Fehlerbehebung bei DHCP im Nur-Layer-2-VLAN (kabelgebunden)

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung bei DHCP für kabelgebundene Endgeräte in einem Layer-2 Only-Netzwerk in SD-Access (SDA) Fabric beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Internet Protocol (IP)-Weiterleitung
- Locator/ID Separation Protocol (LISP)
- Protocol Independent Multicast (PIM) Sparse-Mode

Hardware- und Softwareanforderungen

- Catalyst Switches der Serie 9000
- Catalyst Center Version 2.3.7.9
- Cisco IOS® XE 17.12 und höher

Einschränkungen

- Nur eine L2-Grenze kann gleichzeitig ein eindeutiges VLAN/VNI übergeben, es sei denn, robuste Mechanismen zur Vermeidung von Schleifen, wie FlexLink+ oder EEM-Skripts zum Deaktivieren von Verbindungen, sind ordnungsgemäß konfiguriert.

Nur L2 - Überblick

Überblick

In typischen SD-Access-Bereitstellungen befindet sich die L2/L3-Grenze am Fabric Edge (FE), wo der FE das Client-Gateway in Form einer SVI hostet, die häufig als "Anycast Gateway" bezeichnet wird. L3-VNIs (geroutet) werden für den Datenverkehr zwischen Subnetzen eingerichtet, während L2-VNIs (geswitcht) den Datenverkehr zwischen Subnetzen verwalten. Die konsistente Konfiguration aller FEs ermöglicht ein nahtloses Client-Roaming. Die Weiterleitung ist optimiert: Intra-Subnetz-Datenverkehr (L2) wird direkt zwischen FEs überbrückt, und Intersubnetz-Datenverkehr (L3) wird entweder zwischen FEs oder zwischen einem FE und einem Border Node geroutet.

Für Endpunkte in SDA-Strukturen, die einen strikten Netzwerkeingangspunkt außerhalb der Struktur erfordern, muss die SDA-Struktur einen L2-Kanal vom Edge zu einem externen Gateway bereitstellen.

Dieses Konzept entspricht herkömmlichen Ethernet-Campus-Bereitstellungen, bei denen ein Layer-2-Zugangsnetzwerk mit einem Layer-3-Router verbunden ist. Der VLAN-interne Datenverkehr verbleibt im L2-Netzwerk, während der VLAN-übergreifende Datenverkehr vom L3-Gerät weitergeleitet wird und häufig zu einem anderen VLAN im L2-Netzwerk zurückkehrt.

Innerhalb eines LISP-Kontexts verfolgt die Standortkontrollebene MAC-Adressen und die zugehörigen MAC-zu-IP-Bindungen im Wesentlichen wie traditionelle ARP-Einträge. Reine L2 VNI/L2-Pools erleichtern die Registrierung, Auflösung und Weiterleitung ausschließlich auf Basis dieser beiden EID-Typen. Daher beruht jede LISP-basierte Weiterleitung in einer reinen L2-Umgebung ausschließlich auf MAC- und MAC-zu-IP-Informationen. IPv4- oder IPv6-EIDs werden dabei nicht berücksichtigt. Als Ergänzung zu LISP EIDs hängen L2-Pools stark von Flood-and-Learn-Mechanismen ab, ähnlich wie bei herkömmlichen Switches. Folglich wird L2-Flooding zu einer wichtigen Komponente für die Verarbeitung von Broadcast-, Unknown Unicast- und Multicast (BUM)-Datenverkehr innerhalb dieser Lösung. Dafür ist Underlay Multicast erforderlich.

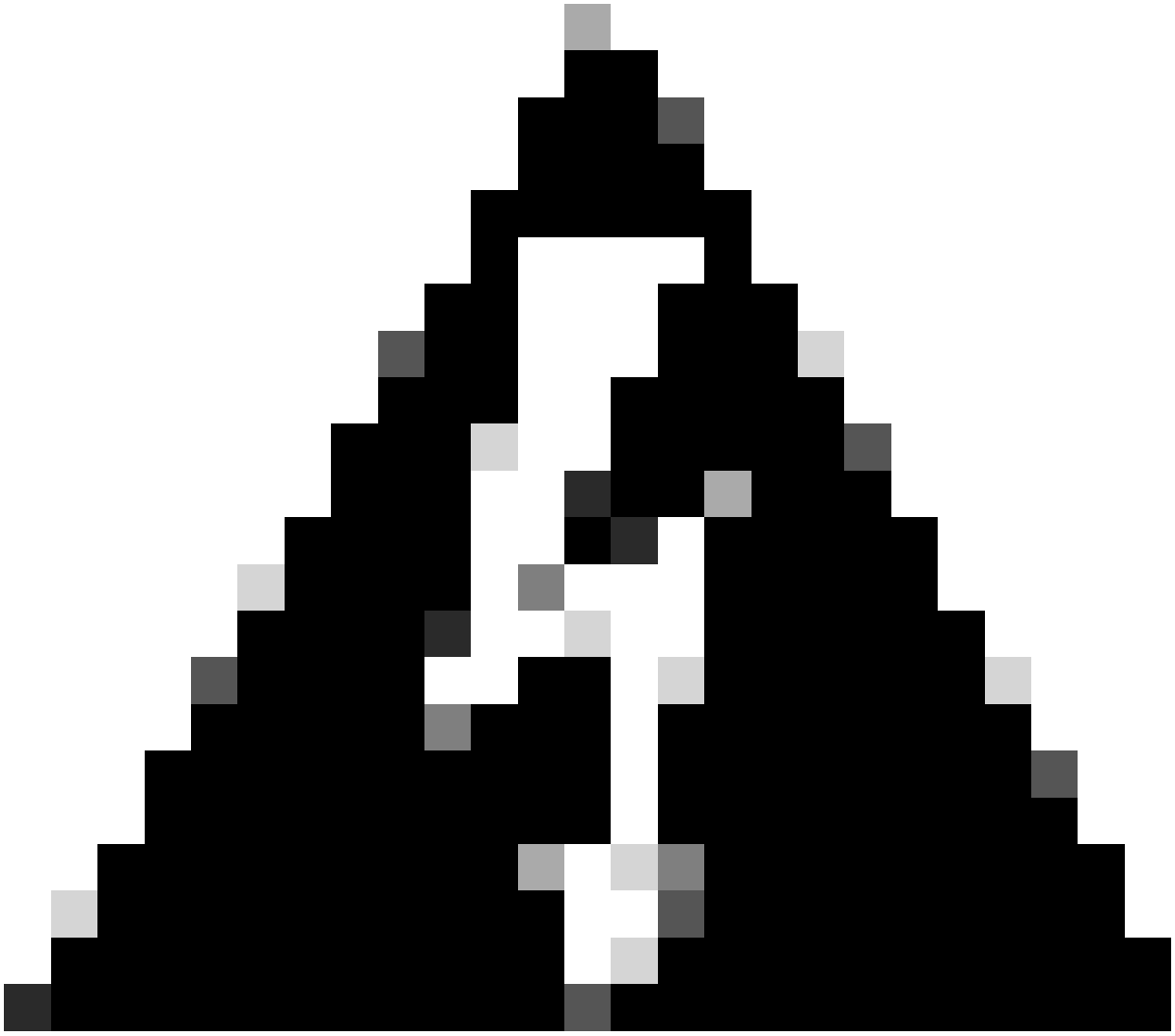
Umgekehrt wird normaler Unicast-Datenverkehr über standardmäßige LISP-Weiterleitungsprozesse weitergeleitet, hauptsächlich über Map-Caches.

Sowohl die Fabric-Edges als auch die "L2-Grenze" (L2B) verwalten L2-VNIs, die lokalen VLANs zugeordnet sind (diese Zuordnung ist innerhalb von SDA lokal gerätespezifisch, sodass verschiedene VLANs dem gleichen L2-VNI knotenübergreifend zugeordnet werden können). In diesem speziellen Anwendungsfall wird auf diesen VLANs an diesen Knoten keine SVI konfiguriert, d. h. es gibt keinen entsprechenden L3-VNI.

Änderung des DHCP-Verhaltens in reinen L2-VLANs

Bei Anycast Gateway-Pools stellt DHCP eine Herausforderung dar, da jeder Fabric Edge als Gateway für seine direkt verbundenen Endpunkte mit derselben Gateway-IP in allen FEs fungiert. Um die ursprüngliche Quelle eines DHCP-weitergeleiteten Pakets richtig zu identifizieren, müssen FEs die DHCP-Option 82 und die zugehörigen Unteroptionen, einschließlich der LISP RLOC-Informationen, einfügen. Dies wird durch DHCP-Snooping auf dem Client-VLAN am Fabric-Edge erreicht. DHCP-Snooping erfüllt in diesem Zusammenhang zwei Zwecke: Sie vereinfacht die Integration von Option 82 und verhindert vor allem die Flut von DHCP-Broadcast-Paketen über die Bridge-Domäne (VLAN/VNI). Selbst wenn Layer-2-Flooding für einen Anycast-Gateway aktiviert ist, unterdrückt DHCP-Snooping das Broadcast-Paket, das als Broadcast vom Fabric Edge weitergeleitet werden soll.

Im Gegensatz dazu fehlt einem Layer-2-Only-VLAN ein Gateway, was die DHCP-Quellenidentifizierung vereinfacht. Da die Pakete nicht über Fabric-Edges weitergeleitet werden, sind komplexe Mechanismen zur Quellenidentifizierung nicht erforderlich. Ohne DHCP-Snooping im L2 Only-VLAN wird der Flood-Kontrollmechanismus für DHCP-Pakete effektiv umgangen. Dadurch können DHCP-Broadcasts über L2 Flooding an ihr endgültiges Ziel weitergeleitet werden. Hierbei kann es sich um einen DHCP-Server handeln, der direkt mit einem Fabric-Knoten oder einem Layer-3-Gerät verbunden ist, das DHCP-Relay-Funktionalität bereitstellt.



Warnung: Die Funktion "Multiple IP to MAC" (Mehrere IP-Adressen zu MAC) in einem L2 Only-Pool aktiviert DHCP-Snooping automatisch im Bridge-VM-Modus, wodurch die DHCP-Flood-Kontrolle erzwungen wird. Dadurch ist der L2 VNI-Pool nicht mehr in der Lage, DHCP für seine Endpunkte zu unterstützen.

Underlay-Multicast

Da DHCP stark auf Broadcast-Datenverkehr angewiesen ist, muss Layer-2-Flooding verwendet werden, um dieses Protokoll zu unterstützen. Wie bei jedem anderen Pool mit aktiviertem L2-Flooding muss das Underlay-Netzwerk für Multicast-Datenverkehr konfiguriert werden, insbesondere für Any-Source-Multicast unter Verwendung des PIM Sparse-Mode. Während die Multicast-Basiskonfiguration über den LAN-Automatisierungs-Workflow automatisiert wird, ist beim Auslassen dieses Schritts eine zusätzliche Konfiguration erforderlich (manuell oder als Vorlage).

- Aktivieren Sie IP-Multicast-Routing auf allen Knoten (Grenzen, Kanten, Zwischenknoten usw.).
- Konfigurieren Sie den PIM Sparse-Mode an der Loopback0-Schnittstelle jedes Border- und

Edge-Knotens.
- Aktivieren Sie PIM Sparse-Mode an jeder IGP-Schnittstelle (Underlay Routing Protocol).
- Konfigurieren Sie den PIM Rendezvous Point (RP) auf allen Knoten (Ränder, Kanten, Zwischenknoten), RP-Platzierung auf Rändern wird empfohlen.
- Überprüfen Sie die PIM-Nachbarn, den PIM RP- und den PIM Tunnel-Status.

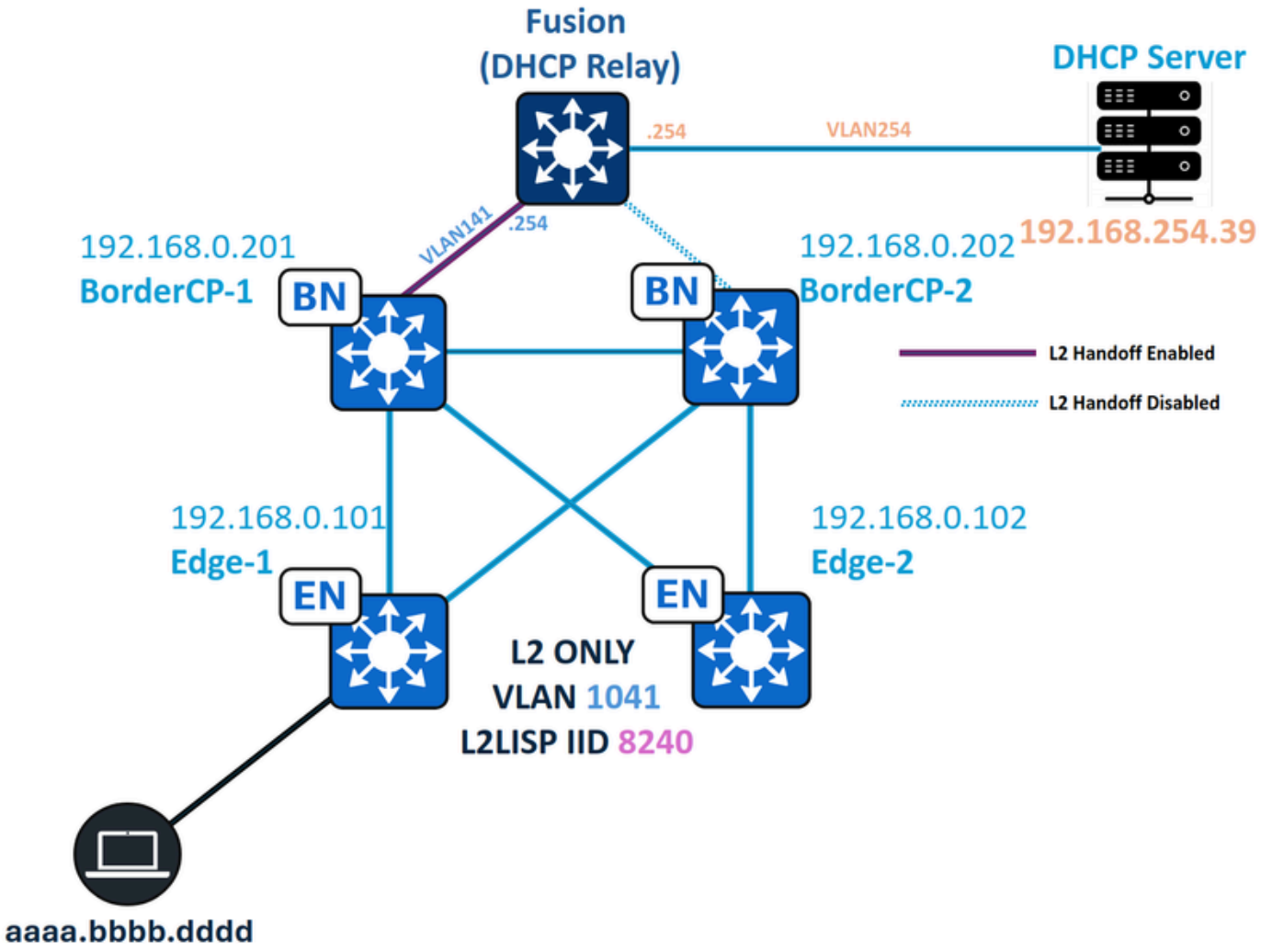
DHCP-Server innerhalb der SD-Access Fabric

Eine häufige Designfrage lautet, ob ein DHCP-Server innerhalb einer SD-Access-Fabric bereitgestellt werden kann. Die Antwort ist im Wesentlichen ja und nein.

Das offizielle Cisco Validated Design empfiehlt, den DHCP-Server außerhalb der Fabric zu platzieren, in der Regel innerhalb des Shared Services-Blocks. Wenn jedoch die physische Verbindung des DHCP-Servers mit einem Fabric-Knoten (z. B. einem Edge oder Border) erforderlich ist, wird als Methode nur ein L2 Only-Netzwerk unterstützt. Dies ist auf das inhärente Verhalten von Anycast Gateway-Pools zurückzuführen, in denen DHCP-Snooping standardmäßig aktiviert ist. Dadurch werden nicht nur DHCP-Angebote und -Bestätigungen vom Server blockiert, sondern auch die Weiterleitung von DHCP-Erkennungs- und -Anforderungspaketen, selbst wenn diese in VXLAN gekapselt sind, wird verhindert. Während "DHCP Snooping Trust" auf DHCP-Server-Ports Angebote und Bestätigungen zulässt, werden Ermittlungs- und Anforderungspakete nicht mit der gleichen Methode weitergeleitet. Darüber hinaus wird die Entfernung von DHCP-Snooping in einem Anycast Gateway-Pool nicht unterstützt, da Catalyst Center eine solche Konfigurationsabweichung bei der Compliance-Validierung markiert.

Umgekehrt wird DHCP-Snooping nicht erzwungen, wenn sich der DHCP-Server in einem reinen L2-Netzwerk befindet, sodass alle DHCP-Pakete ohne richtlinienbasierte Überprüfung oder Blockierung übertragen werden können. Das Netzwerkgerät, das der SD-Access Fabric vorgeschaltet ist (z. B. ein Fusion Router), wird als Gateway für das L2 Only-Netzwerk konfiguriert, sodass der Datenverkehr von mehreren VRFs auf den gleichen DHCP-Server innerhalb dieses L2 Only-Segments zugreifen kann.

Topologie



Netzwerktopologie

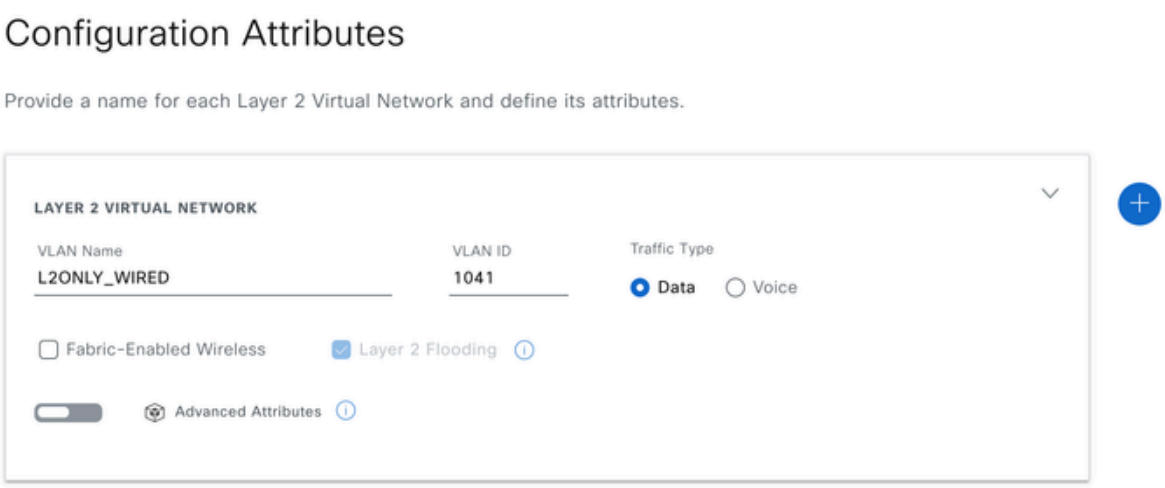
In dieser Topologie gilt Folgendes:

- 192.168.0.201 und 192.168.0.202 sind nebeneinander liegende Ränder für den Fabric-Standort. BorderCP-1 ist der einzige Ränder, bei dem die Layer-2-Handoff-Funktion aktiviert ist.
- 192.168.0.101 und 192.168.0.102 sind Fabric Edge-Knoten
- 192.168.254.39 ist der DHCP-Server
- aaaa.bbb.dddd ist der DHCP-fähige Endpunkt.
- Das Fusion-Gerät fungiert als DHCP-Relay für die Fabric-Subnetze.

Konfiguration des reinen L2-VLANs

L2 Only-VLAN-Bereitstellung von Catalyst Center

Pfad: Catalyst Center/Bereitstellung/Fabric-Standort/Virtuelle Layer-2-Netzwerke/Bearbeiten von virtuellen Layer-2-Netzwerken



L2VNI-Konfiguration

L2 Only-VLAN-Konfiguration - Fabric-Edges

Für Fabric Edge-Knoten ist das VLAN mit aktiviertem CTS, IGMP und IPv6 MLD sowie der erforderlichen L2-LISP-Konfiguration konfiguriert. Dieser L2 Only-Pool ist kein Wireless-Pool. Aus diesem Grund sind Funktionen, die in der Regel nur in L2-Wireless-Pools vorhanden sind, wie RA-Guard, DHCPGuard und Flood Access Tunnel, nicht konfiguriert. Stattdessen wird das Flooding von ARP-Paketen explizit mit "flood arp-nd" aktiviert.

Fabric Edge-Konfiguration (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
```

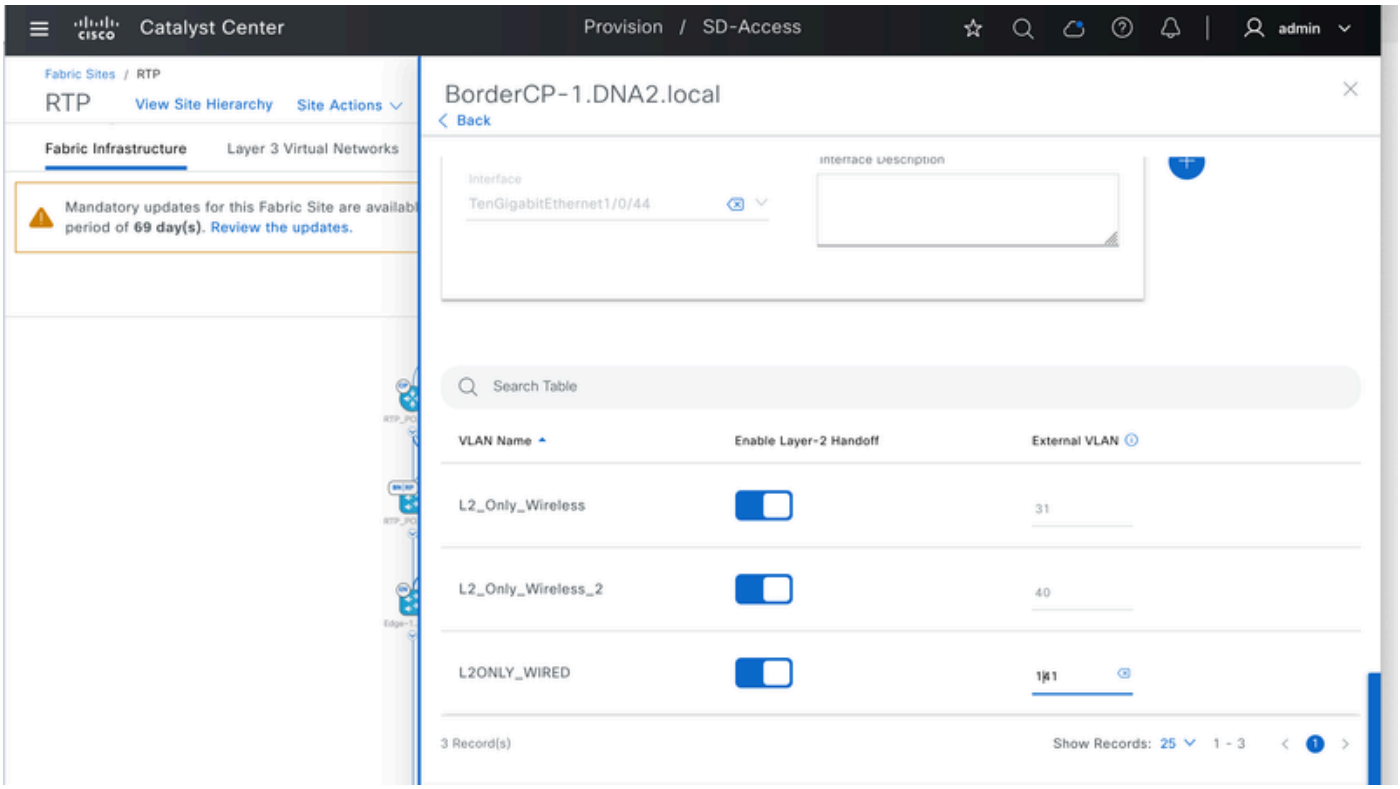
```
router lisp
 instance-id
8240
  remote-rloc-probe on-route-change
  service ethernet
eid-table vlan
1041
   broadcast-underlay
239.0.17.1
flood arp-nd
 flood unknown-unicast
   database-mapping mac locator-set rloc_91947dad-3621-42bd-ab6b-379ecebb5a2b
   exit-service-ethernet
```

L2-Übergabekonfiguration - Fabric Border

Aus betrieblicher Sicht kann der DHCP-Server (oder Router/Relay) mit jedem beliebigen Fabric-Knoten verbunden werden, einschließlich Borders und Edges.

Die Verwendung von Border Nodes zur Verbindung mit dem DHCP-Server ist jedoch der empfohlene Ansatz, erfordert jedoch eine sorgfältige Designüberlegung. Der Grund hierfür ist, dass Border für L2 Hand-Off auf Schnittstellenbasis konfiguriert werden muss. Dadurch kann der Fabric-Pool entweder an dasselbe VLAN wie im Fabric oder an ein anderes übergeben werden. Diese Flexibilität bei VLAN-IDs zwischen Fabric-Edges und -Borders ist möglich, da beide derselben L2-LISP-Instanz-ID zugeordnet sind. Physische L2-Hand-Off-Ports dürfen nicht gleichzeitig mit demselben VLAN aktiviert werden, um Layer-2-Schleifen innerhalb des SD-Zugangsnetzwerks zu verhindern. Aus Redundanzgründen sind Methoden wie StackWise Virtual, FlexLink+ oder EEM-Skripts erforderlich.

Für die Verbindung des DHCP-Servers oder Gateway-Routers mit einem Fabric Edge ist hingegen keine zusätzliche Konfiguration erforderlich.



L2-Übergabekonfiguration

Fabric Border (192.168.0.201)-Konfiguration

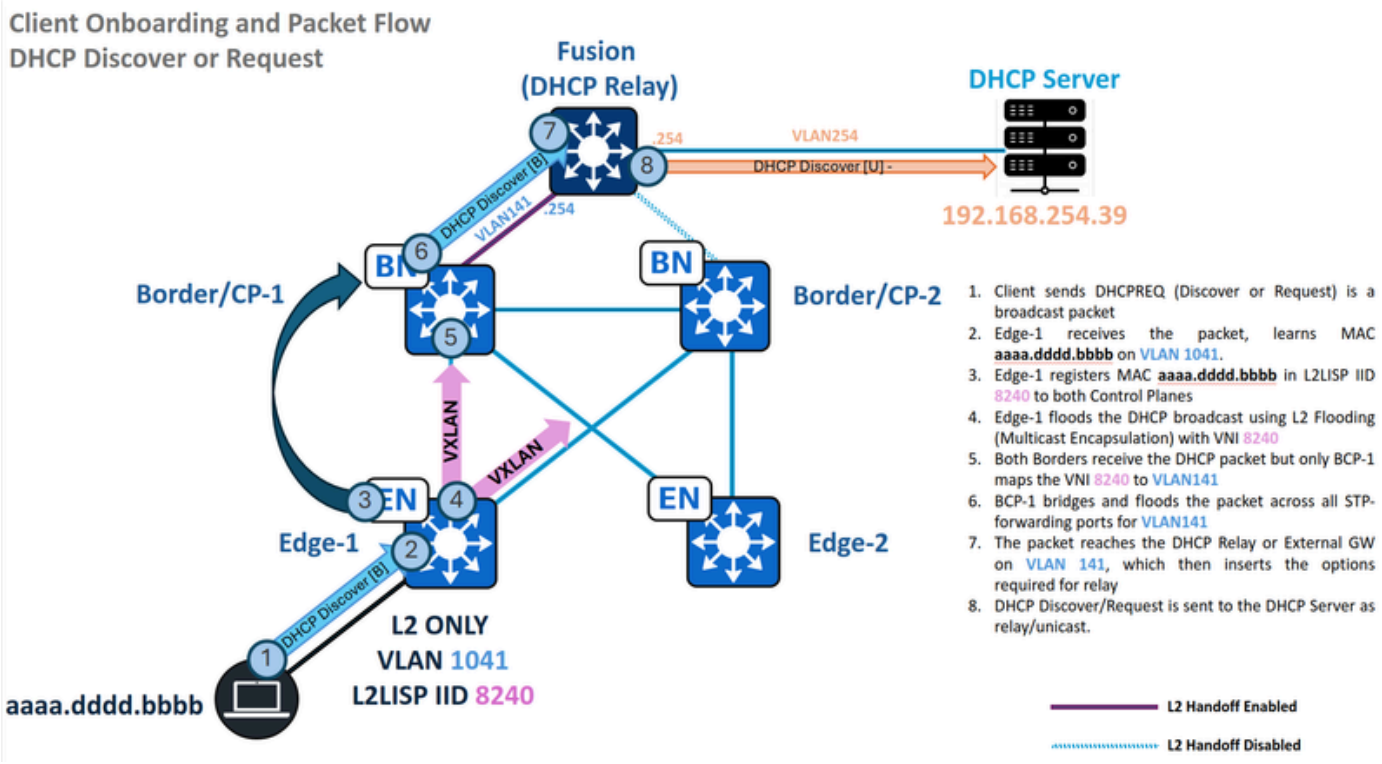
<#root>

```
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-Datenverkehrsfluss

DHCP-Erkennung und -Anforderung - Edge



Datenverkehrsfluss - DHCP-Erkennung und -Anforderung nur in L2

MAC Learning und Endpunktregistrierung

Wenn der Endpunkt aaaa.dddd.bbb eine DHCP-Erkennung oder -Anforderung (ein Broadcast-Paket) sendet, muss der Edge-Knoten die MAC-Adresse des Endpunkts ermitteln, sie seiner MAC-Adresstabelle hinzufügen, dann der L2/MAC-SISF-Tabelle und schließlich der L2LISP-Datenbank für VLAN 1041 zuordnen, L2LISP-Instanz 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
```

Wenn die MAC-Adresse des Endpunkts korrekt ermittelt wurde und das ACK-Flag für die Fabric-Kontrollebenen mit "Yes" markiert wurde, gilt diese Phase als abgeschlossen.

DHCP-Broadcast-Bridge bei L2-Flooding

Wenn DHCP Snooping deaktiviert ist, werden DHCP-Broadcasts nicht blockiert. Stattdessen werden sie für Layer-2-Flooding in Multicast eingekapselt. Umgekehrt verhindert die Aktivierung von DHCP Snooping das Flooding dieser Broadcast-Pakete.

<#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>
```

Da DHCP-Snooping deaktiviert ist, nutzt die DHCP-Erkennung/Anforderung die L2LISP0-

Schnittstelle und überbrückt den Datenverkehr über L2-Flooding. Je nach Catalyst Center-Version und den verwendeten Fabric-Bannern verfügt die L2LISP0-Schnittstelle über in beide Richtungen konfigurierte Zugriffslisten. Stellen Sie deshalb sicher, dass der DHCP-Datenverkehr (UDP-Ports 67 und 68) nicht explizit von Access Control Entries (ACEs) abgelehnt wird.

<#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

Verwenden Sie die konfigurierte Broadcast-Underlay-Gruppe für die L2LISP-Instanz und die Loopback0-IP-Adresse des Fabric Edge, um den L2 Flooding (S,G)-Eintrag zu überprüfen, der dieses Paket mit anderen Fabric-Knoten verbindet. In den mroute- und mfib-Tabellen können Sie Parameter wie die Eingangsschnittstelle, die Liste ausgehender Schnittstellen und die Weiterleitungszähler überprüfen.

<#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:

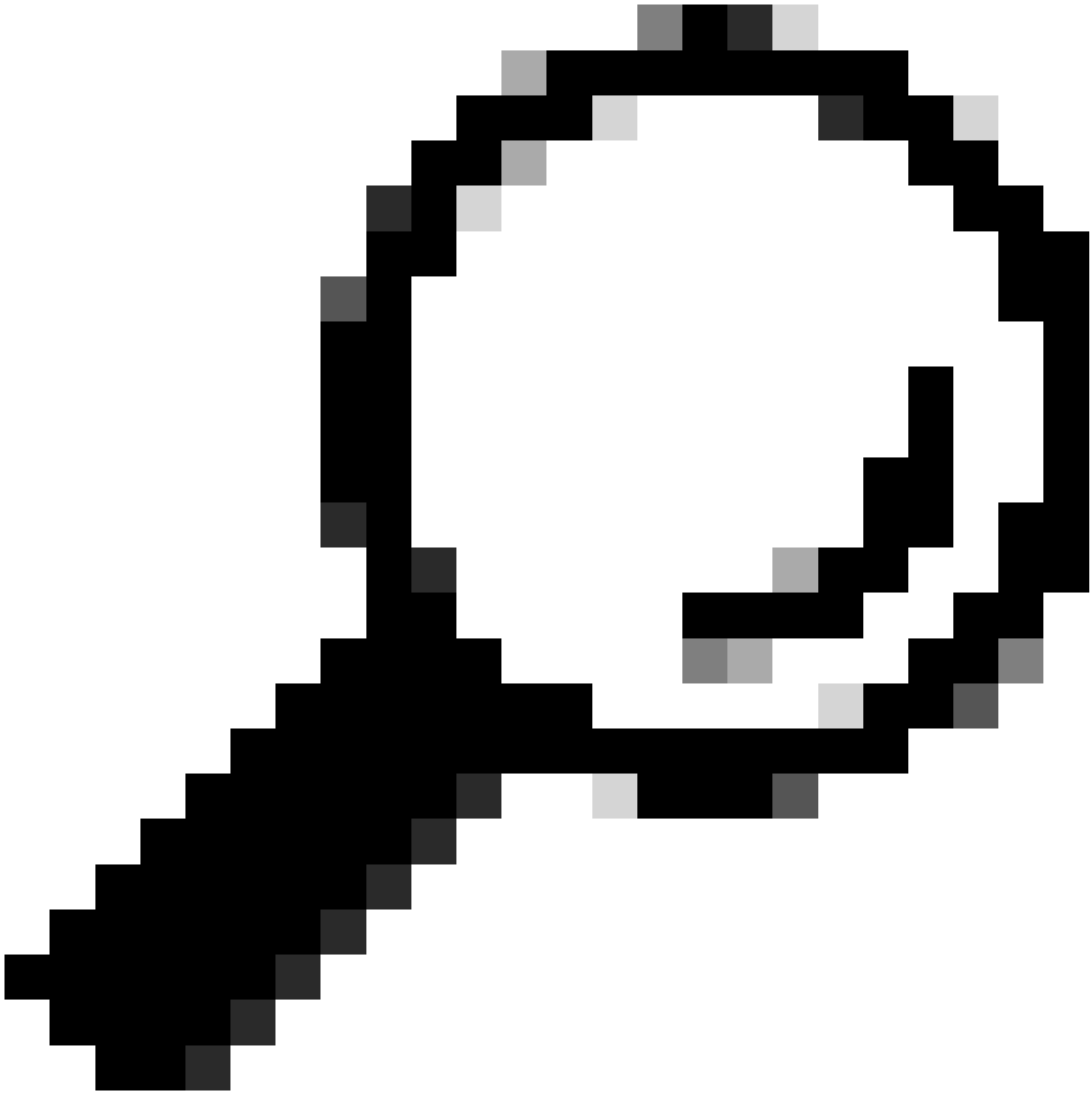
 7

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

<--

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

  Totals - Source count: 1, Packet count: 8



Tipp: Wenn ein (S,G)-Eintrag nicht gefunden wird oder die Outgoing Interface List (OIL) keine Outgoing Interfaces (OIFs) enthält, weist dies auf ein Problem mit der zugrunde liegenden Multicast-Konfiguration oder -Operation hin.

Paketerfassung

Konfigurieren Sie eine gleichzeitige eingebettete Paketerfassung auf dem Switch, um sowohl das eingehende DHCP-Paket vom Endpunkt als auch das entsprechende Ausgangspaket für L2-Flooding aufzuzeichnen. Bei der Paketerfassung sollten zwei verschiedene Pakete beobachtet werden: die ursprüngliche DHCP-Erkennung/Anforderung und das entsprechende VXLAN-gekapselte Gegenstück, das für die Underlay-Gruppe bestimmt ist (239.0.17.1).

Fabric Edge (192.168.0.101) - Paketerfassung

<#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
```

DHCP-Erkennung und -Anforderung - L2-Grenze

Nachdem der Edge die DHCP Discover- und Request-Pakete über Layer-2-Flooding, gekapselt mit der Broadcast-Underlay-Gruppe 239.0.17.1, gesendet hat, werden diese Pakete von der L2-Übergabegrenze empfangen, in diesem Szenario Border/CP-1.

Dazu muss Border/CP-1 über eine Multicast-Route mit dem (S,G) des Edge verfügen, und die Liste der ausgehenden Schnittstellen muss die L2LISP-Instanz des L2-Handoff-VLANs enthalten. Es ist wichtig zu beachten, dass L2-Übergabegrenzen die gleiche L2LISP-Instanz-ID haben, auch wenn sie unterschiedliche VLANs für die Übergabe verwenden.

```
<#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

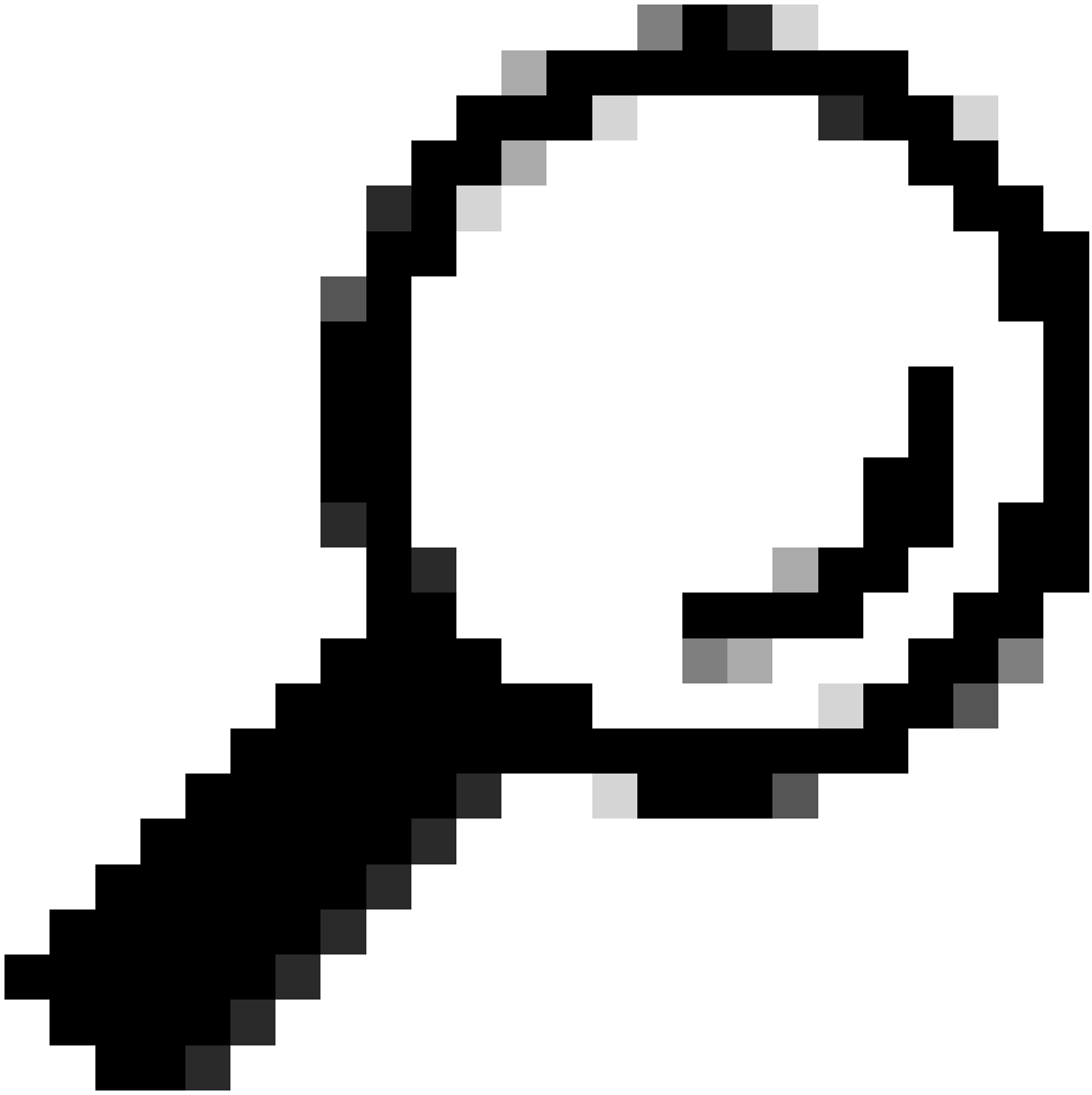
,
   SW Forwarding: 1/0/392/0, Other: 0/0/0
   HW Forwarding:

3

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

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

  Totals - Source count: 1, Packet count: 4



Tipp: Wenn ein (S,G)-Eintrag nicht gefunden wird, weist dies auf ein Problem mit der Multicast-Konfiguration oder -Operation des Underlays hin. Wenn der L2LISP für die erforderliche Instanz nicht als OIF vorhanden ist, weist dies auf ein Problem mit dem Betriebs-UP/DOWN-Status der L2LISP-Subschnittstelle oder dem IGMP-Aktivierungsstatus der L2LISP-Schnittstelle hin.

Stellen Sie wie beim Fabric Edge-Knoten sicher, dass kein Zugriffskontrolleintrag das DHCP-Paket der Fingereinträge an der L2LISP0-Schnittstelle ablehnt.

<#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
```

Nach der Entkapselung des Pakets und seiner Platzierung im VLAN, das dem VNI 8240 entspricht, wird es aufgrund seines Broadcast-Charakters aus allen Spanning Tree Protocol-Weiterleitungs-Ports für das Übergabe-VLAN 141 geflutet.

<#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
```

Die Tabelle für die Geräteverfolgung bestätigt, dass die Schnittstelle Te1/0/44, die mit dem Gateway/DHCP Relay verbunden ist, ein STP-Weiterleitungsport sein muss.

<#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
```

Paketerfassung

Konfigurieren Sie eine gleichzeitige eingebettete Paketerfassung auf dem Switch, um sowohl das eingehende DHCP-Paket von L2 Flooding (S,G eingehende Schnittstelle) als auch das entsprechende Ausgangspaket für den DHCP-Relay aufzuzeichnen. Bei der Paketerfassung sollten zwei unterschiedliche Pakete beobachtet werden: das VXLAN-gekapselte Paket vom Edge-1 und das entkapselte Paket, das an den DHCP-Relay übergeben wird.

Fabric Border/CP (192.168.0.201) zur Paketerfassung

<#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

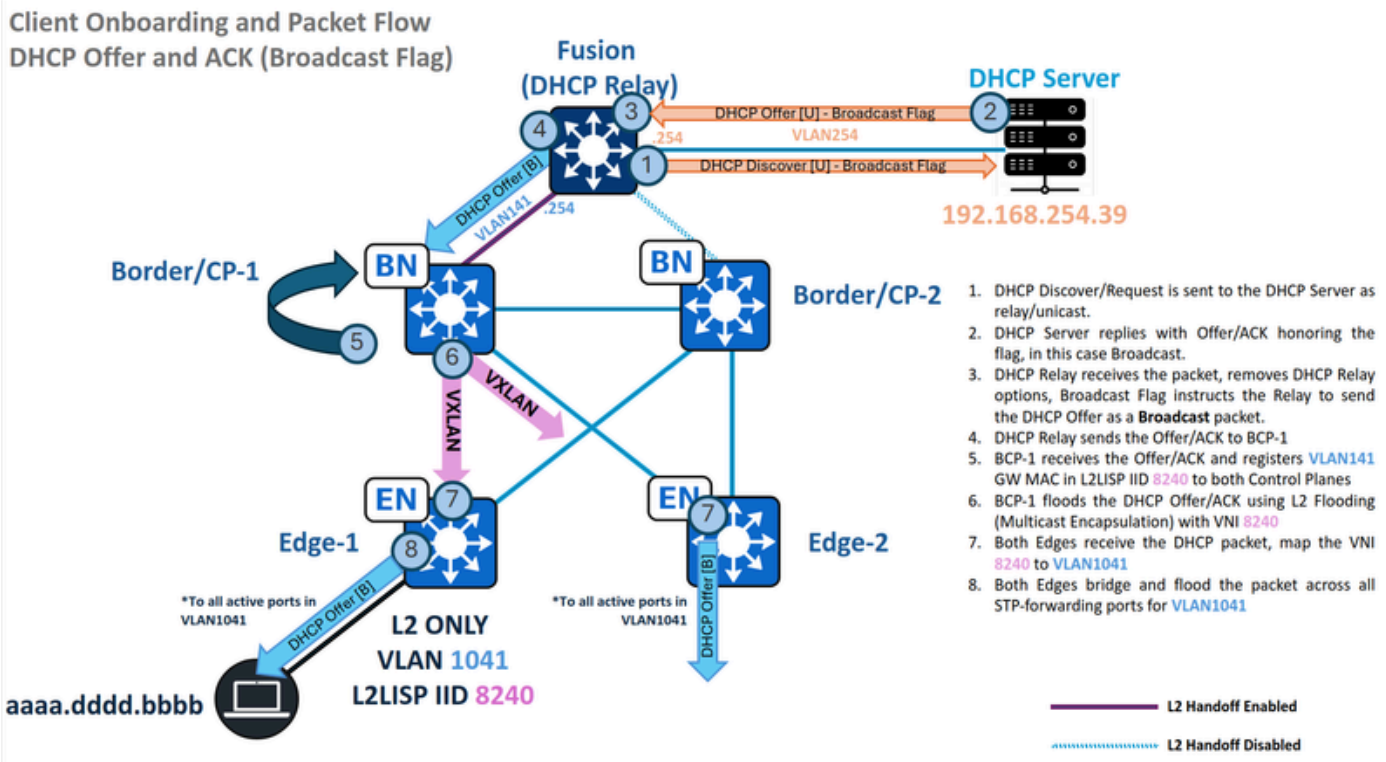
Packet 428: Plain (dot1Q cannot be captured at egress direction)

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

DHCP-Angebot und ACK - Broadcast - L2-Grenze



Datenverkehrsfluss - Senden des DHCP-Angebots und ACK nur in L2

Nachdem die DHCP-Erkennung die SD-Access-Fabric verlassen hat, fügt das DHCP-Relay traditionelle DHCP-Relay-Optionen ein (z. B. GiAddr/GatewayIPAddress) und leitet das Paket als Unicast-Übertragung an den DHCP-Server weiter. In diesem Fluss hängt die SD-Access-Fabric keine speziellen DHCP-Optionen an.

Bei Eingang einer DHCP-Ermittlung/-Anforderung beim Server berücksichtigt der Server die eingebettete Broadcast- oder Unicast-Markierung. Diese Markierung bestimmt, ob der DHCP Relay Agent das DHCP-Angebot als Broadcast- oder Unicast-Frame an das Downstream-Gerät (unsere Grenzen) weiterleitet. Für diese Demonstration wird von einem Broadcast-Szenario ausgegangen.

MAC Learning und Gateway-Registrierung

Wenn das DHCP-Relay ein DHCP Offer oder ACK sendet, muss der L2BN-Knoten die MAC-Adresse des Gateways abrufen, sie der MAC-Adresstabelle des Gateways, der L2/MAC-SISF-Tabelle und schließlich der L2LISP-Datenbank für VLAN 141 hinzufügen, die der L2LISP-Instanz 82400 zugeordnet ist.

```
<#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
```

Wenn die MAC-Adresse des Gateways korrekt ermittelt wurde und die ACK-Markierung für die Fabric-Kontrollebenen als "Yes" (Ja) markiert wurde, gilt diese Phase als abgeschlossen.

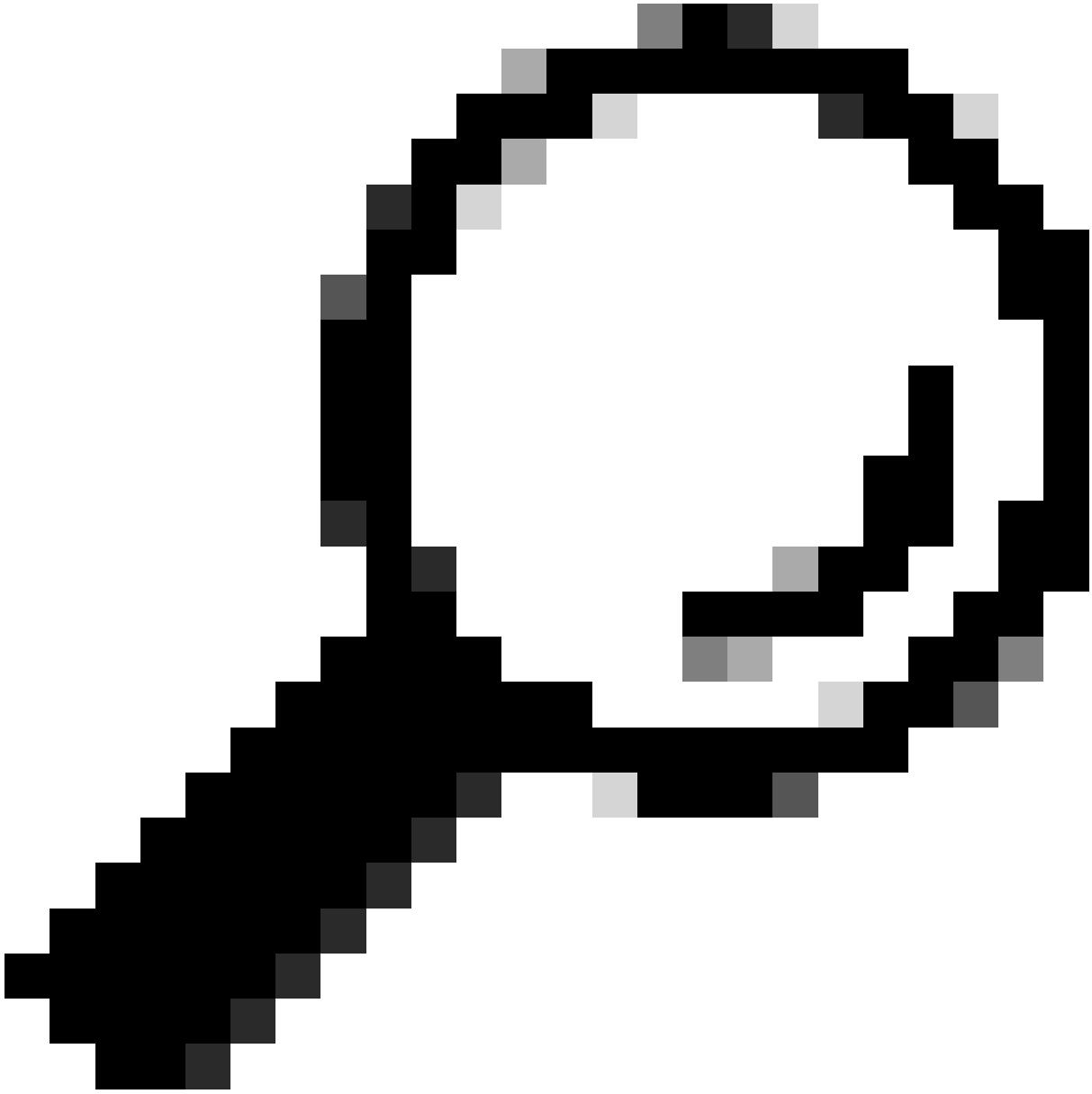
DHCP-Broadcast-Bridge bei L2-Flooding

Ohne aktivierte DHCP-Snooping-Funktion werden DHCP-Broadcasts nicht blockiert und für Layer-2-Flooding in Multicast eingekapselt. Ist dagegen DHCP-Snooping aktiviert, wird eine Flut von DHCP-Broadcast-Paketen verhindert.

<#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



Tipp: Da DHCP-Snooping in L2Border nicht aktiviert ist, ist die Konfiguration der DHCP-Snooping-Vertrauensstellung nicht erforderlich.

Zu diesem Zeitpunkt wird für beide Geräte bereits eine L2LISP-ACL-Validierung durchgeführt.

Verwenden Sie die konfigurierte Broadcast-Underlay-Gruppe für die L2LISP-Instanz und die L2Border Loopback0-IP-Adresse, um den L2 Flooding (S,G)-Eintrag zu überprüfen, der dieses Paket mit anderen Fabric-Knoten verbindet. In den mroute- und mfib-Tabellen können Sie

Parameter wie die Eingangsschnittstelle, die Liste ausgehender Schnittstellen und die Weiterleitungszähler überprüfen.

<#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

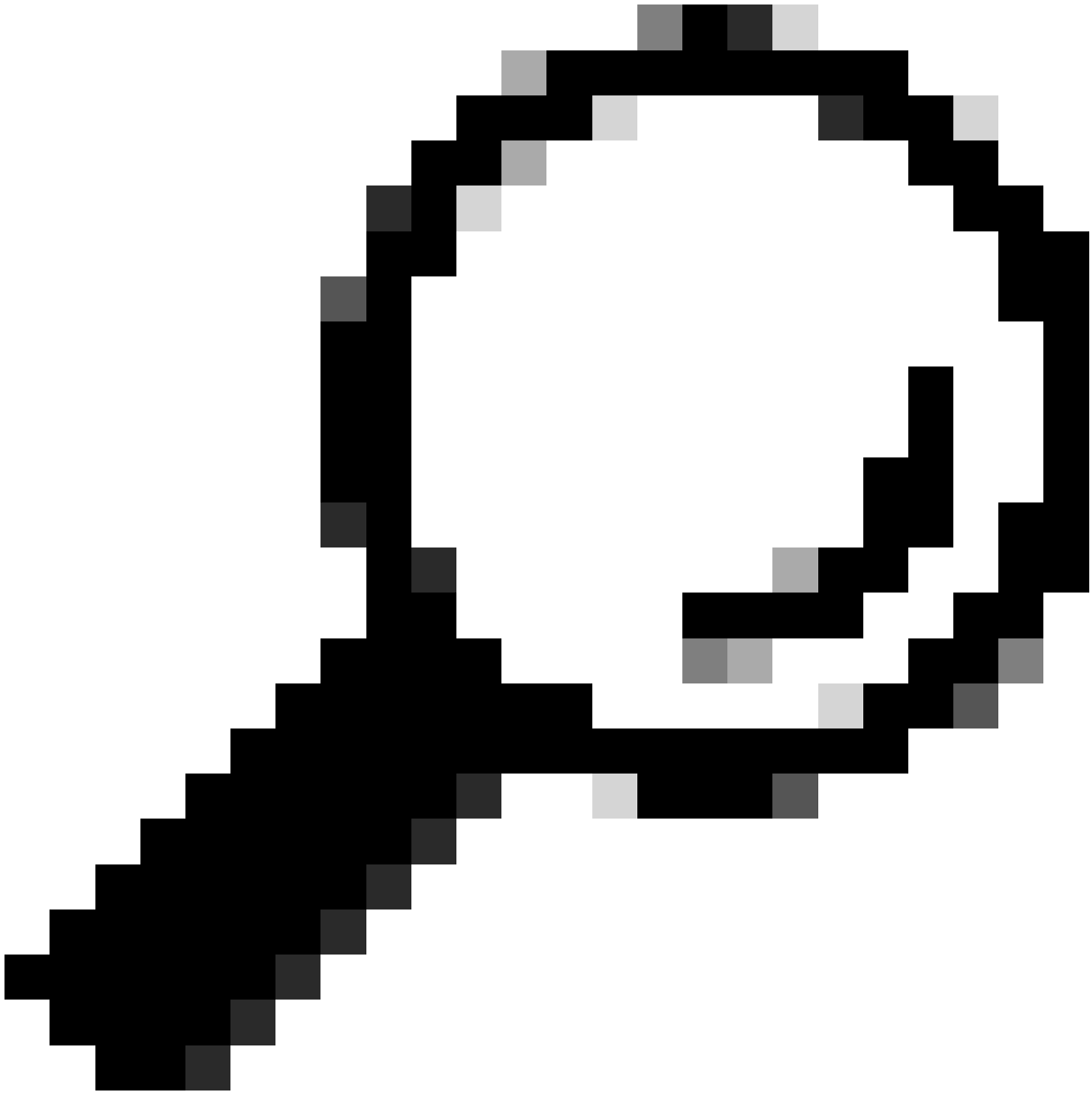
,
SW Forwarding: 1/0/392/0, Other: 1/1/0
HW Forwarding:

92071

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

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

Totals - Source count: 1, Packet count: 92071



Tipp: Wenn ein (S,G)-Eintrag nicht gefunden wird oder die Outgoing Interface List (OIL) keine Outgoing Interfaces (OIFs) enthält, weist dies auf ein Problem mit der zugrunde liegenden Multicast-Konfiguration oder -Operation hin.

Mit diesen Validierungen und den Paketerfassungen, die den vorherigen Schritten ähneln, wird dieser Abschnitt abgeschlossen, da das DHCP-Angebot als Broadcast an alle Fabric-Edges unter Verwendung des Inhalts der ausgehenden Schnittstellenliste weitergeleitet wird, in diesem Fall aus den Schnittstellen TenGig1/0/42 und TenGig1/0/43.

DHCP-Angebot und ACK - Broadcast - Edge

Überprüfen Sie wie beim vorherigen Fluss die L2Border S,G im Fabric Edge, wobei die eingehende Schnittstelle auf L2BN zeigt und das OIL die L2LISP-Instanz enthält, die VLAN 1041 zugeordnet ist.

<#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,

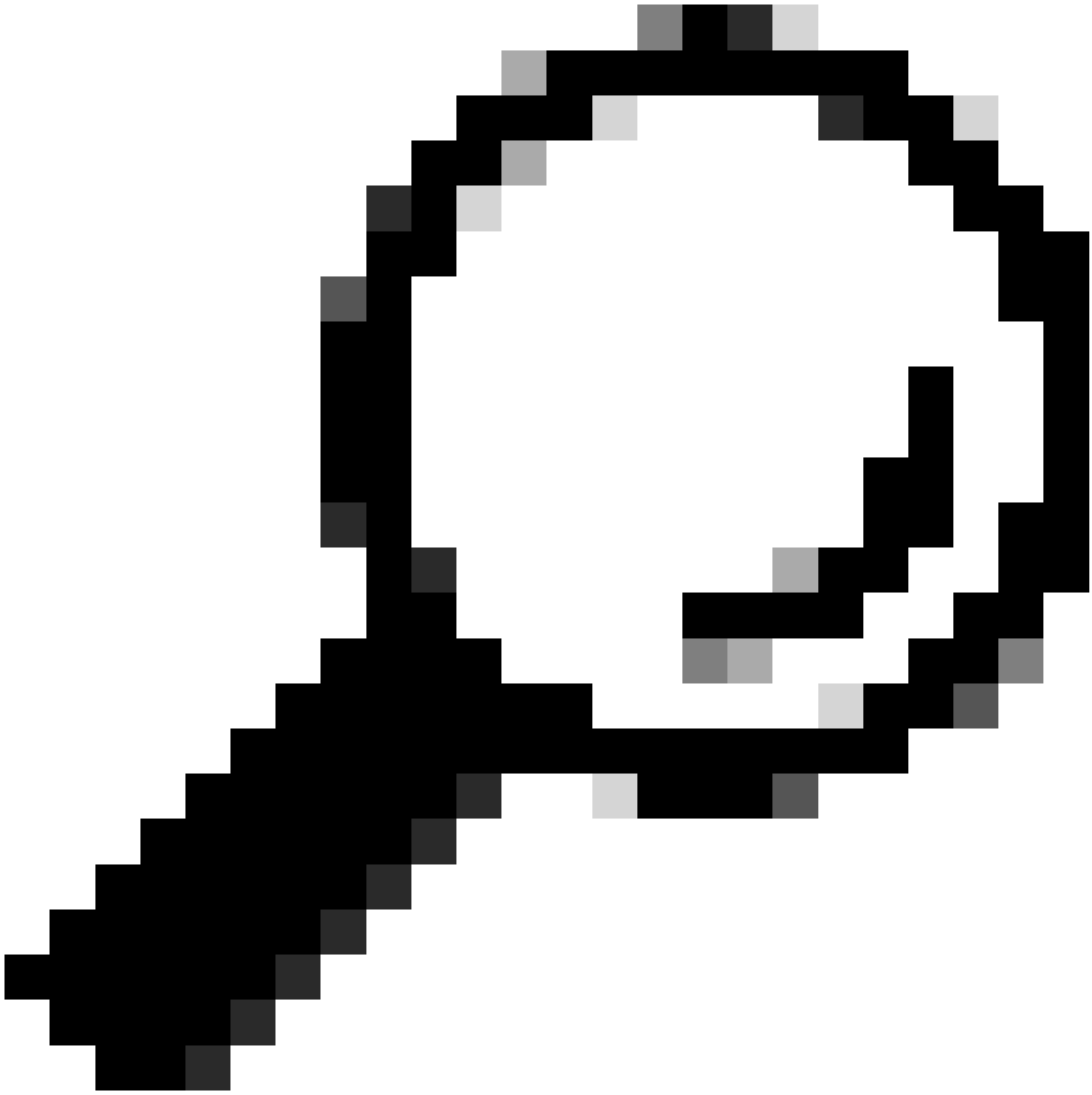
   SW Forwarding: 1/0/96/0, Other: 0/0/0
   HW Forwarding:

76236

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

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

  Totals - Source count: 1, Packet count: 4



Tipp: Wenn ein (S,G)-Eintrag nicht gefunden wird, weist dies auf ein Problem mit der Multicast-Konfiguration oder -Operation des Underlays hin. Wenn der L2LISP für die erforderliche Instanz nicht als OIF vorhanden ist, weist dies auf ein Problem mit dem Betriebs-UP/DOWN-Status der L2LISP-Subschnittstelle oder dem IGMP-Aktivierungsstatus der L2LISP-Schnittstelle hin.

Die L2LISP-ACL-Validierung wurde bereits für beide Geräte durchgeführt.

Nachdem das Paket entkapselt und auf dem VLAN platziert wurde, das mit VNI 8240 übereinstimmt, wird es aufgrund seines Broadcast-Charakters von allen Spanning Tree Protocol-Weiterleitungs-Ports für VLAN1041 geflutet.

```
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
```

Die MAC-Adresstabelle identifiziert Port Te1/0/2 als Endpunkt-Port, der sich im FWD-Zustand befindet. Das Paket wird an den Endpunkt geflutet.

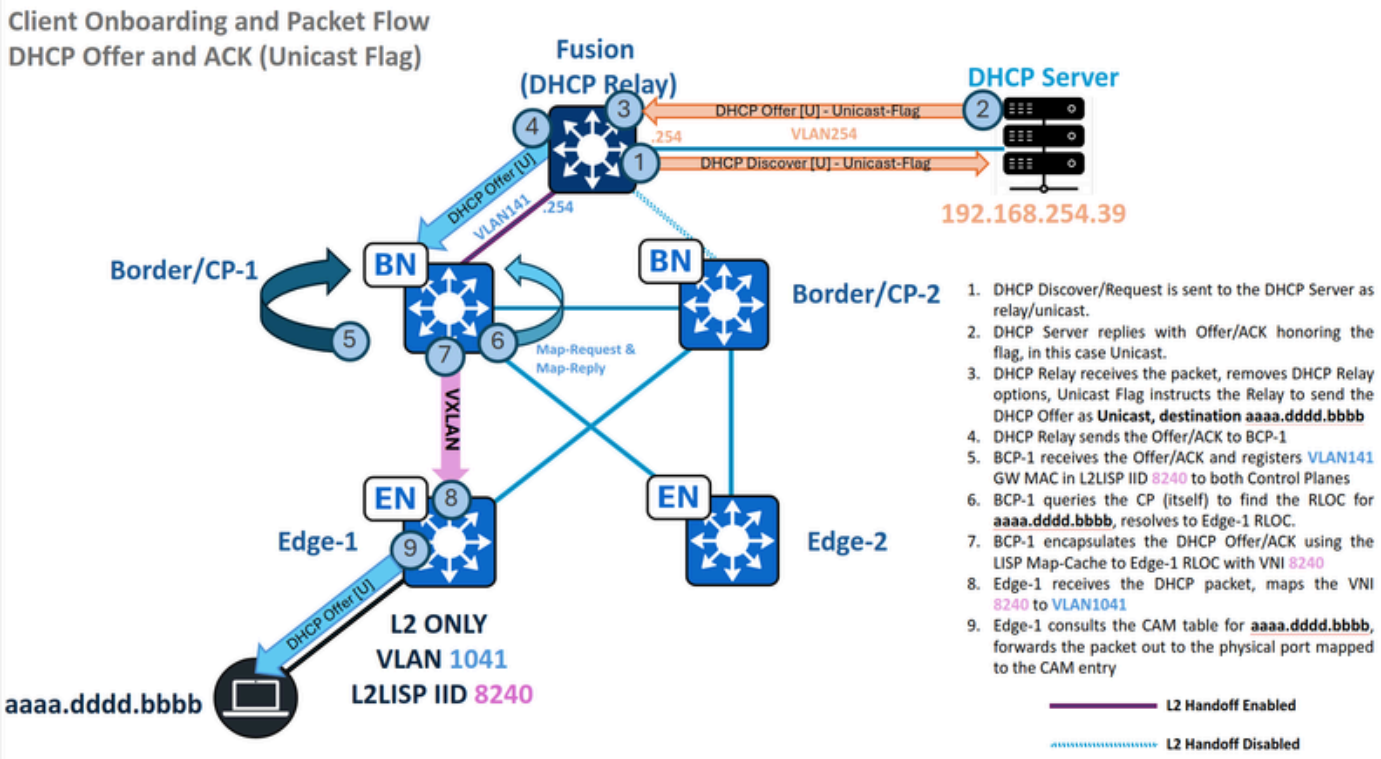
```
<#root>
Edge-1#
show mac address-table interface te1/0/2

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

1041

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

Das DHCP-Angebot und der ACK-Prozess bleiben konsistent. Wenn DHCP Snooping nicht aktiviert ist, werden keine Einträge in der DHCP Snooping-Tabelle erstellt. Folglich wird der Device-Tracking-Eintrag für den DHCP-fähigen Endpunkt durch das Sammeln von ARP-Paketen generiert. Es wird außerdem erwartet, dass Befehle wie "show platform dhcpsnooping client stats" keine Daten anzeigen, da DHCP-Snooping deaktiviert ist.

<#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
```

DHCP-Angebot und ACK - Unicast - L2-Grenze



Datenverkehrsfluss - Unicast-DHCP-Angebot und ACK nur in L2

In diesem Fall ist das Szenario etwas anders, und der Endpunkt setzt das DHCP-Broadcast-Flag auf "unset" (nicht festgelegt) oder "0".

Das DHCP-Relay sendet das DHCP-Angebot/ACK nicht als Broadcast, sondern als Unicast-Paket mit einer Ziel-MAC-Adresse, die von der Client-Hardwareadresse innerhalb der DHCP-Nutzlast abgeleitet wird. Dadurch wird die Paketverarbeitung durch die SD-Access-Fabric drastisch verändert. Zur Weiterleitung des Datenverkehrs wird der L2LISP-Map-Cache verwendet, nicht die Layer-2-Flooding-Multicast-Kapselungsmethode.

Fabric Border/CP (192.168.0.201) Paketregistrierung: DHCP-Eingangsangebot

<#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)
```

In diesem Szenario wird L2 Flooding ausschließlich für die Erkennung/Anforderung verwendet, während Angebote/ACKs über L2LISP-Map-Caches weitergeleitet werden, wodurch der Gesamtbetrieb vereinfacht wird. Gemäß den Unicast-Weiterleitungsprinzipien fragt L2 Border die Kontrollebene nach der MAC-Zieladresse (aaaa.dddd.bbb) ab. Unter der Annahme einer erfolgreichen "MAC Learning and Endpoint Registration" am Fabric Edge ist diese Endpunkt-ID (EID) auf der Kontrollebene registriert.

<#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
```

Nach der Abfrage der Border an die Kontrollebene (lokal oder remote) wird mit der LISP-Auflösung ein Map-Cache-Eintrag für die MAC-Adresse des Endpunkts erstellt.

```
<#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        -
```

Wenn das RLOC aufgelöst ist, wird das DHCP-Angebot in Unicast gekapselt und unter Verwendung von VNI 8240 direkt an Edge-1 unter 192.168.0.101 gesendet.

<#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
```

Mit derselben Methode wie in den vorherigen Abschnitten erfassen Sie den eingehenden Datenverkehr vom DHCP-Relay und zur RLOC-Ausgangsschnittstelle, um die VXLAN-Kapselung in Unicast zum Edge-RLOC zu beobachten.

DHCP-Angebot und ACK - Unicast - Edge

Der Edge empfängt das Unicast-DHCP-Angebot/ACK von der Grenze, entkapselt den Datenverkehr und ermittelt anhand der MAC-Adresstabelle den richtigen Ausgangsport. Im Gegensatz zu Broadcast Offer/ACKs leitet der Edge-Knoten das Paket nur an den spezifischen Port weiter, mit dem der Endpunkt verbunden ist, anstatt es an alle Ports zu fluten.

Die MAC-Adresstabelle identifiziert Port Te1/0/2 als Client-Port, der sich durch STP im FWD-Zustand befindet. Das Paket wird an den Endpunkt weitergeleitet.

```
<#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
```

Das DHCP-Angebot und der ACK-Prozess bleiben konsistent. Wenn DHCP Snooping nicht

aktiviert ist, werden keine Einträge in der DHCP Snooping-Tabelle erstellt. Folglich wird der Device-Tracking-Eintrag für den DHCP-fähigen Endpunkt durch die Glean-ARP-Pakete generiert. Es wird außerdem erwartet, dass Befehle wie "show platform dhcpsnooping client stats" keine Daten anzeigen, da DHCP-Snooping deaktiviert ist.

<#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
```

Dabei ist zu beachten, dass die SD-Access-Fabric die Verwendung der Unicast- oder Broadcast-Markierung nicht beeinflusst, da es sich hierbei lediglich um ein Endgeräteverhalten handelt. Diese Funktionalität kann durch den DHCP-Relay oder den DHCP-Server selbst überschrieben werden, aber beide Mechanismen sind für einen nahtlosen DHCP-Betrieb in einer reinen L2-Umgebung erforderlich: L2-Flooding mit Underlay-Multicast für Broadcast-Angebote/ACKs und ordnungsgemäße Endpunktregistrierung in der Kontrollebene für Unicast-Angebote/ACKs.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.