.168.0.201)の設定

<#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
```

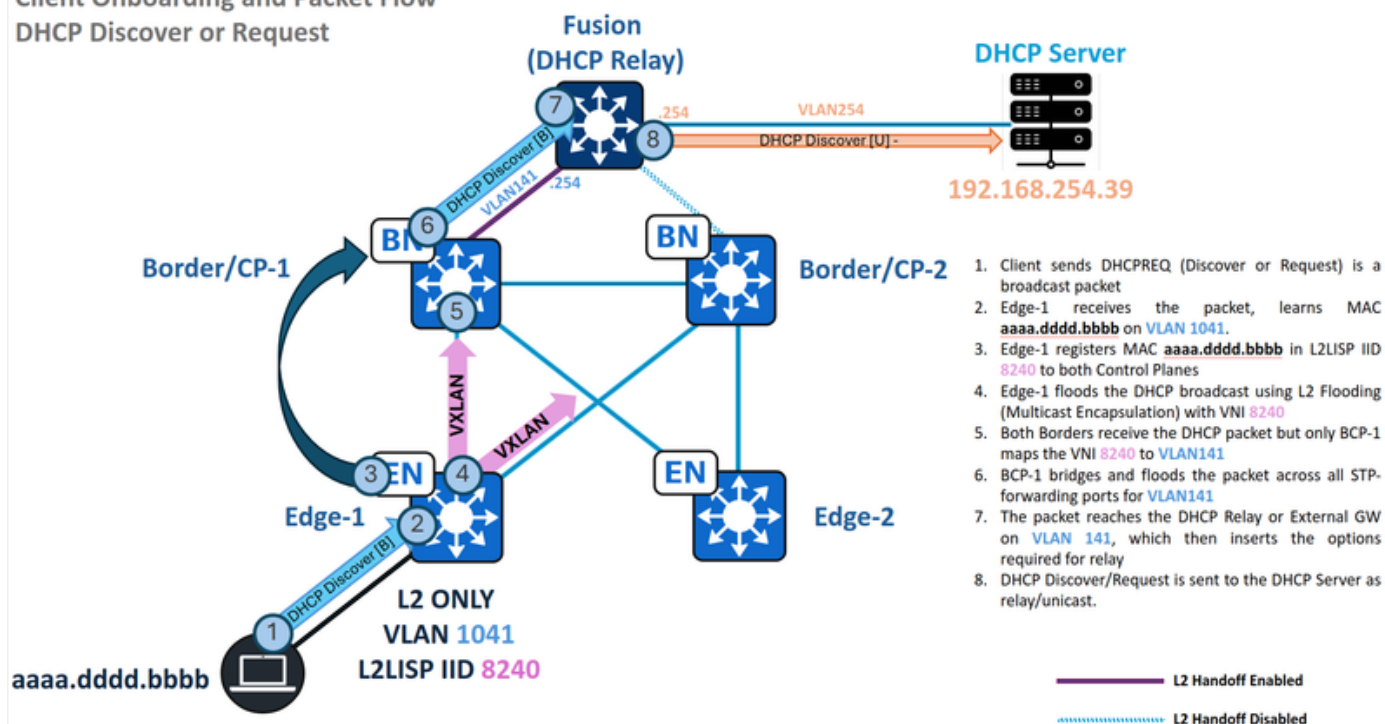
interface TenGigabitEthernet1/0/44

switchport mode trunk

DHCPトラフィックフロー

DHCPの検出と要求 – エッジ

Client Onboarding and Packet Flow DHCP Discover or Request



トラフィックフロー – DHCPによるL2のみの検出および要求

MACラーニングおよびエンドポイント登録

エンドポイントaaaa.dddd.bbbbがDHCP DiscoverまたはRequest (ブロードキャストパケット)を送信する場合、エッジノードはエンドポイントのMACアドレスを学習してMACアドレステーブルに追加した後、L2/MAC SISFテーブルに追加し、最後にL2LISPインスタンス8240にマッピングされたVLAN 1041のL2LISPデータベースに追加する必要があります。

<#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.ddd.bbb|vlan

MAC	Interface	vlan	prlv	state	Time left	Policy
aaaa.ddd.bbb	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.ddd.bbb

Dyn-EID Name	Dynamic-EID	Interface	Uptime	Last	Pending
Auto-L2-group-					
8240					

aaaa.ddd.bbb
 N/A 6d04h never
0

Edge-1#
show lisp instance-id 8240 ethernet database aaaa.ddd.bbb

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.ddd.bbb/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

```

エンドポイントのMACアドレスが正しく学習され、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 is enabled

```

Switch DHCP gleanig 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>

```

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

エイスを使用して、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 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:

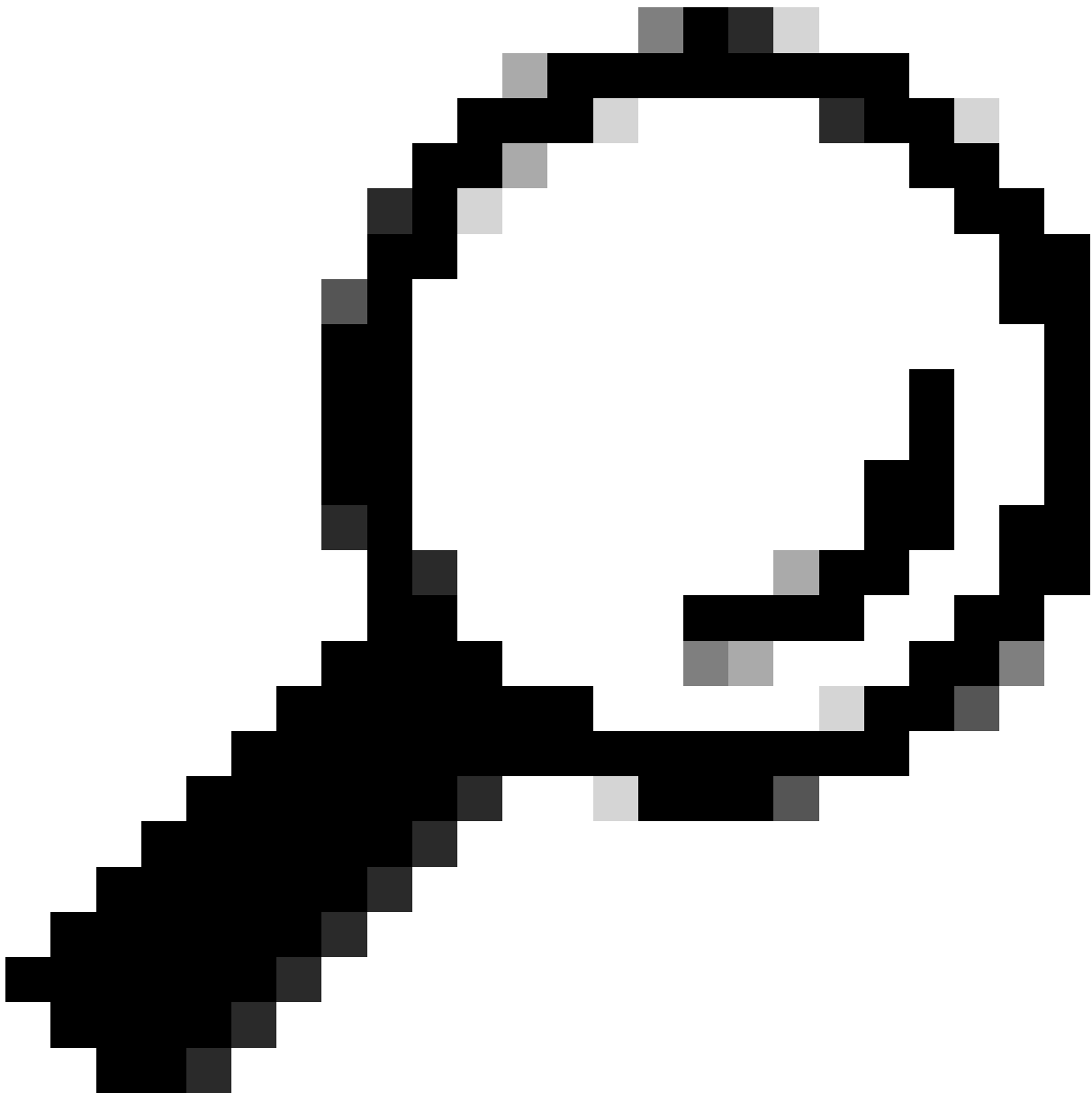
7

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

<--

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

Totals - Source count: 1, Packet count: 8



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

エンドポイントからの着信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、スイッチ上で同時組み込みパケットキャプチャを設定します。パケットキャプチャでは、2つの異なるパケットを確認する必要があります。1つは元のDHCP Discover/Requestで、もう1つはVXLANでカプセル化され、アンダーレイグループ(239.0.17.1)宛てです。

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 TenGigabitEthernet1/0/2 IN      <-- Endpoint Interface
```

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

```
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.ddd.bbb"
```

<-- aaaa.ddd.bbb 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.ddd.bbb 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.ddd.bbb 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
```

DHCPの検出と要求 – L2ボーダー

エッジがレイヤ2フラッディングを介してDHCP DiscoverおよびRequestパケットを送信した後 (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)、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 141

VLAN Name	Status	Ports
141 L2ONLY_WIRED		

active

L2LIO:

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

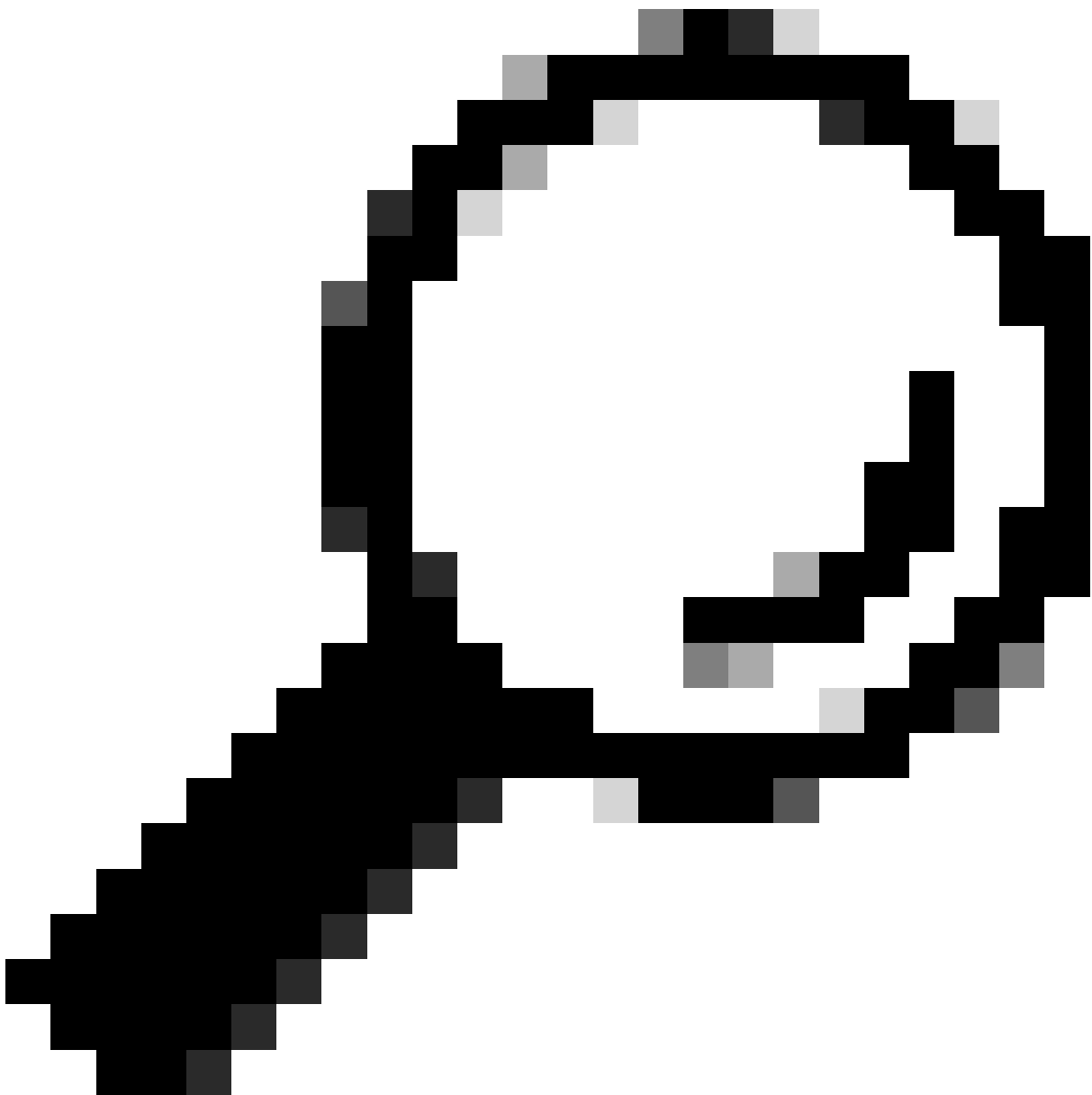
HW Forwarding:

3

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

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

Totals - Source count: 1, Packet count: 4



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 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
```

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 141 | 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	prlv1	age
ARP					
172.16.141.254					
f87b.2003.7fc0					
Te1/0/44					
141					

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

```
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==aaaa.ddd.ddd"
```

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

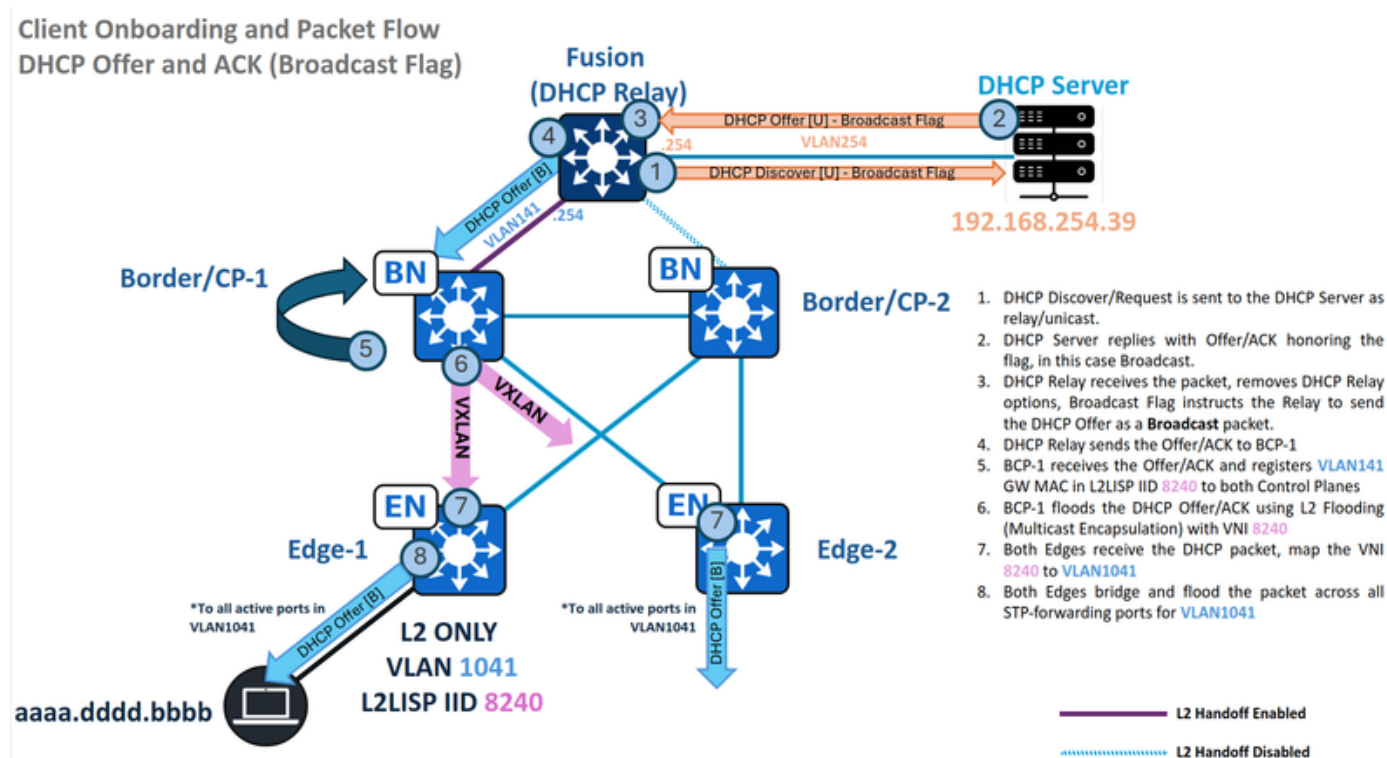
Packet 428: Plain (dot1q cannot be captured at egress direction)

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

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ため、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 SIFSテーブルに追加し、最後にL2LISPインスタンス8240にマッピングされたVLAN 141のL2LISPデータベースに追加する必要があります。

<#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	prlv1	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

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

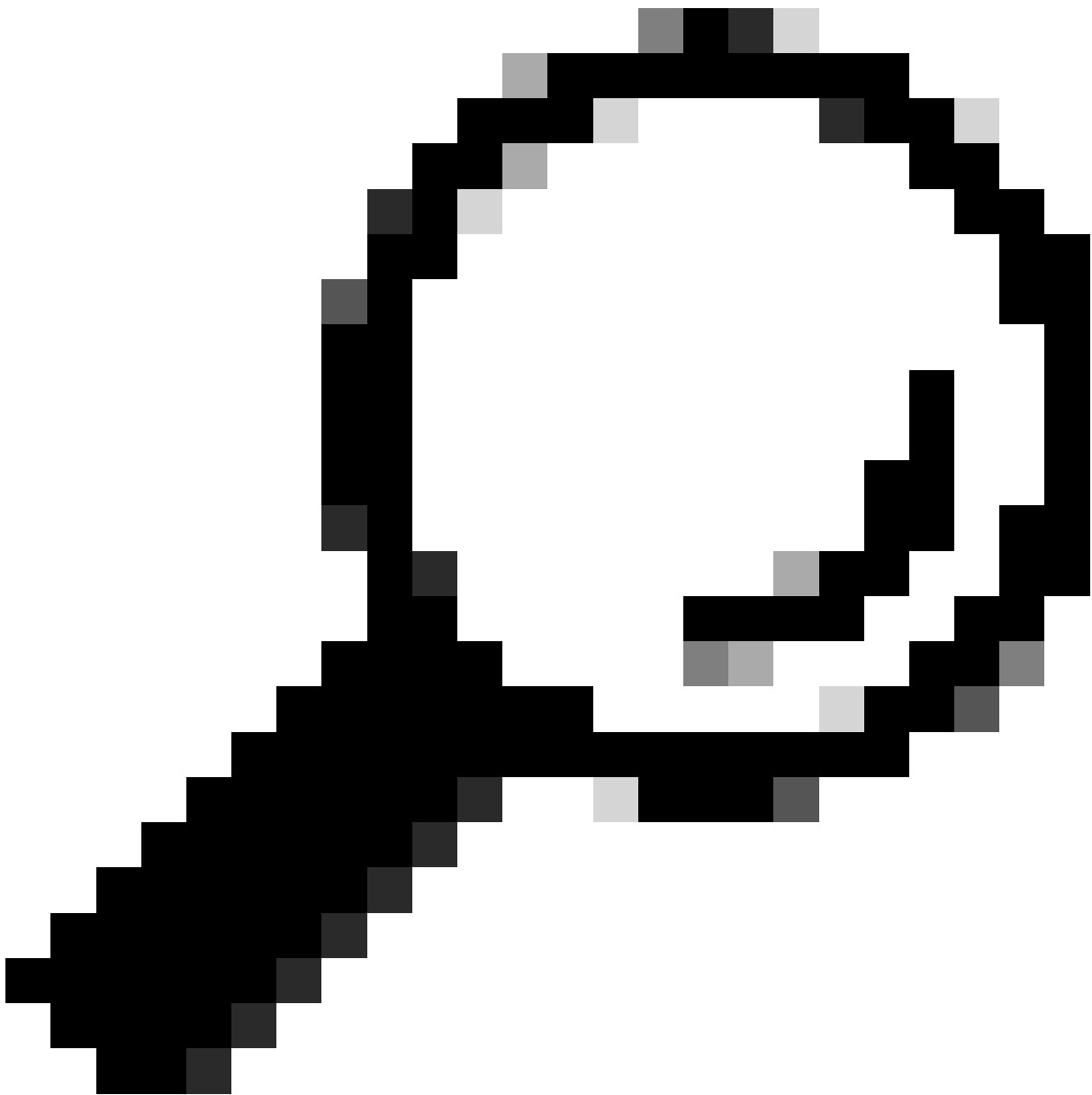
```
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
1001
```

DHCP snooping is operational on following VLANs:

1001 <-- 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



ヒント:DHCPスヌーピングはL2Borderでは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iddiing(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 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

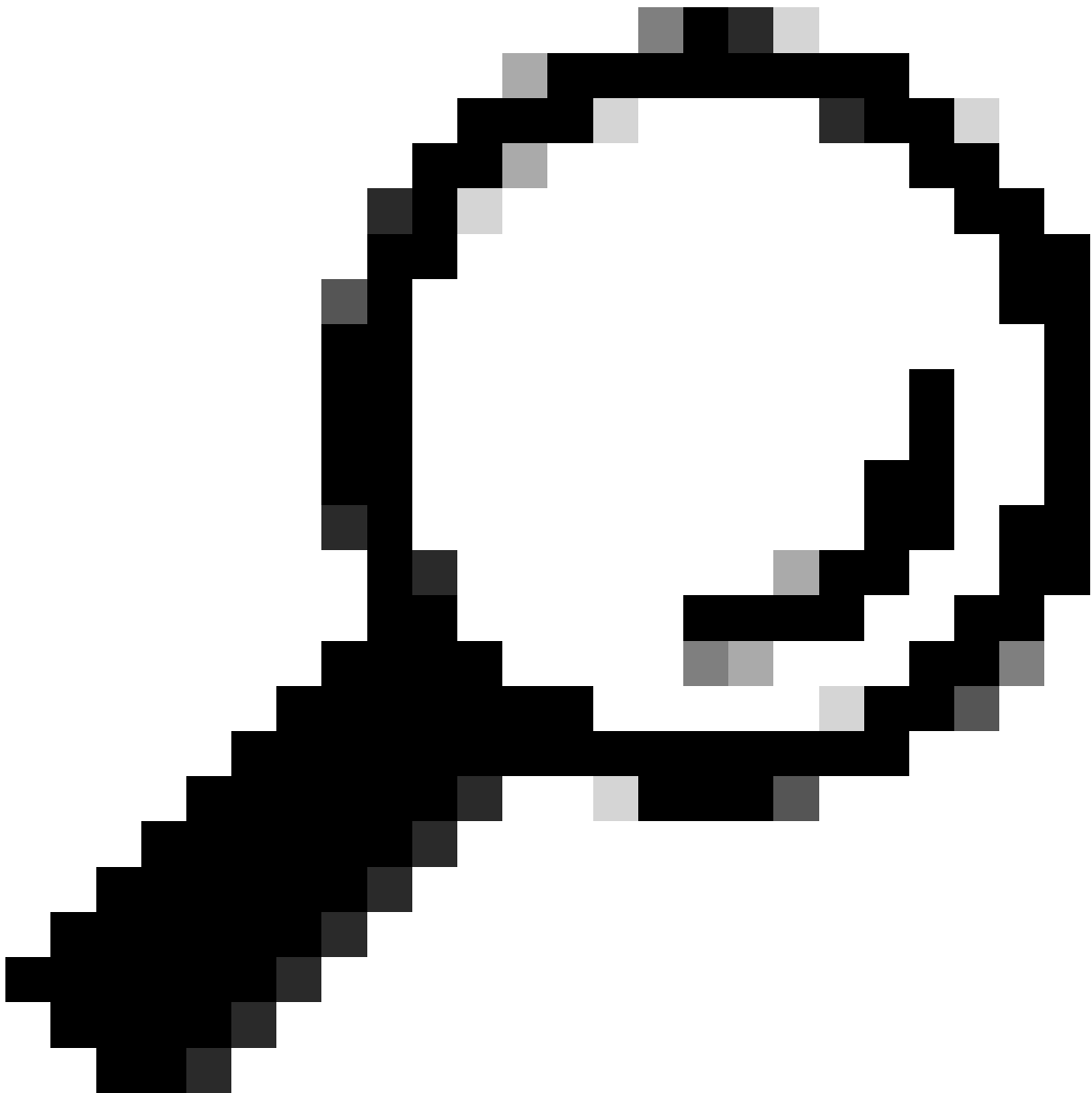
HW Forwarding:

92071

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

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

Totals - Source count: 1, Packet count: 92071



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、DHCPオファーが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転送されるため、このセクションは終了します。

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 1041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 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 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 RL0C)

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,

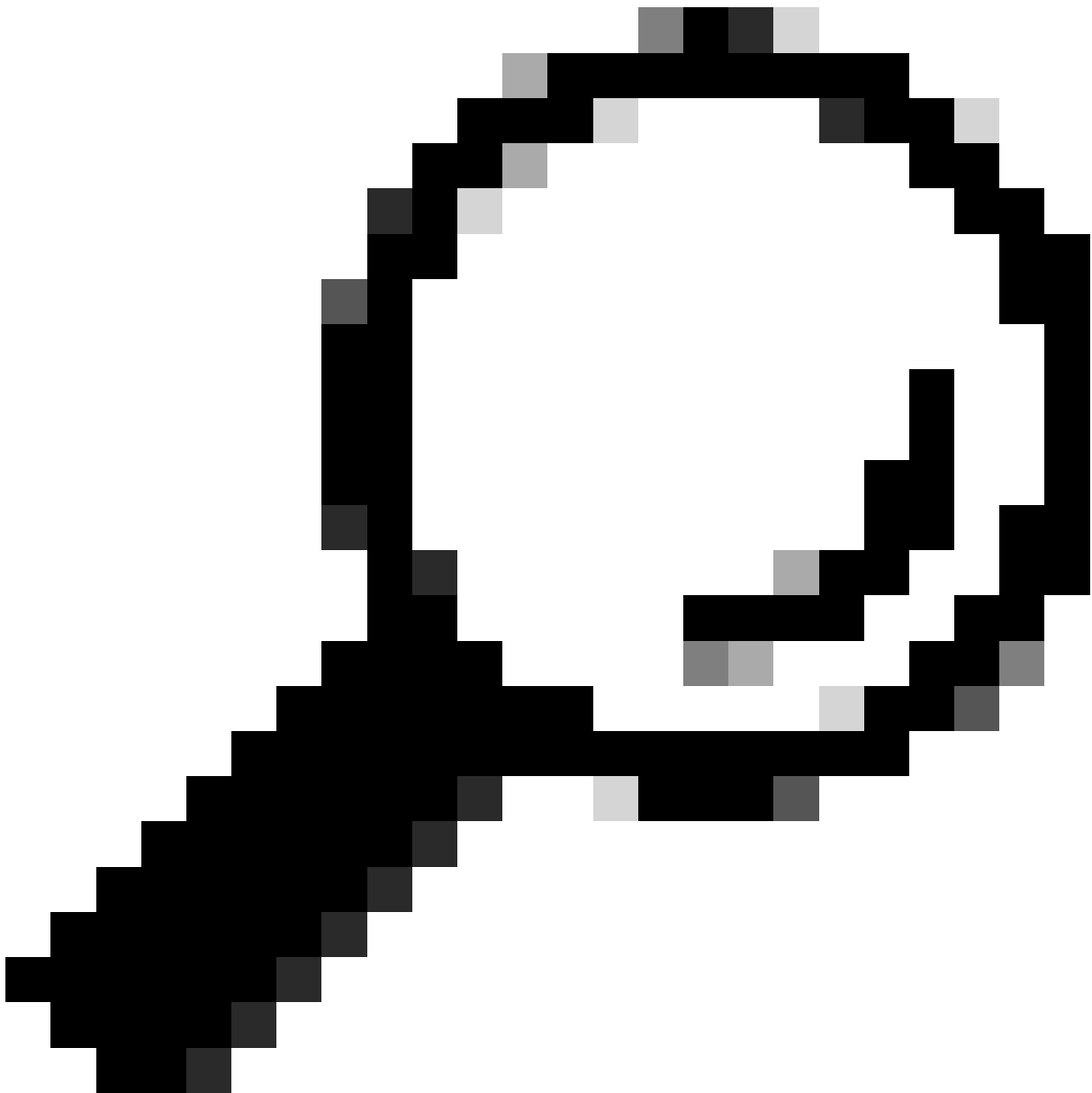
SW Forwarding: 1/0/96/0, Other: 0/0/0
HW Forwarding:

76236

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

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

Totals - Source count: 1, Packet count: 4



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行われています。

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、パケットはVLAN1041のすべての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			

MACアドレステーブルは、ポートTe1/0/2をエンドポイントポートとして識別します。このポートはSTPによってFWD状態になっており、パケットはエンドポイントにフラッディングされます。

<#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			

DHCPオファ―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、ARPパケットの収集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	prlv	ag
ARP					
172.16.141.1					
aaaa.dddd.bbbb					
	Te1/0/2				
1041					
0005	45s	REACHABLE	207 s	try 0	

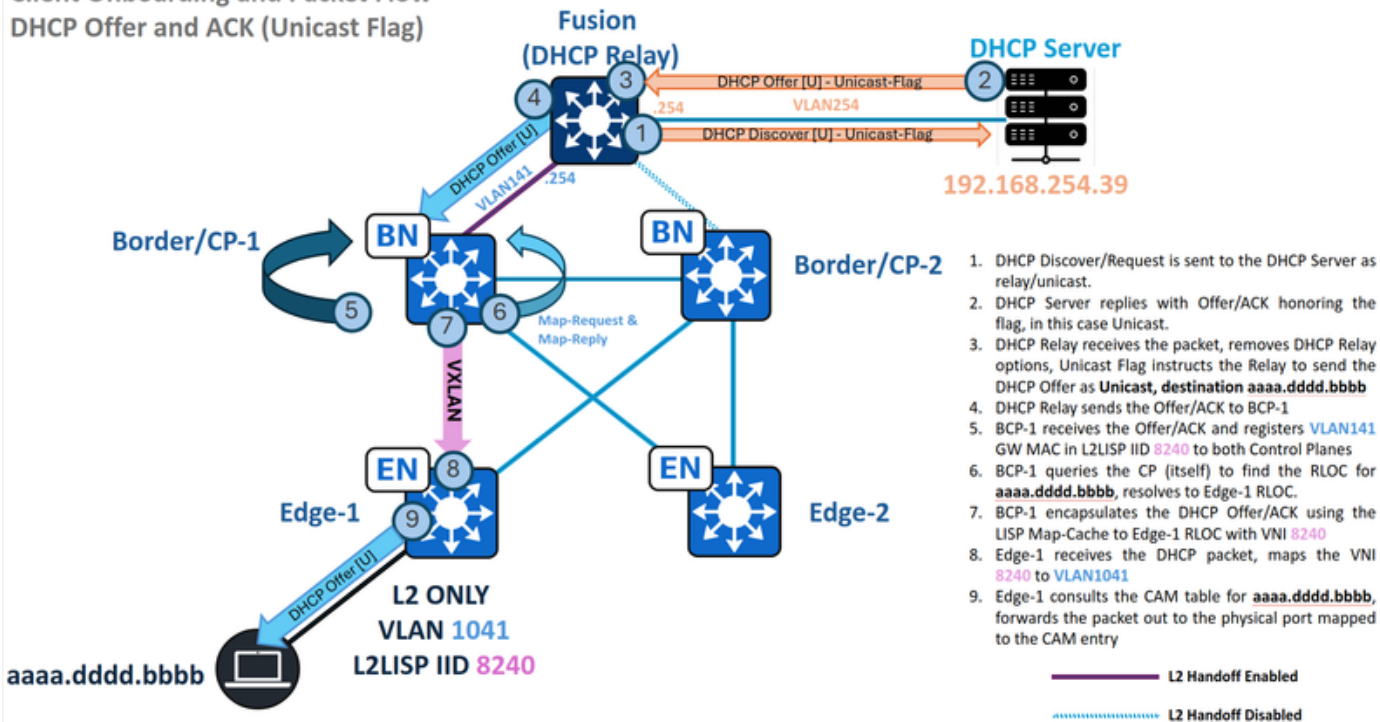
Edge-1#

show ip dhcp snooping binding vlan 1041

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
-----	-----	-----	-----	----	-----
Total number of bindings: 0					

DHCPオファ―およびACK – ユニキャスト – L2ボーダー

DHCP Offer and ACK (Unicast Flag)



トラフィックフロー – ユニキャストDHCPオファアおよび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。

フアブリックBorder/CP(192.168.0.201)/パケットCatPURE：入力DHCPオフア－

<#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 (DHCP)

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)

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、オファア/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(aaaa.dddd.bbbb)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ラーニングとエンドポイント登録」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 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 0xDEFA44F0B-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
```

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 8240 ethernet map-cache aaaa.ddd.ddd

LISP MAC Mapping Cache for LISP 0 EID-table Vlan

141

(IID

8240

), 1 entries

aaa.ddd.ddd/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)がユニキャストにカプセル化され、VNI 8240を使用して192.168.0.101のEdge-1に直接送信されます。

<#root>

BorderCP-1#

show mac address-table address aaaa.ddd.ddd

Mac Address Table			
Vlan	Mac Address	Type	Ports
141	aaaa.ddd.ddd		

aaaa.ddd.ddd

CP_LEARN

L2LI0

BorderCP-1#

show platform software fed switch active matm macTable vlan 141 mac aaaa.ddd.ddd

VLAN	MAC	Type	Seq#	EC_Bi	Flags	machandle	siHandle	riHandle	diHandle
141	aaaa.ddd.ddd								
	0x1000001	0	0	64	0x718eb5271228	0x718eb52b4d68	0x718eb52be578	0x0	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
```

前のセクションと同じ方法で、DHCPリレーからの入力とRLOC出カ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―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。ブロードキャストオファ―/ACKとは異なり、エッジノードは、パケットをすべてのポートにフラッディングするのではなく、エンドポイントが接続されている特定のポートにのみ転送します。

MACアドレステーブルは、ポートTe1/0/2をクライアントポートとして識別します。このクライアントポートはSTPによってFWD状態になっており、パケットはエンドポイントに転送されます。

```
<#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
```

DHCPオファ―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が、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 dhcp snooping 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	prlv1	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

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。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。

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。